UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

ACKNOWLEDGEMENT OF LOSS OF ENTITLEMENT TO ENTITY STATUS DISCOUNT

APPLICATION #	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET #	REQUEST ID
13/240,572	09/22/2011	Stephen Wayne Boyer	BST-004	151089

The entity status change request below filed through Patent Center on 01/18/2024 has been accepted.

Certifications

APPLICANT CHANGING TO REGULAR UNDISCOUNTED FEE STATUS

Signature

I certify, in accordance with 37 CFR 1.4(d)(4), that I am one of the signatories making the entity status change.

Signature	Name	Registration #
/Hunter Malboeuf/	Hunter Malboeuf	79730

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 10,805,331 B2
APPLICATION NO. : 13/240572
DATED : October 13, 2020
INVENTOR(S) : Stephen W. Boyer et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the Claims

In Column 19, Claim number 25, Line number 4, delete "system", and insert --method--.

In Column 19, Claim number 26, Line number 8, delete "system", and insert --method--.

In Column 19, Claim number 27, Line number 10, delete "system", and insert --method--.

Signed and Sealed this
Nineteenth Day of September, 2023

Katherine Kelly Vidal

Katherine Kelly Vidal
Director of the United States Patent and Trademark Office

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/240,572	09/22/2011	Stephen Wayne Boyer	BST-004	2423

51414 7590 08/30/2023

GOODWIN PROCTER LLP
PATENT ADMINISTRATOR
100 NORTHERN AVENUE
BOSTON, MA 02210

EXAMINER	
KANAAN, SIMON P	

ART UNIT	PAPER NUMBER
2492	

NOTIFICATION DATE	DELIVERY MODE
08/30/2023	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JGoodwin@goodwinlaw.com
PSousa-Atwood@goodwinlaw.com
US-PatentBos@goodwinlaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

Patent No.: 10805331
Issue Date: 10/13/2020
Appl. No.: 13/240,572
Filed: 09/22/2011

PART (A) RESPONSE FOR CERTIFICATES OF CORRECTION

This is a decision on the Certificate of Correction request filed 16 August 2023.

The request for issuance of Certificate of Correction for the above-identified correction(s) under the provisions of 37 CFR 1.322 and/or 1.323 is hereby:

(Check one)
☑ Approved ☐ Approved in Part ☐ Denied

Comments: ____

PART (B) PETITION UNDER 37 CFR 1.324 OR 37 CFR 1.48

☐ This is a decision on the petition filed ____ to correct inventorship under 37 CFR 1.324.

☐ This is a decision on the request under 37 CFR 1.48, petition filed ____. In view of the fact that the patent has already issued, the request under 37 CFR 1.48 has been treated as a petition to correct inventorship under 37 CFR 1.324.

The petition is hereby: ☐ Granted ☐ Dismissed

Comment: ____

The patented filed is being forwarded to Certificate of Corrections Branch for issuance of a certificate naming only the actual inventor or inventors.

/SALEH NAJJAR/
Supervisory Patent Examiner, Art Unit 2492
Technology Center 2400
Phone: (571)272-4006

Certificates of Correction Branch email: CustomerServiceCoC@uspto.gov CoC Central Phone Number: (703) 756-1814

Docket No.: BST-004
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Letters Patent of:
Stephen W. Boyer et al.

Patent No.: 10,805,331

Issued: October 13, 2020

For: INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM

Filed Electronically

REQUEST FOR CERTIFICATE OF CORRECTION PURSUANT TO 37 C.F.R. § 1.323

Upon reviewing the above-identified patent, Patentee noted typographical errors in the claims:

In column 19, claim number 25, line number 4, delete "system", and insert --method--.

In column 19, claim number 26, line number 8, delete "system", and insert --method--.

In column 19, claim number 27, line number 10, delete "system", and insert --method--.

The errors were found in the application as filed by applicant.

The errors now sought to be corrected are inadvertent typographical errors the correction of which does not involve new matter or require reexamination.

Transmitted herewith is a proposed Certificate of Correction effecting such amendment. Patentee respectfully solicits the granting of the requested Certificate of Correction.

Please charge our Credit Card in the amount of $160.00 covering the fee set forth in 37 C.F.R. § 1.20(a). The Director is hereby authorized to charge any deficiency in the fees filed, asserted to be filed or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to our Deposit Account No. 07-1700, under Order No. BST-004.

Dated: August 16, 2023

Respectfully submitted,

Electronic signature: /Hunter Malboeuf/
Hunter Malboeuf
Registration No.: 79,730
GOODWIN PROCTER LLP
100 Northern Avenue
IP DOCKETING DEPT./7TH FL
Boston, Massachusetts 02210
(617) 570-1000
Agent For Applicant

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC PAYMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
13/240,572	**08/16/2023 03:13:22 PM ET**	**BST-004**

Title of Invention

INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	10805331
CONFIRMATION #	2423	FILED BY	Anna Beaulieu
PATENT CENTER #	62626565	AUTHORIZED BY	Hunter Malboeuf
CUSTOMER #	51414	FILING DATE	09/22/2011
CORRESPONDENCE ADDRESS	-	FIRST NAMED INVENTOR	Stephen Wayne Boyer

Payment Information

PAYMENT METHOD	PAYMENT TRANSACTION ID	PAYMENT AUTHORIZED BY
CARD / 1146	**E20238FF14585445**	**Anna Beaulieu**

FEE CODE	DESCRIPTION	ITEM PRICE($)	QUANTITY	ITEM TOTAL($)
2811	CERTIFICATE OF CORRECTION	160.00	1	160.00
			TOTAL AMOUNT:	**$160.00**

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES
PATENT AND TRADEMARK OFFICE

P.O. Box 1450
Alexandria, VA 22313 - 1450
www.uspto.gov

ELECTRONIC ACKNOWLEDGEMENT RECEIPT

APPLICATION #	RECEIPT DATE / TIME	ATTORNEY DOCKET #
13/240,572	**08/16/2023 03:13:22 PM ET**	**BST-004**

Title of Invention

INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM

Application Information

APPLICATION TYPE	Utility - Nonprovisional Application under 35 USC 111(a)	PATENT #	10805331
CONFIRMATION #	2423	FILED BY	Anna Beaulieu
PATENT CENTER #	62626565	FILING DATE	09/22/2011
CUSTOMER #	51414	FIRST NAMED INVENTOR	Stephen Wayne Boyer
CORRESPONDENCE ADDRESS	-	AUTHORIZED BY	Hunter Malboeuf

Documents

TOTAL DOCUMENTS: 2

DOCUMENT	PAGES	DESCRIPTION	SIZE (KB)
BST-004 - COC.pdf	1	Request for Certificate of Correction	16 KB
BST-004 - REQ COC.pdf	2	Request for Certificate of Correction	20 KB

Digest

DOCUMENT	MESSAGE DIGEST(SHA-512)
BST-004 - COC.pdf	AF5BF60F2B13EF2666EECD0C5E61F5EB6CD3EE948C3ACFC D87ACDD6826DC282BA78E620E8430144A48111B3FF6CAE32E

D1C5F2C9E3F335F311ACD518D9F5567F

BST-004 - REQ COC.pdf 67F574F53493A31EDF0A7B31E33094BA5ABD1DB80F291C436E0DC1C0E785BA9A717E8928D9F2E204C4BFC1B85B67A213E2171E7CBE06EA14C227E3F3AED9D2D5

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/44 (09-07)
Approved for use through 03/31/2023. OMB 0651-0033
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.
(Also Form PTO-1050)

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO.	:	10,805,331
APPLICATION NO.	:	13/240,572
ISSUE DATE	:	October 13, 2020
INVENTOR(S)	:	Stephen W. Boyer et al.

It is certified that an error appears or errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In column 19, claim number 25, line number 4, delete “system”, and insert --method--.

In column 19, claim number 26, line number 8, delete “system”, and insert --method--.

In column 19, claim number 27, line number 10, delete “system”, and insert --method--.

MAILING ADDRESS OF SENDER (Please do not use Customer Number below):
Hunter Malboeuf
GOODWIN PROCTER LLP
100 Northern Avenue
IP DOCKETING DEPT./7TH FL
Boston, Massachusetts 02210

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/240,572	10/13/2020	10805331	BST-004	2423

51414 7590 09/23/2020

GOODWIN PROCTER LLP
PATENT ADMINISTRATOR
100 NORTHERN AVENUE
BOSTON, MA 02210

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 186 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Stephen Wayne Boyer, Waltham, MA;
Nagarjuna Venna, Waltham, MA;
Megumi Ando, Cambridge, MA;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/240,572	09/22/2011	Stephen Wayne Boyer	BST-004	2423

7590 09/15/2020

GOODWIN PROCTER LLP
PATENT ADMINISTRATOR
100 NORTHERN AVENUE
BOSTON, MA 02210

EXAMINER	
KANAAN, SIMON P	

ART UNIT	PAPER NUMBER
2492	

NOTIFICATION DATE	DELIVERY MODE
09/15/2020	ELECTRONIC

NOTICE OF NON-COMPLIANT INFORMATION DISCLOSURE STATEMENT

An Information Disclosure Statement (IDS) filed 9/01/2020 in the above-identified application fails to meet the requirements of 37 CFR 1.97(d) for the reason(s) specified below. Accordingly, the IDS will be placed in the file, but the information referred to therein has not been considered.

The IDS is not compliant with 37 CFR 1.97(d) because:

☑ The IDS lacks a statement as specified in 37 CFR 1.97(e).

☐ The IDS lacks the fee set forth in 37 CFR 1.17(p).

☐ The IDS was filed after the issue fee was paid. Applicant may wish to consider filing a petition to withdraw the application from issue under 37 CFR 1.313(c) to have the IDS considered. See MPEP 1308.

N. Horne, for

571-272-4200 or 1-888-786-0101
Application Assistance Unit
Office of Data Management

FORM PTOM327-B (Rev. 02/08)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Stephen Wayne Boyer

Application No.: 13/240,572 Confirmation No.: 2423

Filed: September 22, 2011 Art Unit: 2492

For: INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM Examiner: S. P. Kanaan

Filed via EFS-web

INFORMATION DISCLOSURE STATEMENT (IDS)

The Information Disclosure Statement is submitted solely to comply with the duty of candor. It is understood that this Supplemental Information Disclosure Statement does not fall within the provisions of 37 C.F.R. §1.97. Nonetheless, entry and consideration are respectfully requested. Alternatively, entry of this paper into the file without consideration is respectfully requested.

Applicant hereby apprises the Examiner of the following patent application, including the contents of the file wrapper, the claims, any Office Actions issued therein, and any Notices of Allowance issued therefor:

Docket No.	U.S. Serial No.:	Title	Filing Date
BST-001	15/271655 Published as: US2018/0083999	SELF-PUBLISHED SECURITY RISK MANAGEMENT	September 21, 2016
BST-002	15/377,574 9,705,932	METHODS AND SYSTEMS FOR CREATING, DE-DUPLICATING, AND ACCESSING DATA USING AN OBJECT STORAGE SYSTEM	December 13, 2016

BST-003	14/021,585 9,438,615 Published as: US2015/0074579	SECURITY RISK MANAGEMENT	September 9, 2013
BST-003C1	15/216,955 Published as: US2016/0330231	METHODS FOR USING ORGANIZATIONAL BEHAVIOR FOR RISK RATINGS	July 22, 2016
BST-003C2	15/239,063 Published as: US2017/0093901	SECURITY RISK MANAGEMENT	August 17, 2016
BST-003C3	16/405,121 Published as: US2019/0260791	METHODS FOR USING ORGANIZATIONAL BEHAVIOR FOR RISK RATINGS	May 7, 2019
BST-004C1	14/944,484 9,973,524 Published as: US2016/0323308	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM	November 18, 2015
BST-004C1CP	15/142,677 9,830,569 Published as: US/2016/0239772	SECURITY ASSESSMENT USING SERVICE PROVIDER DIGITAL ASSET INFORMATION	April 29, 2016
BST-007	15/134,845 9,680,858	ANNOTATION PLATFORM FOR A SECURITY RISK SYSTEM	April 21, 2016
BST-008	15/044,952 Published as: US2017/0236077	RELATIONSHIPS AMONG TECHNOLOGY ASSETS AND SERVICES AND THE ENTITIES RESPONSIBLE FOR THEM	February 16, 2016
BST-008C2	15/089,375 10,176,445 Published as:	RELATIONSHIPS AMONG TECHNOLOGY ASSETS AND SERVICES AND THE ENTITIES RESPONSIBLE FOR THEM	April 1, 2016

	US2017/0236079		
BST-009DA	29/598,298 D835,631	COMPUTER DISPLAY SCREEN WITH GRAPHICAL USER INTERFACE	March 24, 2017
BST-009DB	29/598,299 D818,475	COMPUTER DISPLAY WITH SECURITY RATINGS GRAPHICAL USER INTERFACE	March 24, 2017
BST-009DC	29/599,622	COMPUTER DISPLAY WITH SECURITY RATINGS GRAPHICAL USER INTERFACE	April 5, 2017
BST-009DD	29/599,620	COMPUTER DISPLAY WITH SECURITY RATINGS GRAPHICAL USER INTERFACE	April 5, 2017
BST-010	16/015,686	METHODS FOR MAPPING IP ADDRESSES AND DOMAINS TO ORGANIZATIONS USING USER ACTIVITY DATA	June 22, 2018
BST-010C1	16/543,075	METHODS FOR MAPPING IP ADDRESSES AND DOMAINS TO ORGANIZATIONS USING USER ACTIVITY DATA	August 16, 2019
BST-010C2	16/738825	METHODS FOR MAPPING IP ADDRESSES AND DOMAINS TO ORGANIZATIONS USING USER ACTIVITY DATA	January 9, 2020
BST-011	15/918,286	CORRELATED RISK IN CYBERSECURITY	March 12, 2018
BST-011C1	16/292,956	CORRELATED RISK IN CYBERSECURITY	May 5, 2019
BST-011C2	16/795,056	CORRELATED RISK IN CYBERSECURITY	February 19, 2020
BST-012	16/170680	SYSTEMS AND METHODS FOR REMOTE DETECTION OF SOFTWARE THROUGH BROWSER WEBINJECTS	October 25, 2018

BST-012C1	16/688647	SYSTEMS AND METHODS FOR REMOTE DETECTION OF SOFTWARE THROUGH BROWSER WEBINJECTS	November 19, 2019
BST-013	15/954921	SYSTEMS AND METHODS FOR EXTERNAL DETECTION OF MISCONFIGURED SYSTEMS	April 17, 2018
BST-014	16/549764	SYSTEMS AND METHODS FOR INFERRING ENTITY RELATIONSHIPS VIA NETWORK COMMUNICATIONS OF USERS OR USER DEVICES	August 23, 2019
BST-015	16/583,991	SYSTEMS AND METHODS FOR NETWORK ASSET DISCOVERY AND ASSOCIATION THEREOF WITH ENTITIES	September 26, 2019
BST-016D	29/666942	COMPUTER DISPLAY WITH GRAPHICAL USER INTERFACE	October 17, 2018
BST-017	16/360,641	SYSTEMS AND METHODS FOR FORECASTING CYBERSECURITY RATINGS BASED ON EVENT-RATE SCENARIOS	March 21, 2019
BST-018	16/514,771	SYSTEMS AND METHODS FOR GENERATING SECURITY IMPROVEMENT PLANS FOR ENTITIES	July 17, 2019
BST-018C1	16/922,273	SYSTEMS AND METHODS FOR GENERATING SECURITY IMPROVEMENT PLANS FOR ENTITIES	July 7, 2020
BST-019D	29/677306	COMPUTER DISPLAY WITH CORPORATE HIERARCHY GRAPHICAL USER INTERFACE COMPUTER DISPLAY WITH CORPORATE HIERARCHY GRAPHICAL USER INTERFACE	January 18, 2019
BST-020	16/775840	SYSTEMS AND METHODS FOR ASSESSING CYBERSECURITY	January 29, 2020

		STATE OF ENTITIES BASED ON COMPUTER NETWORK CHARACTERIZATION	
BST-021	16/779,437	SYSTEMS AND METHODS FOR RAPIDLY GENERATING SECURITY RATINGS	January 31, 2020
BST-023	16/802232	SYSTEMS AND METHODS FOR IMPROVING A SECURITY PROFILE OF AN ENTITY BASED ON PEER SECURITY PROFILES	February 26, 2020
BST-023C1	16/942,452	SYSTEMS AND METHODS FOR IMPROVING A SECURITY PROFILE OF AN ENTITY BASED ON PEER SECURITY PROFILES	July 29, 2020
BST-023DA	29/725724	COMPUTER DISPLAY WITH RISK VECTORS GRAPHICAL USER INTERFACE	February 26, 2020
BST-023DB	29/736,641	COMPUTER DISPLAY WITH PEER ANALYTICS GRAPHICAL USER INTERFACE	June 2, 2020
BST-026	16/884,607	SYSTEMS AND METHODS FOR MANAGING CYBERSECURITY ALERTS	May 27, 2020

Additionally, Applicant hereby apprises the Examiner of the following patents and patent applications, including the contents of the file wrappers, the claims, any Office Actions issued therein, and any Notices of Allowance issued therefor:

1. U.S.S.N. 15/271,655 (Attorney Docket No. BST-001), the Office Actions mailed 02/21/2017 and 08/18/2017;

2. U.S.S.N. 15/377,574 (Attorney Docket No. BST-002), now U.S. Patent No. 9,705,932, the Office Action mailed 03/02/2017 and the Notice of Allowance mailed 06/01/2017;

3. U.S.S.N. 14/021,585 (Attorney Docket No. BST-003), now U.S. Patent No. 9,438,615, the Office Action mailed 03/11/2016 and the Notice of Allowance mailed 08/09/2016;

4. U.S.S.N. 15/216,955 (Attorney Docket No. BST-003C1), now U.S. Patent No. 10,326,786, the Office Actions mailed 11/04/2016, 03/09/2017, 06/06/2017, 12/05/2017, and 08/29/2018, and the Notice of Allowance mailed 02/06/2019;

5. U.S.S.N. 15/239,063 (Attorney Docket No. BST-003C2), now U.S. Patent No. 10,341,370, the Office Action mailed 03/21/2018 and the Notice of Allowance mailed 01/14/2019;

6. U.S.S.N. 16/405,121 (Attorney Docket No. BST-003C3), the Office Actions mailed 08/01/2019 and 11/21/2019 and the Notice of Allowance mailed now 05/22/2020 and 07/10/2020;

7. U.S.S.N. 14/944,484 (Attorney Docket No. BST-004C1), now U.S. Patent No. 9,973,524, the Office Actions mailed 03/11/2016, 07/05/2016, and 01/17/2017 and the Notice of Allowance mailed 10/20/2017;

8. U.S.S.N. 15/142,677 (Attorney Docket No. BST-004C1CP), now U.S. Patent No. 9,830,569, the Office Actions mailed 07/26/2016, and 04/24/2017 and the Notice of Allowance mailed 10/11/2017;

9. U.S.S.N. 15/134,845 (Attorney Docket No. BST-007), now U.S. Patent No. 9,680,858, the Office Actions mailed 07/19/2016 and 01/26/2017, and the Notices of Allowance mailed 04/27/2017 and 05/09/2017;

10. U.S.S.N. 15/044,952 (Attorney Docket No. BST-008), the Office Actions mailed 07/08/2019 and 02/21/2020;

11. U.S.S.N. 15/089,375 (Attorney Docket No. BST-008C2), now U.S. Patent No. 10,176,445, the Office Actions mailed 09/09/2016, 05/17/2017, and 11/17/2017 and the Notice of Allowance mailed 08/09/2018;

12. U.S.S.N. 29/598,298 (Attorney Docket No. BST-009DA), now U.S. Patent No. D835,631, the Notice of Allowance mailed 08/15/2018;

13. U.S.S.N. 29/598,299 (Attorney Docket No. BST-009DB), now U.S. Patent No. D818,475, the Notice of Allowance mailed 01/02/2018;

14. U.S.S.N. 29/599,622 (Attorney Docket No. BST-009DC), now U.S. Patent No. D847,169, the Notice of Allowance mailed 12/11/2018;

15. U.S.S.N. 29/599,620 (Attorney Docket No. BST-009DD), now U.S. Patent No. D846,562, the Office Action mailed 05/03/2018, the Notice of Allowance mailed 11/27/2018;

16. U.S.S.N. 16/015,686 (Attorney Docket No. BST-010), now U.S. Patent No. 10,425,380, the Office Action mailed 11/16/2018 and the Notice of Allowance mailed 05/10/2019;

17. U.S.S.N. 16/543,075 (Attorney Docket No. BST-010C1), the Notice of Allowance mailed 09/25/2019;

18. U.S.S.N. 16/738,825 (Attorney Docket No. BST-010C2), the Office Actions mailed 07/08/2019 and 02/21/2020;

19. U.S.S.N. 15/918,286 (Attorney Docket No. BST-011), now U.S. Patent No. 10,257,219, the Office Action mailed 08/07/2018 and the Notice of Allowance mailed 11/29/2018;

20. U.S.S.N. 16/292,956 (Attorney Docket No. BST-011C1), the Office Action mailed 07/10/2019 and the Notices of Allowance mailed 01/08/2020 and 01/27/2020;

21. U.S.S.N. 16/795,056 (Attorney Docket No. BST-011C2), the Office Action mailed 05/01/2020;

22. U.S.S.N. 16/170,680 (Attorney Docket No. BST-012), the Office Action mailed 03/26/2019; the Notices of Allowance mailed 10/29/2019 and 08/27/2019;

23. U.S.S.N. 16/688,647 (Attorney Docket No. BST-012C1), the Office Action mailed 01/29/2020; the Notice of Allowance mailed 05/12/2020;

24. U.S.S.N. 15/954,921 (Attorney Docket No. BST-013), the Office Actions mailed 09/04/2018, 01/03/2019, 08/19/2019, and 12/05/2019; Advisory Action mailed 03/03/2020, and the Notice of Allowance mailed 07/07/2020;

25. U.S.S.N. 16/787,650 (Attorney Docket No. BST-014C1), the Notice of Allowance mailed 04/07/2020;

26. U.S.S.N. 16/583,991 (Attorney Docket No. BST-015), the Office Action mailed 01/13/2020;

27. U.S.S.N. 29/666,942 (Attorney Docket No. BST-016D), the Notice of Allowance mailed 04/30/2020;

28. U.S.S.N. 16/360,641 (Attorney Docket No. BST-017), the Office Action mailed 08/07/2019 and 02/20/2020;

29. U.S.S.N. 16/514,771 (Attorney Docket No. BST-018), the Office Action mailed 12/04/2019; the Notice of Allowance mailed 03/18/2020;

30. U.S.S.N. 29/677,306 (Attorney Docket No. BST-019D), the Notice of Allowance mailed on 08/20/2020;

31. U.S.S.N. 16/775,840 (Attorney Docket No. BST-020), the Notice of Allowance mailed on 05/19/2020;

32. U.S.S.N. 16/779,437 (Attorney Docket No. BST-021), the Notice of Allowance mailed 08/12/2020; and

33. U.S.S.N. 16/802,232 (Attorney Docket No. BST-023), the Notice of Allowance mailed 04/24/2020.

Applicant believes no fee is due with this paper. The Director is hereby authorized to charge any deficiency in the fees filed, asserted to be filed or which should have been filed

herewith (or with any paper hereafter filed in this application by this firm) to our Deposit Account No. 07-1700, under Order No. BST-004.

Dated: September 1, 2020

Respectfully submitted,

Electronic signature: /Gozde Guckaya/
Gozde Guckaya
Registration No.: 74,989
GOODWIN PROCTER LLP
100 Northern Avenue
IP DOCKETING DEPT./7TH FL
Boston, Massachusetts 02210
(617) 570-1000
Agent For Applicant

Electronic Patent Application Fee Transmittal

Application Number:	13240572
Filing Date:	22-Sep-2011
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Filer:	Gozde Guckaya/Christina Andrews
Attorney Docket Number:	BST-004

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
UTILITY APPL ISSUE FEE	2501	1	500	500

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**500**

Electronic Acknowledgement Receipt

EFS ID:	40437785
Application Number:	13240572
International Application Number:	
Confirmation Number:	2423
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Customer Number:	51414
Filer:	Gozde Guckaya/Christina Andrews
Filer Authorized By:	Gozde Guckaya
Attorney Docket Number:	BST-004
Receipt Date:	01-SEP-2020
Filing Date:	22-SEP-2011
Time Stamp:	12:12:29
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$500
RAM confirmation Number	E202091C13343571
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	BST-004_IssueFee.pdf	301642 02837f2bdc492004ad4ed10dd8e0ee8e320a2a67	no	1
Warnings:					
Information:					
2	Non Patent Literature	NPL1SearchQuery.pdf	347911 d330e40b9893ed491393fdd23f68c2ec7e76e25f	no	5
Warnings:					
Information:					
3	Non Patent Literature	BST-013NPL2Camelo.pdf	390433 a37127b19dbd5df23cd116b976050046725e7b8c	no	8
Warnings:					
Information:					
4	Non Patent Literature	Camelo_BotnetClusterIdentification.pdf	22428020 bfedea5f38b963e4aa448790059c0ca8bb43e0b7	no	88
Warnings:					
Information:					
5	Non Patent Literature	NPL_Azman.pdf	855249 b318f639b2b94dbca91d65b3fb6bc22a9cfe09d5	no	6
Warnings:					
Information:					
6	Non Patent Literature	NPL_Basinya.pdf	1078904 c22c28b8728c62345c93a53ae410b5a82a43113d	no	7
Warnings:					
Information:					

7	Non Patent Literature	NPL_Luo.pdf	982327 371a512e79050dd130e851180164b82364d40c80	no	5
Warnings:					
Information:					
8	Non Patent Literature	Seigneur.pdf	1877939 1a324db933b8e9bcd8a5648effded79fad75663b	no	11
Warnings:					
Information:					
9	Information Disclosure Statement (IDS) Form (SB08)	BST-004_SB08.pdf	145634 22200fb7a00bfefef51a16d59d52fa59560e6975	no	3
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
10	Information Disclosure Statement (IDS) Form (SB08)	BST-004_DutyofCandorIDS.pdf	115526 8d0b20a9e85e3154ba640b41a67057a68c9808d2	no	9
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
11	Fee Worksheet (SB06)	fee-info.pdf	30207 efe3b7a4a906f7f285de5c18cd6f665240690d99	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	28553792		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

51414 7590 06/01/2020
GOODWIN PROCTER LLP
PATENT ADMINISTRATOR
100 NORTHERN AVENUE
BOSTON, MA 02210

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/240,572	09/22/2011	Stephen Wayne Boyer	BST-004	2423

TITLE OF INVENTION: INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$500	$0.00	$0.00	$500	09/01/2020

EXAMINER	ART UNIT	CLASS-SUBCLASS
KANAAN, SIMON P	2492	726-025000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Goodwin Procter LLP
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: BitSight Technologies, Inc.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Boston, MA

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. Fees submitted: ☒ Issue Fee ☐ Publication Fee (if required) ☐ Advance Order - # of Copies _____

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

☒ Electronic Payment via EFS-Web ☐ Enclosed check ☐ Non-electronic payment by credit card (Attach form PTO-2038)

☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. 07-7100

5. **Change in Entity Status** (from status indicated above)

☐ Applicant certifying micro entity status. See 37 CFR 1.29

☐ Applicant asserting small entity status. See 37 CFR 1.27

☐ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature /Gozde Guckaya/ Date September 1, 2020

Typed or printed name Gozde Guckaya Registration No. 74,989

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 3

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1	US-D880,512	04-07-2020	Greenwald et al.	
	A2	US-9,075,990	07-07-2015	Yang	
	A3	US-9,373,144	06-21-2016	Ng et al.	
	A4	US-10,331,502	06-25-2019	Hart	
	A5	US-10,348,755	07-09-2019	Shavell et al.	
	A6	US-2004/0133689-A1	07-08-2004	Vasisht	
	A7	US-2005/0234767-A1	10-20-2005	Bolzman et al.	
	A8	US-2007/0016948-A1	01-18-2007	Dubrovsky et al.	
	A9	US-2007/0179955-A1	08-02-2007	CROFT et al.	
	A10	US-2007/0214151-A1	09-13-2007	Thomas et al.	
	A11	US-2008/0017526-A1	01-24-2008	Prescott et al.	
	A12	US-2008/0140728-A1	06-12-2008	Fraser et al.	
	A13	US-2009/0323632-A1	12-31-2009	Nix	
	A14	US-2011/0219455-A1	09-08-2011	Bhagwan et al.	
	A15	US-2012/0198558-A1	08-02-2012	Liu et al.	
	A16	US-2013/0227078-A1	08-29-2013	WEI et al.	
	A17	US-2014/0334336-A1	11-13-2014	Chen et al.	
	A18	US-2015/0033331-A1	01-29-2015	STERN et al.	
	A19	US-2015/0156084-A1	06-04-2015	KAMINSKY et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO				***Complete if Known***	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/240,572-Conf. #2423
				Filing Date	September 22, 2011
				First Named Inventor	Stephen Wayne Boyer
				Art Unit	2492
(Use as many sheets as necessary)				Examiner Name	S. P. Kanaan
Sheet	2	of	3	Attorney Docket Number	BST-004

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A20	US-2015/0264061-A1	09-17-2015	IBATULLIN et al.	
	A21	US-2015/0317672-A1	11-05-2015	Espinoza et al.	
	A22	US-2016/0036849-A1	02-04-2016	Zakian	
	A23	US-2016/0182537-A1	06-23-2016	Tatourian et al.	
	A24	US-2016/0191554-A1	06-30-2016	KAMINSKY	
	A25	US-2016/0364496-A1	12-15-2016	Li	
	A26	US-2016/0373485-A1	12-22-2016	Kamble	
	A27	US-2017/0300911-A1	10-19-2017	Alnajem	
	A28	US-2017/0318045-A1	11-02-2017	JOHNS et al.	
	A29	US-2018/0123934-A1	05-03-2018	Gissing et al.	
	A30	US-2019/0089711-A1	03-21-2019	Faulkner	
	A31	US-2019/0098025-A1	03-28-2019	LIM	
	A32	US-2019/0215331-A1	07-11-2019	Anakata et al.	
	A33	US-2019/0303574-A1	10-03-2019	Lamay et al.	
	A34	US-2020/0053127-A1	02-13-2020	Brotherton et al.	
	A35	US-2020/0074084-A1	03-05-2020	DORRANS et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08b (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	3	of	3

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	C1	Search Query Report form IP.com (performed 04/27/2020).	
	C2	Camelo et al., "CONDENSER: A Graph-Based Approach for Detecting Botnets," AnubisNetworks R&D, Amadora, Portugal, 8 pages	
	C3	Camelo, "Botnet Cluster Identification," September 2014, 2 pages	
	C4	Azman, Mohamed et al. Wireless Daisy Chain and Tree Topology Networks for Smart Cities. 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT). https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber= 8869252 (Year: 2019)	
	C5	Basinya, Evgeny A.; Yushmanov, Anton A. Development of a Comprehensive Security System. 2019 Dynamics of Systems, Mechanisms and Machines (Dynamics). https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8944700 (Year: 2019)	
	C6	Luo, Hui; Henry, Paul. A Secure Public Wireless LAN Access Technique That Supports Walk-Up Users. GLOBECOM '03. IEEE Global Telecommunications Conference. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber= 1258471 (Year: 2003)	
	C7	SEIGNEUR et al., A Survey of Trust and Risk Metrics for a BYOD Mobile Worker World: Third International Conference on Social Eco-Informatics, 2013, 11 pages"	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

51414 7590 06/01/2020

GOODWIN PROCTER LLP
PATENT ADMINISTRATOR
100 NORTHERN AVENUE
BOSTON, MA 02210

EXAMINER
KANAAN, SIMON P

ART UNIT	PAPER NUMBER
2492	

DATE MAILED: 06/01/2020

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/240,572	09/22/2011	Stephen Wayne Boyer	BST-004	2423

TITLE OF INVENTION: INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$500	$0.00	$0.00	$500	09/01/2020

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Maintenance fees are due in utility patents issuing on applications filed on or after Dec. 12, 1980. It is patentee's responsibility to ensure timely payment of maintenance fees when due. More information is available at www.uspto.gov/PatentMaintenanceFees.

Black Kite Ex. 1002, Page 33 of 1060

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), by mail or fax, or via EFS-Web.

By mail, send to: Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

By fax, send to: (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

51414 7590 06/01/2020

GOODWIN PROCTER LLP
PATENT ADMINISTRATOR
100 NORTHERN AVENUE
BOSTON, MA 02210

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being transmitted to the USPTO via EFS-Web or by facsimile to (571) 273-2885, on the date below.

(Typed or printed name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/240,572	09/22/2011	Stephen Wayne Boyer	BST-004	2423

TITLE OF INVENTION: INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	$500	$0.00	$0.00	$500	09/01/2020

EXAMINER	ART UNIT	CLASS-SUBCLASS
KANAAN, SIMON P	2492	726-025000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-09 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) The names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document must have been previously recorded, or filed for recordation, as set forth in 37 CFR 3.11 and 37 CFR 3.81(a). Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. Fees submitted: ❑ Issue Fee ❑ Publication Fee (if required) ❑ Advance Order - # of Copies _____

4b. Method of Payment: *(Please first reapply any previously paid fee shown above)*

❑ Electronic Payment via EFS-Web ❑ Enclosed check ❑ Non-electronic payment by credit card (Attach form PTO-2038)

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment to Deposit Account No. _____

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29

❑ Applicant asserting small entity status. See 37 CFR 1.27

❑ Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

Black Kite Ex. 1002, Page 34 of 1060

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/240,572	09/22/2011	Stephen Wayne Boyer	BST-004	2423

51414 7590 06/01/2020

GOODWIN PROCTER LLP
PATENT ADMINISTRATOR
100 NORTHERN AVENUE
BOSTON, MA 02210

EXAMINER	
KANAAN, SIMON P	
ART UNIT	**PAPER NUMBER**
2492	

DATE MAILED: 06/01/2020

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Black Kite Ex. 1002, Page 35 of 1060

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 13/240,572	Applicant(s) Boyer et al.	
	Examiner SIMON P KANAAN	Art Unit 2492	AIA (FITF) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☑ This communication is responsive to 5/15/2020.
   ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

3. ☑ The allowed claim(s) is/are See Continuation Sheet . As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see **http://www.uspto.gov/patents/init_events/pph/index.jsp** or send an inquiry to **PPHfeedback@uspto.gov.**

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   Certified copies:

   a) ☐ All b) ☐ Some *c) ☐ None of the:

   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☑ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 5/15/20, 5/15/20, 3/31/16, 10/8/15.
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material _____.
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date. _____.
5. ☐ Examiner's Amendment/Comment
6. ☐ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/SIMON P KANAAN/
Primary Examiner, Art Unit 2492

Continuation of 3. The allowed claim(s) is/are: 1,4-5,7-14,16,121,124,126-132 and 134-141

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/240,572	Boyer et al.
	Examiner	**Art Unit**
	SIMON P KANAAN	2492

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

CLAIMS

☑ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	05/26/2020	05/26/2020	05/26/2020	05/26/2020	05/26/2020	05/26/2020	05/26/2020	05/26/2020	05/26/2020
	1	✓	✓	✓	✓	✓	✓	✓	✓	=
	2	✓	✓	-	-	-	-	-	-	-
	3	✓	✓	✓	✓	✓	-	-	-	-
	4	✓	✓	✓	✓	✓	✓	✓	✓	=
	5	✓	✓	✓	✓	✓	✓	✓	✓	=
	6	✓	✓	-	-	-	-	-	-	-
	7	✓	✓	✓	✓	✓	✓	✓	✓	=
	8	✓	✓	✓	✓	✓	✓	✓	✓	=
	9	✓	✓	✓	✓	✓	✓	✓	✓	=
	10	✓	✓	✓	✓	✓	✓	✓	✓	=
	11	✓	✓	✓	✓	✓	✓	✓	✓	=
	12	✓	✓	✓	✓	✓	✓	✓	✓	=
	13	✓	✓	✓	✓	✓	✓	✓	✓	=
	14	✓	✓	✓	✓	✓	✓	✓	✓	=
	15	✓	✓	-	-	-	-	-	-	-
	16	✓	✓	✓	✓	✓	✓	✓	✓	=
	17	✓	✓	-	-	-	-	-	-	-
	18	✓	✓	-	-	-	-	-	-	-
	19	✓	✓	-	-	-	-	-	-	-
	20	✓	✓	-	-	-	-	-	-	-
	21	-	-	-	-	-	-	-	-	-
	22	-	-	-	-	-	-	-	-	-
	23	-	-	-	-	-	-	-	-	-
	24	-	-	-	-	-	-	-	-	-
	25	-	-	-	-	-	-	-	-	-
	26	-	-	-	-	-	-	-	-	-
	27	-	-	-	-	-	-	-	-	-
	28	-	-	-	-	-	-	-	-	-
	29	-	-	-	-	-	-	-	-	-
	30	-	-	-	-	-	-	-	-	-
	31	-	-	-	-	-	-	-	-	-
	32	-	-	-	-	-	-	-	-	-
	33	-	-	-	-	-	-	-	-	-
	34	-	-	-	-	-	-	-	-	-
	35	-	-	-	-	-	-	-	-	-
	36	-	-	-	-	-	-	-	-	-
	37	-	-	-	-	-	-	-	-	-
	38	-	-	-	-	-	-	-	-	-
	39	-	-	-	-	-	-	-	-	-
	40	-	-	-	-	-	-	-	-	-
	41	-	-	-	-	-	-	-	-	-
	42	-	-	-	-	-	-	-	-	-

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/240,572	Boyer et al.
	Examiner	**Art Unit**
	SIMON P KANAAN	2492

CLAIM		DATE								
Final	Original	05/26/2020	05/26/2020	05/26/2020	05/26/2020	05/26/2020	05/26/2020	05/26/2020	05/26/2020	05/26/2020
	43	-	-	-	-	-	-	-	-	-
	44	-	-	-	-	-	-	-	-	-
	45	-	-	-	-	-	-	-	-	-
	46	-	-	-	-	-	-	-	-	-
	47	-	-	-	-	-	-	-	-	-
	48	-	-	-	-	-	-	-	-	-
	49	-	-	-	-	-	-	-	-	-
	50	-	-	-	-	-	-	-	-	-
	51	-	-	-	-	-	-	-	-	-
	52	-	-	-	-	-	-	-	-	-
	53	-	-	-	-	-	-	-	-	-
	54	-	-	-	-	-	-	-	-	-
	55	-	-	-	-	-	-	-	-	-
	56	-	-	-	-	-	-	-	-	-
	57	-	-	-	-	-	-	-	-	-
	58	-	-	-	-	-	-	-	-	-
	59	-	-	-	-	-	-	-	-	-
	60	-	-	-	-	-	-	-	-	-
	61	-	-	-	-	-	-	-	-	-
	62	-	-	-	-	-	-	-	-	-
	63	-	-	-	-	-	-	-	-	-
	64	-	-	-	-	-	-	-	-	-
	65	-	-	-	-	-	-	-	-	-
	66	-	-	-	-	-	-	-	-	-
	67	-	-	-	-	-	-	-	-	-
	68	-	-	-	-	-	-	-	-	-
	69	-	-	-	-	-	-	-	-	-
	70	-	-	-	-	-	-	-	-	-
	71	-	-	-	-	-	-	-	-	-
	72	-	-	-	-	-	-	-	-	-
	73	-	-	-	-	-	-	-	-	-
	74	-	-	-	-	-	-	-	-	-
	75	-	-	-	-	-	-	-	-	-
	76	-	-	-	-	-	-	-	-	-
	77	-	-	-	-	-	-	-	-	-
	78	-	-	-	-	-	-	-	-	-
	79	-	-	-	-	-	-	-	-	-
	80	-	-	-	-	-	-	-	-	-
	81	-	-	-	-	-	-	-	-	-
	82	-	-	-	-	-	-	-	-	-
	83	-	-	-	-	-	-	-	-	-
	84	-	-	-	-	-	-	-	-	-
	85	-	-	-	-	-	-	-	-	-
	86	-	-	-	-	-	-	-	-	-
	87	-	-	-	-	-	-	-	-	-
	88	-	-	-	-	-	-	-	-	-
	89	-	-	-	-	-	-	-	-	-
	90	-	-	-	-	-	-	-	-	-
	91	-	-	-	-	-	-	-	-	-
	92	-	-	-	-	-	-	-	-	-
	93	-	-	-	-	-	-	-	-	-
	94	-	-	-	-	-	-	-	-	-

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/240,572	Boyer et al.
	Examiner	**Art Unit**
	SIMON P KANAAN	2492

CLAIM		DATE								
Final	Original	05/26/2020	05/26/2020	05/26/2020	05/26/2020	05/26/2020	05/26/2020	05/26/2020	05/26/2020	05/26/2020
	95	-	-	-	-	-	-	-	-	-
	96	-	-	-	-	-	-	-	-	-
	97	-	-	-	-	-	-	-	-	-
	98	-	-	-	-	-	-	-	-	-
	99	-	-	-	-	-	-	-	-	-
	100	-	-	-	-	-	-	-	-	-
	101	-	-	-	-	-	-	-	-	-
	102	-	-	-	-	-	-	-	-	-
	103	-	-	-	-	-	-	-	-	-
	104	-	-	-	-	-	-	-	-	-
	105	-	-	-	-	-	-	-	-	-
	106	-	-	-	-	-	-	-	-	-
	107	-	-	-	-	-	-	-	-	-
	108	-	-	-	-	-	-	-	-	-
	109	-	-	-	-	-	-	-	-	-
	110	-	-	-	-	-	-	-	-	-
	111	-	-	-	-	-	-	-	-	-
	112	-	-	-	-	-	-	-	-	-
	113	-	-	-	-	-	-	-	-	-
	114	-	-	-	-	-	-	-	-	-
	115	-	-	-	-	-	-	-	-	-
	116	-	-	-	-	-	-	-	-	-
	117	-	-	-	-	-	-	-	-	-
	118	-	-	-	-	-	-	-	-	-
	119	-	-	-	-	-	-	-	-	-
	120	-	-	-	-	-	-	-	-	-
	121			✓	✓	✓	✓	✓	✓	=
	122			✓	✓	✓	✓	✓	✓	=
	123			✓	✓	✓	-	-	-	-
	124			✓	✓	✓	✓	✓	✓	=
	125			✓	-	-	-	-	-	-
	126			✓	✓	✓	✓	✓	✓	=
	127			✓	✓	✓	✓	✓	✓	=
	128			✓	✓	✓	✓	✓	✓	=
	129			✓	✓	✓	✓	✓	✓	=
	130			✓	✓	✓	✓	✓	✓	=
	131			✓	✓	✓	✓	✓	✓	=
	132			✓	✓	✓	✓	✓	✓	=
	133			✓	-	-	-	-	-	-
	134			✓	✓	✓	✓	✓	✓	=
	135			✓	✓	✓	✓	✓	✓	=
	136				✓	✓	✓	✓	✓	=
	137				✓	✓	✓	✓	✓	=
	138				✓	✓	✓	✓	✓	=
	139				✓	✓	✓	✓	✓	=
	140				✓	✓	✓	✓	✓	=
	141							✓	✓	=

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/240,572	Boyer et al.
	Examiner	Art Unit
	SIMON P KANAAN	2492

CPC - Searched*		
Symbol	Date	Examiner

CPC Combination Sets - Searched*		
Symbol	Date	Examiner
H04L63/20	05/26/2020	SK

US Classification - Searched*			
Class	Subclass	Date	Examiner

* See search history printout included with this form or the SEARCH NOTES box below to determine the scope of the search.

Search Notes		
Search Notes	Date	Examiner
Inventor and Assignee Search (PALM)	4/18/2013	SK
class/subclass search + text (EAST: 726/1,2,22,25+text)	3/7/2016	SK
CPC + text (EAST: H04L63/20,145,14,0236,1433,104 OR H04L67/306 OR H04L51/12 OR H04L61/1511 OR H04L9/321 OR G06F21/00,577 + text)	2/7/2017	SK
Interference Search + text (EAST)	05/26/2020	SK

Interference Search			
US Class/CPC Symbol	US Subclass/CPC Group	Date	Examiner
H04L63	20 + text	05/26/2020	SK

/SIMON P KANAAN/ Primary Examiner, Art Unit 2492	

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/240,572	Boyer et al.
	Examiner	Art Unit
	SIMON P KANAAN	2492

CPC								
Symbol							Type	Version
H04L	/	63	/	1433			F	2013-01-01
G06Q	/	10	/	0639			I	2013-01-01
H04L	/	43	/	062			I	2013-01-01
H04L	/	43	/	0876			I	2013-01-01
H04L	/	61	/	2007			I	2013-01-01
H04L	/	67	/	20			I	2013-01-01
H04L	/	63	/	145			A	2013-01-01

CPC Combination Sets								
Symbol					Type	Set	Ranking	Version
	/		/					

NONE		Total Claims Allowed:	
(Assistant Examiner)	(Date)	28	
/SIMON P KANAAN/ Primary Examiner, Art Unit 2492	26 May 2020	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	1

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/240,572	Boyer et al.
	Examiner	**Art Unit**
	SIMON P KANAAN	2492

INTERNATIONAL CLASSIFICATION					
CLAIMED					
H04L	/	29	/	06	

NON-CLAIMED					
	/		/		

US ORIGINAL CLASSIFICATION	
CLASS	**SUBCLASS**

CROSS REFERENCES(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					

NONE (Assistant Examiner) (Date)	**Total Claims Allowed:** 28	
/SIMON P KANAAN/ Primary Examiner, Art Unit 2492 (Primary Examiner) 26 May 2020 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 1

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13/240,572	Boyer et al.
	Examiner	**Art Unit**
	SIMON P KANAAN	2492

☑ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIMS

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
	1		19		37		55		73		91		109		127
	2		20		38		56		74		92		110		128
	3		21		39		57		75		93		111		129
	4		22		40		58		76		94		112		130
	5		23		41		59		77		95		113		131
	6		24		42		60		78		96		114		132
	7		25		43		61		79		97		115		133
	8		26		44		62		80		98		116		134
	9		27		45		63		81		99		117		135
	10		28		46		64		82		100		118		136
	11		29		47		65		83		101		119		137
	12		30		48		66		84		102		120		138
	13		31		49		67		85		103		121		139
	14		32		50		68		86		104		122		140
	15		33		51		69		87		105		123		141
	16		34		52		70		88		106		124		
	17		35		53		71		89		107		125		
	18		36		54		72		90		108		126		

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 28	
/SIMON P KANAAN/ Primary Examiner, Art Unit 2492 (Primary Examiner)	26 May 2020 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 1

EAST Search History

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 11:13
L2	80755	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 11:13
L4	93	(resilien$3 duration (vulnerability or down)).clm.	US-PGPUB; USPAT	AND	ON	2020/05/26 11:13
L5	562	((orginazation or company or bank$3) resilien$3).clm.	US-PGPUB; USPAT	AND	ON	2020/05/26 11:14
L6	0	((external$5 or third party) (security) and (commercial data) and reputation).clm.	US-PGPUB; USPAT	ADJ	ON	2020/05/26 11:14
L7	0	(reputation and ((insustry reports) or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)).clm.	US-PGPUB; USPAT	ADJ	ON	2020/05/26 11:15
L9	46	(network reputation (rat$3 or assess$4) and public).clm.	US-PGPUB; USPAT	AND	ON	2020/05/26 11:20

5/26/2020 11:46:06 AM
C:\Users\skanaan\Documents\EAST\Workspaces\13240572.wsp

Docket No.: BST-004
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Stephen Wayne Boyer et al.

Application No.: 13/240,572 Confirmation No.: 2423

Filed: September 22, 2011 Art Unit: 2492

For: INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM Examiner: S. P. Kanaan

Submitted via EFS-Web

INFORMATION DISCLOSURE STATEMENT (IDS)

Pursuant to 37 C.F.R. §§ 1.56, 1.97, and 1.98, the attention of the United States Patent and Trademark Office is hereby directed to the references listed on the attached PTO/SB/08. It is respectfully requested that the information be expressly considered during the prosecution of the above-identified application, and that the references be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Information Disclosure Statement is being submitted with a Request for Continued Examination.

In accordance with 37 CFR 1.98(a)(2)(ii), Applicant has not submitted copies of U.S. patents and U.S. patent applications.

In accordance with 37 C.F.R. § 1.97(g), the filing of this Information Disclosure Statement shall not be construed as a representation that a search has been made. In accordance with 37 C.F.R. § 1.97(h), the filing of this Information Disclosure Statement shall not be construed to be an admission that the information cited in this Information Disclosure Statement is, or is considered to be, material to patentability as defined in 37 C.F.R. § 1.56(b).

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

Applicant has cited for the Examiner's consideration certain co-pending U.S. patent applications that are owned at least in part by the assignee of this application, that describe subject matter that may be related to the present invention. The co-pending applications are listed herewith in accordance with M.P.E.P. 609.06 which states: "Applicant may wish to list U.S. patent application numbers on other than a form PTO/SB/08A and 08B format to avoid the application numbers of pending applications being published on the patent. If a citation is not printed on the patent but has been considered by the examiner, the patented file will reflect that fact as noted in MPEP § 609.05(b)."

No copies of the co-pending applications have been provided. If the Examiner wishes to have copies of the co-pending applications, Examiner should contact the Attorney or Agent of record. Applicant respectfully requests that the Examiner consider these listed documents and indicate that each was considered by making appropriate notations on this Information Disclosure Statement.

Docket No.	**U.S. Serial No.:**	**Title**	**Filing Date**
BST-002	15/377,574 9,705,932	METHODS AND SYSTEMS FOR CREATING, DE-DUPLICATING, AND ACCESSING DATA USING AN OBJECT STORAGE SYSTEM	December 13, 2016
BST-003	14/021,585 9,438,615 Published as: US2015/0074579	SECURITY RISK MANAGEMENT	September 9, 2013
BST-003C1	15/216,955 Published as: US2016/0330231	METHODS FOR USING ORGANIZATIONAL BEHAVIOR FOR RISK RATINGS	July 22, 2016
BST-003C2	15/239,063 Published as: US2017/0093901	SECURITY RISK MANAGEMENT	August 17, 2016

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

Docket No.	U.S. Serial No.:	Title	Filing Date
BST-004C1	14/944,484 9,973,524 Published as: US2016/0323308	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM	November 18, 2015
BST-004C1CP	15/142,677 9,830,569 Published as: US/2016/0239772	SECURITY ASSESSMENT USING SERVICE PROVIDER DIGITAL ASSET INFORMATION	April 29, 2016
BST-007	15/134,845 9,680,858	ANNOTATION PLATFORM FOR A SECURITY RISK SYSTEM	April 21, 2016
BST-008	15/044,952 Published as: US2017/0236077	RELATIONSHIPS AMONG TECHNOLOGY ASSETS AND SERVICES AND THE ENTITIES RESPONSIBLE FOR THEM	February 16, 2016
BST-008C2	15/089,375 10,176,445 Published as: US2017/0236079	RELATIONSHIPS AMONG TECHNOLOGY ASSETS AND SERVICES AND THE ENTITIES RESPONSIBLE FOR THEM	April 1, 2016
BST-009DA	29/598,298 D835,631	COMPUTER DISPLAY SCREEN WITH GRAPHICAL USER INTERFACE	March 24, 2017
BST-009DB	29/598,299 D818,475	COMPUTER DISPLAY WITH SECURITY RATINGS GRAPHICAL USER INTERFACE	March 24, 2017
BST-009DC	29/599,622	COMPUTER DISPLAY WITH SECURITY RATINGS GRAPHICAL USER INTERFACE	April 5, 2017

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

Docket No.	U.S. Serial No.:	Title	Filing Date
BST-009DD	29/599,620	COMPUTER DISPLAY WITH SECURITY RATINGS GRAPHICAL USER INTERFACE	April 5, 2017
BST-010	16/015,686	METHODS FOR MAPPING IP ADDRESSES AND DOMAINS TO ORGANIZATIONS USING USER ACTIVITY DATA	June 22, 2018
BST-011	15/918,286	CORRELATED RISK IN CYBERSECURITY	March 12, 2018
BST-011C1	16/292,956	CORRELATED RISK IN CYBERSECURITY	May 5, 2019
BST-011C2	16/795,056	CORRELATED RISK IN CYBERSECURITY	February 19, 2020
BST-012	16/170680	SYSTEMS AND METHODS FOR REMOTE DETECTION OF SOFTWARE THROUGH BROWSER WEBINJECTS	October 25, 2018
BST-012C1	16/688647	SYSTEMS AND METHODS FOR REMOTE DETECTION OF SOFTWARE THROUGH BROWSER WEBINJECTS	November 19, 2019
BST-013	15/954921	SYSTEMS AND METHODS FOR EXTERNAL DETECTION OF MISCONFIGURED SYSTEMS	April 17, 2018
BST-014	16/549764	SYSTEMS AND METHODS FOR INFERRING ENTITY RELATIONSHIPS VIA NETWORK COMMUNICATIONS OF USERS OR USER DEVICES	August 23, 2019
BST-014C1	16/787,650	SYSTEMS AND METHODS FOR INFERRING ENTITY RELATIONSHIPS VIA NETWORK COMMUNICATIONS OF USERS OR	February 11, 2020

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

Docket No.	U.S. Serial No.:	Title	Filing Date
		USER DEVICES	
BST-015	16/583991	SYSTEMS AND METHODS FOR NETWORK ASSET DISCOVERY AND ASSOCIATION THEREOF WITH ENTITIES	September 26, 2019
BST-016D	29/666942	COMPUTER DISPLAY WITH GRAPHICAL USER INTERFACE	October 17, 2018
BST-017	16/360,641	SYSTEMS AND METHODS FOR FORECASTING CYBERSECURITY RATINGS BASED ON EVENT-RATE SCENARIOS	March 21, 2019
BST-018	16/514,771	SYSTEMS AND METHODS FOR GENERATING SECURITY IMPROVEMENT PLANS FOR ENTITIES	July 17, 2019
BST-019D	29/677306	COMPUTER DISPLAY WITH CORPORATE HIERARCHY GRAPHICAL USER INTERFACE COMPUTER DISPLAY WITH CORPORATE HIERARCHY GRAPHICAL USER INTERFACE	January 18, 2019
BST-020	16/775840	SYSTEMS AND METHODS FOR ASSESSING CYBERSECURITY STATE OF ENTITIES BASED ON COMPUTER NETWORK CHARACTERIZATION	January 29, 2020
BST-021	16/779437	SYSTEMS AND METHODS FOR RAPIDLY GENERATING SECURITY RATINGS	January 31, 2020
BST-023	16/802232	SYSTEMS AND METHODS FOR IMPROVING A SECURITY PROFILE OF AN ENTITY BASED ON PEER SECURITY PROFILES	February 26, 2020

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

Docket No.	U.S. Serial No.:	Title	Filing Date
BST-023DA	29/725724	COMPUTER DISPLAY WITH RISK VECTORS GRAPHICAL USER INTERFACE	February 26, 2020

Additionally, Applicant hereby apprises the Examiner of the following patents and patent applications, including the contents of the file wrappers, the claims, any Office Actions issued therein, and any Notices of Allowance issued therefor:

1. U.S.S.N. 15/377,574 (Attorney Docket No. BST-002), now U.S. Patent No. 9,705,932, the Office Action mailed 03/02/2017 and the Notice of Allowance mailed 06/01/2017;

2. U.S.S.N. 14/021,585 (Attorney Docket No. BST-003), now U.S. Patent No. 9,438,615, the Office Action mailed 03/11/2016 and the Notice of Allowance mailed 08/09/2016;

3. U.S.S.N. 15/216,955 (Attorney Docket No. BST-003C1), the Office Actions mailed 11/04/2016, 03/09/2017, 06/06/2017, 12/05/2017, and 08/29/2018, and the Notice of Allowance mailed 02/06/2019;

4. U.S.S.N. 15/239,063 (Attorney Docket No. BST-003C2), the Office Action mailed 03/21/2018 and the Notice of Allowance mailed 01/14/2019;

5. U.S.S.N. 14/944,484 (Attorney Docket No. BST-004C1), now U.S. Patent No. 9,973,524, the Office Actions mailed 03/11/2016, 07/05/2016, and 01/17/2017 and the Notice of Allowance mailed 10/20/2017;

6. U.S.S.N. 15/142,677 (Attorney Docket No. BST-004C1CP), now U.S. Patent No. 9,830,569, the Office Actions mailed 07/26/2016, and 04/24/2017 and the Notice of Allowance mailed 10/11/2017;

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

7. U.S.S.N. 15/134,845 (Attorney Docket No. BST-007), now U.S. Patent No. 9,680,858, the Office Actions mailed 07/19/2016 and 01/26/2017, and the Notices of Allowance mailed 04/27/2017 and 05/09/2017;

8. U.S.S.N. 15/089,375 (Attorney Docket No. BST-008C2), now U.S. Patent No. 10,176,445, the Office Actions mailed 09/09/2016, 05/17/2017, and 11/17/2017 and the Notice of Allowance mailed 08/09/2018;

9. U.S.S.N. 29/598,298 (Attorney Docket No. BST-009DA), now U.S. Patent No. D835,631, the Notice of Allowance mailed 08/15/2018;

10. U.S.S.N. 29/598,299 (Attorney Docket No. BST-009DB), now U.S. Patent No. D818,475, the Notice of Allowance mailed 01/02/2018;

11. U.S.S.N. 29/599,622 (Attorney Docket No. BST-009DC), the Notice of Allowance mailed 12/11/2018;

12. U.S.S.N. 29/599,620 (Attorney Docket No. BST-009DD), the Notice of Allowance mailed 11/27/2018;

13. U.S.S.N. 16/015,686 (Attorney Docket No. BST-010), the Office Action mailed 11/16/2018; the Notice of Allowance mailed 05/10/2019;

14. U.S.S.N. 15/918,286 (Attorney Docket No. BST-011), the Office Action mailed 08/07/2018 and the Notice of Allowance mailed 11/29/2018; and

15. U.S.S.N. 16/292,956 (Attorney Docket No. BST-011C1), the Office Action mailed 07/10/2019; the Notices of Allowance mailed 01/08/2020 and 01/27/2020;

16. U.S.S.N. 16/795,056 (Attorney Docket No. BST-011C2), the Office Action mailed 05/01/2020;

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

17. U.S.S.N. 16/170,680 (Attorney Docket No. BST-012), the Office Action mailed 03/26/2019; the Notices of Allowance mailed 10/29/2019 and 08/27/2019;

18. U.S.S.N. 16/688,647 (Attorney Docket No. BST-012C1), the Office Action mailed 01/29/2020;

19. U.S.S.N. 15/954,921 (Attorney Docket No. BST-013), the Office Actions mailed 08/19/2019, 09/04/2018 and 01/03/2019; Advisory Action mailed 03/03/2020;

20. U.S.S.N. 16/787,650 (Attorney Docket No. BST-014C1), the Notice of Allowance mailed 04/07/2020;

21. U.S.S.N. 16/583,991 (Attorney Docket No. BST-015), the Office Action mailed 01/13/2020;

22. U.S.S.N. 29/666,942 (Attorney Docket No. BST-016D), the Notice of Allowance mailed 04/30/2020;

23. U.S.S.N. 16/360,641 (Attorney Docket No. BST-017), the Office Action mailed 08/07/2019 and 02/20/2020;

24. U.S.S.N. 16/514,771 (Attorney Docket No. BST-018), the Office Action mailed 12/04/2019; the Notice of Allowance mailed 03/18/2020; and

25. U.S.S.N. 16/802,232 (Attorney Docket No. BST-023), the Notice of Allowance mailed 04/24/2020.

As stated above, a Request for Continued Examination and related fee are being submitted with this paper. If any additional fees are due, the Director is hereby authorized to charge such fees to our Deposit Account No. 07-1700, under Order No. BST-004.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

Dated: May 15, 2020

Respectfully submitted,

Electronic signature: /Gozde Guckaya/
Gozde Guckaya
Registration No.: 74,989
GOODWIN PROCTER LLP
100 Northern Avenue
Boston, Massachusetts 02210
(617) 305-6778
Agent for Applicant

/SIMON P KANAAN/ 05/25/2020

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

Sheet 1 of 1

Substitute Disclosure Form / U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No.	Application No.
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))	38879-0006001	13/240,572
	Applicant: Boyer et al.	
	Filing Date: September 22, 2011	Group Art Unit: 2492

U.S. Patent Documents

Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	1.	2012/0158725	06-2012	Molloy et al.			
	2.	2014/0204803	07-2014	Nguyen			
	3.	5,867,799	02-1999	Lang			
	4.	6,016,475	01-2000	Miller			
	5.	7,100,195	08-2006	Underwood			
	6.	2012/0166458	06-2012	Laudanski			
	7.	2005/0080720	04-2005	Betz			
	8.	2004/0221296	11-2004	Ogielski			
	9.	7,748,038	06-2010	Olivier			

Foreign Patent Documents or Published Foreign Patent Applications

Examiner Initial	Desig. ID	Document Number	Publication Date	Country or Patent Office	Class	Subclass	Translation Yes	Translation No

Other Documents (include Author, Title, Date, and Place of Publication)

Examiner Initial	Desig. ID	Document
	10.	PAIR transaction history of US application no. 14/021,585 and pending claims as of March 22, 2016.
	11.	PAIR transaction history of US application no. 14/944,484, application as filed and pending claims as of March 22, 2016.

Examiner Signature	Date Considered
05/26/2020	/SIMON P KANAAN/

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:13
L2	13	726/25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:13
L3	0	apparatus and method for network vulnerability detection and compliance	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:13
L4	0	network vulnerability detection and compliance assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:13
L5	0	network vulnerability detection compliance assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:13
L6	0	network with vulnerability with detection with compliance with assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:13
L7	14	network with vulnerability with detection with compliance with assessment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:13
L8	42	726/2,22,25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:13
L9	35	726/2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:13
L10	49	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:13
L11	6	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14

L12	195	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L13	0	(external$5 or third party) with (security) with (commercial near data) with reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L14	0	(external$5 or third party) with (commercial near data) with reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L15	39	internet monitoring with report	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L16	23	internet monitoring with report and public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L17	0	malwareurl	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L18	0	malwareurl$5	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L19	3	www$malwareurl$5	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L20	3	www$malwareurl$com	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L21	257	arbor networks	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L22	4	arbor networks and renesys	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L23	10317	reputation and domain	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L24	121	reputation and domain and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14

L25	234	reputation and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L26	113	L25 not L24	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L27	20	US-7194769-$.DID. OR US-7290275-$.DID. OR US-7971252-$.DID. OR US-20040010709-$.DID. OR US-20050138413-$.DID. OR US-20080047018-$.DID. OR US-20080209565-$.DID. OR US-20090265787-$.DID. OR US-20090293128-$.DID. OR US-2007304-$.DID. OR US-5200596-$.DID. OR US-2009104-$.DID. OR US-422009D-$.DID. OR US-1331018-$.DID.	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:14
L28	0	L25 and L27	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L29	0	(insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L27	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L30	0	(industry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L27	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L31	0	(industry reports or internet monitoring or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L27	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L32	0	L27 and user behavior	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L33	0	L27 and behavior	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L34	0	L27 and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14

L35	0	L27 and public with features	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:14
L36	0	L27 and externally	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:14
L37	7	L27 and external	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:14
L38	2	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L39	33	((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L40	503	((external$5 or third party) with audit$4)and reputation and security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L41	1006	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L42	931	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L43	539	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L44	3	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial data sources	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14

L45	9	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial data	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L46	9	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rating and commercial data	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L47	8	security and renesys	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L48	1	abor networks	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L50	115	(network near3 vulnerability) with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L51	40	(network near3 assessment) with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L52	99	(network near3 assessment) with external$3	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L53	1919	site secure	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L54	688	L53 and third party	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L55	259	L54 and assess$3	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L56	337	network reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L57	316	network reputation and (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L58	20	network reputation with (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L59	10	network reputation with (rat$3 or assess$4) and public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14

L60	3	network reputation with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L61	1042	network (reputation or assess$4 or rat$3) with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L62	766	network (reputation or assess$4 or rat$3) with public and security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L63	19	network (reputation or assess$4 or rat$3) with public with security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L64	33	network (reputation or assess$4 or rat$3) with public with secur$5	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L65	14	L64 not L63	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L66	2	"20040250122"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L67	2	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L68	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L70	7720	(organization or company or entity) same reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L71	1983	(organization or company or entity) same reputation same (score or rating)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L72	20155	726/1,2,22,25.ccls.	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L73	129	L71 and L72	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L74	1132	(organization or company) same reputation same (score or rating)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15

L75	62	L74 and L72	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L76	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L77	13	726/25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L78	0	apparatus and method for network vulnerability detection and compliance	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L79	0	network vulnerability detection and compliance assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L80	0	network vulnerability detection compliance assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L81	0	network with vulnerability with detection with compliance with assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L82	14	network with vulnerability with detection with compliance with assessment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L83	42	726/2,22,25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L84	35	726/2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L85	49	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L86	6	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L87	195	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15

L88	0	(external$5 or third party) with (security) with (commercial near data) with reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L89	0	(external$5 or third party) with (commercial near data) with reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L90	39	internet monitoring with report	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L91	23	internet monitoring with report and public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L92	0	malwareurl	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L93	0	malwareurl$5	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L94	3	www$malwareurl$5	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L95	3	www$malwareurl$com	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L96	257	arbor networks	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L97	4	arbor networks and renesys	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L98	10317	reputation and domain	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L99	121	reputation and domain and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L100	234	reputation and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15

L101	113	L100 not L99	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L102	20	US-7194769-$.DID. OR US-7290275-$.DID. OR US-7971252-$.DID. OR US-20040010709-$.DID. OR US-20050138413-$.DID. OR US-20080047018-$.DID. OR US-20080209565-$.DID. OR US-20090265787-$.DID. OR US-20090293128-$.DID. OR US-2007304-$.DID. OR US-5200596-$.DID. OR US-2009104-$.DID. OR US-422009D-$.DID. OR US-1331018-$.DID.	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:15
L103	0	L100 and L102	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L104	0	(insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L102	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L105	0	(industry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L102	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L106	0	(industry reports or internet monitoring or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L102	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L107	0	L102 and user behavior	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L108	0	L102 and behavior	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L109	0	L102 and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L110	0	L102 and public with features	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:15

L111	0	L102 and externally	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:15
L112	7	L102 and external	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:15
L113	36	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L114	2	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L115	33	((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L116	503	((external$5 or third party) with audit$4)and reputation and security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L117	1006	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L118	931	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L119	539	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L120	3	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial data sources	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L121	9	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial data	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15

L122	9	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rating and commercial data	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L123	8	security and renesys	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L124	1	abor networks	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L125	115	(network near3 vulnerability) with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L126	40	(network near3 assessment) with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:15
L127	99	(network near3 assessment) with external$3	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L128	1919	site secure	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L129	688	L128 and third party	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L130	259	L129 and assess$3	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L131	337	network reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L132	316	network reputation and (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L133	20	network reputation with (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L134	10	network reputation with (rat$3 or assess$4) and public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L135	3	network reputation with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16

L136	1042	network (reputation or assess$4 or rat$3) with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L137	766	network (reputation or assess$4 or rat$3) with public and security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L138	19	network (reputation or assess$4 or rat$3) with public with security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L139	33	network (reputation or assess$4 or rat$3) with public with secur$5	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L140	14	L139 not L138	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L141	2	"20040250122"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L142	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L143	7720	(organization or company or entity) same reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L144	1983	(organization or company or entity) same reputation same (score or rating)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L145	20155	726/1,2,22,25.ccls.	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L146	129	L144 and L145	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L147	1132	(organization or company) same reputation same (score or rating)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L148	62	L147 and L145	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L151	2	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16

L152	33	network (reputation or assess$4 or rat$3) with public with secur$5	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L153	36	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L154	25	L153 AND ((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L155	273	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.) and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L156	80755	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L157	777	(network or organization or entity) reputation and (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L158	246	L157 and L156	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L159	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L160	0	"11237642"	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:16
L163	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16

L164	13	726/25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L165	0	apparatus and method for network vulnerability detection and compliance	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L166	0	network vulnerability detection and compliance assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L167	0	network vulnerability detection compliance assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L168	0	network with vulnerability with detection with compliance with assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L169	14	network with vulnerability with detection with compliance with assessment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L170	42	726/2,22,25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L171	35	726/2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L172	49	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L173	6	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L174	195	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L175	13	726/25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L176	0	network with vulnerability with detection with compliance with assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16

L177	20	US-7194769-$.DID. OR US-7290275-$.DID. OR US-7971252-$.DID. OR US-20040010709-$.DID. OR US-20050138413-$.DID. OR US-20080047018-$.DID. OR US-20080209565-$.DID. OR US-20090265787-$.DID. OR US-20090293128-$.DID. OR US-2007304-$.DID. OR US-5200596-$.DID. OR US-2009104-$.DID. OR US-422009D-$.DID. OR US-1331018-$.DID.	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:16
L178	0	(insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L177	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L179	766	network (reputation or assess$4 or rat$3) with public and security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L180	273	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.) and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L181	195	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L183	273	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.) and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L184	195	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L185	3	L183 and L184	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17

L186	539	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L187	3	L183 and L185	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L188	14	L183 and L186	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L189	80755	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L190	30	L184 and L189	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L191	189	L186 and L189	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L192	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L193	13	726/25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L194	0	apparatus and method for network vulnerability detection and compliance	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L195	0	network vulnerability detection and compliance assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L196	0	network vulnerability detection compliance assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L197	0	network with vulnerability with detection with compliance with assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L198	14	network with vulnerability with detection with compliance with assessment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17

L199	42	726/2,22,25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L200	35	726/2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L201	49	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L202	6	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L203	195	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L204	0	(external$5 or third party) with (security) with (commercial near data) with reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L205	0	(external$5 or third party) with (commercial near data) with reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L206	39	internet monitoring with report	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L207	23	internet monitoring with report and public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L208	0	malwareurl	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L209	0	malwareurl$5	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L210	3	www$malwareurl$5	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L211	3	www$malwareurl$com	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17

L212	257	arbor networks	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L213	4	arbor networks and renesys	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L214	10317	reputation and domain	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L215	121	reputation and domain and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L216	234	reputation and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L217	113	L216 not L215	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L218	20	US-7194769-$.DID. OR US-7290275-$.DID. OR US-7971252-$.DID. OR US-20040010709-$.DID. OR US-20050138413-$.DID. OR US-20080047018-$.DID. OR US-20080209565-$.DID. OR US-20090265787-$.DID. OR US-20090293128-$.DID. OR US-2007304-$.DID. OR US-5200596-$.DID. OR US-2009104-$.DID. OR US-422009D-$.DID. OR US-1331018-$.DID.	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:17
L219	0	L216 and L218	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L220	0	(insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L218	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L221	0	(industry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L218	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17

L222	0	(industry reports or internet monitoring or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L218	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L223	0	L218 and user behavior	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L224	0	L218 and behavior	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L225	0	L218 and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L226	0	L218 and public with features	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:17
L227	0	L218 and externally	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:17
L228	7	L218 and external	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:17
L229	2	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L230	33	((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L231	503	((external$5 or third party) with audit$4)and reputation and security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17
L232	1006	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:17

L233	931	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L234	539	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L235	3	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial data sources	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L236	9	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial data	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L237	9	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rating and commercial data	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L238	8	security and renesys	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L239	1	abor networks	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L240	115	(network near3 vulnerability) with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L241	40	(network near3 assessment) with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L242	99	(network near3 assessment) with external$3	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L243	1919	site secure	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L244	688	L243 and third party	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L245	259	L244 and assess$3	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18

L246	337	network reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L247	316	network reputation and (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L248	20	network reputation with (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L249	10	network reputation with (rat$3 or assess$4) and public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L250	3	network reputation with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L251	1042	network (reputation or assess$4 or rat$3) with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L252	766	network (reputation or assess$4 or rat$3) with public and security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L253	19	network (reputation or assess$4 or rat$3) with public with security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L254	33	network (reputation or assess$4 or rat$3) with public with secur$5	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L255	14	L254 not L253	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L256	2	"20040250122"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L257	2	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L258	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L259	7720	(organization or company or entity) same reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18

L260	1983	(organization or company or entity) same reputation same (score or rating)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L261	20155	726/1,2,22,25.ccls.	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L262	129	L260 and L261	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L263	1132	(organization or company) same reputation same (score or rating)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L264	62	L263 and L261	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L265	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L266	13	726/25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L267	0	apparatus and method for network vulnerability detection and compliance	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L268	0	network vulnerability detection and compliance assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L269	0	network vulnerability detection compliance assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L270	0	network with vulnerability with detection with compliance with assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L271	14	network with vulnerability with detection with compliance with assessment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L272	42	726/2,22,25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L273	35	726/2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18

L274	49	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L275	6	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L276	195	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L277	0	(external$5 or third party) with (security) with (commercial near data) with reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L278	0	(external$5 or third party) with (commercial near data) with reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L279	39	internet monitoring with report	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:18
L280	23	internet monitoring with report and public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L281	0	malwareurl	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L282	0	malwareurl$5	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L283	3	www$malwareurl$5	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L284	3	www$malwareurl$com	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L285	257	arbor networks	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L286	4	arbor networks and renesys	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L287	10317	reputation and domain	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19

L288	121	reputation and domain and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L289	234	reputation and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L290	113	L289 not L288	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L291	20	US-7194769-$.DID. OR US-7290275-$.DID. OR US-7971252-$.DID. OR US-20040010709-$.DID. OR US-20050138413-$.DID. OR US-20080047018-$.DID. OR US-20080209565-$.DID. OR US-20090265787-$.DID. OR US-20090293128-$.DID. OR US-2007304-$.DID. OR US-5200596-$.DID. OR US-2009104-$.DID. OR US-422009D-$.DID. OR US-1331018-$.DID.	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:19
L292	0	L289 and L291	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L293	0	(insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L291	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L294	0	(industry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L291	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L295	0	(industry reports or internet monitoring or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L291	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L296	0	L291 and user behavior	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19

L297	0	L291 and behavior	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L298	0	L291 and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L299	0	L291 and public with features	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:19
L300	0	L291 and externally	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:19
L301	7	L291 and external	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:19
L302	36	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L303	2	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L304	33	((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L305	503	((external$5 or third party) with audit$4)and reputation and security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L306	1006	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L307	931	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19

L308	539	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L309	3	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial data sources	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L310	9	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial data	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L311	9	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rating and commercial data	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L312	8	security and renesys	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L313	1	abor networks	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L314	115	(network near3 vulnerability) with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L315	40	(network near3 assessment) with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L316	99	(network near3 assessment) with external$3	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L317	1919	site secure	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L318	688	L317 and third party	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L319	259	L318 and assess$3	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L320	337	network reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19

L321	316	network reputation and (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L322	20	network reputation with (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L323	10	network reputation with (rat$3 or assess$4) and public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:19
L324	3	network reputation with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L325	1042	network (reputation or assess$4 or rat$3) with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L326	766	network (reputation or assess$4 or rat$3) with public and security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L327	19	network (reputation or assess$4 or rat$3) with public with security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L328	33	network (reputation or assess$4 or rat$3) with public with secur$5	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L329	14	L328 not L327	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L330	2	"20040250122"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L331	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L332	7720	(organization or company or entity) same reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L333	1983	(organization or company or entity) same reputation same (score or rating)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L334	20155	726/1,2,22,25.ccls.	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L335	129	L333 and L334	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20

L336	1132	(organization or company) same reputation same (score or rating)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L337	62	L336 and L334	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L338	2	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L339	33	network (reputation or assess$4 or rat$3) with public with secur$5	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L340	36	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L341	25	L340 AND ((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L342	273	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.) and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L343	80755	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L344	777	(network or organization or entity) reputation and (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L345	246	L344 and L343	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20

L346	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L347	0	"11237642"	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:20
L348	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L349	13	726/25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L350	0	apparatus and method for network vulnerability detection and compliance	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L351	0	network vulnerability detection and compliance assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L352	0	network vulnerability detection compliance assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L353	0	network with vulnerability with detection with compliance with assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L354	14	network with vulnerability with detection with compliance with assessment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L355	42	726/2,22,25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L356	35	726/2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L357	49	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L358	6	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20

L359	195	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L360	13	726/25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L361	0	network with vulnerability with detection with compliance with assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L362	20	US-7194769-$.DID. OR US-7290275-$.DID. OR US-7971252-$.DID. OR US-20040010709-$.DID. OR US-20050138413-$.DID. OR US-20080047018-$.DID. OR US-20080209565-$.DID. OR US-20090265787-$.DID. OR US-20090293128-$.DID. OR US-2007304-$.DID. OR US-5200596-$.DID. OR US-2009104-$.DID. OR US-422009D-$.DID. OR US-1331018-$.DID.	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:20
L363	0	(insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L362	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L364	766	network (reputation or assess$4 or rat$3) with public and security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L365	273	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.) and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L366	195	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L367	273	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20

		G06F21/00).CPC.) and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)				
L368	195	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L369	3	L367 and L368	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L370	539	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L371	3	L367 and L369	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:20
L372	14	L367 and L370	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:21
L373	80755	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:21
L374	30	L368 and L373	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:21
L375	189	L370 and L373	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:21
L383	9	(US-20040193918-$ or US-20050080720-$ or US-20040221296-$ or US-20050108415-$ or US-20040250122-$).did. or (US-5867799-$ or US-6016475-$ or US-7100195-$ or US-7748038-$).did.	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:21
L384	0	L383 and resilie$4	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:21

L385	5661	(network or orginazation) near3 resilien$3	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:21
L386	23	((network or orginazation) near3 resilien$3) with report$3	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:21
L387	0	((orginazation) near3 resilien$3)	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:21
L388	89	((orginazation or company) near3 resilien$3)	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:21
L389	1	((orginazation or company) near3 resilien$3) with report$3	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:21
L390	1	((orginazation or company or bank$3) near3 resilien$3) with report$3	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:21
L391	298	((orginazation or company or bank$3) near3 resilien$3)	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:21
L392	1	((orginazation or company or bank$3) near3 resilien$3) with (bounce)	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:21
L393	0	((orginazation or company or bank$3) near3 resilien$3) with (recover$3)	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:21
L394	273	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.) and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:21

L395	0	((orginazation or company or bank$3) near3 resilien$3) and L394	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:21
L396	931	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:21
L397	0	((orginazation or company or bank$3) near3 resilien$3) and L396	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:21
L398	20155	726/1,2,22,25.ccls.	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:21
L399	0	((orginazation or company or bank$3) near3 resilien$3) and L398	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:21
L400	6	((orginazation or company or bank$3) near3 resilien$3) and reputation	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:21
L402	2	"15089375"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:21
L403	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:21
L404	13	726/25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:21
L405	0	apparatus and method for network vulnerability detection and compliance	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:21
L406	0	network vulnerability detection and compliance assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:21
L407	0	network vulnerability detection compliance assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:21
L408	0	network with vulnerability with detection with compliance with assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:21

L409	14	network with vulnerability with detection with compliance with assessment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:21
L410	42	726/2,22,25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:22
L411	35	726/2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:22
L412	49	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:22
L413	6	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:22
L414	195	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:22
L415	0	(external$5 or third party) with (security) with (commercial near data) with reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:22
L416	0	(external$5 or third party) with (commercial near data) with reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:22
L417	39	internet monitoring with report	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:22
L418	23	internet monitoring with report and public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:22
L419	0	malwareurl	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:22
L420	0	malwareurl$5	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:22
L421	3	www$malwareurl$5	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:22

L422	3	www$malwareurl$com	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:22
L423	257	arbor networks	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:22
L424	4	arbor networks and renesys	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:22
L425	10317	reputation and domain	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:22
L426	121	reputation and domain and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:22
L427	234	reputation and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:22
L428	113	L427 not L426	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:22
L429	20	US-7194769-$.DID. OR US-7290275-$.DID. OR US-7971252-$.DID. OR US-20040010709-$.DID. OR US-20050138413-$.DID. OR US-20080047018-$.DID. OR US-20080209565-$.DID. OR US-20090265787-$.DID. OR US-20090293128-$.DID. OR US-2007304-$.DID. OR US-5200596-$.DID. OR US-2009104-$.DID. OR US-422009D-$.DID. OR US-1331018-$.DID.	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:22
L430	0	L427 and L429	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:22
L431	0	(insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L429	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:22

L432	0	(industry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L429	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:22
L433	0	(industry reports or internet monitoring or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L429	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:22
L434	0	L429 and user behavior	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:22
L435	0	L429 and behavior	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:22
L436	0	L429 and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:22
L437	0	L429 and public with features	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:22
L438	0	L429 and externally	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:22
L439	7	L429 and external	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:22
L440	2	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:22
L441	33	((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:22

L442	503	((external$5 or third party) with audit$4)and reputation and security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:22
L443	1006	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:22
L444	931	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L445	539	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L446	3	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial data sources	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L447	9	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial data	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L448	9	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rating and commercial data	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L449	8	security and renesys	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L450	1	abor networks	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L451	115	(network near3 vulnerability) with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L452	40	(network near3 assessment) with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L453	99	(network near3 assessment) with external$3	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L454	1919	site secure	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23

L455	688	L454 and third party	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L456	259	L455 and assess$3	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L457	337	network reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L458	316	network reputation and (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L459	20	network reputation with (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L460	10	network reputation with (rat$3 or assess$4) and public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L461	3	network reputation with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L462	1042	network (reputation or assess$4 or rat$3) with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L463	766	network (reputation or assess$4 or rat$3) with public and security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L464	19	network (reputation or assess$4 or rat$3) with public with security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L465	33	network (reputation or assess$4 or rat$3) with public with secur$5	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L466	14	L465 not L464	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L467	2	"20040250122"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L468	2	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23

L469	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L470	7720	(organization or company or entity) same reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L471	1983	(organization or company or entity) same reputation same (score or rating)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L472	20155	726/1,2,22,25.ccls.	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L473	129	L471 and L472	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L474	1132	(organization or company) same reputation same (score or rating)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L475	62	L474 and L472	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L476	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L477	13	726/25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L478	0	apparatus and method for network vulnerability detection and compliance	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L479	0	network vulnerability detection and compliance assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L480	0	network vulnerability detection compliance assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:23
L481	0	network with vulnerability with detection with compliance with assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24
L482	14	network with vulnerability with detection with compliance with assessment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24

L483	42	726/2,22,25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24
L484	35	726/2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24
L485	49	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24
L486	6	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24
L487	195	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24
L488	0	(external$5 or third party) with (security) with (commercial near data) with reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24
L489	0	(external$5 or third party) with (commercial near data) with reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24
L490	39	internet monitoring with report	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24
L491	23	internet monitoring with report and public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24
L492	0	malwareurl	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24
L493	0	malwareurl$5	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24
L494	3	www$malwareurl$5	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24
L495	3	www$malwareurl$com	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24

L496	257	arbor networks	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24
L497	4	arbor networks and renesys	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24
L498	10317	reputation and domain	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24
L499	121	reputation and domain and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24
L500	234	reputation and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24
L501	113	L500 not L499	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24
L502	20	US-7194769-$.DID. OR US-7290275-$.DID. OR US-7971252-$.DID. OR US-20040010709-$.DID. OR US-20050138413-$.DID. OR US-20080047018-$.DID. OR US-20080209565-$.DID. OR US-20090265787-$.DID. OR US-20090293128-$.DID. OR US-2007304-$.DID. OR US-5200596-$.DID. OR US-2009104-$.DID. OR US-422009D-$.DID. OR US-1331018-$.DID.	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:24
L503	0	L500 and L502	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24
L504	0	(insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L502	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24
L505	0	(industry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L502	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24

L506	0	(industry reports or internet monitoring or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L502	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24
L507	0	L502 and user behavior	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24
L508	0	L502 and behavior	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24
L509	0	L502 and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24
L510	0	L502 and public with features	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:24
L511	0	L502 and externally	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:24
L512	7	L502 and external	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:24
L513	36	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24
L514	2	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24
L515	33	((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24
L516	503	((external$5 or third party) with audit$4)and reputation and security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24

L517	1006	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:24
L518	931	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L519	539	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L520	3	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial data sources	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L521	9	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial data	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L522	9	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rating and commercial data	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L523	8	security and renesys	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L524	1	abor networks	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L525	115	(network near3 vulnerability) with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L526	40	(network near3 assessment) with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L527	99	(network near3 assessment) with external$3	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L528	1919	site secure	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L529	688	L528 and third party	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25

L530	259	L529 and assess$3	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L531	337	network reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L532	316	network reputation and (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L533	20	network reputation with (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L534	10	network reputation with (rat$3 or assess$4) and public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L535	3	network reputation with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L536	1042	network (reputation or assess$4 or rat$3) with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L537	766	network (reputation or assess$4 or rat$3) with public and security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L538	19	network (reputation or assess$4 or rat$3) with public with security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L539	33	network (reputation or assess$4 or rat$3) with public with secur$5	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L540	14	L539 not L538	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L541	2	"20040250122"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L542	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L543	7720	(organization or company or entity) same reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L544	1983	(organization or company or entity) same reputation same (score or rating)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25

L545	20155	726/1,2,22,25.ccls.	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L546	129	L544 and L545	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L547	1132	(organization or company) same reputation same (score or rating)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L548	62	L547 and L545	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L549	2	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L550	33	network (reputation or assess$4 or rat$3) with public with secur$5	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L551	36	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L552	25	L551 AND ((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L553	273	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.) and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L554	80755	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25

L555	777	(network or organization or entity) reputation and (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L556	246	L555 and L554	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L557	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:25
L558	0	"11237642"	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:25
L559	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L560	13	726/25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L561	0	apparatus and method for network vulnerability detection and compliance	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L562	0	network vulnerability detection and compliance assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L563	0	network vulnerability detection compliance assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L564	0	network with vulnerability with detection with compliance with assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L565	14	network with vulnerability with detection with compliance with assessment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L566	42	726/2,22,25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L567	35	726/2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26

L568	49	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L569	6	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L570	195	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L571	13	726/25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L572	0	network with vulnerability with detection with compliance with assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L573	20	US-7194769-$.DID. OR US-7290275-$.DID. OR US-7971252-$.DID. OR US-20040010709-$.DID. OR US-20050138413-$.DID. OR US-20080047018-$.DID. OR US-20080209565-$.DID. OR US-20090265787-$.DID. OR US-20090293128-$.DID. OR US-2007304-$.DID. OR US-5200596-$.DID. OR US-2009104-$.DID. OR US-422009D-$.DID. OR US-1331018-$.DID.	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:26
L574	0	(insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L573	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L575	766	network (reputation or assess$4 or rat$3) with public and security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L576	273	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.) and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26

L577	195	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L578	273	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.) and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L579	195	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L580	3	L578 and L579	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L581	539	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L582	3	L578 and L580	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L583	14	L578 and L581	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L584	80755	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L585	30	L579 and L584	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L586	189	L581 and L584	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L587	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26

L588	13	726/25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L589	0	apparatus and method for network vulnerability detection and compliance	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L590	0	network vulnerability detection and compliance assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L591	0	network vulnerability detection compliance assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L592	0	network with vulnerability with detection with compliance with assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L593	14	network with vulnerability with detection with compliance with assessment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L594	42	726/2,22,25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L595	35	726/2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:26
L596	49	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:27
L597	6	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:27
L598	195	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:27
L599	0	(external$5 or third party) with (security) with (commercial near data) with reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:27
L600	0	(external$5 or third party) with (commercial near data) with reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:27

L601	39	internet monitoring with report	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:27
L602	23	internet monitoring with report and public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:27
L603	0	malwareurl	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:27
L604	0	malwareurl$5	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:27
L605	3	www$malwareurl$5	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:27
L606	3	www$malwareurl$com	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:27
L607	257	arbor networks	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:27
L608	4	arbor networks and renesys	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:27
L609	10317	reputation and domain	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:27
L610	121	reputation and domain and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:27
L611	234	reputation and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:27
L612	113	L611 not L610	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:27
L613	20	US-7194769-$.DID. OR US-7290275-$.DID. OR US-7971252-$.DID. OR US-20040010709-$.DID. OR US-20050138413-$.DID. OR US-20080047018-$.DID. OR US-	US-PGPUB; USPAT; USOCR;	ADJ	ON	2020/05/26 09:27

		20080209565-$.DID. OR US-20090265787-$.DID. OR US-20090293128-$.DID. OR US-2007304-$.DID. OR US-5200596-$.DID. OR US-2009104-$.DID. OR US-422009D-$.DID. OR US-1331018-$.DID.	EPO; DERWENT			
L614	0	L611 and L613	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:27
L615	0	(insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L613	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:27
L616	0	(industry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L613	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:27
L617	0	(industry reports or internet monitoring or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L613	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:27
L618	0	L613 and user behavior	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:27
L619	0	L613 and behavior	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:27
L620	0	L613 and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:27
L621	0	L613 and public with features	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:27
L622	0	L613 and externally	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:27

L623	7	L613 and external	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:27
L624	2	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:27
L625	33	((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:27
L626	503	((external$5 or third party) with audit$4)and reputation and security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:27
L627	1006	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:27
L628	931	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:27
L629	539	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:27
L630	3	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial data sources	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L631	9	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial data	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L632	9	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rating and commercial data	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L633	8	security and renesys	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L634	1	abor networks	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28

L635	115	(network near3 vulnerability) with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L636	40	(network near3 assessment) with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L637	99	(network near3 assessment) with external$3	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L638	1919	site secure	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L639	688	L638 and third party	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L640	259	L639 and assess$3	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L641	337	network reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L642	316	network reputation and (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L643	20	network reputation with (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L644	10	network reputation with (rat$3 or assess$4) and public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L645	3	network reputation with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L646	1042	network (reputation or assess$4 or rat$3) with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L647	766	network (reputation or assess$4 or rat$3) with public and security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L648	19	network (reputation or assess$4 or rat$3) with public with security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L649	33	network (reputation or assess$4 or rat$3) with public with secur$5	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28

L650	14	L649 not L648	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L651	2	"20040250122"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L652	2	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L653	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L654	7720	(organization or company or entity) same reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L655	1983	(organization or company or entity) same reputation same (score or rating)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L656	20155	726/1,2,22,25.ccls.	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L657	129	L655 and L656	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L658	1132	(organization or company) same reputation same (score or rating)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L659	62	L658 and L656	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L660	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L661	13	726/25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L662	0	apparatus and method for network vulnerability detection and compliance	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L663	0	network vulnerability detection and compliance assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28

L664	0	network vulnerability detection compliance assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:28
L665	0	network with vulnerability with detection with compliance with assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:29
L666	14	network with vulnerability with detection with compliance with assessment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:29
L667	42	726/2,22,25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:29
L668	35	726/2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:29
L669	49	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:29
L670	6	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:29
L671	195	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:29
L672	0	(external$5 or third party) with (security) with (commercial near data) with reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:29
L673	0	(external$5 or third party) with (commercial near data) with reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:29
L674	39	internet monitoring with report	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:29
L675	23	internet monitoring with report and public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:29
L676	0	malwareurl	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:29

L677	0	malwareurl$5	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:29
L678	3	www$malwareurl$5	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:29
L679	3	www$malwareurl$com	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:29
L680	257	arbor networks	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:29
L681	4	arbor networks and renesys	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:29
L682	10317	reputation and domain	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:29
L683	121	reputation and domain and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:29
L684	234	reputation and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:29
L685	113	L684 not L683	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:29
L686	20	US-7194769-$.DID. OR US-7290275-$.DID. OR US-7971252-$.DID. OR US-20040010709-$.DID. OR US-20050138413-$.DID. OR US-20080047018-$.DID. OR US-20080209565-$.DID. OR US-20090265787-$.DID. OR US-20090293128-$.DID. OR US-2007304-$.DID. OR US-5200596-$.DID. OR US-2009104-$.DID. OR US-422009D-$.DID. OR US-1331018-$.DID.	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:29
L687	0	L684 and L686	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:29

L688	0	(insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L686	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:29
L689	0	(industry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L686	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:29
L690	0	(industry reports or internet monitoring or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L686	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:29
L691	0	L686 and user behavior	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:29
L692	0	L686 and behavior	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:29
L693	0	L686 and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:29
L694	0	L686 and public with features	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:29
L695	0	L686 and externally	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:29
L696	7	L686 and external	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:29
L697	36	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:29

L698	2	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L699	33	((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L700	503	((external$5 or third party) with audit$4)and reputation and security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L701	1006	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L702	931	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L703	539	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L704	3	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial data sources	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L705	9	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial data	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L706	9	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rating and commercial data	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L707	8	security and renesys	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L708	1	abor networks	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L709	115	(network near3 vulnerability) with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30

L710	40	(network near3 assessment) with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L711	99	(network near3 assessment) with external$3	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L712	1919	site secure	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L713	688	L712 and third party	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L714	259	L713 and assess$3	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L715	337	network reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L716	316	network reputation and (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L717	20	network reputation with (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L718	10	network reputation with (rat$3 or assess$4) and public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L719	3	network reputation with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L720	1042	network (reputation or assess$4 or rat$3) with public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L721	766	network (reputation or assess$4 or rat$3) with public and security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L722	19	network (reputation or assess$4 or rat$3) with public with security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L723	33	network (reputation or assess$4 or rat$3) with public with secur$5	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L724	14	L723 not L722	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30

L725	2	"20040250122"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L726	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L727	7720	(organization or company or entity) same reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L728	1983	(organization or company or entity) same reputation same (score or rating)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L729	20155	726/1,2,22,25.ccls.	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L730	129	L728 and L729	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L731	1132	(organization or company) same reputation same (score or rating)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:30
L732	62	L731 and L729	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31
L733	2	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31
L734	33	network (reputation or assess$4 or rat$3) with public with secur$5	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31
L735	36	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31
L736	25	L735 AND ((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31
L737	273	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31

		H04L9/321 OR G06F21/577 OR G06F21/00).CPC.) and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)				
L738	80755	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31
L739	777	(network or organization or entity) reputation and (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31
L740	246	L739 and L738	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31
L741	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31
L742	0	"11237642"	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:31
L743	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31
L744	13	726/25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31
L745	0	apparatus and method for network vulnerability detection and compliance	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31
L746	0	network vulnerability detection and compliance assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31
L747	0	network vulnerability detection compliance assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31
L748	0	network with vulnerability with detection with compliance with assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31

L749	14	network with vulnerability with detection with compliance with assessment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31
L750	42	726/2,22,25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31
L751	35	726/2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31
L752	49	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31
L753	6	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31
L754	195	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31
L755	13	726/25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31
L756	0	network with vulnerability with detection with compliance with assesment	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31
L757	20	US-7194769-$.DID. OR US-7290275-$.DID. OR US-7971252-$.DID. OR US-20040010709-$.DID. OR US-20050138413-$.DID. OR US-20080047018-$.DID. OR US-20080209565-$.DID. OR US-20090265787-$.DID. OR US-20090293128-$.DID. OR US-2007304-$.DID. OR US-5200596-$.DID. OR US-2009104-$.DID. OR US-422009D-$.DID. OR US-1331018-$.DID.	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2020/05/26 09:31
L758	0	(insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L757	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31

L759	766	network (reputation or assess$4 or rat$3) with public and security	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31
L760	273	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.) and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31
L761	195	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31
L762	273	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.) and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31
L763	195	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31
L764	3	L762 and L763	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31
L765	539	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31
L766	3	L762 and L764	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:31
L767	14	L762 and L765	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:32
L768	80755	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:32

		H04L9/321 OR G06F21/577 OR G06F21/00).CPC.)				
L769	30	L763 and L768	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:32
L770	189	L765 and L768	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:32
L771	9	(US-20040193918-$ or US-20050080720-$ or US-20040221296-$ or US-20050108415-$ or US-20040250122-$).did. or (US-5867799-$ or US-6016475-$ or US-7100195-$ or US-7748038-$).did.	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:32
L772	0	L771 and resilie$4	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:32
L773	5661	(network or orginazation) near3 resilien$3	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:32
L774	23	((network or orginazation) near3 resilien$3) with report$3	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:32
L775	0	((orginazation) near3 resilien$3)	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:32
L776	89	((orginazation or company) near3 resilien$3)	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:32
L777	1	((orginazation or company) near3 resilien$3) with report$3	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:32
L778	1	((orginazation or company or bank$3) near3 resilien$3) with report$3	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:32

L779	298	((orginazation or company or bank$3) near3 resilien$3)	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:32
L780	1	((orginazation or company or bank$3) near3 resilien$3) with (bounce)	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:32
L781	0	((orginazation or company or bank$3) near3 resilien$3) with (recover$3)	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:32
L782	273	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.) and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:32
L783	0	((orginazation or company or bank$3) near3 resilien$3) and L782	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:32
L784	931	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:32
L785	0	((orginazation or company or bank$3) near3 resilien$3) and L784	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:32
L786	20155	726/1,2,22,25.ccls.	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:32
L787	0	((orginazation or company or bank$3) near3 resilien$3) and L786	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:32
L788	6	((orginazation or company or bank$3) near3 resilien$3) and reputation	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:32

L789	289	graph with node with business with relationship	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:32
L790	0	L789 and L760	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:32
L791	80755	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:32
L792	43	L789 and L791	US-PGPUB; USPAT; USOCR	ADJ	ON	2020/05/26 09:32
L808	20	portfolio with business with reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:33
L809	12	(US-20040193918-$ or US-20050080720-$ or US-20040221296-$ or US-20050108415-$ or US-20040250122-$ or US-20080091834-$ or US-20120253890-$ or US-20140019196-$).did. or (US-5867799-$ or US-6016475-$ or US-7100195-$ or US-7748038-$).did.	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:33
L810	3	L808 AND ((705/26.7 OR 705/38 OR 705/7.28 OR 705/7.29 OR 705/7.33 OR 705/7.39).CCLS.)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:33
L812	12	(US-20040193918-$ or US-20050080720-$ or US-20040221296-$ or US-20050108415-$ or US-20040250122-$ or US-20080091834-$ or US-20120253890-$ or US-20140019196-$).did. or (US-5867799-$ or US-6016475-$ or US-7100195-$ or US-7748038-$).did.	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:33
L813	20	portfolio with business with reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:33

L814	3	L813 AND ((705/26.7 OR 705/38 OR 705/7.28 OR 705/7.29 OR 705/7.33 OR 705/7.39).CCLS.)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:33
L815	273	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.) and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:33
L816	195	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:33
L817	10	network reputation with (rat$3 or assess$4) and public	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:33
L818	31	(resilien$3) with (malicious or vulnerability) with (duration or time)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:33
L819	234	reputation and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:33
L820	121	reputation and domain and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:33
L822	784	resilien$3 with duration	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:33
L823	4	resilien$3 with duration with (vulnerability or down)	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:33

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp

L49	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L69	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:14
L149	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L150	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L161	0	"11237642"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L162	1	"11368329"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L182	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:16
L376	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:21
L377	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:21
L378	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:21
L379	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:21
L380	0	"11237642"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:21
L381	1	"11368329"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:21
L382	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:21
L401	1	"Term Removed"	US-PGPUB	ADJ	ON	2020/05/26 09:21
L793	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:32
L794	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:32
L795	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:32
L796	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:32
L797	0	"11237642"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:32
L798	1	"11368329"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:32
L799	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:33

L800	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:33
L801	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:33
L802	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:33
L803	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:33
L804	0	"11237642"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:33
L805	1	"11368329"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:33
L806	5	"13240572"	US-PGPUB; USPAT	ADJ	ON	2020/05/26 09:33
L807	1	"Term Removed"	US-PGPUB	ADJ	ON	2020/05/26 09:33
L811	1	"Term Removed"	US-PGPUB	ADJ	ON	2020/05/26 09:33
L821	1	"Term Removed"	US-PGPUB	ADJ	ON	2020/05/26 09:33

5/26/2020 10:52:21 AM
C:\Users\skanaan\Documents\EAST\Workspaces\13240572.wsp

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1	US-7,062,572	06-13-2006	Hampton	
	A2	US-7,650,570	01-19-2010	Torrens	
	A3	US-7,747,778	06-29-2010	King	
	A4	US-7,827,607	11-02-2010	Sobel et al.	
	A5	US-8,370,933	02-05-2013	Buckler	
	A6	US-8,621,621	12-31-2013	Burns et al.	
	A7	US-8,661,146	02-25-2014	Alex et al.	
	A8	US-8,677,481-B1	03-18-2014	Lee	
	A9	US-8,825,662	09-02-2014	Kingman et al.	
	A10	US-9,053,210	06-09-2015	Elnikety	
	A11	US-9,241,252	01-19-2016	Dua et al.	
	A12	US-9,244,899	01-26-2016	Greenbaum	
	A13	US-9,294,498-B1	03-22-2016	Yampolskiy et al.	
	A14	US-9,372,994-B1	06-21-2016	Yampolskiy et al.	
	A15	US-9,384,206	07-05-2016	Bono et al	
	A16	US-9,401,926	07-26-2016	Dubow et al.	
	A17	US-9,407,658-B1	08-02-2016	Kuskov et al.	
	A18	US-9,424,333	08-23-2016	Bisignani	
	A19	US-9,501,647-B2	11-22-2016	Yampolskiy et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
	B1	WO-2017/142694-A1	08-24-2017	Security Scorecard, Inc		
	B2	WO-2019/023045-A1	01-31-2019	Security Scorecard, Inc		

Examiner Signature	/SIMON P KANAAN/	Date Considered	05/25/2020

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A20	US-9,560,072	01-31-2017	Xu	
	A21	US-9,620,079	04-11-2017	Curtis	
	A22	US-9,641,547-B2	05-02-2017	Yampolskiy et al.	
	A23	US-9,646,110	05-09-2017	Byrne	
	A24	US-9,954,893	04-24-2018	Zhao et al.	
	A25	US-10,044,750-B2	08-07-2018	Livshits et al.	
	A26	US-10,079,854	09-18-2018	Scott et al.	
	A27	US-10,142,364	11-27-2018	Baukes et al	
	A28	US-10,185,924	01-22-2019	McClintock et al.	
	A29	US-10,217,071	02-26-2019	Mo et al.	
	A30	US-10,230,753-B2	03-12-2019	Yampolskiy et al.	
	A31	US-10,230,764	03-12-2019	Ng et al.	
	A32	US-10,235,524	03-19-2019	Ford	
	A33	US-10,257,219-B1	04-09-2019	Geil et al.	
	A34	US-10,305,854	05-28-2019	Alizadeh-Shabdiz et al.	
	A35	US-10,339,321	07-02-2019	Tedeschi	
	A36	US-10,339,484	07-02-2019	Pai et al.	
	A37	US-10,412,083	09-10-2019	Zou et al.	
	A38	US-10,469,515	11-05-2019	Helmsen et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/SIMON P KANAAN/	Date Considered	05/25/2020

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 3 of 16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A39	US-10,491,619	11-26-2019	Yampolskiy et al.	
	A40	US-10,491,620	11-26-2019	Yampolskiy et al.	
	A41	US-10,521,583	12-31-2019	Bagulho Monteiro Pereira	
	A42	US-2002/0133365-A1	09-19-2002	Grey et al	
	A43	US-2002/0164983-A1	11-07-2002	Raviv et al.	
	A44	US-2003/0187967-A1	10-02-2003	Walsh et al.	
	A45	US-2004/0003284-A1	01-01-2004	Campbell et al.	
	A46	US-2004/0098375-A1	05-20-2004	DeCarlo	
	A47	US-2004/0193907-A1	09-30-2004	Patanella	
	A48	US-2005/0066195-A1	03-24-2005	Jones	
	A49	US-2005/0076245-A1	04-07-2005	Graham et al.	
	A50	US-2005/0160002-A1	07-21-2005	Roetter et al.	
	A51	US-2005/0278726-A1	12-15-2005	Cano, Charles E.	
	A52	US-2006/0036335-A1	02-16-2006	Banter	
	A53	US-2006/0107226-A1	05-18-2006	Matthews	
	A54	US-2006/0253581-A1	11-09-2006	Dixon et al	
	A55	US-2007/0067845-A1	03-22-2007	Wiemer et al.	
	A56	US-2007/0198275-A1	08-23-2007	Malden et al.	
	A57	US-2008/0033775-A1	02-07-2008	Dawson et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/SIMON P KANAAN/	Date Considered	05/25/2020

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 4 of 16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A58	US-2008/0091834-A1	04-17-2008	Norton	
	A59	US-2008/0172382-A1	07-17-2008	Prettejohn	
	A60	US-2008/0208995-A1	08-28-2008	TAKAHASHI et al.	
	A61	US-2008/0222287-A1	09-11-2008	Bahl et al.	
	A62	US-2009/0125427-A1	05-14-2009	ATWOOD et al.	
	A63	US-2009/0161629-A1	06-25-2009	Purkayastha et al.	
	A64	US-2009/0216700-A1	08-27-2009	Bouchard et al.	
	A65	US-2009/0299802-A1	12-03-2009	Brennan	
	A66	US-2009/0300768-A1	12-03-2009	Krishnamurthy et al	
	A67	US-2009/0319420-A1	12-24-2009	Sanchez et al	
	A68	US-2009/0328063-A1	12-31-2009	Corvera et al.	
	A69	US-2010/0017880-A1	01-21-2010	Masood	
	A70	US-2010/0042605-A1	02-18-2010	Cheng et al	
	A71	US-2010/0057582-A1	03-04-2010	Arfin	
	A72	US-2010/0186088-A1	07-22-2010	Banerjee et al.	
	A73	US-2010/0205042-A1	08-12-2010	Mun	
	A74	US-2010/0218256-A1	08-26-2010	Thomas et al	
	A75	US-2010/0275263-A1	10-28-2010	Bennett et al.	
	A76	US-2010/0281124-A1	11-04-2010	Westman et al	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/SIMON P KANAAN/	Date Considered	05/25/2020

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 5 of 16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A77	US-2010/0281151-A1	11-04-2010	Ramankutty et al	
	A78	US-2011/0137704-A1	06-09-2011	Mitra	
	A79	US-2011/0145576-A1	06-16-2011	Bettan	
	A80	US-2011/0213742-A1	09-01-2011	LEMMOND et al.	
	A81	US-2011/0231395-A1	09-22-2011	Vadlamani	
	A82	US-2011/0239300-A1	09-29-2011	KLEIN et al.	
	A83	US-2011/0296519-A1	12-01-2011	Ide et al	
	A84	US-2012/0036263-A1	02-09-2012	Madden et al.	
	A85	US-2012/0089745-A1	04-12-2012	Turakhia	
	A86	US-2012/0215892-A1	08-23-2012	Wanser	
	A87	US-2012/0255027-A1	10-04-2012	Kanakapura et al.	
	A88	US-2012/0291129-A1	11-15-2012	SHULMAN et al.	
	A89	US-2013/0014253-A1	01-10-2013	Vivian et al	
	A90	US-2013/0060351-A1	03-07-2013	Imming et al	
	A91	US-2013/0080505-A1	03-28-2013	Nielsen et al	
	A92	US-2013/0086521-A1	04-04-2013	Grossele	
	A93	US-2013/0091574-A1	04-11-2013	Howes et al.	
	A94	US-2013/0124644-A1	05-16-2013	Hunt et al	
	A95	US-2013/0124653-A1	05-16-2013	Vick et al	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/SIMON P KANAAN/	Date Considered	05/25/2020

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 6 of 16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A96	US-20130142050-A1	06-06-2013	Luna	
	A97	US-2013/0173791-A1	07-04-2013	Longo	
	A98	US-2013/0291105-A1	10-31-2013	Zheng	
	A99	US-2013/0298244-A1	11-07-2013	Kumar et al	
	A100	US-2013/0305368-A1	11-14-2013	Ford	
	A101	US-2013/0333038-A1	12-12-2013	Chien	
	A102	US-2013/0347116-A1	12-26-2013	Flores	
	A103	US-2014/0006129-A1	01-02-2014	Heath	
	A104	US-2014/0019196-A1	01-16-2014	Wiggins	
	A105	US-2014/0114843-A1	04-24-2014	KLEIN et al.	
	A106	US-2014/0130158-A1	05-08-2014	WANG et al.	
	A107	US-2014/0146370-A1	05-29-2014	Banner et al.	
	A108	US-2014/0189098-A1	07-03-2014	MaGill et al	
	A109	US-2014/0244317-A1	08-28-2014	Roberts et al	
	A110	US-2014/0283068-A1	09-18-2014	Call et al.	
	A111	US-2014/0288996-A1	09-25-2014	Rence et al	
	A112	US-2014/0304816-A1	10-09-2014	KLEIN et al.	
	A113	US-2014/0337633-A1	11-13-2014	Yang et al.	
	A114	US-2015/0033341-A1	01-29-2015	Schmidtler et al	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/SIMON P KANAAN/	Date Considered	05/25/2020

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 7 of 16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A115	US-2015/0081860-A1	03-19-2015	Kuehnel et al.	
	A116	US-2015/0180883-A1	06-25-2015	Aktas et al.	
	A117	US-2015/0261955-A1	09-17-2015	Huang et al	
	A118	US-2015/0288706-A1	10-08-2015	MARSHALL	
	A119	US-2015/0288709-A1	10-08-2015	Singhal et al.	
	A120	US-2015/0310213-A1	10-29-2015	Ronen et al	
	A121	US-2015/0347756-A1	12-03-2015	Hidayat et al.	
	A122	US-2015/0350229-A1	12-03-2015	Mitchell	
	A123	US-2015/0381649-A1	12-31-2015	Schultz et al.	
	A124	US-2016/0065613-A1	03-03-2016	Cho et al.	
	A125	US-2016/0119373-A1	04-28-2016	Fausto et al.	
	A126	US-2016/0140466-A1	05-19-2016	Sidebottom	
	A127	US-2016/0147992-A1	05-26-2016	ZHAO et al.	
	A128	US-2016/0162602-A1	06-09-2016	Bradish et al.	
	A129	US-2016/0171415-A1	06-16-2016	Yampolskiy et al.	
	A130	US-2016/0173522-A1	06-16-2016	Yampolskiy et al.	
	A131	US-2016/0189301-A1	06-30-2016	Ng et al.	
	A132	US-2016/0205126-A1	07-14-2016	Boyer et al	
	A133	US-2016/0248797-A1	08-25-2016	Yampolskiy et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/SIMON P KANAAN/	Date Considered	05/25/2020

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 8 of 16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A134	US-2016/0253500-A1	09-01-2016	Alme et al.	
	A135	US-2016/0259945-A1	09-08-2016	Yampolskiy et al.	
	A136	US-2016/0337387-A1	11-17-2016	Hu et al.	
	A137	US-2016/0344801-A1	11-24-2016	Akkarawittayapoom	
	A138	US-2017/0048267-A1	02-16-2017	Yampolskiy et al.	
	A139	US-2017/0063901-A1	03-02-2017	Muddu et al.	
	A140	US-2017/0161409-A1	06-08-2017	Martin	
	A141	US-2017/0236078-A1	08-17-2017	Rasumov	
	A142	US-2017/0237764-A1	08-17-2017	Rasumov	
	A143	US-2017/0279843-A1	09-28-2017	Schultz et al.	
	A144	US-2017/0316324-A1	11-02-2017	Barrett et al.	
	A145	US-2017/0324766-A1	11-09-2017	Gonzalez	
	A146	US-2017/0337487-A1	11-23-2017	Nock et al.	
	A147	US-2018/0013716-A1	01-11-2018	Connell et al.	
	A148	US-2018/0103043-A1	04-12-2018	Kupreev et al.	
	A149	US-2018/0124110-A1	05-03-2018	Hunt et al	
	A150	US-2018/0139180-A1	05-17-2018	NAPCHI et al.	
	A151	US-2018/0157468-A1	06-07-2018	Stachura	
	A152	US-2018/0322584-A1	11-08-2018	Crabtree et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/SIMON P KANAAN/	Date Considered	05/25/2020

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 9 of 16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A153	US-2018/0336348-A1	11-22-2018	Ng et al.	
	A154	US-2018/0337938-A1	11-22-2018	Kneib et al.	
	A155	US-2018/0337941-A1	11-22-2018	Kraning et al	
	A156	US-2018/0365519-A1	12-20-2018	Pollard et al.	
	A157	US-2018/0375896-A1	12-27-2018	Wang et al.	
	A158	US-2019/0034845-A1	01-31-2019	MO et al.	
	A159	US-2019/0140925-A1	05-09-2019	Pon et al.	
	A160	US-2019/0147378-A1	05-16-2019	Mo et al.	
	A161	US-2019/0379632-A1	12-12-2019	Dahlberg et al.	
	A162	US-2019/0392252-A1	12-26-2019	FIGHEL et al.	
	A163	US-D525,264	07-18-2006	Chotai	
	A164	US-D525,629	07-25-2006	Chotai	
	A165	US-D604,740	11-24-2009	Matheny	
	A166	US-D630,645	01-11-2011	Tokunaga	
	A167	US-D652,048	01-10-2012	Joseph	
	A168	US-D667,022	09-11-2012	LoBosco	
	A169	US-D682,287	05-14-2013	Cong	
	A170	US-D688,260	08-20-2013	Pearcy	
	A171	US-D691,164	10-08-2013	Lim	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/SIMON P KANAAN/	Date Considered	05/25/2020

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 10 of 16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A172	US-D694,252	11-26-2013	Helm	
	A173	US-D694,253	11-26-2013	Helm	
	A174	US-D700,616	03-04-2014	Chao	
	A175	US-D730,918	06-02-2015	Park	
	A176	US-D740,847	10-13-2015	Yampolskiy et al.	
	A177	US-D740,848	10-13-2015	Bolts	
	A178	US-D741,351	10-20-2015	Kito	
	A179	US-D746,832	01-05-2016	Pearcy	
	A180	US-D754,690	04-26-2016	Park	
	A181	US-D754,696	04-26-2016	Follett	
	A182	US-D756,371	05-17-2016	Bertnick	
	A183	US-D756,372	05-17-2016	Bertnick	
	A184	US-D756,392	05-17-2016	Yun	
	A185	US-D759,084	06-14-2016	Yampolskiy et al.	
	A186	US-D759,689	06-21-2016	Olson	
	A187	US-D760,782	07-05-2016	Kendler	
	A188	US-D771,695	11-15-2016	Yampolskiy et al.	
	A189	US-D772,276	11-22-2016	Yampolskiy et al.	
	A190	US-D773,507	12-06-2016	Sagrillo	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/SIMON P KANAAN/	Date Considered	05/25/2020

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 11 of 16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A191	US-D775,635	01-03-2017	Raji	
	A192	US-D776,136	01-10-2017	Chen	
	A193	US-D776,153	01-10-2017	Yampolskiy et al.	
	A194	US-D777,177	01-24-2017	Chen	
	A195	US-D778,927	02-14-2017	Bertnick	
	A196	US-D778,928	02-14-2017	Bertnick	
	A197	US-D779,512	02-21-2017	Kimura	
	A198	US-D779,514	02-21-2017	Baris	
	A199	US-D779,531	02-21-2017	List	
	A200	US-D780,770	03-07-2017	Sum	
	A201	US-D785,009	04-25-2017	Lim	
	A202	US-D785,010	04-25-2017	Bachman	
	A203	US-D785,016	04-25-2017	Berwick	
	A204	US-D787,530	05-23-2017	Huang	
	A205	US-D788,128	05-30-2017	Wada	
	A206	US-D789,947	06-20-2017	Sun	
	A207	US-D789,957	06-20-2017	Wu	
	A208	US-D791,153	07-04-2017	Rice	
	A209	US-D791,834	07-11-2017	Eze	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/SIMON P KANAAN/	Date Considered	05/25/2020

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 12 of 16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A210	US-D792,427	07-18-2017	Weaver	
	A211	US-D795,891	08-29-2017	Kohan	
	A212	US-D796,523	09-05-2017	Bhandari	
	A213	US-D801,989	11-07-2017	Iketsuki	
	A214	US-D803,237	11-21-2017	Wu	
	A215	US-D804,528	12-05-2017	Martin	
	A216	US-D806,735	01-02-2018	Olsen	
	A217	US-D806,737	01-02-2018	Chung	
	A218	US-D809,523	02-06-2018	Lipka	
	A219	US-D812,633	03-13-2018	Saneii	
	A220	US-D814,483	04-03-2018	Gavaskar	
	A221	US-D815,119	04-10-2018	Chalker	
	A222	US-D815,148	04-10-2018	Martin	
	A223	US-D816,105	04-24-2018	Rudick	
	A224	US-D816,116	04-24-2018	Selassie	
	A225	US-D817,970	05-15-2018	Chang	
	A226	US-D817,977	05-15-2018	Kato	
	A227	US-D819,687	06-05-2018	Yampolskiy et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/SIMON P KANAAN/	Date Considered	05/25/2020

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

PTO/SB/08b (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	13	of	16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	C1	BitSight, "Cyber Security Myths Versus Reality: How Optimism Bias Contributes to Inaccurate Perceptions of Risk", June 2015, Dimensional Research, Pages 1-9.	
	C2	PAIR transaction history of US application no. 13/240,572 as of October 7, 2015, application as filed and pending claims, 45 pages.	
	C3	PAIR transaction history of US application no. 13/240,572 and pending claims as of March 22, 2016, 10 pages.	
	C4	Provos et al., "The Ghost In the Browser Analysis of Web-based Malware", 2007 (9 pages).	
	C5	Li et al., "Finding the Linchpins of the Dark Web: a Study on Topologically Dedicated Hosts on Malicious Web Infrastructures", IEEE, 2013 (15 pages).	
	C6	Bhilare et al., "Protecting Intellectual Property and Sensitive Information in Academic Campuses from Trusted Insiders: Leveraging Active Directory", SIGUCC, October 2009 (5 pages).	
	C7	Jin et al, "Identifying and tracking suspicious activities through IP gray space analysis", MineNet, June 12, 2007 (6 pages).	
	C8	Chuvakin, "SIEM: Moving beyond compliance", RSA White Paper (2010) (16 pages).	
	C9	PAIR transaction history and pending claims for USSN 14/021,585, as of April 29, 2016, 2 pages.	
	C10	PAIR transaction history, application as filed and pending claims for USSN 13/240,572 as of April 29, 2016, 46 pages.	

Examiner Signature	/SIMON P KANAAN/	Date Considered	05/25/2020

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

PTO/SB/08b (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	14	of	16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	C11	PAIR transaction history, application as filed and pending claims for USSN 14/944,484 as of April 29, 2016, 4 pages.	
	C12	PAIR transaction history and pending claims for USSN 14/021,585, as of November 18, 2015, 6 pages.	
	C13	Application as filed, PAIR transaction history and pending claims of USSN 13/240,572 as of November 18, 2015, 45 pages.	
	C14	Hachem, Sara; Toninelli, Alessandra; Pathak, Animesh; Issany, Valerie. Policy-Based Access Control in Mobile Social Ecosystems. 2011 IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY).	
	C15	Srivastava, Divesh; Velegrakis, Yannis. Using Queries to Associate Metadata with Data. IEEE 23rd International Conference on Data Engineering. Pub. Date: 2007. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4221823, 3 pages.	
	C16	Gephi (gephi.org), accessed on the internet at https://web.archive.org/web/20151216223216/https://gephi.org/; 12/16/2015; 1 page.	
	C17	mile 2 CPTE Maltego Demo, accessed on the internet at https://www.youtube.com/watch?v=o2oNKOUzPOU; 7/12/2012; 1 page.	
	C18	"Neo4j (neo4j.com)," accessed on the internet at https://web.archive.org/web/20151220150341 /http://neo4j.com:80/developer/guide-data-visualization/; 12/20/2015; 1 page.	
	C19	"Creating Transparency with Palantir," accessed on the internet at https://www.youtube.com/watch?v=8cbGChfagUA; 7/5/2012; 1 page.	
	C20	"Palantir Cyber: Uncovering malicious behavior at petabyte scale," accessed on the internet at https://www.youtube.com/watch?v= EhYezV06EE; 12/21/2012; 1 page.	

Examiner Signature	/SIMON P KANAAN/	Date Considered	05/25/2020

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

PTO/SB/08b (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	15	of	16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	C21	BORGATTI, et al., "ON SOCIAL NETWORK ANALYSIS IN A SUPPLY CHAIN CONTEXT," Journal of Supply Chain Management; 45(2): 5-22; Apr. 2009, 18 pages.	
	C22	CARSTENS, et al., "Modeling Company Risk and Importance in Supply Graphs," European Semantic Web Conference 2017: The Semantic Web pp18-31.	
	C23	GUNDERT, Levi, "Big Data in Security - Part III: Graph Analytics," accessed on the Internet at https://blogs.cisco.com/security/big-data-in-security-part-iii-graph-analytics; Cisco Blog, December 2013, 8 pages.	
	C24	JEAN, "Cyber Security: How to use graphs to do an attack analysis," accessed on the internet at https://linkurio.us/blog/cyber-security-use-graphs-attack-analysis/; August 2014, 11 pages.	
	C25	"Palantir.com," accessed on the internet at http://www.palantir.com/; December 2015; 2 pages.	
	C26	KC CLAFFY, "Internet measurement and data analysis: topology, workload, performance and routing statistics," accessed on the Internet at http://www.caida.org/publications/papers/1999/Nae/Nae.html., NAE '99 workshop, 1999, 22 pages.	
	C27	"Maltego XL," accessed on the Internet at https://www.paterva.com/web7/buy/maltegoclients/maltego-xl.php, 5 pages.	
	C28	MASSIMO CANDELA, "Real-time BGP Visualisation with BGPlay," accessed on the Internet at https://labs.ripe.net/Members/massimo_candela/real-time-bgp-visualisationwith-bgplay), Sept. 30, 2015, 8 pages.	
	C29	NOEL, et al., "Big-Data Architecture for Cyber Attack Graphs, Representing Security Relationships in NoSQL Graph Databases," The MITRE Corporation, 2014, 6 pages.	
	C30	WAGNER, et al., "Assessing the vulnerability of supply chains using graph theory," Int. J. Production Economics 126 (2010) 121-129.	

Examiner Signature	/SIMON P KANAAN/	Date Considered	05/25/2020

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

PTO/SB/08b (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	16	of	16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	C31	MORADI, et al., "Quantitative Models for Supply Chain Management," IGI Global, 2012, 29 pages.	
	C32	JOSLYN, et al., "Massive Scale Cyber Traffic Analysis: A Driver for Graph Database Research," Proceedings of the First International Workshop on Graph Data Management Experience and Systems (GRADES 2013), 6 pages.	
	C33	"About Neo4j," 1 page.	
	C34	"Amazon Mechanical Turk," accessed on the internet at https://www.mturk.com/; 7 pages	
	C35	"Rapid7 Nexpose Vulnerability Scanner," accessed on the internet at https://www.rapid7.com/products/nexpose/download/, 3 pages.	
	C36	"Tenable Nessus Network Vulnerability Scanner," accessed on the internet at https://www.tenable.com/products/nessus/nessus-professional; 13 pages.	
	C37	"Computer Network Graph," http://www.opte.org; 1 page.	
	C38	MCNAB, "Network Security Assessment," copyright 2004, 56 pages.	
	C39	GILGUR, et al., "Percentile-Based Approach to Forecasting Workload Growth" Proceedings of CMG'15 Performance and Capacity International Conference by the Computer Measurement Group. No. 2015 (Year: 2015)	
	C40	SENEVIRATNE et al., "SSIDs in the Wild: Extracting Semantic Information from WiFi SSIDs" HAL archives-ouvertes.fr, HAL Id: hal-01181254, 07/29/15, 5 pages.	

Examiner Signature	/SIMON P KANAAN/	Date Considered	05/25/2020

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

Sheet 1 of 1

Substitute Disclosure Form / U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No.	Application No.
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))	38879-0006001	13/240,572
	Applicant: Boyer et al.	
	Filing Date: September 22, 2011	Group Art Unit: 2432

U.S. Patent Documents

Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	1.	2015/0074579	3-2015	Gladstone et al			

Foreign Patent Documents or Published Foreign Patent Applications

Examiner Initial	Desig. ID	Document Number	Publication Date	Country or Patent Office	Class	Subclass	Translation Yes	Translation No

Other Documents (include Author, Title, Date, and Place of Publication)

Examiner Initial	Desig. ID	Document
	2.	PAIR transaction history of US application no. 14/021,585 as of October 7, 2015 and application as filed.
	3.	PAIR transaction history of US application no. 61/386,156 as of October 7, 2015.

Examiner Signature	Date Considered
/SIMON P KANAAN/	05/26/2020

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A1	US-7,062,572	06-13-2006	Hampton	
	A2	US-7,650,570	01-19-2010	Torrens	
	A3	US-7,747,778	06-29-2010	King	
	A4	US-7,827,607	11-02-2010	Sobel et al.	
	A5	US-8,370,933	02-05-2013	Buckler	
	A6	US-8,621,621	12-31-2013	Burns et al.	
	A7	US-8,661,146	02-25-2014	Alex et al.	
	A8	US-8,677,481-B1	03-18-2014	Lee	
	A9	US-8,825,662	09-02-2014	Kingman et al.	
	A10	US-9,053,210	06-09-2015	Elnikety	
	A11	US-9,241,252	01-19-2016	Dua et al.	
	A12	US-9,244,899	01-26-2016	Greenbaum	
	A13	US-9,294,498-B1	03-22-2016	Yampolskiy et al.	
	A14	US-9,372,994-B1	06-21-2016	Yampolskiy et al.	
	A15	US-9,384,206	07-05-2016	Bono et al	
	A16	US-9,401,926	07-26-2016	Dubow et al.	
	A17	US-9,407,658-B1	08-02-2016	Kuskov et al.	
	A18	US-9,424,333	08-23-2016	Bisignani	
	A19	US-9,501,647-B2	11-22-2016	Yampolskiy et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
	B1	WO-2017/142694-A1	08-24-2017	Security Scorecard, Inc		
	B2	WO-2019/023045-A1	01-31-2019	Security Scorecard, Inc		

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A20	US-9,560,072	01-31-2017	Xu	
	A21	US-9,620,079	04-11-2017	Curtis	
	A22	US-9,641,547-B2	05-02-2017	Yampolskiy et al.	
	A23	US-9,646,110	05-09-2017	Byrne	
	A24	US-9,954,893	04-24-2018	Zhao et al.	
	A25	US-10,044,750-B2	08-07-2018	Livshits et al.	
	A26	US-10,079,854	09-18-2018	Scott et al.	
	A27	US-10,142,364	11-27-2018	Baukes et al	
	A28	US-10,185,924	01-22-2019	McClintock et al.	
	A29	US-10,217,071	02-26-2019	Mo et al.	
	A30	US-10,230,753-B2	03-12-2019	Yampolskiy et al.	
	A31	US-10,230,764	03-12-2019	Ng et al.	
	A32	US-10,235,524	03-19-2019	Ford	
	A33	US-10,257,219-B1	04-09-2019	Geil et al.	
	A34	US-10,305,854	05-28-2019	Alizadeh-Shabdiz et al.	
	A35	US-10,339,321	07-02-2019	Tedeschi	
	A36	US-10,339,484	07-02-2019	Pai et al.	
	A37	US-10,412,083	09-10-2019	Zou et al.	
	A38	US-10,469,515	11-05-2019	Helmsen et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 3 of 16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A39	US-10,491,619	11-26-2019	Yampolskiy et al.	
	A40	US-10,491,620	11-26-2019	Yampolskiy et al.	
	A41	US-10,521,583	12-31-2019	Bagulho Monteiro Pereira	
	A42	US-2002/0133365-A1	09-19-2002	Grey et al	
	A43	US-2002/0164983-A1	11-07-2002	Raviv et al.	
	A44	US-2003/0187967-A1	10-02-2003	Walsh et al.	
	A45	US-2004/0003284-A1	01-01-2004	Campbell et al.	
	A46	US-2004/0098375-A1	05-20-2004	DeCarlo	
	A47	US-2004/0193907-A1	09-30-2004	Patanella	
	A48	US-2005/0066195-A1	03-24-2005	Jones	
	A49	US-2005/0076245-A1	04-07-2005	Graham et al.	
	A50	US-2005/0160002-A1	07-21-2005	Roetter et al.	
	A51	US-2005/0278726-A1	12-15-2005	Cano, Charles E.	
	A52	US-2006/0036335-A1	02-16-2006	Banter	
	A53	US-2006/0107226-A1	05-18-2006	Matthews	
	A54	US-2006/0253581-A1	11-09-2006	Dixon et al	
	A55	US-2007/0067845-A1	03-22-2007	Wiemer et al.	
	A56	US-2007/0198275-A1	08-23-2007	Malden et al.	
	A57	US-2008/0033775-A1	02-07-2008	Dawson et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 4 of 16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A58	US-2008/0091834-A1	04-17-2008	Norton	
	A59	US-2008/0172382-A1	07-17-2008	Prettejohn	
	A60	US-2008/0208995-A1	08-28-2008	TAKAHASHI et al.	
	A61	US-2008/0222287-A1	09-11-2008	Bahl et al.	
	A62	US-2009/0125427-A1	05-14-2009	ATWOOD et al.	
	A63	US-2009/0161629-A1	06-25-2009	Purkayastha et al.	
	A64	US-2009/0216700-A1	08-27-2009	Bouchard et al.	
	A65	US-2009/0299802-A1	12-03-2009	Brennan	
	A66	US-2009/0300768-A1	12-03-2009	Krishnamurthy et al	
	A67	US-2009/0319420-A1	12-24-2009	Sanchez et al	
	A68	US-2009/0328063-A1	12-31-2009	Corvera et al.	
	A69	US-2010/0017880-A1	01-21-2010	Masood	
	A70	US-2010/0042605-A1	02-18-2010	Cheng et al	
	A71	US-2010/0057582-A1	03-04-2010	Arfin	
	A72	US-2010/0186088-A1	07-22-2010	Banerjee et al.	
	A73	US-2010/0205042-A1	08-12-2010	Mun	
	A74	US-2010/0218256-A1	08-26-2010	Thomas et al	
	A75	US-2010/0275263-A1	10-28-2010	Bennett et al.	
	A76	US-2010/0281124-A1	11-04-2010	Westman et al	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 5 of 16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A77	US-2010/0281151-A1	11-04-2010	Ramankutty et al	
	A78	US-2011/0137704-A1	06-09-2011	Mitra	
	A79	US-2011/0145576-A1	06-16-2011	Bettan	
	A80	US-2011/0213742-A1	09-01-2011	LEMMOND et al.	
	A81	US-2011/0231395-A1	09-22-2011	Vadlamani	
	A82	US-2011/0239300-A1	09-29-2011	KLEIN et al.	
	A83	US-2011/0296519-A1	12-01-2011	Ide et al	
	A84	US-2012/0036263-A1	02-09-2012	Madden et al.	
	A85	US-2012/0089745-A1	04-12-2012	Turakhia	
	A86	US-2012/0215892-A1	08-23-2012	Wanser	
	A87	US-2012/0255027-A1	10-04-2012	Kanakapura et al.	
	A88	US-2012/0291129-A1	11-15-2012	SHULMAN et al.	
	A89	US-2013/0014253-A1	01-10-2013	Vivian et al	
	A90	US-2013/0060351-A1	03-07-2013	Imming et al	
	A91	US-2013/0080505-A1	03-28-2013	Nielsen et al	
	A92	US-2013/0086521-A1	04-04-2013	Grossele	
	A93	US-2013/0091574-A1	04-11-2013	Howes et al.	
	A94	US-2013/0124644-A1	05-16-2013	Hunt et al	
	A95	US-2013/0124653-A1	05-16-2013	Vick et al	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 6 of 16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A96	US-20130142050-A1	06-06-2013	Luna	
	A97	US-2013/0173791-A1	07-04-2013	Longo	
	A98	US-2013/0291105-A1	10-31-2013	Zheng	
	A99	US-2013/0298244-A1	11-07-2013	Kumar et al	
	A100	US-2013/0305368-A1	11-14-2013	Ford	
	A101	US-2013/0333038-A1	12-12-2013	Chien	
	A102	US-2013/0347116-A1	12-26-2013	Flores	
	A103	US-2014/0006129-A1	01-02-2014	Heath	
	A104	US-2014/0019196-A1	01-16-2014	Wiggins	
	A105	US-2014/0114843-A1	04-24-2014	KLEIN et al.	
	A106	US-2014/0130158-A1	05-08-2014	WANG et al.	
	A107	US-2014/0146370-A1	05-29-2014	Banner et al.	
	A108	US-2014/0189098-A1	07-03-2014	MaGill et al	
	A109	US-2014/0244317-A1	08-28-2014	Roberts et al	
	A110	US-2014/0283068-A1	09-18-2014	Call et al.	
	A111	US-2014/0288996-A1	09-25-2014	Rence et al	
	A112	US-2014/0304816-A1	10-09-2014	KLEIN et al.	
	A113	US-2014/0337633-A1	11-13-2014	Yang et al.	
	A114	US-2015/0033341-A1	01-29-2015	Schmidtler et al	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 7 of 16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A115	US-2015/0081860-A1	03-19-2015	Kuehnel et al.	
	A116	US-2015/0180883-A1	06-25-2015	Aktas et al.	
	A117	US-2015/0261955-A1	09-17-2015	Huang et al	
	A118	US-2015/0288706-A1	10-08-2015	MARSHALL	
	A119	US-2015/0288709-A1	10-08-2015	Singhal et al.	
	A120	US-2015/0310213-A1	10-29-2015	Ronen et al	
	A121	US-2015/0347756-A1	12-03-2015	Hidayat et al.	
	A122	US-2015/0350229-A1	12-03-2015	Mitchell	
	A123	US-2015/0381649-A1	12-31-2015	Schultz et al.	
	A124	US-2016/0065613-A1	03-03-2016	Cho et al.	
	A125	US-2016/0119373-A1	04-28-2016	Fausto et al.	
	A126	US-2016/0140466-A1	05-19-2016	Sidebottom	
	A127	US-2016/0147992-A1	05-26-2016	ZHAO et al.	
	A128	US-2016/0162602-A1	06-09-2016	Bradish et al.	
	A129	US-2016/0171415-A1	06-16-2016	Yampolskiy et al.	
	A130	US-2016/0173522-A1	06-16-2016	Yampolskiy et al.	
	A131	US-2016/0189301-A1	06-30-2016	Ng et al.	
	A132	US-2016/0205126-A1	07-14-2016	Boyer et al	
	A133	US-2016/0248797-A1	08-25-2016	Yampolskiy et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 8 of 16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A134	US-2016/0253500-A1	09-01-2016	Alme et al.	
	A135	US-2016/0259945-A1	09-08-2016	Yampolskiy et al.	
	A136	US-2016/0337387-A1	11-17-2016	Hu et al.	
	A137	US-2016/0344801-A1	11-24-2016	Akkarawittayapoom	
	A138	US-2017/0048267-A1	02-16-2017	Yampolskiy et al.	
	A139	US-2017/0063901-A1	03-02-2017	Muddu et al.	
	A140	US-2017/0161409-A1	06-08-2017	Martin	
	A141	US-2017/0236078-A1	08-17-2017	Rasumov	
	A142	US-2017/0237764-A1	08-17-2017	Rasumov	
	A143	US-2017/0279843-A1	09-28-2017	Schultz et al.	
	A144	US-2017/0316324-A1	11-02-2017	Barrett et al.	
	A145	US-2017/0324766-A1	11-09-2017	Gonzalez	
	A146	US-2017/0337487-A1	11-23-2017	Nock et al.	
	A147	US-2018/0013716-A1	01-11-2018	Connell et al.	
	A148	US-2018/0103043-A1	04-12-2018	Kupreev et al.	
	A149	US-2018/0124110-A1	05-03-2018	Hunt et al	
	A150	US-2018/0139180-A1	05-17-2018	NAPCHI et al.	
	A151	US-2018/0157468-A1	06-07-2018	Stachura	
	A152	US-2018/0322584-A1	11-08-2018	Crabtree et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 9 of 16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A153	US-2018/0336348-A1	11-22-2018	Ng et al.	
	A154	US-2018/0337938-A1	11-22-2018	Kneib et al.	
	A155	US-2018/0337941-A1	11-22-2018	Kraning et al	
	A156	US-2018/0365519-A1	12-20-2018	Pollard et al.	
	A157	US-2018/0375896-A1	12-27-2018	Wang et al.	
	A158	US-2019/0034845-A1	01-31-2019	MO et al.	
	A159	US-2019/0140925-A1	05-09-2019	Pon et al.	
	A160	US-2019/0147378-A1	05-16-2019	Mo et al.	
	A161	US-2019/0379632-A1	12-12-2019	Dahlberg et al.	
	A162	US-2019/0392252-A1	12-26-2019	FIGHEL et al.	
	A163	US-D525,264	07-18-2006	Chotai	
	A164	US-D525,629	07-25-2006	Chotai	
	A165	US-D604,740	11-24-2009	Matheny	
	A166	US-D630,645	01-11-2011	Tokunaga	
	A167	US-D652,048	01-10-2012	Joseph	
	A168	US-D667,022	09-11-2012	LoBosco	
	A169	US-D682,287	05-14-2013	Cong	
	A170	US-D688,260	08-20-2013	Pearcy	
	A171	US-D691,164	10-08-2013	Lim	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 10 of 16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A172	US-D694,252	11-26-2013	Helm	
	A173	US-D694,253	11-26-2013	Helm	
	A174	US-D700,616	03-04-2014	Chao	
	A175	US-D730,918	06-02-2015	Park	
	A176	US-D740,847	10-13-2015	Yampolskiy et al.	
	A177	US-D740,848	10-13-2015	Bolts	
	A178	US-D741,351	10-20-2015	Kito	
	A179	US-D746,832	01-05-2016	Pearcy	
	A180	US-D754,690	04-26-2016	Park	
	A181	US-D754,696	04-26-2016	Follett	
	A182	US-D756,371	05-17-2016	Bertnick	
	A183	US-D756,372	05-17-2016	Bertnick	
	A184	US-D756,392	05-17-2016	Yun	
	A185	US-D759,084	06-14-2016	Yampolskiy et al.	
	A186	US-D759,689	06-21-2016	Olson	
	A187	US-D760,782	07-05-2016	Kendler	
	A188	US-D771,695	11-15-2016	Yampolskiy et al.	
	A189	US-D772,276	11-22-2016	Yampolskiy et al.	
	A190	US-D773,507	12-06-2016	Sagrillo	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 11 of 16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A191	US-D775,635	01-03-2017	Raji	
	A192	US-D776,136	01-10-2017	Chen	
	A193	US-D776,153	01-10-2017	Yampolskiy et al.	
	A194	US-D777,177	01-24-2017	Chen	
	A195	US-D778,927	02-14-2017	Bertnick	
	A196	US-D778,928	02-14-2017	Bertnick	
	A197	US-D779,512	02-21-2017	Kimura	
	A198	US-D779,514	02-21-2017	Baris	
	A199	US-D779,531	02-21-2017	List	
	A200	US-D780,770	03-07-2017	Sum	
	A201	US-D785,009	04-25-2017	Lim	
	A202	US-D785,010	04-25-2017	Bachman	
	A203	US-D785,016	04-25-2017	Berwick	
	A204	US-D787,530	05-23-2017	Huang	
	A205	US-D788,128	05-30-2017	Wada	
	A206	US-D789,947	06-20-2017	Sun	
	A207	US-D789,957	06-20-2017	Wu	
	A208	US-D791,153	07-04-2017	Rice	
	A209	US-D791,834	07-11-2017	Eze	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08a (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 12 of 16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A210	US-D792,427	07-18-2017	Weaver	
	A211	US-D795,891	08-29-2017	Kohan	
	A212	US-D796,523	09-05-2017	Bhandari	
	A213	US-D801,989	11-07-2017	Iketsuki	
	A214	US-D803,237	11-21-2017	Wu	
	A215	US-D804,528	12-05-2017	Martin	
	A216	US-D806,735	01-02-2018	Olsen	
	A217	US-D806,737	01-02-2018	Chung	
	A218	US-D809,523	02-06-2018	Lipka	
	A219	US-D812,633	03-13-2018	Saneii	
	A220	US-D814,483	04-03-2018	Gavaskar	
	A221	US-D815,119	04-10-2018	Chalker	
	A222	US-D815,148	04-10-2018	Martin	
	A223	US-D816,105	04-24-2018	Rudick	
	A224	US-D816,116	04-24-2018	Selassie	
	A225	US-D817,970	05-15-2018	Chang	
	A226	US-D817,977	05-15-2018	Kato	
	A227	US-D819,687	06-05-2018	Yampolskiy et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08b (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	13	of	16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	C1	BitSight, "Cyber Security Myths Versus Reality: How Optimism Bias Contributes to Inaccurate Perceptions of Risk", June 2015, Dimensional Research, Pages 1-9.	
	C2	PAIR transaction history of US application no. 13/240,572 as of October 7, 2015, application as filed and pending claims, 45 pages.	
	C3	PAIR transaction history of US application no. 13/240,572 and pending claims as of March 22, 2016, 10 pages.	
	C4	Provos et al., "The Ghost In the Browser Analysis of Web-based Malware", 2007 (9 pages).	
	C5	Li et al., "Finding the Linchpins of the Dark Web: a Study on Topologically Dedicated Hosts on Malicious Web Infrastructures", IEEE, 2013 (15 pages).	
	C6	Bhilare et al., "Protecting Intellectual Property and Sensitive Information in Academic Campuses from Trusted Insiders: Leveraging Active Directory", SIGUCC, October 2009 (5 pages).	
	C7	Jin et al, "Identifying and tracking suspicious activities through IP gray space analysis", MineNet, June 12, 2007 (6 pages).	
	C8	Chuvakin, "SIEM: Moving beyond compliance", RSA White Paper (2010) (16 pages).	
	C9	PAIR transaction history and pending claims for USSN 14/021,585, as of April 29, 2016, 2 pages.	
	C10	PAIR transaction history, application as filed and pending claims for USSN 13/240,572 as of April 29, 2016, 46 pages.	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08b (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	14	of	16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	C11	PAIR transaction history, application as filed and pending claims for USSN 14/944,484 as of April 29, 2016, 4 pages.	
	C12	PAIR transaction history and pending claims for USSN 14/021,585, as of November 18, 2015, 6 pages.	
	C13	Application as filed, PAIR transaction history and pending claims of USSN 13/240,572 as of November 18, 2015, 45 pages.	
	C14	Hachem, Sara; Toninelli, Alessandra; Pathak, Animesh; Issany, Valerie. Policy-Based Access Control in Mobile Social Ecosystems. 2011 IEEE International Symposium on Policies for Distributed Systems and Networks (POLICY).	
	C15	Srivastava, Divesh; Velegrakis, Yannis. Using Queries to Associate Metadata with Data. IEEE 23rd International Conference on Data Engineering. Pub. Date: 2007. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4221823, 3 pages.	
	C16	Gephi (gephi.org), accessed on the internet at https://web.archive.org/web/20151216223216/https://gephi.org/; 12/16/2015; 1 page.	
	C17	mile 2 CPTE Maltego Demo, accessed on the internet at https://www.youtube.com/watch?v=o2oNKOUzPOU; 7/12/2012; 1 page.	
	C18	"Neo4j (neo4j.com)," accessed on the internet at https://web.archive.org/web/20151220150341 /http://neo4j.com:80/developer/guide-data-visualization/; 12/20/2015; 1 page.	
	C19	"Creating Transparency with Palantir," accessed on the internet at https://www.youtube.com/watch?v=8cbGChfagUA; 7/5/2012; 1 page.	
	C20	"Palantir Cyber: Uncovering malicious behavior at petabyte scale," accessed on the internet at https://www.youtube.com/watch?v= EhYezV06EE; 12/21/2012; 1 page.	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08b (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	15	of	16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	C21	BORGATTI, et al., "ON SOCIAL NETWORK ANALYSIS IN A SUPPLY CHAIN CONTEXT," Journal of Supply Chain Management; 45(2): 5-22; Apr. 2009, 18 pages.	
	C22	CARSTENS, et al., "Modeling Company Risk and Importance in Supply Graphs," European Semantic Web Conference 2017: The Semantic Web pp18-31.	
	C23	GUNDERT, Levi, "Big Data in Security - Part III: Graph Analytics," accessed on the Internet at https://blogs.cisco.com/security/big-data-in-security-part-iii-graph-analytics; Cisco Blog, December 2013, 8 pages.	
	C24	JEAN, "Cyber Security: How to use graphs to do an attack analysis," accessed on the internet at https://linkurio.us/blog/cyber-security-use-graphs-attack-analysis/; August 2014, 11 pages.	
	C25	"Palantir.com," accessed on the internet at http://www.palantir.com/; December 2015; 2 pages.	
	C26	KC CLAFFY, "Internet measurement and data analysis: topology, workload, performance and routing statistics," accessed on the Internet at http://www.caida.org/publications/papers/1999/Nae/Nae.html., NAE '99 workshop, 1999, 22 pages.	
	C27	"Maltego XL," accessed on the Internet at https://www.paterva.com/web7/buy/maltegoclients/maltego-xl.php, 5 pages.	
	C28	MASSIMO CANDELA, "Real-time BGP Visualisation with BGPlay," accessed on the Internet at https://labs.ripe.net/Members/massimo_candela/real-time-bgp-visualisationwith-bgplay), Sept. 30, 2015, 8 pages.	
	C29	NOEL, et al., "Big-Data Architecture for Cyber Attack Graphs, Representing Security Relationships in NoSQL Graph Databases," The MITRE Corporation, 2014, 6 pages.	
	C30	WAGNER, et al., "Assessing the vulnerability of supply chains using graph theory," Int. J. Production Economics 126 (2010) 121-129.	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08b (07-09)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	16	of	16

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Wayne Boyer
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	C31	MORADI, et al., "Quantitative Models for Supply Chain Management," IGI Global, 2012, 29 pages.	
	C32	JOSLYN, et al., "Massive Scale Cyber Traffic Analysis: A Driver for Graph Database Research," Proceedings of the First International Workshop on Graph Data Management Experience and Systems (GRADES 2013), 6 pages.	
	C33	"About Neo4j," 1 page.	
	C34	"Amazon Mechanical Turk," accessed on the internet at https://www.mturk.com/; 7 pages	
	C35	"Rapid7 Nexpose Vulnerability Scanner," accessed on the internet at https://www.rapid7.com/products/nexpose/download/, 3 pages.	
	C36	"Tenable Nessus Network Vulnerability Scanner," accessed on the internet at https://www.tenable.com/products/nessus/nessus-professional; 13 pages.	
	C37	"Computer Network Graph," http://www.opte.org; 1 page.	
	C38	MCNAB, "Network Security Assessment," copyright 2004, 56 pages.	
	C39	GILGUR, et al., "Percentile-Based Approach to Forecasting Workload Growth" Proceedings of CMG'15 Performance and Capacity International Conference by the Computer Measurement Group. No. 2015 (Year: 2015)	
	C40	SENEVIRATNE et al., "SSIDs in the Wild: Extracting Semantic Information from WiFi SSIDs" HAL archives-ouvertes.fr, HAL Id: hal-01181254, 07/29/15, 5 pages.	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

Electronic Patent Application Fee Transmittal

Application Number:	13240572
Filing Date:	22-Sep-2011
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Filer:	Gozde Guckaya/Christina Andrews
Attorney Docket Number:	BST-004

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
RCE- 2ND AND SUBSEQUENT REQUEST	2820	1	950	950
		Total in USD ($)		**950**

Electronic Acknowledgement Receipt

EFS ID:	39455718
Application Number:	13240572
International Application Number:	
Confirmation Number:	2423
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Customer Number:	51414
Filer:	Gozde Guckaya/Christina Andrews
Filer Authorized By:	Gozde Guckaya
Attorney Docket Number:	BST-004
Receipt Date:	15-MAY-2020
Filing Date:	22-SEP-2011
Time Stamp:	16:52:41
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$950
RAM confirmation Number	E20205EG53282149
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Foreign Reference	BST-003C2_-_WO2017142694A1.pdf	2792815 69e1e08e309bdfffc4109fcc17a71b53756706ef	no	51
Warnings:					
Information:					
2	Foreign Reference	BST-003C2_-_WO2019023045A1.pdf	2091574 54b6bb702a4bbd7793eb5231a792f37f175c7c18	no	42
Warnings:					
Information:					
3	Non Patent Literature	BST-003C1_-_BitSightReport.pdf	1153826 87eb38601b36a098a9dda8661f652ab780ef18f5	no	9
Warnings:					
Information:					
4	Non Patent Literature	BST-003C1_-_Transaction_Histroy_13240572_and_application_as_of_107.pdf	5084989 5a83309cd74aceb82418c2ea67735db6acf0d2bd	no	45
Warnings:					
Information:					
5	Non Patent Literature	BST-003C1_-_Transaction_Histroy_13240572_and_pending_claims_as_of_322.pdf	1085431 5e117ba3c3a7ed26323a90b1004c7079249377d5	no	10
Warnings:					
Information:					
6	Non Patent Literature	BST-010_-_Provos_et_al.pdf	1974099 ec32872acc04acc8446ece6e253c2dc145f4390b	no	9
Warnings:					
Information:					

7	Non Patent Literature	BST-010_-_Li_et_al.pdf	3555385 a11ec687f1bb81c92a43493a5bc2e3a9fd2e2bb1	no	15
Warnings:					
Information:					
8	Non Patent Literature	BST-010_-_Bhilare_et_al.pdf	1105877 da0cfd9e6b1f8cff5dc1ee4b62eed7a9f5bdc34d	no	5
Warnings:					
Information:					
9	Non Patent Literature	BST-010_-_Jin_et_al.pdf	1472270 58237288f5e7ddace5467347eac914a33a281c2c	no	6
Warnings:					
Information:					
10	Non Patent Literature	BST-010_-_SIEM.pdf	2321009 0b65e3728b1f845fe8112fd0fcb5e80d2bebc771	no	16
Warnings:					
Information:					
11	Non Patent Literature	BST-003C1_-_Tranaction_History_14021585_as_of_429.pdf	244211 6f20d6b48fc967ae7269b57433e1e849959679d3	no	2
Warnings:					
Information:					
12	Non Patent Literature	BST-003C1_-_Transaction_History_13240572_application_as_filed_and_pending_claims_as_of_42.pdf	5072860 a4e69ae7e1b061fe0f49374c97f053b5b65eeb0f	no	46
Warnings:					
Information:					
13	Non Patent Literature	BST-003C1_-_Transaction_Histroy_14944484_and_pending_claims_as_of_429.pdf	374445 4a87910b16deac9b34b093f2c597f73179a846a9	no	4
Warnings:					
Information:					

14	Non Patent Literature	BST-003C1_-_Transaction_History_14021585_as_of_1118.pdf	607033 753d6f7e1a119897baf2a8af00d507b53d7350db	no	6
Warnings:					
Information:					
15	Non Patent Literature	BST-003C1_-_Transaction_History_13240572_application_as_filed_dated_1118.pdf	5124924 8cb24d55d4d04c822defae54c6319a0414f12fec	no	45
Warnings:					
Information:					
16	Non Patent Literature	BST-003C1_-_Srivastava_et_al.pdf	619173 ed0402cbd6e1b2a81c48b92d69cc272b4b3de354	no	3
Warnings:					
Information:					
17	Non Patent Literature	BST-015_-_Gephi.PDF	187381 42fffc20178cba2de15adc1e32759ee4e9193afa	no	1
Warnings:					
Information:					
18	Non Patent Literature	BST-015_-_Mile_2_Capture.pdf	467242 9f4aac9884f5bbdc800cc97fa0182047b8ceabbf	no	1
Warnings:					
Information:					
19	Non Patent Literature	Neo4j.PDF	283525 c7fe799e0eb726c1037fc2d910f275ffced6d5ed	no	1
Warnings:					
Information:					
20	Non Patent Literature	Palantir_Youtube_7_5_12.PDF	197543 ee7ad6fceffbc331975947c6564558551dacb0bf	no	1
Warnings:					
Information:					

21	Non Patent Literature	BST-015_-_Palantir_Youtube_7_5_12.PDF	197543 ee7ad6fceffbc331975947c6564558551dacb0bf	no	1
Warnings:					
Information:					
22	Non Patent Literature	Borgatti.PDF	322871 13dc58d300bdc68a0c35b8c4a317ea9a4876620e	no	18
Warnings:					
Information:					
23	Non Patent Literature	Carstens.PDF	895352 4fbff709833bebf56db2c4236ac8e552224c8fba	no	16
Warnings:					
Information:					
24	Non Patent Literature	BST-015_-_BST-010_-_Gundert.pdf	1576316 45cb6d0cbe375b163e89f8e9f2809460a962ce41	no	8
Warnings:					
Information:					
25	Non Patent Literature	cyber-security-use-graphs-attack-analy.PDF	393980 c58a8c41e7f9a874c0180e938c4f5149ec3c75fd	no	11
Warnings:					
Information:					
26	Non Patent Literature	BST-003C1_-_BST_Palantir.pdf	165037 e0aae46e611d666d313e91ed6b47539999bc262e	no	2
Warnings:					
Information:					
27	Non Patent Literature	CLAFFY.PDF	914258 47080ac773302dc024403736e9470cdf3c4d287c	no	22
Warnings:					
Information:					

28	Non Patent Literature	BST-015_-_Maltego_XL.PDF	714210 dc8897f8b95e17321ad99cec09d95022ea2e9c58	no	5
Warnings:					
Information:					
29	Non Patent Literature	BST-015_-_RIPE_real-time-bgp-vis.PDF	1109261 dcf790c7769d27cc9fbc17f2ed66df90f8dc8e6c	no	8
Warnings:					
Information:					
30	Non Patent Literature	Noel.PDF	1315246 da6d5d779ff26461f05f0621deff3ca9dd670b28	no	6
Warnings:					
Information:					
31	Non Patent Literature	Wagner_Assessing.PDF	184175 aee834ec96767de7fc53be800ef19dd8698bbc7f	no	9
Warnings:					
Information:					
32	Non Patent Literature	BST-013_-_MORADI.PDF	2400916 65a061bf58b9a0c9cacb9d9560c78865b6991e67	no	29
Warnings:					
Information:					
33	Non Patent Literature	Joslyn.PDF	769429 658e9af13bf9e102a95115e0bcd7310f6dc1f495	no	6
Warnings:					
Information:					
34	Non Patent Literature	AboutNeo4j.PDF	75053 9d28d0d53b4e9949860a01dd03572da1efc66105	no	1
Warnings:					
Information:					

35	Non Patent Literature	BST-003C1_-_Amazon_Mechanical.pdf	571776 6f53ff125eccabda6bf8e8be391baddf07d5a953	no	7
Warnings:					
Information:					
36	Non Patent Literature	BST-015_-_BST-003C1_-_Rapid7.pdf	447017 5618f37585737b6683f22c4f3f9c5b71b1dc34ca	no	3
Warnings:					
Information:					
37	Non Patent Literature	BST-015_-_BST-003C1_-_Tenable_Nessus.pdf	1003962 cde3c937f748c15225be9d787a43b8d16be56912	no	13
Warnings:					
Information:					
38	Non Patent Literature	BST-003C1_-_Computer_Network_Graph.pdf	222465 aa9628530a0c777eabb6bdb509c849f45d6db598	no	1
Warnings:					
Information:					
39	Non Patent Literature	BST-015_-_BST-003C2_-_Network_Security_Assessment.pdf	1803210 8851b10c8673685c1ebb024df2d9d024cda8a0e7	no	13
Warnings:					
Information:					
40	Non Patent Literature	BST-010_-_NPL_-_Percentile-Based_Approach_to_Forecasting.pdf	774615 3676ecb37874a3833c17f90b3327997173c1d98a	no	16
Warnings:					
Information:					
41	Non Patent Literature	Seneviratne_SSIDs_in_the_Wild.PDF	728699 77919e016d1e31254fe6b3eb22a91b383958d6d6	no	5
Warnings:					
Information:					

42	Request for Continued Examination (RCE)	BST-004RCE.pdf	1349850 882dc97ff56fb2e8281c6d523de07b1cd0820706	no	3
Warnings:					
Information:					
43		BST-004_ResponsewithRCE.pdf	105302 a1ecab47d441f04dfcf983ff304b521390b37976	yes	10
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Amendment/Argument after Patent Board Decision		1	1	
	Claims		2	8	
	Applicant Arguments/Remarks Made in an Amendment		9	10	
Warnings:					
Information:					
44	Information Disclosure Statement (IDS) Form (SB08)	BST-004_IDS.pdf	114641 2e60f32619582425f79b12244d59558c3cc137f0	no	9
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
45	Information Disclosure Statement (IDS) Form (SB08)	BST-004_SB08.pdf	253659 ef2b8d691b705e45a251c9428a822642d081d6f6	no	16
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
46	Non Patent Literature	BST-003C1_Hachem.pdf	1680736 d80901c701f1bbc035d76e21f649b30c5584bf8c	no	8
Warnings:					
Information:					

47	Fee Worksheet (SB06)	fee-info.pdf	30681 541176da9422840ef6d70bb81dd30b0b80cec6fd	no	2

Warnings:	
Information:	
Total Files Size (in bytes):	55935872

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 August 2017 (24.08.2017)

WIPO | PCT

(10) International Publication Number
WO 2017/142694 A1

(51) International Patent Classification:
G06Q 10/00 (2012.01)

(21) International Application Number:
PCT/US2017/015483

(22) International Filing Date:
27 January 2017 (27.01.2017)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
15/046,318 17 February 2016 (17.02.2016) US
15/198,560 30 June 2016 (30.06.2016) US

(71) Applicant: **SECURITY SCORECARD, INC.** [US/US]; 214 W 29th Street, 5th Floor, New York, NY 10001 (US).

(72) Inventor: **RASUMOV, Nikon**; 283 Avenue 6a, New York, NY 12559 (US).

(74) Agent: **BRAXDALE, Allan**; Norton Rose Fulbright US LLP, 2200 Ross Avenue,s Uite 3600, Dallas, TX 75201-7932 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE,

[Continued on next page]

(54) Title: NON-INTRUSIVE TECHNIQUES FOR DISCOVERING AND USING ORGANIZATIONAL RELATIONSHIPS

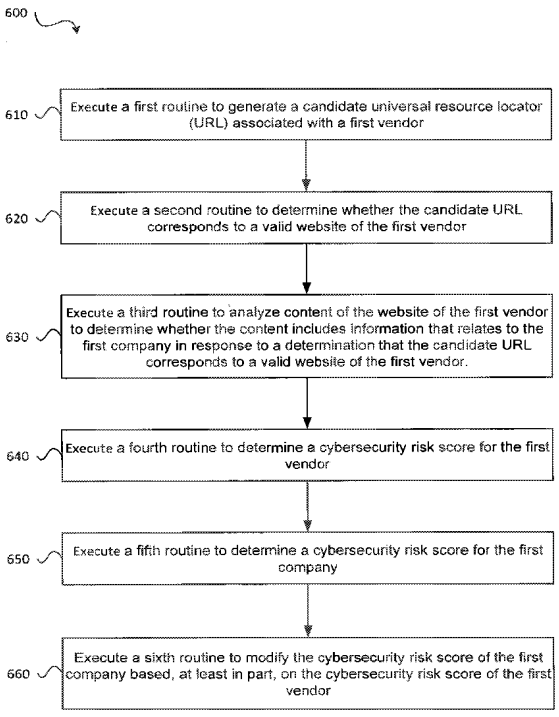


FIG. 6

(57) Abstract: The present disclosure provides techniques for calculating an entity's cybersecurity risk based on identified relationships between the entity and one or more vendors. Customer/vendor relationships may impact the cybersecurity risk for each of the parties involved because a security compromise of a downstream or upstream provider can lead to a compromise of multiple other companies. For example, if organization A uses B (e.g., a cloud service provider) to store files, and B is compromised, this may lead to organization A being compromised (e.g., the files organization A stored using B may have been compromised by the breach of B's cybersecurity). Embodiments of the present disclosure further provide a technique for calculating a cybersecurity risk score for an organization based on identified customer/vendor relationships.

WO 2017/142694 A1

DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

— *with international search report (Art. 21(3))*

NON-INTRUSIVE TECHNIQUES FOR DISCOVERING AND USING ORGANIZATIONAL RELATIONSHIPS

CROSS-REFERENCE TO RELATED APPLICATION

[0001] This application claims priority to U.S. Patent Application No. 15/046,318, filed February 17, 2016 and entitled, "NON-INTRUSIVE TECHNIQUES FOR DISCOVERING AND USING ORGANIZATIONAL RELATIONSHIPS;" and U.S. Patent Application No. 15/198,560, filed June 30, 2016 and entitled, "NON-INTRUSIVE TECHNIQUES FOR DISCOVERING AND USING ORGANIZATIONAL RELATIONSHIPS;" both of which are expressly incorporated by reference herein in its entirety.

TECHNICAL FIELD

[0002] The present application is generally related to the technical field of corporate cybersecurity technology, and more particularly to techniques for discovering organizational relationships and calculating an entity's cybersecurity risk based on discovered organizational relationships.

BACKGROUND OF THE INVENTION

[0003] As the availability of access to various networks, such as the Internet, cellular data networks, etc., has increased, so too has the mobility of electronic devices. As a result of this increased mobility and access, more and more information is being stored in, and services provided through, the cloud. This has created an Internet ecosystem where corporate entities establish relationships (e.g., customer/vendor relationships, vendor/vendor relationship, etc.) with various third parties that provide cloud and other network accessible services (e.g., software-as-a-service applications, etc.) to the corporate entities. For example, many corporations use Box.com® to store and access data. Such corporations may be considered to have a customer/vendor relationship with Box.com®, where Box.com® is the vendor, and each of the corporate entities that use Box.com® are the customers. Such relationships make it difficult to assess the cybersecurity risk of an organization (e.g., because the risk may be dependent upon not only the level of cybersecurity that an organization has, but also on the level of cybersecurity that its vendors have). However, identifying these types of relationships is often

difficult, as vendors do not readily provide or otherwise make their customer list available to third parties. Thus, discovering such relationships is often difficult. Further, the lack of accurate relationship information makes assessing aggregate cybersecurity risk for an organization difficult, and often inaccurate (e.g., because of unknown relationships).

BRIEF SUMMARY OF THE INVENTION

[0004] Embodiments of the present disclosure provide systems, methods, and computer-readable storage media that provide non-intrusive techniques for discovering relationships between organizations (e.g., customer/vendor relationships, vendor/vendor relationships, and the like). For example, if an organization (e.g., a bank) uses cloud services provided by one or more vendors (e.g., cloud service providers), embodiments of the present disclosure provide non-intrusive techniques for discovering the existence of the relationships (e.g., a customer/vendor relationship) between the organization and each of the one or more vendors (e.g., the organization is a customer of each of the one or more vendors).

[0005] Additionally, embodiments of the present disclosure provide systems, methods, and computer-readable storage media for calculating an entity's cybersecurity risk based on discovered organizational relationships. Organizational relationships may impact the cybersecurity risk for each of the organizations involved because a security compromise of a downstream or upstream organization can lead to a compromise of multiple other organizations. As an example, if organization A uses B (e.g., a cloud service provider) to store files, and B is compromised, this may lead to organization A being compromised (e.g., the files organization A stored using B may have been compromised by the breach of B's cybersecurity). This type of cybersecurity threat may also be indirect (e.g., the breached organization does not have a direct customer/vendor relationship with the breached party). For example, if B, above, is hosted by an organization C, and then organization C is compromised, this could lead to a domino effect where multiple other organizations are compromised, such as B and/or A. In the scenarios above, it can be seen that the aggregate cybersecurity risk of A is dependent upon: 1) the level of cybersecurity that A has; and 2) the level of cybersecurity that various vendors having direct and indirect relationships with A have. Embodiments of the present disclosure provide a technique for identifying customer/vendor relationships between organizations. Additionally,

embodiments of the present disclosure provide techniques for calculating a cybersecurity risk score for an organization based on identified customer/vendor relationships of the organization.

[0006] The foregoing has outlined rather broadly the features and technical advantages of the present invention in order that the detailed description of the invention that follows may be better understood. Additional features and advantages of the embodiments will be described hereinafter which form the subject of the claims of the present disclosure. It should be appreciated by those skilled in the art that the conception and specific embodiment disclosed may be readily utilized as a basis for modifying or designing other structures for carrying out the same purposes of the present disclosure. It should also be realized by those skilled in the art that such equivalent constructions do not depart from the scope of the present disclosure as set forth in the appended claims. The novel features which are believed to be characteristic of the embodiments, both as to its organization and method of operation, together with further objects and advantages will be better understood from the following description when considered in connection with the accompanying figures. It is to be expressly understood, however, that each of the figures is provided for the purpose of illustration and description only and is not intended as a definition of the limits of the present invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0007] For a more complete understanding of the present invention, reference is now made to the following descriptions taken in conjunction with the accompanying drawings, in which:

[0008] FIG. 1 is a block diagram of a system that includes a server for discovering organizational relationships and for calculating an entity's cybersecurity risk based on the discovered organizational relationships according to an embodiment;

[0009] FIG. 2 is a block diagram of an embodiment of system for discovering organizational relationships according to an embodiment;

[0010] FIG. 3 is a model illustrating organizational relationship information captured according to an embodiment;

[0011] FIG. 4 is another model illustrating additional organizational relationship information captured according to an embodiment;

[0012] FIG. 5 is yet another model illustrating organizational relationship information captured according to an embodiment;

[0013] FIG. 6 is a flow diagram of a method for determining a cybersecurity score of a first company based on a cybersecurity posture of one or more vendors that have a relationship with the first company through analysis of content of one or more vendor websites containing information that is unique to the first company according to an embodiment;

[0014] FIG. 7 is a block diagram illustrating various aspects of an embodiment for identifying relationships between an entity and one or more vendors according to an embodiment;

[0015] FIG. 8 is a block diagram of a system for calculating an entity's cybersecurity risk score based on discovered organizational relationships according to an embodiment; and

[0016] FIG. 9 is a flow diagram of a method for non-intrusively discovering relationships between organizations according to embodiments.

DETAILED DESCRIPTION OF THE INVENTION

[0017] An entity's knowledge of its cybersecurity risks, as well as those of its current, former, and potential future business partners, such as any vendors that may provide services to the entity, may serve as strategic information used to guide the entity's cybersecurity and business decisions. To provide an accurate picture of an entity's cybersecurity risk, the concepts and embodiments described herein involve discovering organizational relationships between the entity and other organizations (e.g., the entity's vendors, the entity's customers, etc.). Non-intrusive data collection involves collecting data from a source for which permission from the entity whose cybersecurity risk is calculated is not required. In contrast, intrusive data collection involves collecting data from a source for which permission from the entity whose cybersecurity risk is calculated is required. Embodiments of the present disclosure utilize various non-intrusive techniques, described in more detail below, to collect information that would most

likely not be accessible via intrusive techniques. For example, a company may be reluctant to provide information regarding all of the vendors that it uses in its ordinary course of business, and a vendor may likewise be reluctant to provide a list of all of its customers (e.g., for purposes of calculating a cybersecurity risk for the entity). Non-intrusive data collection techniques utilized in accordance with embodiments of the present disclosure may be employed to discover organizational relationships between various organizations, and to provide a detailed assessment of an entity's cybersecurity risk (e.g., based on discovered organizational relationships). Nevertheless, these non-intrusive data collection techniques may be used in conjunction with other data collection techniques, such as intrusive data collection techniques, to provide a requisite level of performance - depending on the objective.

[0018] The collected data is used to identify relationships between various entities to create a mapping or graph of an Internet ecosystem representing vendor/client relationships. In an embodiment, these relationships may be used to calculate or assess an aggregate cybersecurity risk for an entity. The aggregate cybersecurity risk may provide an indication of the level of cybersecurity for a target entity, and may further indicate how the entity's cybersecurity risk is affected by the entity's relationships with one or more third parties.

[0019] In an embodiment, a scorecard system may be used to calculate the cybersecurity risk score based on discovered relationships. The scorecard system may use the calculated cybersecurity risk score to determine ranking, percentile, and other detailed cybersecurity risk information about the entity, and this information may be used to determine how various relationships that the entity has with third parties impact the entity's cybersecurity risk. Additionally, the cybersecurity risk score calculated according to embodiments may provide information that may be used by third parties to assess the cybersecurity risk of the entity in connection with establishing a relationship with the entity.

[0020] As will be further discussed below, the disclosed embodiments facilitate the discovery of organizational relationships, and allow the cybersecurity risk score for an entity to be updated via real-time monitoring based on the discovered relationships. Also, the scorecard system allows the cybersecurity risk score to be determined nearly instantly, or in near real-time. As a result, an entity can use the scorecard system to track its historical performance, as well as

monitoring how the entity's cybersecurity risk is impacted by third parties that have relationships with the entity, which may allow the entity to be proactive in preventing a cybersecurity threat.

[0021] Certain units described in this specification have been labeled as modules in order to more particularly emphasize their implementation independence. A module is ''[a] self-contained hardware or software component that interacts with a larger system." Alan Freedman, "The Computer Glossary" 268 (8th ed. 1998). A module may comprise a machine- or machines-executable instructions. For example, a module may be implemented as a hardware circuit comprising custom VLSI circuits or gate arrays, off-the-shelf semiconductors such as logic chips, transistors, or other discrete components. A module may also be implemented in programmable hardware devices such as field programmable gate arrays, programmable array logic, programmable logic devices or the like.

[0022] Modules may also include software-defined units or instructions, that when executed by a processing machine or device, transform data stored on a data storage device from a first state to a second state. An identified module of executable code may, for instance, comprise one or more physical or logical blocks of computer instructions that may be organized as an object, procedure, or function. Nevertheless, the executables of an identified module need not be physically located together, but may comprise disparate instructions stored in different locations that, when joined logically together, comprise the module, and when executed by the processor, achieve the stated data transformation. A module of executable code may be a single instruction, or many instructions, and may even be distributed over several different code segments, among different programs, and/or across several memory devices. Similarly, operational data may be identified and illustrated herein within modules, and may be embodied in any suitable form and organized within any suitable type of data structure. The operational data may be collected as a single data set, or may be distributed over different locations including over different storage devices.

[0023] In the following description, numerous specific details are provided, such as examples of programming, software modules, user selections, network transactions, database queries, database structures, hardware modules, hardware circuits, hardware chips, etc., to provide a thorough understanding of the present embodiments. One skilled in the relevant art

will recognize, however, that the invention may be practiced without one or more of the specific details, or with other methods, components, materials, and so forth. In other instances, well-known structures, materials, or operations are not shown or described in detail to avoid obscuring aspects of the invention.

[0024] Referring to FIG. 1, a block diagram of network 100 that includes a relationship server 110, a communication network 120, an entity server 130, an entity 140, data sources 150, and user station 160 is shown. In an embodiment, the relationship server 110 may include one or more servers that, according to one embodiment, are configured to perform several of the functions described herein with reference to FIG. 2. One or more of the servers comprising the relationship server 110 may include memory, storage hardware, software residing thereon, and one or more processors configured to perform functions associated with network 100. For example, components comprising user station 160, such as CPU 162, can be used to interface and/or implement the relationship server 110. Accordingly, the user station 160 may serve as a cybersecurity risk assessment portal by which a user may access a scorecard system disclosed herein. The portal can function to allow multiple users, inside and outside network 100 (e.g., at multiple instances of user station 160), to interface with one another. One of skill in the art will readily recognize that different server and computer architectures can be utilized to implement the relationship server 110, and that the relationship server 110 is not limited to a particular architecture so long as the hardware implementing relationship server 110 supports the functions of the scorecard system disclosed herein with reference to FIGs. 1-7.

[0025] The communication network 120 may facilitate communication of data between the relationship server 110 and the data sources 150. The communication network 120 may also facilitate communication of data between the relationship server 110 and other servers/processors, such as entity server 130. The communication network 120 may include any type of communications network, such as a direct PC-to-PC connection, a local area network (LAN), a wide area network (WAN), a modem-to-modem connection, the Internet, a combination of the above, or any other communications network now known or later developed within the networking arts which permits two or more electronic devices to communicate.

[0026] The entity server 130 may comprise the servers which the entity 140 uses to support its operations. In some embodiments, the relationship server 110 may access the entity server 13 to collect information that may be used to calculate an entity's cybersecurity risk. The data sources 150 include the sources from which the relationship server 110 collects information to calculate and benchmark an entity's cybersecurity risk.

[0027] The entity 140 may include any organization, company, corporation, or group of individuals. For example, one entity may be a corporation with thousands of employees and headquarters in New York City, while another entity may be a group of one or more individuals associated with a website and having headquarters in a residential home.

[0028] Data sources 150 may include any source of data accessible over communication network 120. By way of example, and not limitation, one source of data can include a website associated with a company, while another source of data may be an online database of various information. In general, the data sources 150 may be sources of any kind of data, such as domain name data, social media data, multimedia data, IP address data, and the like. One of skill in the art would readily recognize that data sources 150 are not limited to a particular data source, and that any source from which data may be retrieved may serve as a data source so long as it can be accessed via the communication network 120.

[0029] With respect to user station 160, the central processing unit ("CPU") 161 is coupled to the system bus 162. The CPU 161 may be a CPU or microprocessor, a graphics processing unit ("GPU,), and/or microcontroller that has been programmed to perform the functions of the relationship server 110, as described in more detail below with reference to FIGs. 2, 6, and 7. Embodiments are not restricted by the architecture of the CPU 161 so long as the CPU 161, whether directly or indirectly, supports the operations described herein. The CPU 161 is one component that may execute the various described logical instructions.

[0030] The user station 160 also comprises random access memory (RAM) 163, which can be synchronous RAM (SRAM), dynamic RAM (DRAM), synchronous dynamic RAM (SDRAM), or the like. The user station 160 may utilize the RAM 163 to store the various data structures used by a software application. The user station 160 may also comprise read only memory (ROM) 164 which can be PROM, EPROM, EEPROM, optical storage, or the like. The

ROM may store configuration information for booting the user station 160. The RAM 163 and the ROM 164 hold user and system data, and both the RAM 163 and the ROM 164 may be randomly accessed.

[0031] The user station 160 may also comprise an input/output (I/O) adapter 165, a communications adapter 166, a user interface adapter 167, and a display adapter 168. The I/O adapter 165 and/or the user interface adapter 167 may, in certain embodiments, enable a user to interact with the user station 160. In a further embodiment, the display adapter 168 may display a graphical user interface (GUI) associated with a software or web-based application on a display device 169, such as a monitor or touch screen.

[0032] The I/O adapter 165 may couple one or more storage devices 170, such as one or more of a hard drive, a solid state storage device, a flash drive, a compact disc (CD) drive, a floppy disk drive, and a tape drive, to the user station 160. Also, the data storage 170 can be a separate server coupled to the user station 160 through a network connection to the I/O adapter 165. The communications adapter 166 can be adapted to couple the user station 160 to a network, which can be one or more of a LAN, WAN, and/or the Internet. Therefore, in some embodiments, the cybersecurity risk assessment portal 160 may be an online portal. The user interface adapter 167 couples user input devices, such as a keyboard 171, a pointing device 172, and/or a touch screen (not shown) to the user station 160. The display adapter 168 can be driven by the CPU 161 to control the display on the display device 169. Any of the devices 161-168 may be physical and/or logical.

[0033] The concepts described herein are not limited to the architecture of user station 160. Rather, the user station 160 is provided as an example of one type of computing device that can be adapted to perform the functions of the relationship server 110 of embodiments and/or the user interface device 165. For example, any suitable processor-based device can be utilized including, without limitation, personal data assistants (PDAs), tablet computers, smartphones, computer game consoles, multi-processor servers, and the like. Moreover, the systems and methods of the present disclosure can be implemented on application specific integrated circuits (ASIC), very large scale integrated (VLSI) circuits, or other circuitry. In fact, persons of ordinary skill in the art may utilize any number of suitable structures capable of executing logical

operations according to the described embodiments. Additionally, it should be appreciated that user station 160, or certain components thereof, may reside at, or be installed in, different locations within network 100.

[0034] Referring to FIG. 2, a block diagram of a system for discovering organizational relationships according to an embodiment is shown as a system 200. In an embodiment, the system 200 may be implemented with one or more computing devices, such as the relationship server 110, entity servers 130, and user station(s) 160 of FIG. 1. As shown in FIG. 2, in an embodiment, the system 200 may comprise a gather initial data set module 210, a template generation module 220, a template analysis module 230, a template exploration module 240, a quality control analysis module 250, a relationship analysis module 260, a weighting module 270, and an additional data sources module 280. In an embodiment, the system 200 may be configured to execute one or more routines that perform various operations to discover organizational relationships, as described in more detail below.

[0035] The gather initial data set module 210 may access information (e.g., information stored in the data storage 170) to identify a set of data that may be used passed to the template generation module 220 in connection with generation of one or more candidate URL templates. In an embodiment, the set of data may be determined using a list "S" comprising company names and a list "K" of keywords. In an embodiment, the company names identified in the list "S" and the keywords identified in list "K" may be selected from a list "T" comprising a database of all known company names and keywords. The keywords may correspond to words that have been identified as suggesting a relationship between a vendor and a company. For example, the keywords may comprise words such as "signin" and its various other permutations (e.g., "sign in," "sign on," "login," "log on," and the like), or other words indicative of an account with a vendor, such as "username," "user name," "password," and the like. The keywords included in the list "K" may be indicative of a relationship (e.g., an account that a company has with a vendor), as will be described in more detail below. The companies identified in the list "S" may correspond to companies of interest (e.g., companies for which a cybersecurity risk score is desired), and/or may comprise companies that are likely to be relevant to the companies of interest (e.g., vendors of interest). In an embodiment, the companies identified in the list "S" may be identified from the list "T." Once the gather initial data set

module 210 has identified the initial set of data, it may pass the initial set of data to the template generation module 220.

[0036] The template generation module 220 may comprise one or more routines, executable by one or more processors (e.g., the CPU 161 of FIG. 1) to generate one or more candidate universal resource locators (URLs) associated with a first vendor. In an embodiment, the one or more routines may be stored as instructions that are executable by a processor, such as the CPU 161 of FIG. 1. Each of the candidate URLs may comprise first information corresponding to a website associated with a vendor, and second information associated with a company (e.g., one of the companies identified in list "S" of the initial data set received from the gather initial data set module 210).

[0037] For example, and referring briefly to FIG. 7, a block diagram illustrating various aspects of an embodiment for identifying relationships between an entity and one or more vendors according to an embodiment is shown. In FIG. 7, various embodiments of candidate URLs 710 are illustrated. Each of the candidate URLs 710 includes first information (e.g., "genericwebsite.com") associated with a website of a vendor, and second information (e.g., "<company A>" and "<company B>") associated with a company. As further illustrated in FIG. 7, in an embodiment, the first and second information may be formatted differently for different candidate URLs. For example, in the candidate URL "https://genericwebsite.com/<company A>" the first information corresponds to a domain (e.g., the genericwebsite.com domain) of the first vendor, and the second information (e.g., the "/<company A>") corresponds to a directory within the domain of the vendor that is associated with the company A. As another example, in the candidate URL https://<company B>.genericwebsite.com the first information corresponds to the domain (e.g., the genericwebsite.com domain) of the first vendor, and the second information corresponds to a subdomain within the domain of the vendor that is associated with the company B. As can be appreciated from the candidate URLs 710 illustrated in FIG. 7, the template generation module 220 may generate multiple candidate URLs (e.g., URL templates) comprising first information corresponding to a vendor's website, where different candidate URLs comprise different second information representing potential relationships between the vendor and different companies, such as company A and company B.

[0038] Referring back to FIG. 2, in an embodiment, the routine(s) of the template generation module 220 may generate templates automatically using a search engine. For example, the routine(s) may be configured to receive the initial data set as an input parameter, and may use the initial data set to generate one or more queries that may be provided to a search engine. An exemplary search engine query that may be generated by the template generation module 220 is illustrated in FIG. 7 as a search engine query 720. The search engine query 720 may query the search engine to return a list of all known websites (or URLs, uniform resource identifier (URIs), and the like) that contain the domain "genericwebsite.com" and that contain the keywords "signon," "sign on," "signin," "sign in," "login," "log in," "username" or "password." The URLs returned as a result of the search engine query 720 are limited to webpages within the domain "genericwebsite.com" that also contain one of the keywords following the "-inurl:" command of the search engine query 720 (e.g., "www," "www2," "www3," "support," "community," "developer," "developers," "help," "helpdesk," "blog," "forum," "forums," "wiki," or "https"). As a result of providing the search engine query 720 to a search engine, the template generation module 220 may receive a list of one or more candidate URLs that satisfy the search engine query 720. Such search results may correspond to a list of candidate URLs that may be used to identify relationships between a vendor (e.g., an owner of the domain "genericwebsite.com" and one or more companies. It is noted that other commands, syntaxes, keyword combinations, domains, and the like may be used by the template generation module 220 to generate search engine queries, and that the search engine query 720 is provided for purposes of illustration, rather than by way of limitation. Thus, the present disclosure is not to be limited to search queries of the exact structure shown in FIG. 7. In addition to automatically generating search engine queries, the template generation module 220 may be configured to provide a graphical user interface (GUI) that allows a user to customize, create, or otherwise edit search engine queries for use in generating a list of candidate URLs. In an embodiment, the user may access the GUI using the portal 160 of FIG. 1. As a result of the search engine query, a set of candidate URLs may be obtained or generated.

[0039] In an embodiment, the set of candidate URLs may include candidate URLs associated with different URL templates. For example, a first template may correspond to a domain and subdomain combination, such as the candidate URL "https://<company B>.genericwebsite.com" of FIG. 7, where the domain is "genericwebsite.com" and the

subdomain is "<company B>" (e.g., the name of company B). As another example, the set of candidate URLs may include a second template corresponding to a domain and directory combination, such as the candidate URL "https://genericwebsite.com/<company A>" of FIG. 7, where the domain is "genericwebsite.com" and the directory is "<company A>" (e.g., the name of company A). It is noted that other structures of URL templates and candidate URLs may be generated by the template generation module 220, and the examples above are provided for purposes of illustration, rather than by way of limitation.

[0040] The template analysis module 230 may comprise one or more routines, executable by one or more processors (e.g., the CPU 161 of FIG. 1) to analyze the set of candidate URLs for various attributes, such as template frequency. For example, in an embodiment, the template analysis module 230 may analyze the set of candidate URLs. As a result of the analysis, the set of candidate URLs may be reorganized or collated such that all candidate URLs matching a particular template are grouped together. For example, as explained above, a first template may correspond to a domain of a first entity (e.g., a vendor) followed a directory associated with a second entity (e.g,. a client of the vendor), as in the candidate URL "https://genericwebsite.com/<company A>" of FIG. 7, and a second template may correspond to a subdomain of a second entity (e.g., a client of a vendor) followed by a domain of the first entity (e.g., the vendor), as in the candidate URL "https://<company B>.genericwebsite.com" of FIG. 7. The template analysis module 230 may further analyze the set of candidate URLs to determine a count for each of the identified URL templates. For example, as shown at 730 of FIG. 7, the analysis may indicate that the set of candidate URLs included five candidate URLs (each associated with a different company) of the first template type (e.g., "https://genericwebsite.com/<company>") for a particular vendor (e.g., the owner of the domain "genericwebsite.com"), and may indicate that the set of candidate URLs included one thousand candidate URLs (each associated with a different company) of a second template type (e.g., https://<company>.my.salesforce.com) for another particular vendor. In an embodiment, the counts associated with each different identified candidate URL template/template type may be used to determine a cutoff point for exploring the template further. For example, in an embodiment, the template analysis module 230 may calculate a cutoff point for exploring a template further based on the total count of candidate URLs included in the set of candidate URLs as a fraction of the list S for the same template. In an embodiment, a low count for a

particular URL template may indicate that the URL template is not valid, and candidate URLs matching the particular URL template may be discarded. In an embodiment, a high count for a particular URL template may indicate that the particular URL template is valid, and candidate URLs matching the particular URL template may be designated for further exploration and analysis, as described in more detail below. In an additional or alternative embodiment, the template analysis module 230 may comprise a routine (or subroutine) that implements machine learning algorithms to prune false positives from the set of candidate URLs. In an embodiment, the template analysis module 230 may provide a GUI that enables a human operator to review and/or approve/reject templates for further use in identifying relationships between a vendor and one or more companies.

[0041] In an embodiment, a threshold may be configured for use in determining whether a URL template count is indicative of an invalid URL template or a valid URL template. For example, if a count of ten or less candidate URLs for a particular URL template type indicates a high probability that the particular URL template is invalid, the threshold may be set to ten. Thus, any URL templates generated by the system 200 that have a count less than the threshold may be discarded as invalid. In an embodiment, the threshold may be set by a user of the system 200. In an additional or alternative embodiment, the threshold may be dynamically configured (e.g., by machine learning algorithms) based on historical data analysis associated with URL templates and candidate URLs. For example, when the system 200 is first operated, all URL templates may be determined to be valid, and may be explored, as described in more detail below. As a result of that analysis and exploration, the system 200 may generate historical URL template analysis information that identifies counts for various URL template and indicates whether URL templates having a particular count resulted in valid relationship information being obtained. Over time, this historical URL template analysis information may be used to dynamically configure the threshold. In an embodiment, each time a set of candidate URLs are generated for a new vendor (e.g., the first time that a vendor is associated with the first information), all templates may be counted, and explored irrespective of counts. This may be beneficial as an initial run to discover relationships for a new vendor (e.g., a vendor for which no relationship information has been previously discovered) because the potential scope in terms of relationships the new vendor may have is unknown. Thus, a relatively low count may still be indicative of a valid template, and should be explored to determine or configure the threshold for

discarding URL templates. For example, if the new vendor is a startup company, the vendor may have a relatively low number of relationships. As time passes, the number of relationships the company has may increase as the vendor establishes new relationships. As this occurs, the threshold may be dynamically updated to increase threshold. Similarly, for existing vendors (e.g., vendors for which relationships have been previously discovered), the threshold may be dynamically adjusted up or down depending on whether the vendor is gaining or losing relationships. Exemplary techniques for discovering lost relationships are described in more detail below.

[0042] The template exploration module 240 may comprise one or more routines, executable by one or more processors (e.g., the CPU 161 of FIG. 1) to explore templates (e.g., analyze the candidate URLs) to determine whether a relationship exists between a vendor (e.g., an entity identified by the first information of a particular candidate URL) and a company (e.g., an entity associated with the second information of the particular candidate URL). In an embodiment, the template exploration module 240 may, as an initial matter, determine whether each candidate URL corresponds to a valid website for the vendor. For example, the template exploration module 240 may determine whether a particular candidate URL results in an error, results in a generic landing page, or results in a website of the vendor that includes information unique to the company associated the particular candidate URL's second information.

[0043] Referring briefly to FIG. 7, exemplary aspects of determining whether a candidate URL corresponds to a valid website for the vendor are shown as template exploration results 740. As shown in FIG. 7, the template exploration results 740 illustrate that a first candidate URL (e.g., "https://genericwebsite.com/<company A>") of a first URL template type (e.g., a URL template comprising vendor domain information and company directory information) results in a 404 error (e.g., an invalid website of the vendor), a second candidate URL (e.g., "https://genericwebsite.com/<company B>") resolves to a landing page with a generic logo (e.g., a logo of the vendor), and that a third candidate URL (e.g., "https://genericwebsite.com/<company C>") resolves in a landing page for a login with the logo of company C. Thus, under the initial analysis performed by the template exploration module, the second candidate URL and the third candidate URL may be determined to be associated with valid websites of the vendor (e.g., the owner of the "genericwebsite.com" domain).

[0044] In response to a determination that one or more candidate URLs correspond to valid websites of the vendor, the template exploration module 240 may analyze content of each valid website to determine whether the content includes information that is unique to the company identified by each corresponding candidate URL's second information. The presence of information that is unique to the first company within the content of a website of the vendor may indicate that a relationship exists between the company and the vendor. For example, the second candidate URL illustrated at 740 of FIG. 7, while resolving to a valid website of the vendor, only includes generic logo information. Thus, the template exploration module 240 may determine that the website corresponding to the second candidate URL does not suggest to within a threshold confidence level that a relationship exists between the vendor that owns the "genericwebsite.com" domain and company B. However, the third candidate URL illustrated at 740 of FIG. 7 resolves to a landing page (e.g., a valid website of the vendor) that includes content (e.g., company C's logo) that is uniquely associated with company C. Thus, the template exploration module 240 may determine that the website corresponding to the third candidate URL suggests to within the threshold confidence level that a relationship exists between the vendor that owns the "genericwebsite.com" domain and company C.

[0045] In an embodiment, the template exploration module 240 may further analyze the content of valid websites to determine where in the valid websites the content uniquely associated with a company is located. For example, when the content is located on a login page, this may more strongly suggest that a relationship exists than when information uniquely associated with the company is found within text in the body of the website. In an embodiment, the template exploration module 240 may store information representative of the type of content (e.g., logo, company name in text, redirect link, etc.) identified as unique to the company of interest, and the location of the content within the valid website at a database (e.g., the data storage 170 of FIG. 1). In an embodiment, this information may later be utilized (e.g., by the quality control analysis module 250) to assess the performance of the system 200 or weight the strength of the relationship, as described below in more detail. In an embodiment, the template exploration module 240 may analyze the content of the website through analysis of source code of the website, metadata associated with the website, analysis of image content included of the website, analysis of text content of the website, traversal of one or more links of the website to identify additional content of the website that should be analyzed, or a combination thereof.

[0046] In an embodiment, once a candidate URL and/or template is found that resolves to a valid website that includes content unique to a particular company, the template exploration module 240 may analyze or explore the template using additional company information. For example, if the initial set of candidate URLs for a particular template only included five candidate URLs for five different companies (e.g., five different companies selected from the list "S" and/or the list "T"), the template exploration module 240 may generate additional candidate URLs (or instruct the template generation module 220 to generate the additional candidate URLs) using additional company names (e.g., candidate URLs containing second information corresponding to companies that are different from the five different companies included in the initial set of candidate URLs), and may evaluate/analyze the additional candidate URLs in the manner described above to determine whether any of the additional candidate URLs correspond to a valid website that includes content unique to one of the additional companies. This may facilitate discovery of additional relationships that the vendor has. It is noted that a company may be both a vendor, and a client. Thus, in embodiments, some of the candidate URLs may include a particular company as a vendor (e.g., associated with the first information included in the candidate URL), while other candidate URLs may include the particular company as a client (e.g., associated with the second information included in the candidate URL).

[0047] The quality control analysis module 250 may comprise one or more routines, executable by one or more processors (e.g., the CPU 161 of FIG. 1) to evaluate the performance of the system 200. The performance of the system 200 may be evaluated to determine a likelihood that the relationships between vendors and companies, as identified by the system 200, are actual relationships (e.g., a likelihood that companies identified as having a relationship with a particular vendor, do actually have a relationship with that particular vendor, or are clients of that particular vendor). As briefly described above, the source for the content within a vendor's valid website that is unique to a company may provide some indication as to the reliability of that information. For example, the presence of the company's logo on a login page may strongly suggest that the relationship exists, whereas the presence of the company's name on the vendor's social media site, or within body text on the vendor's website may be deemed a weaker suggestion that the relationship exists. In an embodiment, the quality control analysis module 250 may analyze the information stored at the data storage by the template exploration module 240, and may flag relationships based on weak relationship indicators (e.g., relationships

identified based on text only, or identified based on content of a social media site of the vendor). These flagged relationships may then be presented to a user via a GUI, and the user may verify whether the content is sufficient to support a conclusion that the company and the vendor have a relationship. In an additional or alternative embodiment, the quality control analysis module 250 may verify that content within a website that appears to be unique to the company identified by the second information, is in fact unique to the company. For example, it may be possible that some company information, such as company name acronyms, may lead to identification of ambiguous content. When ambiguous content associated with a company is identified, the quality control analysis module 250 may initiate operations to validate, or authenticate, the information (e.g., using one or more of the other data sources facilitated by the other data sources module 280). This may include seeking to corroborate the content by finding additional content from another source that suggests that the company included in the content of the valid website is in fact the company identified by the second information of the corresponding candidate URL, and that corroborates the existence of the relationship between the vendor and the company.

[0048] The relationship analysis module 260 may comprise one or more routines, executable by one or more processors (e.g., the CPU 161 of FIG. 1), to analyze the results of the template exploration results output by the template exploration module 240 to generate relationship information. For example, and referring briefly to FIG. 7, as a result of the template exploration performed by the template exploration module 240, a vendor client list 750 may be generated. The vendor client list 750 may identify various companies that were identified as clients of a vendor through analysis of one or more valid websites of the vendor. For example, each of the clients identified in the vendor client list 750 may have been identified by detecting the presence of content unique to each of the clients in one or more valid websites of the vendor (e.g., company A in this example). Once a vendor client list 750 has been created, the graph may be reversed to plot all of the vendors for a particular client. This may result in a list of companies and clients 760, as shown in FIG. 7. In an embodiment, as a result of the analysis of the relationships between companies and vendors, the relationship analysis module 260 may generate relationship information 262. In an embodiment, the relationship information 262 may be stored in a database, such as the data store 170 of FIG. 1. In an embodiment, the relationship analysis module 260 may be configured to identify multiple relationships between a vendor and particular company. For example, a vendor (e.g., Google®) may provide e-mail services (e.g.,

Gmail®), cloud data hosting services (e.g., Google Drive™), analytics services (e.g., Google Analytics™), etc. The system 200 of embodiments may facilitate discovery of multiple relationships between a single client and the vendor through discovery of one or more services of the vendor that are used by the client. Such information may provide a further indication that a relationship exists between the client and the vendor. In an additional or alternative embodiment, the relationship information 262 may be provided to the weighting module 270 for use in weighting the relationship between the vendor and one or more clients of the vendor. In an embodiment, graphs (e.g., the vendor client list 750 and the list of companies and clients 760) may be generated by the routine(s) of the relationship analysis module 260. These graphs may depict organizational interactions between various corporate entities, and may be used to generate alternative representations of an internet ecosystem. Exemplary alternative representations of internet ecosystems are illustrated with reference to FIGs. 3-5, which are described in more detail below

[0049] In an embodiment, the additional data sources module 280 may comprise one or more routines, executable by one or more processors (e.g, the processor 161 of FIG. 1), to analyze other data sources for information indicating the existence of a relationship between a company and a vendor. These other data sources may include information obtained through source code analysis of one or more websites of a vendor for indications that a particular company is a client of the vendor, information obtained through social media sites, information obtained through analysis of the vendor's press releases, information obtained from hosting service and infrastructure providers, and/or information obtained through network analysis (e.g., content delivery networks (CDNs) and objects embedded in web pages, such as Ad providers). Information that may be obtained through source code analysis may include detection of the presence of icons associated with a particular company within a website of the vendor, for example. Network analysis may be used to deduce, with high accuracy, a vendor's network devices and network providers. For example, by taking snapshots of portions of the Internet, and then applying searches for specific device fingerprints within the network footprint of a

secure socket layer (SSL) certificates, content delivery networks, internet service providers, hosting providers, e-mail service providers, hardware providers, self-hosted vendor subdomains, and the utilization of one or more payment providers.

[0050] Social media site and job posting site analysis may be used to analyze information that employees of a company post within the social media profiles or job posting sites that may indicate a relationship between the employer and one or more vendors. For example, if a person working for a particular company posts a particular technology (e.g., SQL Server®) was used at their job, it can be deduced that the particular company has Microsoft as a vendor (e.g., because SQL Server® is a product produced by Microsoft). In an embodiment, frequency analysis may be performed in connection with such information to increase the reliability of any relationships determined from such information. For example, if a high percentage of people working at a particular company indicate that a particular technology is used at their job, this may more strongly suggest that their employer has a client/vendor relationship with the provider/manufacturer of the particular technology. Additionally, analysis of press releases may reveal information about various relationships that an entity has with one or more third party vendors.

[0051] The weighting module 270 may comprise one or more routines, executable by a processor (e.g., the processor 161 of FIG. 1) for weighting discovered relationships, where the weight of a relationship may indicate the relationship strength, a risk factor associated with the relationship, or a combination thereof. In an embodiment, the relationships may be weighted based on a number of connections between a client and a vendor. For example, if the client has numerous relationships with a vendor (e.g., a relationship relating to cloud services of the vendor, a relationship relating to e-mail services provided by the vendor, etc.), that relationship may be assigned a higher weight than a relationship where the client has a single relationship with the vendor. This is because relationships between a client and a vendor based on multiple connections may indicate that the two entities are more closely integrated than relationships based on a single connection. In an embodiment, described in more detail below with reference to FIG. 8, the weighting module 270 may be configured to assign weights to discovered relationships based on characteristics of the relationship. In an additional or alternative embodiment, the weights applied to various relationships may be based on more than just the

relationships/number of relationships. For example, is a large percentage of employees of a company indicate (e.g., in a social media profile) that they use a particular technology corresponding to a particular vendor, this may indicate a strong relationship between the employer and the particular vendor. In an embodiment, information representative of the weights applied to various relationships may be generated by the weighting module 270, and may be output as weighted relationship information 272. In an embodiment, the weighted relationship information 272 may be stored in a database, such as the database 170 of FIG. 1.

[0052] To date, relationship information, such as the information obtained using the techniques of the system 200 described above, has not been easily accessible, and thus, organizational relationships determined according to embodiments of the present disclosure may provide a higher degree of accuracy with respect to organizational relationships. This is because traditional techniques primarily utilized analysis of website source code, but such analysis did not often turn up information indicating the existence of a relationship between a vendor and a company, and often resulted in obtaining only a small fraction of the relationships identified according to embodiments of the system 200. Thus, embodiments of the present disclosure improve the functioning of relationship servers, such as the relationship server 110 of FIG. 1, by increasing the accuracy of the discovered relationships. Additionally, it is noted that the techniques utilized by the various routines of the system 200 are all non-intrusive, and are not dependent upon an particular vendor providing information regarding its clients, or a particular company providing information regarding its vendors. Thus, the system 200 may operate autonomously, providing the ability to monitor the corporate interaction and relationship ecosystem using the techniques described above to maintain real-time information about the organizational relationships for various companies.

[0053] In some embodiments, the system 200 may be configured to periodically refresh the relationship information. This refreshing of the relationship information may be further analyzed to discover various types of information. For example, periodically updating the relationship information may facilitate tracking the growth of companies, such as when a company is adding new relationships (e.g., relationships with new clients, or additional relationships/connections with existing clients), or the decline of companies, such as when a company is losing relationships faster than the company is adding new relationships. This may

facilitate competitive market analysis (e.g., how a company is doing relative to its competitors). As another example, the refreshing of the relationship information may facilitate analysis of the health of the Internet ecosystem as discovered by the system 200 (e.g., are particular market segments adding relationships, which is a sign of good health for that segment of the Internet ecosystem, or losing relationships, which would indicate poor health for that segment of the Internet ecosystem). It is noted that the various uses for the relationship information provided herein have been provided for purposes of illustration, rather than by way of limitation, and the relationship information generated according to embodiments of the present disclosure may be used for many other purposes without departing from the scope of the present disclosure.

[0054] Referring to FIG. 3, a model illustrating relationship information captured according to an embodiment is shown. In FIG. 3, a subset of an ecosystem of companies in the United States is shown. Each of the dots in the model corresponds to a company operating in the United States, and lines between dots represent the existence of a relationship (e.g., a business relationship, a customer/vendor relationship, etc.) between the companies corresponding to the corresponding dots.

[0055] Referring to FIG. 4, another model illustrating additional relationship information captured according to an embodiment. In FIG. 4, a cloud of companies is shown, and illustrates connections between 30,000 entities with 60,000 links (which is a subset of the entire database). The insert 410 displays a few nodes of the model that correspond to different companies, and illustrates that of the 6 entities in the insert 410, only the entities 412 and 414 have a relationship between them. In this particular example, the relationship is a client/vendor relationship based on software services (e.g., between cnn.com and slack.com). It is noted that the different grey scales may symbolize the security posture and/or other features of the entities. For example, the dark grey colors associated with the entities 412, 414 may indicate a strong security posture (e.g., good level of cybersecurity), the two intermediate shades of grey closest to the entity 412 may indicate an average security posture (e.g,. a medium level of cybersecurity), and the lighter shade of grey entity closest to the entity 414 may indicate a poor security posture (e.g., low level of cybersecurity).

[0056] Referring to FIG. 5, yet another model illustrating relationship information captured according to an embodiment is shown. In FIG. 5, the model illustrates companies and their connections (e.g., relationships) with security rankings represented as different shades of grey. The black dots correspond to entities having a poor security posture (e.g., a low level of cybersecurity), the dark grey dots correspond to entities having a good security posture (e.g., a high level of cybersecurity), and other shades of grey indicating other security postures (e.g., levels of cybersecurity that are between the high and low levels of cybersecurity). The grey lines illustrate how the various companies are connected via client/vendor relationships. The big dot 510 corresponds to a particular entity of interest, which, in this graph, represents www.cnn.com.

[0057] FIG. 6 is a flow diagram of a method for determining a cybersecurity score of a first company based on a cybersecurity posture of one or more vendors that have a relationship with the first company through analysis of content of one or more vendor websites containing information that is unique to the first company according to an embodiment is shown as a method 600. In an embodiment, the method 600 may be stored in a computer-readable storage medium as instructions that, when executed by one or more processors, cause the one or more processors to perform the operations of the method 600. In an embodiment, the method 600 may be performed by the relationship server 110 of FIG. 1, by the system 800 of FIG. 8, or a combination thereof.

[0058] At 610, the method 600 includes executing a first routine to generate a candidate universal resource locator (URL) associated with a first vendor. In an embodiment, the first routine may correspond to the routine of the template generation module 220 of FIG. 2. The candidate URL may comprise first information corresponding to a website associated with the first vendor and second information associated with the first company, and the first vendor and the first company are different. In an embodiment, the candidate URL may be generated using a search engine query, such as the search engine query 720 of FIG. 7, as described above with reference to FIG. 2.

[0059] At 620, the method 600 includes executing a second routine to determine whether the candidate URL corresponds to a valid website of the first vendor, and, at 630, executing a third routine to analyze content of the website of the first vendor to determine whether the

content includes information that is unique to the first company in response to a determination that the candidate URL corresponds to a valid website of the first vendor. In an embodiment, the second routine and/or the third routine may correspond to one or more of the routines described in connection with the template analysis module 230 and the template exploration module 240 described in connection with FIG. 2, and may generate information similar to the candidate URL analysis 730 and/or the template exploration results 740 described with reference to FIG. 7. In an embodiment, the presence of information that is unique to the first company within the content of the website of the first vendor may indicate that a relationship exists between the first company and the first vendor.

[0060] At 640, the method 600 may include executing a fourth routine to determine a cybersecurity risk score for the first vendor, and, at 650, executing a fifth routine to determine a cybersecurity risk score for the first company. In an embodiment, the fourth routine and the fifth routine may correspond to the routine described in connection with the scoring module 810 of FIG. 8. In an embodiment, the cybersecurity risk scores calculated by the fourth and fifth routines may only account for the individual cybersecurity level of the first vendor and the first company, respectively, and may not account for how any relationships between the first vendor and the first company affect the aggregate cybersecurity risk of the respective entities.

[0061] At 660, the method 600 includes executing a sixth routine to modify the cybersecurity risk score of the first company based, at least in part, on the cybersecurity risk score of the first vendor. In an embodiment, the sixth routine may correspond to one or more of the routines described in connection with the weighting module 270 of FIGs. 2 and 8, and the scoring module 810 of FIG. 8. In an embodiment, the modification may reflect that the cybersecurity of the first company is dependent upon the cybersecurity of the first vendor by virtue of the relationship between the first company and the first vendor.

[0062] Referring to FIG. 8, a block diagram of a system for calculating an entity's cybersecurity risk score based on discovered organizational relationships according to an embodiment is shown as a system 800. As shown in FIG. 2, the system 800 includes the gather initial data set module 210, the template generation module 220, the template analysis module 230, the template exploration module 240, the quality control analysis module 250, the

relationship analysis module 260, the weighting module 270, and the additional data sources module 280 of FIG. 2. Additionally, the system 800 includes a scoring module 810. The scoring module 810 may be configured to calculate a cybersecurity risk score for an entity based, at least in part, on relationships discovered according to the techniques described above with reference to FIG. 2, as described below.

[0063] The scoring module 810 may comprise one or more routines, executable by one or more processors (e.g., the CPU 161 of FIG. 1) to calculate a cybersecurity risk score for each of the various entities identified by the system 800. In an embodiment, the cybersecurity risk score for a particular entity may be calculated at an arbitrary time (e.g., upon the system 800 learning of the existence of the particular entity, such as when the particular entity is added to the list "T" by the gather initial data set module 210. Subsequently, and in response to a determination that the content of the website of a vendor includes information that is unique to the particular entity (e.g., that a relationship exists between the vendor and the particular entity), the scoring module may determine whether to modify the cybersecurity risk score of the particular entity based, at least in part, on the cybersecurity risk score of the vendor. The modification may reflect that the cybersecurity of the particular entity may be dependent upon the cybersecurity of the vendor (e.g., because of the relationship between the particular entity and the vendor). Due to the periodic modification of a company's cybersecurity risk score based on the relationships that each company has, a company that has a good cybersecurity risk score when considered individually, may have a lower score when considered in view of its various vendor/client relationships (e.g., because one or more of the vendors that the company has a relationship with may have poor cybersecurity). Such information (e.g., relationship information, and cybersecurity risk scores that have been adjusted to account for the security posture of vendors having a relationship with a vendor) may be important to various entities, such as entities that insure companies against losses and out of pocket expenses caused by cybersecurity breaches. In an embodiment, the degree to which the cybersecurity risk score is modified or adjusted may reflect the level of cybersecurity for various tiers of vendors/clients.

[0064] In an embodiment, the weighted relationship information 272 generated by the weighting module 270, as described with reference to FIG. 2, may be used to dynamically adjust cybersecurity risk scores for various entities. For example, the strength of the relationship, as

indicated by the weight applied to the relationship information by the weighting module 270, may be used to determine the degree to which a cybersecurity risk score is adjusted up or down based on a relationship. For example, a strong relationship (e.g,. high weight) may cause the cybersecurity risk score to adjusted up or down to a higher degree than a weak relationship (e.g., low weight).

[0065] In an embodiment, the weighting module 270 may be further configured to determine the weight of a relationship based on risk factors, and the scoring module 810 may generate a cybersecurity score based on the risk factors. In an embodiment, the risk factor(s) may represent the affect that, or degree to which, a breach of the vendor's cybersecurity will expose sensitive data of the company being scored. For example, if the relationship is between a company and a cloud data storage provider, a breach of the cloud storage provider's systems may expose some or all of the data stored in the cloud by the company. In such instances, the weighting module 270 may determine that a breach of the vendor's cybersecurity may potentially expose sensitive data of the company being scored, and may give that relationship more weight. Based on the risk factor(s), the weighting module 270 may determine the weight of the relationship, and scoring module 810 may modify or adjust the cybersecurity score of the company based, at least in part, on the weighting of the relationship. Thus, the weighting may account for, or indicate the risk level indicated by the risk factor. For example, in the scenario above, the risk factor may indicate a high risk level because the company is storing information at the cloud offered by the vendor, and a compromise of the vendor may result in a breach of information that the company may has stored within the cloud. If the cybersecurity risk score for the vendor is low and the risk factor indicates a high risk level, the weighting of the relationship may result in a lower cybersecurity risk score for the company. If the cybersecurity risk score for the vendor is high, the weighting factor may result in no change or only a slight decrease to the cybersecurity score of the company. In an embodiment, the risk factors and weights may be stored at the data storage 170 of FIG. 1. Such information may be used to monitor and identify trends in cybersecurity levels of various entities. It is noted that in some embodiments, the cybersecurity risk score for a company may be increased or decreased based on relationships that the company has with many different vendors. In an embodiment, the relationships from which the cybersecurity risk score is modified or adjusted may be direct relationships (e.g., when the company is a direct client of the vendor), indirect relationships (e.g., when the company utilizes

a vendor, and the vendor in turn utilizes another vendor to provide the service/solution to the company), or a combination thereof. As a result of the modifications or adjustment to the cybersecurity risk score of the company, a cybersecurity risk score 812 may be generated and stored in the database (e.g., the data storage 170 of FIG. 1).

[0066] The cybersecurity risk score 812 may be provided to a third party that may be interested in the aggregate cybersecurity risk for a company (e.g., the cybersecurity risk of the company, as may be impacted by the company's relationships, whether direct or indirect, with one or more vendors). For example, when an insurance provider is assessing the cybersecurity risk of a company in connection with underwriting an insurance policy covering costs associated with breaches of information security, the insurance provider may desire to consider how any vendors that the potential insured company has relationships with, as those relationships may change how the insurance company views the cybersecurity risk of the company. For example, if the potential insured has a high level of cybersecurity, but exchanges and stores data with several vendors who have a low level of cybersecurity, the aggregate cybersecurity risk of the potential insured may be higher (e.g., greater risk) than the cybersecurity risk of the potential insured alone.

[0067] In some embodiments, the system 800 may be configured to periodically refresh the relationship information. For example, after a threshold period of time has elapsed, the system 800 may capture another snapshot of relationships between various entities using the techniques described above. This may allow the system 800 to keep the cybersecurity risk scores up-to-date with the most recent set of relationship information for each entity included in the analysis. For example, when a first snapshot is taken and the cybersecurity risk scores are calculated, a first company may have a relationship with a first vendor having poor cybersecurity, which may negatively impact the aggregate cybersecurity risk score for the first company, as described above. However, a second snapshot may be captured after some threshold time period has elapsed since the first snapshot was taken, and the information captured in the second snapshot may indicate that the first company no longer has a relationship with the first vendor, and instead has a new relationship with a second vendor having a good cybersecurity posture, which may result in the weighting and scoring modules modifying or adjusting the aggregate cybersecurity risk score for the first company to indicate an improved or

higher level of cybersecurity (e.g., an improved cybersecurity risk score), and lower cybersecurity risk. In an additional or alternative embodiment, the scoring module 810 may be configured to determine the cybersecurity risk score for various entities without applying weights to the relationship information, as indicated by the arrow 864. Using relationship information, whether weighted or unweighted, to determine an entity's cybersecurity risk score may improve the accuracy of the cybersecurity risk scores by accounting for how those relationships impact the cybersecurity of the entity being scored. Thus, embodiments of the present disclosure improve the functioning of a computer programmed to determine cybersecurity risk score, and improve the technical field of assessing cybersecurity risks associated with entities. In an embodiment, the scoring module 810 may be configured to determine, at least in part, cybersecurity scores using one or more of the techniques described in commonly-owned and co-pending U.S. Patent Application No. 14/702,661, entitled "CALCULATING AND BENCHMARKING AN ENTITY'S CYBERSECURITY RISK SCORE," the contents of which are incorporated herein by reference in its entirety, and then weight an entity's cybersecurity score based on the weighted relationship information and cybersecurity risk scores of the entities having relationships with the entity.

[0068] Referring to FIG. 9, a flow diagram of a method for non-intrusively discovering relationships between organizations according to embodiments is shown as a method 900. In an embodiment, the method 600 may be stored in a computer-readable storage medium as instructions that, when executed by one or more processors, cause the one or more processors to perform the operations of the method 600. In an embodiment, the method 600 may be performed by the relationship server 110 of FIG. 1, by the system 200 of FIG. 2, or a combination thereof.

[0069] At 910, the method 900 includes executing, by one or more processors, a first routine to generate a candidate universal resource locator (URL) associated with a first vendor. In an embodiment, the candidate URL may comprise first information corresponding to a website associated with the first vendor and second information associated with the first company, where the first vendor and the first company are different, as described with reference to FIG. 2. At 920, the method 900 includes executing, by the one or more processors, a second routine to determine whether the candidate URL corresponds to a valid website of the first vendor, and, in response to a determination that the candidate URL corresponds to a valid

website of the first vendor, the method 900 may include, at 930, executing, by the one or more processors, a third routine to analyze content of the website of the first vendor to determine whether the content includes information that relates to the first company. In an embodiment, the presence of information that relates to the first company within the content of the website of the first vendor may indicate a relationship between the first company and the first vendor. At 940, the method 900 includes generating relationship information. In an embodiment, the relationship information may be the relationship information 262 described with reference to FIG. 2, or may be the weighted relationship information 272 of FIG. 2. In an embodiment, the relationship information may be stored in a database, such as the data store 170 of FIG. 1.

[0070] In an additional or alternative embodiment, the relationship information may be used to determine various other types of information associated with the first company and/or the first vendor, such as whether the first company or first vendor is adding new relationships, losing relationships, etc., as described above with reference to FIG. 2. The operations of the method 900 for discovering organizational relationships may be performed in a non-intrusive manner. In an embodiment, additional data sources and techniques may be used to validate or otherwise confirm the relationship, such as using the quality control analysis module 250 and the other data sources module 280 of FIG. 2.

[0071] Although the present invention and its advantages have been described in detail, it should be understood that various changes, substitutions and alterations can be made herein without departing from the spirit and scope of the invention as defined by the appended claims. Moreover, the scope of the present application is not intended to be limited to the particular embodiments of the process, machine, manufacture, composition of matter, means, methods and steps described in the specification. As one of ordinary skill in the art will readily appreciate from the disclosure of the present invention, processes, machines, manufacture, compositions of matter, means, methods, or steps, presently existing or later to be developed that perform substantially the same function or achieve substantially the same result as the corresponding embodiments described herein may be utilized according to the present invention. Accordingly, the appended claims are intended to include within their scope such processes, machines, manufacture, compositions of matter, means, methods, or steps.

CLAIMS

What is claimed is:

1. A method for adjusting a cybersecurity score of a first company based on a cybersecurity posture of one or more vendors that have a relationship with the first company through analysis of content of one or more vendor websites containing information that relates to the first company, the method comprising:

executing, by one or more processors, a first routine to generate a candidate universal resource locator (URL) associated with a first vendor, wherein the candidate URL comprises first information corresponding to a website associated with the first vendor and second information associated with the first company, and wherein the first vendor and the first company are different;

executing, by the one or more processors, a second routine to determine whether the candidate URL corresponds to a valid website of the first vendor;

in response to a determination that the candidate URL corresponds to a valid website of the first vendor, executing, by the one or more processors, a third routine to analyze content of the website of the first vendor to determine whether the content includes information that relates to the first company, wherein the presence of information that relates to the first company within the content of the website of the first vendor indicates a relationship between the first company and the first vendor;

in response to a determination that the content of the website of the first vendor includes information that relates to the first company, executing, by the one or more processors, a fourth routine to determine a cybersecurity risk score for the first vendor; and

executing, by the one or more processors, a fifth routine to adjust a cybersecurity risk score for the first company based on the cybersecurity risk score for the first vendor.

2. The method of claim 1, wherein the first information corresponds to a domain of the first vendor, and wherein the second information corresponds to a subdomain within the domain of the first vendor that is associated with the first company.

3. The method of claim 1, wherein the first information corresponds to a domain of the first vendor, and wherein the second information corresponds to a directory within the domain of the first vendor that is associated with the first company.

4. The method of claim 1, wherein analyzing the content of the website includes analysis of source code of the website, analysis of image content included of the website, analysis of text content of the website, traversal of one or more links of the website to identify additional content of the website that is to be analyzed, or a combination thereof.

5. The method of claim 1, wherein the method further comprises executing, by the one or more processors, a seventh routine to identify additional relationships between the first company and additional vendors that are different from the first vendor based on other information sources, wherein the other information sources include network footprints of one or more of the additional vendors, social network information, press release information for one or more of the additional vendors, or a combination thereof.

6. The method of claim 1, wherein the method further comprises:

determining a risk factor based on the relationship between the first company and the first vendor, wherein the risk factor represents the affect that a breach of the first vendor's cybersecurity will expose sensitive data of the first company; and

determining a weighting factor associated with the risk factor, wherein the cybersecurity score of the first company is determined based, at least in part, on the risk factor.

7. The method of claim 6, wherein the method further comprises:

identifying relationships between the first company and one or more additional vendors that are different that the first vendor;

determining a cybersecurity risk score for each of the one or more additional vendors; and

adjusting the cybersecurity risk score of the first company based, at least in part, on the cybersecurity risk scores for each of the one or more additional vendors that have relationships with the first company.

8. The method of claim 7, wherein the method further comprises weighting the adjustments to the cybersecurity risk score of the first company based on the cybersecurity scores of each of the one or more additional vendors.

9. The method of claim 7, wherein the method further comprises generating a graph that depicts the relationships between the first company and the first vendor and between the first company and each of the one or more additional vendors.

10. The method of claim 7, wherein the method further comprises determining the cybersecurity risk score for the first vendor based on cybersecurity risk scores of other vendors that have relationships with the first vendor.

11. The method of claim 1, wherein the method further comprises:

in response to the determination that the content of the website of the first vendor includes information that is unique to the first company, generating, by the one or more processors, a plurality of additional candidate URLs, wherein each of the plurality of additional candidate URLs comprises the same first information as the candidate URL and different second information, and wherein the different second information corresponds to additional companies different from the first company;

executing, by the one or more processors, the second routine with respect to each of the plurality of additional candidate URLs to identify additional valid websites of the first vendor;

in response to identifying the additional websites of the first vendor, executing, by the one or more processors, the third routine to analyze content of each of the additional websites to determine whether any of the additional websites include information that relates to one of the additional companies, wherein the presence of information that relates to one of the additional companies within the content of the additional websites of the first vendor indicates a relationship between the first vendor and each of the additional companies; and

executing, by the one or more processors, the fifth routine to determine a cybersecurity risk score for each of the additional companies based, at least in part, on the cybersecurity risk score of the first vendor.

12. The method of claim 1, wherein the method further comprises:

executing, by the one or more processors, the first routine to generate a plurality of additional candidate URLs, wherein each of the plurality of additional candidate URLs comprises the different first information and the same second information, and wherein, for each of the plurality of additional candidate URLs, the different first information corresponds to a vendor other than the first vendor;

executing, by the one or more processors, the second routine with respect to each of the plurality of additional candidate URLs to identify valid websites of different vendors;

in response to identifying the valid websites of the different vendors, executing, by the one or more processors, the third routine to analyze content of each of the valid websites to determine whether any of the valid websites include information that relates to the first company, wherein the presence of information that is unique to the first company within the content of one of the valid websites of the different vendors indicates a relationship between the first company and one of the different vendors;

executing, by the one or more processors, the fourth routine to determine a cybersecurity risk score for each of the different vendors; and

executing, by the one or more processors, the fifth routine to adjust the cybersecurity risk score of the first company based, at least in part, on the cybersecurity risk score of each of the different vendors having a relationship with the first company.

13. A non-transitory computer-readable storage medium storing instructions that, when executed by one or more processors, cause the one or more processors to perform operations for adjusting a cybersecurity score of a first company based on a cybersecurity posture of one or more vendors that have a relationship with the first company through analysis of content of one or more vendor websites containing information that relates to the first company, the operations comprising:

executing a first routine to generate a candidate universal resource locator (URL) associated with a first vendor, wherein the candidate URL comprises first information corresponding to a website associated with the first vendor and second information associated with the first company, and wherein the first vendor and the first company are different;

executing a second routine to determine whether the candidate URL corresponds to a valid website of the first vendor;

in response to a determination that the candidate URL corresponds to a valid website of the first vendor, executing a third routine to analyze content of the website of the first vendor to determine whether the content includes information that relates to the first company, wherein the presence of information that relates to the first company within the content of the website of the first vendor indicates a relationship between the first company and the first vendor;

executing a fourth routine to determine a cybersecurity risk score for the first vendor; and

executing a fifth routine to adjust a cybersecurity risk score for the first company based, at least in part, on the cybersecurity risk score of the first vendor.

14. The non-transitory computer-readable storage medium of claim 13, wherein the first information corresponds to a domain of the first vendor, and wherein the second information corresponds to a subdomain within the domain of the first vendor that is associated with the first company.

15. The non-transitory computer-readable storage medium of claim 13, wherein the first information corresponds to a domain of the first vendor, and wherein the second information corresponds to a directory within the domain of the first vendor that is associated with the first company.

16. The non-transitory computer-readable storage medium of claim 13, wherein analyzing the content of the website includes analysis of source code of the website, analysis of image content included of the website, analysis of text content of the website, traversal of one or more links of the website to identify additional content of the website that is to be analyzed, or a combination thereof.

17. The non-transitory computer-readable storage medium of claim 13, wherein the operations further comprise executing a seventh routine to identify additional relationships between the first company and additional vendors that are different from the first vendor based on other information sources, wherein the other information sources include network footprints of one or more of the additional vendors, social network information, press release information for one or more of the additional vendors, or a combination thereof.

18. The non-transitory computer-readable storage medium of claim 13, wherein the operations further comprise:

determining a risk factor based on the relationship between the first company and the first vendor, wherein the risk factor represents the affect that a breach of the first vendor's cybersecurity will expose sensitive data of the first company; and

determining a weighting factor associated with the risk factor, wherein the cybersecurity score of the first company is adjusted based, at least in part, on the risk factor.

19. The non-transitory computer-readable storage medium of claim 18, wherein the operations further comprise:

identifying relationships between the first company and one or more additional vendors that are different that the first vendor;

determining a cybersecurity risk score for each of the one or more additional vendors; and

adjusting the cybersecurity risk score of the first company based, at least in part, on the cybersecurity risk scores for each of the one or more additional vendors that have relationships with the first company.

20. The non-transitory computer-readable storage medium of claim 19, wherein the operations further comprise weighting the cybersecurity risk score of the first company based on the cybersecurity scores of each of the one or more additional vendors.

21. The non-transitory computer-readable storage medium of claim 19, wherein the operations further comprise generating a model that graphically depicts the relationships between the first company and the first vendor and between the first company and each of the one or more additional vendors.

22. The non-transitory computer-readable storage medium of claim 13, wherein the operations further comprise:

periodically determining whether any changes have occurred with respect to one or more previously identified relationships between the first company the one or more vendors; and

recalculating the cybersecurity risk score for the first company based on any changes that have occurred with respect to one or more previously identified relationships between the first company the one or more vendors.

23. A system for adjusting a cybersecurity score of a first company based on a cybersecurity posture of one or more vendors that have a relationship with the first company through analysis of content of one or more vendor websites containing information that relates to the first company, the system comprising:

a memory; and

one or more processors coupled to the memory, the one or more processors configured to:

execute a first routine to generate a candidate universal resource locator (URL) associated with a first vendor, wherein the candidate URL comprises first information corresponding to a website associated with the first vendor and second information associated with the first company, and wherein the first vendor and the first company are different;

execute a second routine to determine whether the candidate URL corresponds to a valid website of the first vendor;

execute a third routine to analyze content of the website of the first vendor to determine whether the content includes information that is unique to the first company in response to a determination that the candidate URL corresponds to a valid website of the first vendor, wherein the presence of information that relates to the first company within the content of the website of the first vendor indicates a relationship between the first company and the first vendor;

execute a fourth routine to determine a cybersecurity risk score for the first vendor; and

execute a fifth routine to adjust a cybersecurity risk score for the first company based, at least in part, on the cybersecurity risk score of the first vendor.

24. The system of claim 23, wherein the first information corresponds to a domain of the first vendor, and wherein the second information corresponds to a subdomain within the domain of the first vendor that is associated with the first company.

25. The system of claim 23, wherein the first information corresponds to a domain of the first vendor, and wherein the second information corresponds to a directory within the domain of the first vendor that is associated with the first company.

26. The system of claim 23, wherein analyzing the content of the website includes analysis of source code of the website, analysis of image content included of the website, analysis of text content of the website, traversal of one or more links of the website to identify additional content of the website that is to be analyzed, or a combination thereof.

27. The system of claim 23, wherein the one or more processors are configured to execute a seventh routine to identify additional relationships between the first company and additional vendors that are different from the first vendor based on other information sources, wherein the other information sources include network footprints of one or more of the additional vendors, social network information, press release information for one or more of the additional vendors, or a combination thereof.

28. The system of claim 23, wherein the one or more processors are configured to :

determine a risk factor based on the relationship between the first company and the first vendor, wherein the risk factor represents the affect that a breach of the first vendor's cybersecurity will expose sensitive data of the first company; and

determine a weighting factor associated with the risk factor, wherein the adjustment of the cybersecurity score of the first company is determined based, at least in part, on the risk factor.

29. The system of claim 28, wherein the one or more processors are configured to:

identify relationships between the first company and one or more additional vendors that are different that the first vendor;

determine a cybersecurity risk score for each of the one or more additional vendors; and

adjust the cybersecurity risk score of the first company based, at least in part, on the cybersecurity risk scores for each of the one or more additional vendors.

30. The system of claim 29, wherein one or more processors are configured to weight the adjustment to the cybersecurity risk score of the first company based on the cybersecurity scores of each of the one or more additional vendors.

Black Kite Ex. 1002, Page 209 of 1060

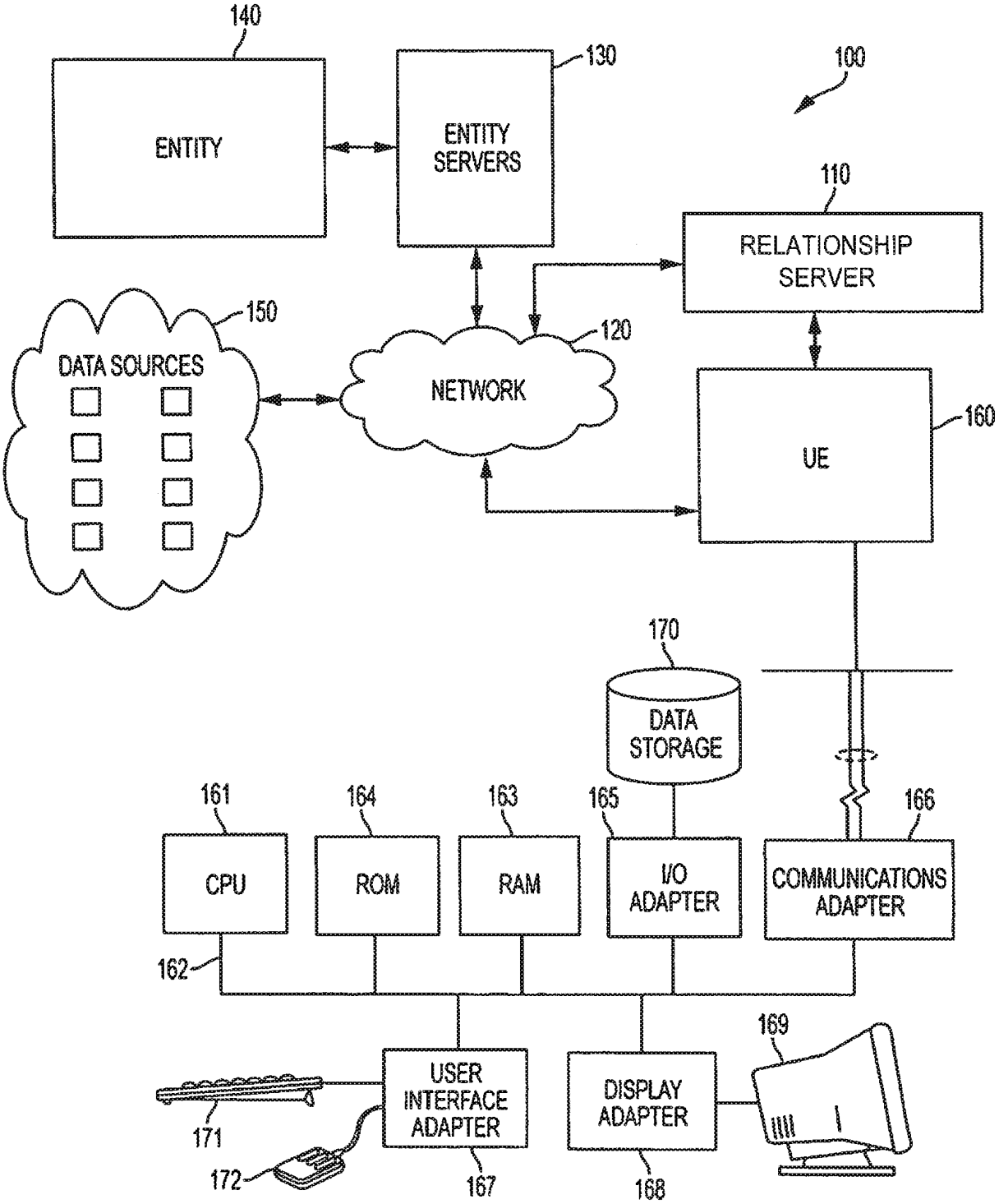

140
ENTITY
130
ENTITY SERVERS
100
110
RELATIONSHIP SERVER
150
DATA SOURCES
120
NETWORK
160
UE
170
DATA STORAGE
161
CPU
164
ROM
163
RAM
165
I/O ADAPTER
166
COMMUNICATIONS ADAPTER
162
169
USER INTERFACE ADAPTER
DISPLAY ADAPTER
171
172
167
168

FIG. 1

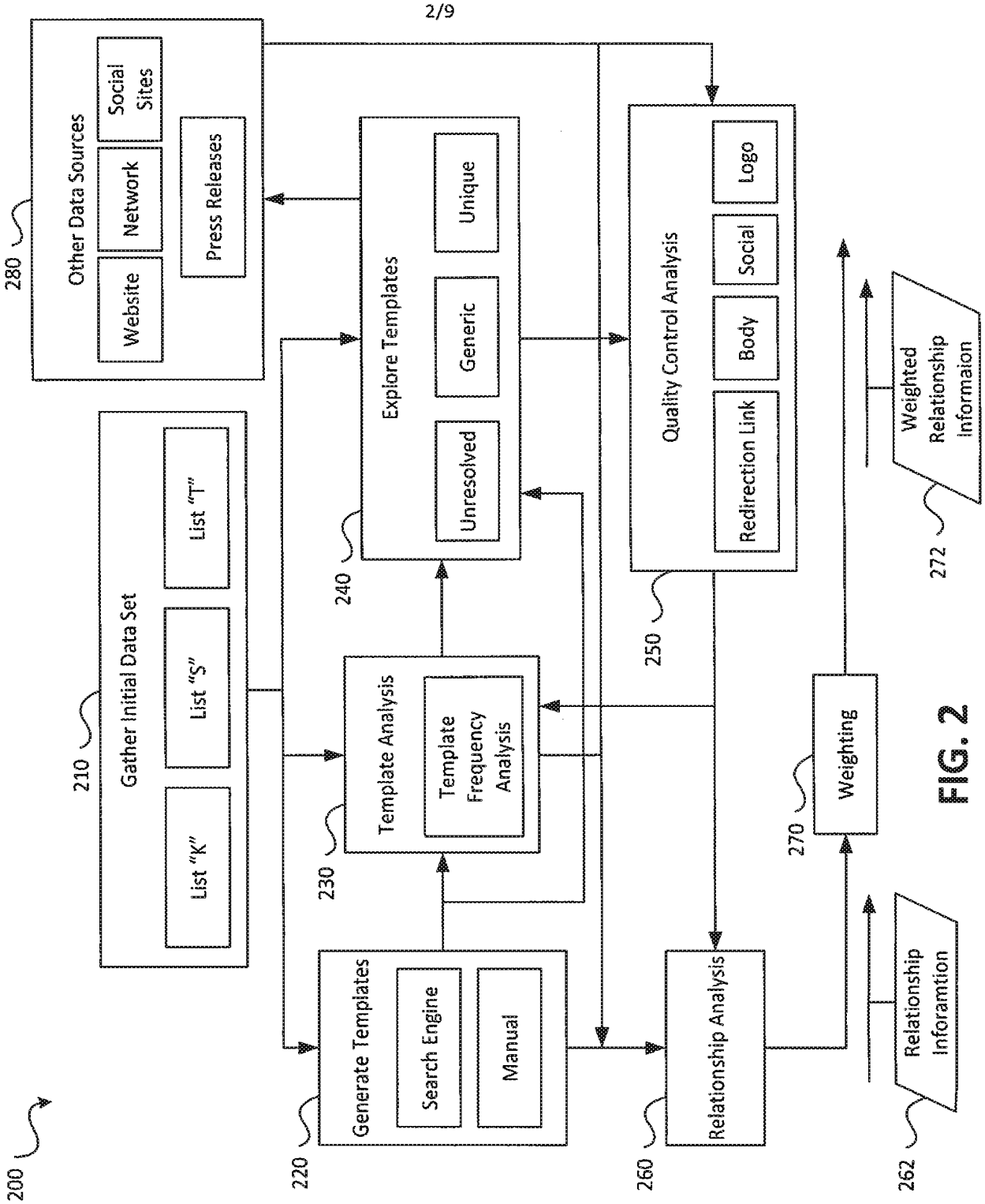

200
Other Data Sources
280
Website
Network
Social Sites
Press Releases
Gather Initial Data Set
210
List "K"
List "S"
List "T"
Explore Templates
240
Unresolved
Generic
Unique
Quality Control Analysis
250
Redirection Link
Body
Social
Logo
Template Analysis
230
Template Frequency Analysis
Generate Templates
220
Search Engine
Manual
Relationship Analysis
260
Weighting
270
Weighted Relationship Informaion
272
Relationship Inforamtion
262

FIG. 2

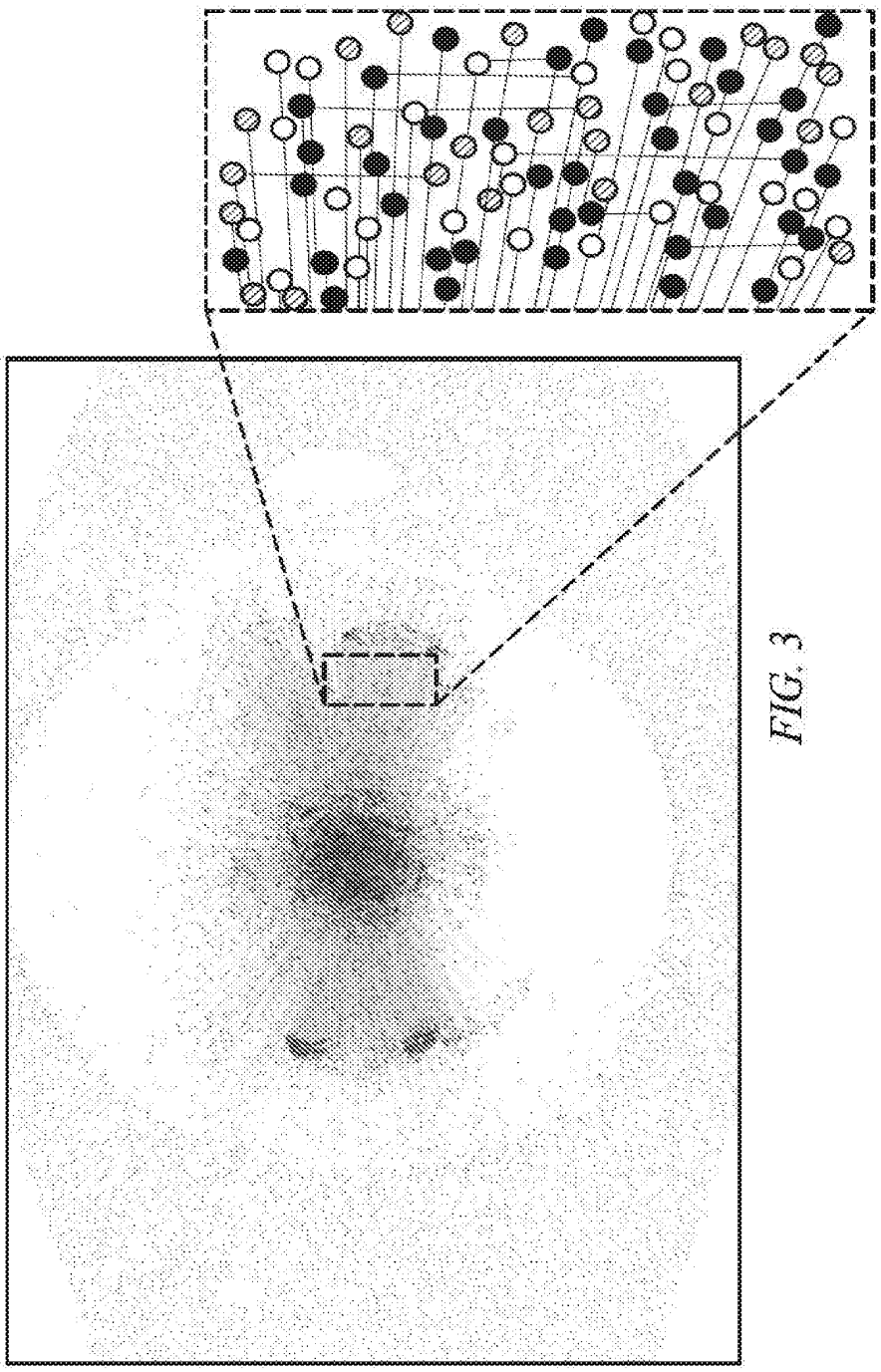


FIG. 3

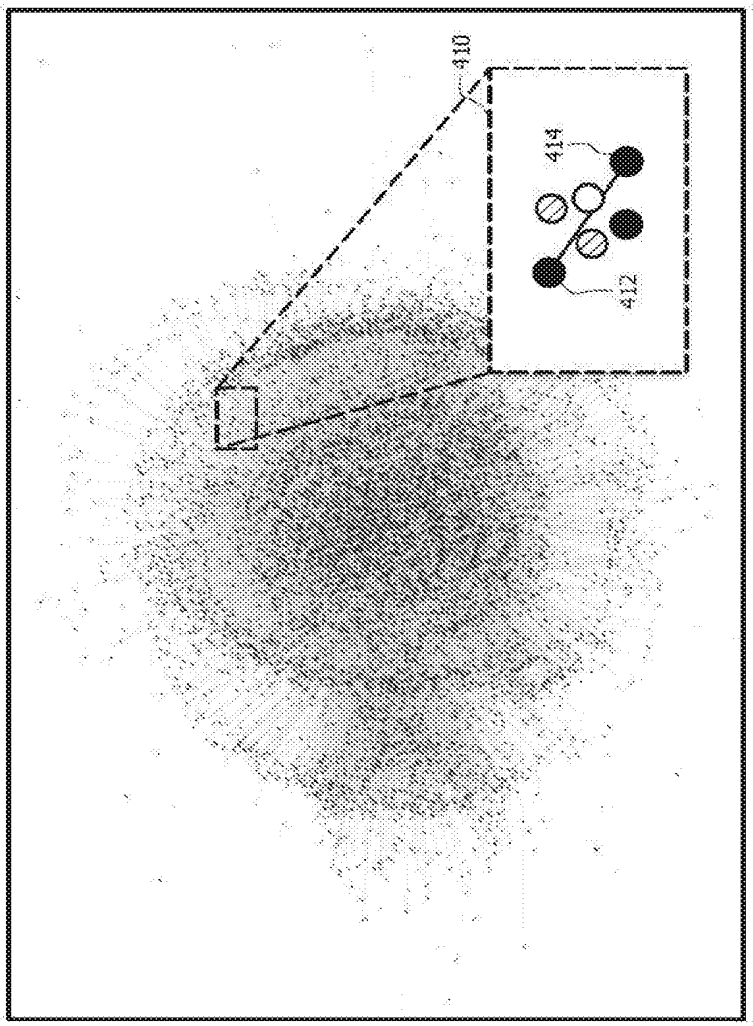


FIG. 4

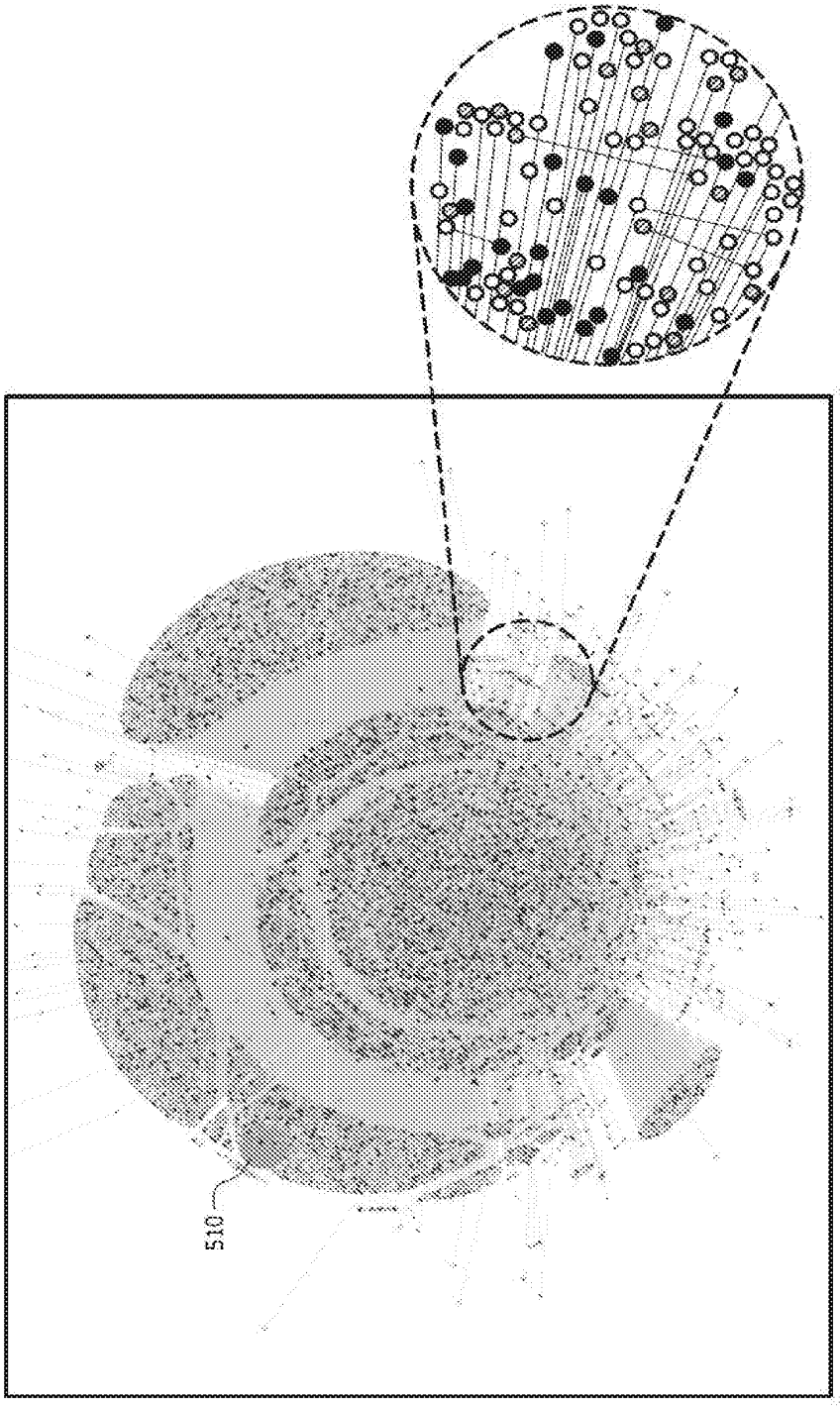


FIG. 5

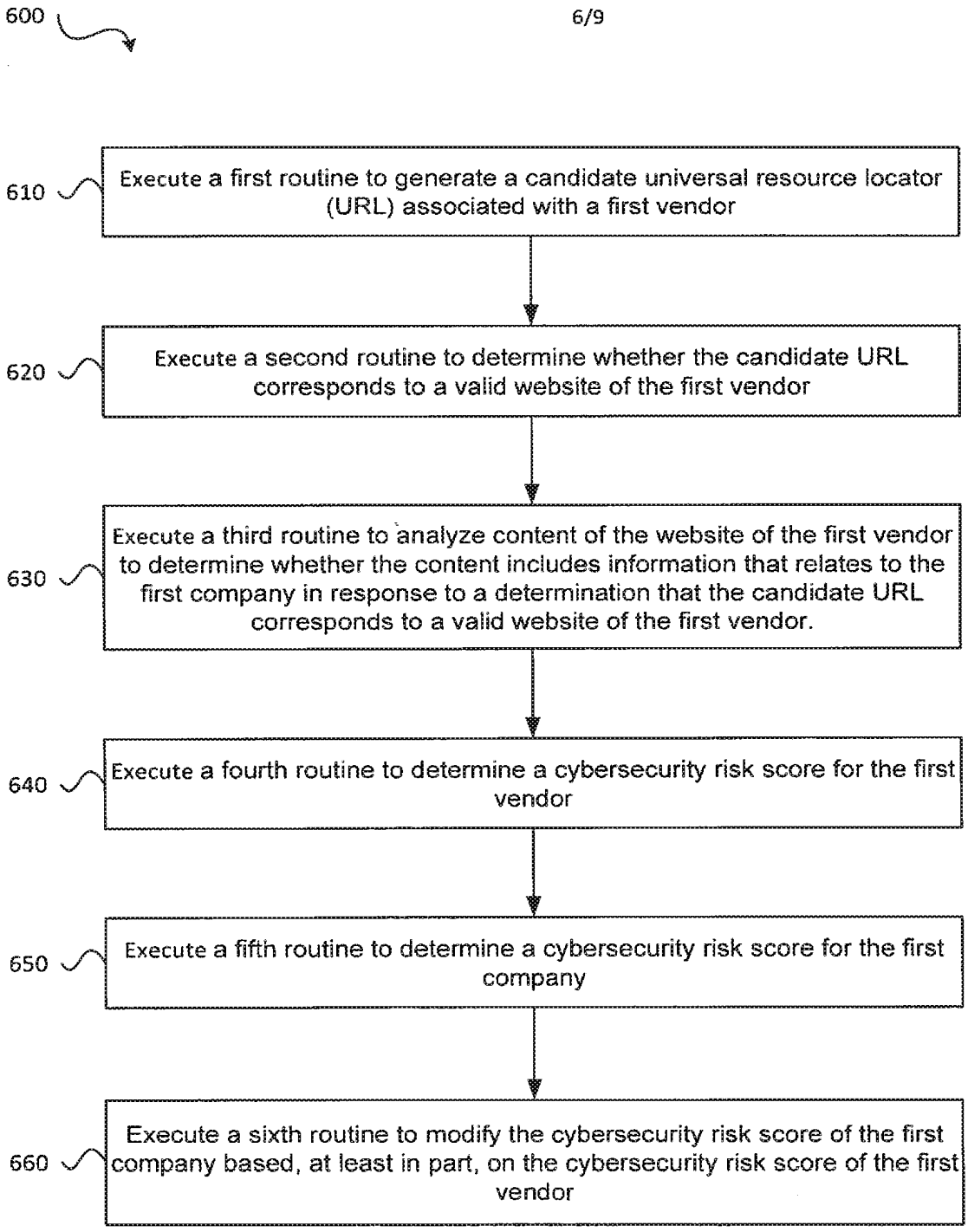

600
610
Execute a first routine to generate a candidate universal resource locator (URL) associated with a first vendor
620
Execute a second routine to determine whether the candidate URL corresponds to a valid website of the first vendor
630
Execute a third routine to analyze content of the website of the first vendor to determine whether the content includes information that relates to the first company in response to a determination that the candidate URL corresponds to a valid website of the first vendor.
640
Execute a fourth routine to determine a cybersecurity risk score for the first vendor
650
Execute a fifth routine to determine a cybersecurity risk score for the first company
660
Execute a sixth routine to modify the cybersecurity risk score of the first company based, at least in part, on the cybersecurity risk score of the first vendor

FIG. 6

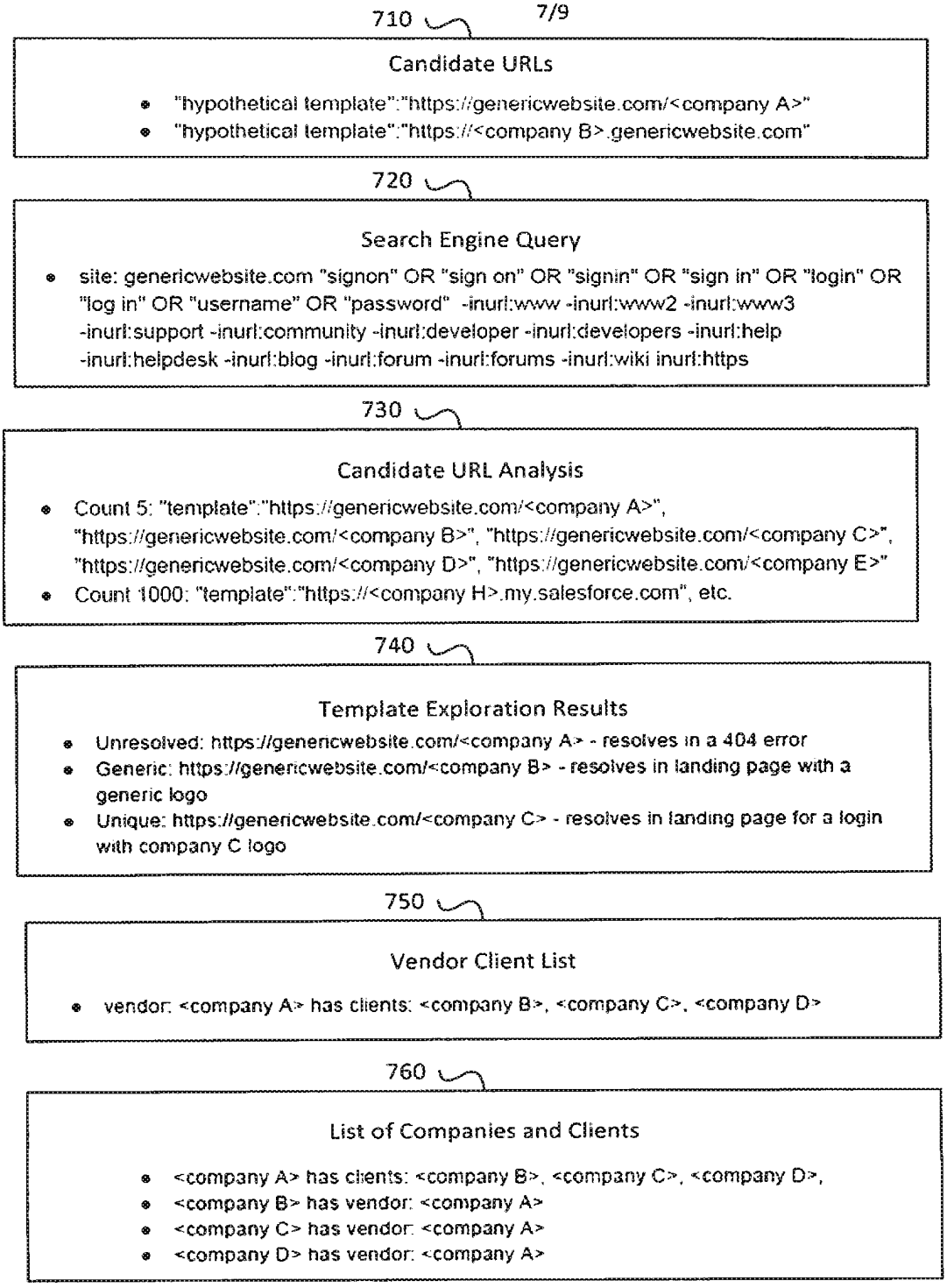

710
Candidate URLs
"hypothetical template":"https://genericwebsite.com/<company A>"
"hypothetical template":"https://<company B>.genericwebsite.com"
720
Search Engine Query
site: genericwebsite.com "signon" OR "sign on" OR "signin" OR "sign in" OR "login" OR "log in" OR "username" OR "password" -inurl:www -inurl:www2 -inurl:www3 -inurl:support -inurl:community -inurl:developer -inurl:developers -inurl:help -inurl:helpdesk -inurl:blog -inurl:forum -inurl:forums -inurl:wiki inurl:https
730
Candidate URL Analysis
Count 5: "template":"https://genericwebsite.com/<company A>", "https://genericwebsite.com/<company B>", "https://genericwebsite.com/<company C>", "https://genericwebsite.com/<company D>", "https://genericwebsite.com/<company E>"
Count 1000: "template":"https://<company H>.my.salesforce.com", etc.
740
Template Exploration Results
Unresolved: https://genericwebsite.com/<company A> - resolves in a 404 error
Generic: https://genericwebsite.com/<company B> - resolves in landing page with a generic logo
Unique: https://genericwebsite.com/<company C> - resolves in landing page for a login with company C logo
750
Vendor Client List
vendor: <company A> has clients: <company B>, <company C>, <company D>
760
List of Companies and Clients
<company A> has clients: <company B>, <company C>, <company D>,
<company B> has vendor: <company A>
<company C> has vendor: <company A>
<company D> has vendor: <company A>

FIG. 7

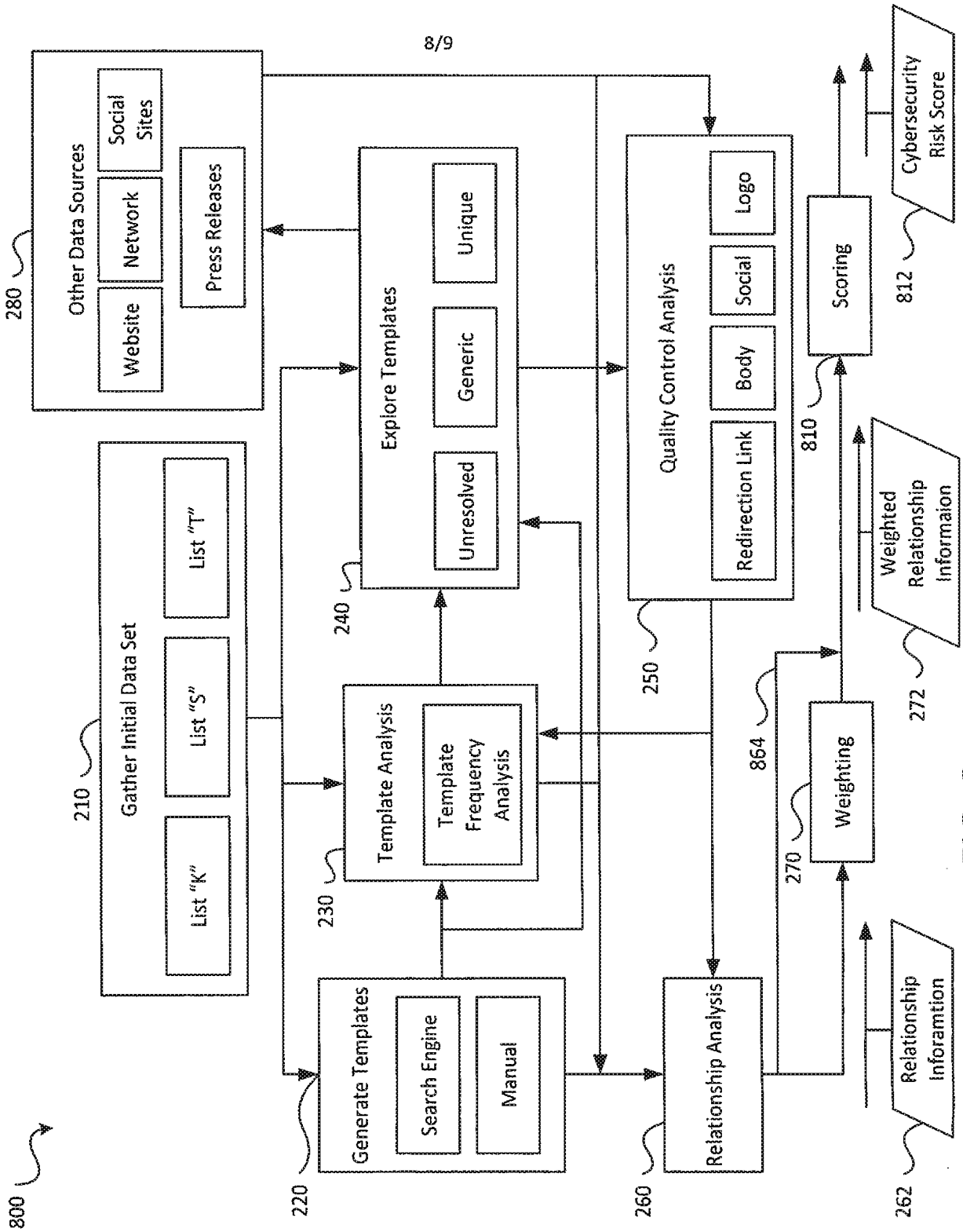

800
Other Data Sources
Website
Network
Social Sites
Press Releases
280
Gather Initial Data Set
List "K"
List "S"
List "T"
210
Generate Templates
Search Engine
Manual
220
Template Analysis
Template Frequency Analysis
230
Explore Templates
Unresolved
Generic
Unique
240
Quality Control Analysis
Redirection Link
Body
Social
Logo
250
Relationship Analysis
260
Relationship Inforamtion
262
Weighting
270
Weighted Relationship Informaion
272
Scoring
810
Cybersecurity Risk Score
812
864

FIG. 8

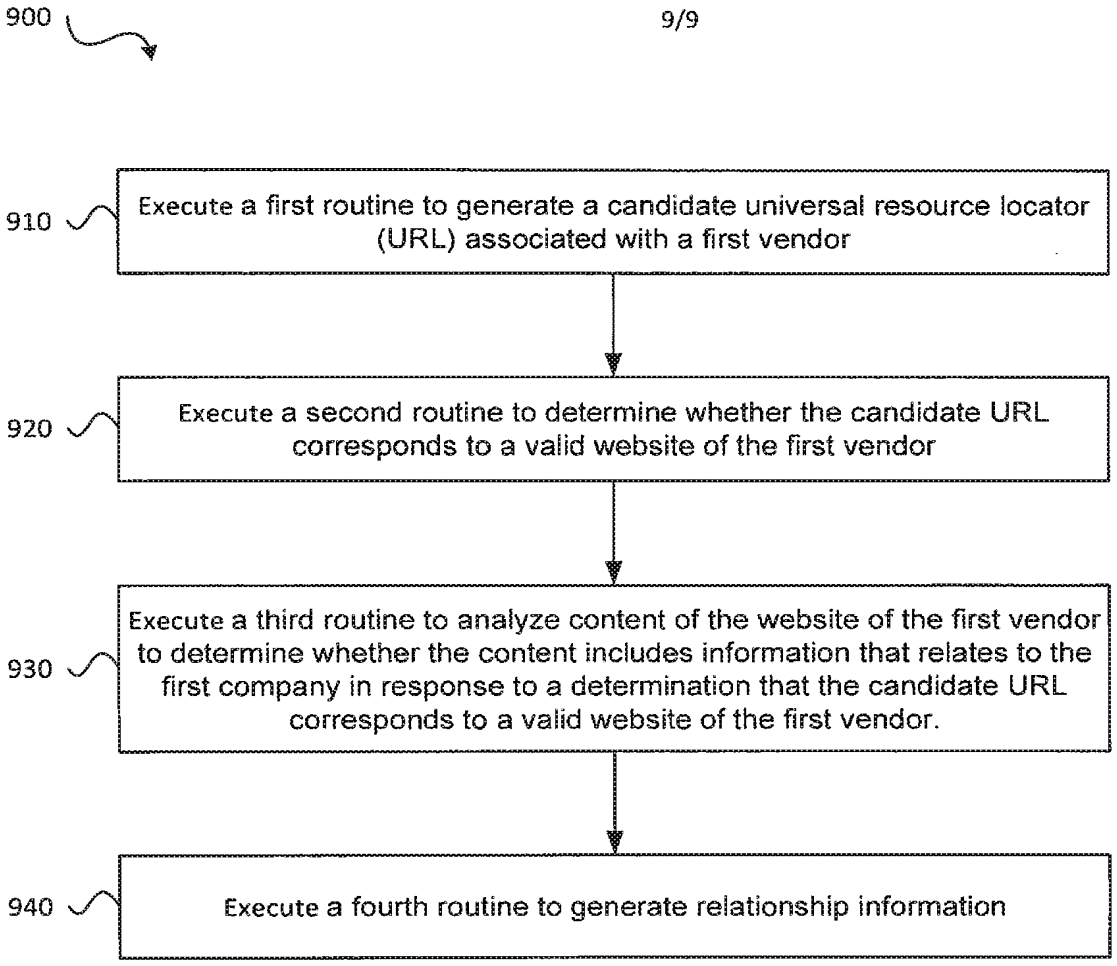

900
910
Execute a first routine to generate a candidate universal resource locator (URL) associated with a first vendor
920
Execute a second routine to determine whether the candidate URL corresponds to a valid website of the first vendor
930
Execute a third routine to analyze content of the website of the first vendor to determine whether the content includes information that relates to the first company in response to a determination that the candidate URL corresponds to a valid website of the first vendor.
940
Execute a fourth routine to generate relationship information

FIG. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US17/15483

A. CLASSIFICATION OF SUBJECT MATTER
IPC: **G06Q 10/00**(2012.01)

CPC: 705/007.240
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
CPC : 705/007.240

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2010/0186088 A1 (BANERJEE et al) 22 July 2010 (22.07.2010), see entire documents.	1-30
Y	US 2008/0270209 A1 (MAUSETH et al) 30 October 2008 (30.10.2008), see entire documents.	1-30

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
15 February 2017 (15.02.2017)

Date of mailing of the international search report
23 FEB 2017

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (571) 273-8300

Authorized officer
John Nguyen
Telephone No. 571-272-6952

Form PCT/ISA/210 (second sheet) (April 2007)

Continuation of B. FIELDS SEARCHED Item 3:
US-PGPUB, USPAT, USOCR, EPO, JPO, DERWENT, IBM_TDB: website, risk, near, web, hyperlink, advertise, market, link, webpage, score, same, analyze, manage, threshold, control, project, planning, assess, monitor, supervise, track, quantify, value, number, output, plan, administer, assessment, contract, assignment, job, tracking, characteristic, requirement, amount, valuation, reconcile, correspond, quantity, attribute, factor, correlate, parameter, variance, match, appraise, valuation.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 January 2019 (31.01.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/023045 A1

(51) International Patent Classification:
G06F 15/16 (2006.01) *G06Q 10/06* (2012.01)
G06F 17/30 (2006.01) *H04L 29/06* (2006.01)
G06F 21/57 (2013.01)

(21) International Application Number:
PCT/US2018/042957

(22) International Filing Date:
19 July 2018 (19.07.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
15/663,541 28 July 2017 (28.07.2017) US
16/019,243 26 June 2018 (26.06.2018) US

(71) Applicant: **SECURITYSCORECARD, INC.** [US/US]; 214 W. 29th Street, 5th Floor, New York, New York 10001 (US).

(72) Inventors: **MO, Jue**; Security Scorecard, Inc., 214 W. 29th Street, 5th Floor, New York, New York 10001 (US). **VARGAS, Luis**; Security Scorecard, Inc., 214 W. 29th Street, 5th Floor, New York, New York 10001 (US). **SOHVAL, A. Robert**; Security Scorecard, Inc., 214 W. 29th Street, 5th Floor, New York, New York 10001 (US).

(74) Agent: **GREESON, Robert L**; Norton Rose Fulbright US LLP, 2200 Ross Avenue, Suite 3600, Dallas, Texas 75201-7932 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

(54) Title: REDUCING CYBERSECURITY RISK LEVEL OF A PORTFOLIO OF COMPANIES USING A CYBERSECURITY RISK MULTIPLIER

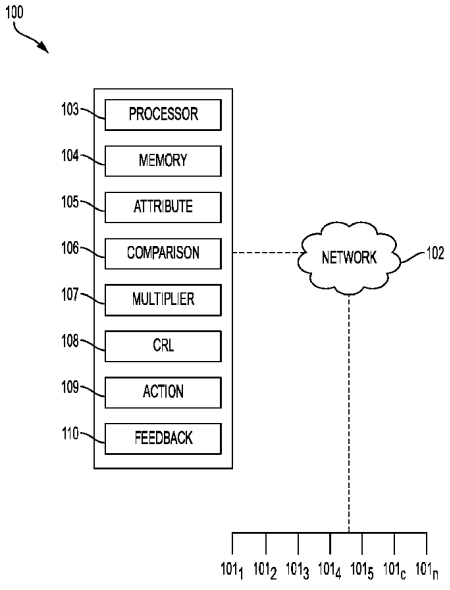


FIG. 1

(57) Abstract: A multiplier is utilized to quantify a cybersecurity risk level of a portfolio of entities (e.g., companies) and enable actions to mitigate that quantified risk. In doing so, features or attributes of one or more companies in a portfolio are compared to features or attributes of one or more companies that experienced an adverse cybersecurity event (e.g. a data breach). Further, a degree of dependency, such as a matrix of a number of shared vendors and the proximity of those vendors to the companies, can be measured between (1) portfolio companies and one or more companies that experienced a cybersecurity event, and/or (2) the portfolio companies themselves to better quantify the risk. That is, to more meaningfully analyze a cybersecurity event that occurred at one or more companies and better predict the likelihood of an occurrence at portfolio companies, embodiments can determine an n-degree interdependency between companies.

WO 2019/023045 A1

[Continued on next page]

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))*

Published:

— *with international search report (Art. 21(3))*

REDUCING CYBERSECURITY RISK LEVEL OF A PORTFOLIO OF COMPANIES USING A CYBERSECURITY RISK MULTIPLIER

PRIORITY CLAIMS AND CROSS REFERENCE TO RELATED PATENT APPLICATIONS

[0001] This application claims priority to and the benefit of U.S. Utility Patent Application No. 15/663,541 filed July 28, 2017, entitled "REDUCING CYBERSECURITY RISK LEVEL OF A PORTFOLIO OF COMPANIES USING A CYBERSECURITY RISK MULTIPLIER" (Attorney Docket No. SCOR.P0009US); and to a Continuation U.S. Patent Application No. 16/019,243 filed June 26, 2018, entitled "REDUCING CYBERSECURITY RISK LEVEL OF A PORTFOLIO OF COMPANIES USING A CYBERSECURITY RISK MULTIPLIER" (Attorney Docket No. SCOR.P0009USC1); and is related to commonly-owned U.S. Patent Application No. 15/198,560 filed June 30, 2016, and entitled "NON-INTRUSIVE TECHNIQUES FOR DISCOVERING AND USING ORGANIZATIONAL RELATIONSHIPS" (Attorney Docket No. SCOR.P0008US.C1), the disclosures of which are hereby incorporated herein by reference in their entirety.

TECHNICAL FIELD

[0002] The disclosed technology generally relates to reducing a cybersecurity risk level of a portfolio of companies. In particular, the disclosed technology relates to identifying common attributes between companies and their relevance to a cybersecurity risk for portfolio companies, quantifying the risk level using a multiplier, and enabling steps to reduce the risk level.

BACKGROUND OF THE INVENTION

[0003] A manager of a portfolio of companies may be interested in understanding the portfolio's aggregate cyber security risk level because, once understood, the manager can take action to manage or reduce that risk. Doing so can be advantageous in a number of scenarios where, e.g., an insurance company underwriting cyber-insurance needs to minimize the chance of catastrophic loss due to correlated risk, or an organization needs to minimize its exposure to breach or business interruption stemming from its vendors (e.g., third party vendor risk management). Examples of such adverse cybersecurity events include Distributed Denial of Service (DDoS) and the like, which lead to significant business interruption.

[0004] Currently available technologies for managing a portfolio's cybersecurity risk level suffer from certain drawbacks. For example, while certain technologies determine how diverse a set of companies may be, they do not provide meaningful information with regard to whether the companies' shared features actually influence or are indicative of the occurrence of a cybersecurity risk event. In other words, known technologies do not meaningfully inform a user of a portfolio's reduced or increased correlated risk of experiencing a cybersecurity event.

BRIEF SUMMARY OF THE INVENTION

[0005] In view of the foregoing, inventive concepts encompass a system and method for utilizing a multiplier to quantify a cybersecurity risk level of a portfolio of entities and enable actions to mitigate that quantified risk. For example, according to one embodiment, a method for reducing a cybersecurity risk level of a portfolio of companies is provided. According to such an embodiment, at least one company that experienced a cybersecurity risk event during a certain time period is identified. Also, at least one attribute common to the at least one identified company that experienced the cybersecurity risk event and a plurality of companies in the portfolio is identified. A degree of mutuality of the at least one attribute is also identified. A cybersecurity risk multiplier for the portfolio is generated based on (1) a number of the identified attributes, (2) a number of the plurality of companies having the identified attributes, and (3) degrees of mutuality of the number of identified attributes. Further, a portfolio cybersecurity risk level is generated that is a function of cybersecurity risk multiplier, and one or more tools are enabled for reducing the generated portfolio cybersecurity risk level.

[0006] According to another embodiment, a system for reducing a cybersecurity risk level of a portfolio of companies is provided. The system comprises a memory communicatively coupled to one or more processors configured to execute a number of steps where, e.g., at least one company that experienced a cybersecurity risk event during a certain time period is identified. Also, at least one attribute common to the at least one identified company that experienced the cybersecurity risk event and a plurality of companies in the portfolio is identified. A degree of mutuality of the at least one attribute is also identified. A cybersecurity risk multiplier for the portfolio is generated based on (1) a number of the identified attributes, (2) a number of the plurality of companies having the identified attributes, and (3) degrees of mutuality of the number of identified attributes. Further, a portfolio cybersecurity risk level is generated that is a function of cybersecurity risk multiplier, and one or more tools are enabled for reducing the generated portfolio cybersecurity risk level.

[0007] The foregoing has outlined rather broadly the features and technical advantages of the present disclosure in order that the detailed description of the disclosure that follows may be better understood. Additional features and advantages of the embodiments will be described hereinafter which form the subject of the claims of the present disclosure. It should be appreciated by those skilled in the art that the conception and specific embodiment disclosed may be readily utilized as a basis for modifying or designing other structures for carrying out the same purposes of the present disclosure. It should also be realized by those skilled in the art that such equivalent constructions do not depart from the scope of the present disclosure as set forth in the appended claims. The novel features which are believed to be characteristic of the embodiments, both as to its organization and method of operation, together with further objects and advantages will be better understood from the following description when considered in connection with the accompanying figures. It is to be expressly understood, however, that each of the figures is provided for the purpose of illustration and description only and is not intended as a definition of the limits of the present disclosure.

BRIEF DESCRIPTION OF THE FIGURES

[0008] For a more complete understanding of the present disclosure, reference is now made to the following descriptions taken in conjunction with the accompanying figures, in which:

[0009] FIGURE 1 shows aspects of a system that quantifies a cybersecurity risk level of a portfolio of companies according to an embodiment;

[0010] FIGURE 2 shows aspects of a method for quantifying a cybersecurity risk level of a portfolio of companies according to an embodiment;

[0011] FIGURE 3A shows a relationship between a risk score and number of shared attributes according to an embodiment;

[0012] FIGURE 3B shows a relationship between the likelihood a company will experience a cybersecurity risk event and a number of attributes it shares with a company that experienced a cybersecurity risk event according to an embodiment;

[0013] FIGURE 4A shows a probability density function of multiplier values for portfolios of companies with different counts for co-occurrence of cyber data breach over two-year time period according to an embodiment;

[0014] FIGURE 4B shows a probability density function of multiplier values for portfolios of companies with different counts for co-occurrence of cyber data breach over one-year time period according to an embodiment;

[0015] FIGURE 5 shows multiplier values as a function of average cybersecurity risk score according to an embodiment;

[0016] FIGURE 6A illustrates clusters of common attributes among companies for portfolio companies that have a high multiplier value and a low total score according to an embodiment;

[0017] FIGURE 6B illustrates clusters of common attributes among companies for portfolio companies that have a low multiplier value and a high total score according to an embodiment; and

[0018] FIGURE 7 shows the probability density functions of multiplier values for different numbers of common attributes according to an embodiment.

DETAILED DESCRIPTION OF THE INVENTION

[0019] Inventive concepts utilize a multiplier to quantify a cybersecurity risk level of a portfolio of entities (e.g., companies) and enable actions to mitigate that quantified risk. In doing so, features or attributes of one or more companies in a portfolio are compared to features or attributes of one or more companies that experienced an adverse cybersecurity event (e.g. a data breach). Further, a degree of dependency, such as a matrix of a number of shared vendors and the similarity (i.e. quantity and type of shared features) of those vendors to the companies, can be measured between (1) portfolio companies and one or more companies that experienced a cybersecurity event, and/or (2) the portfolio companies themselves, to better quantify the risk. That is, to more meaningfully analyze a cybersecurity event that occurred at one or more companies and better predict the likelihood of an occurrence at portfolio companies, embodiments can determine an n-degree interdependency between companies. In other words, embodiments consider not only a number of attributes common to companies (i.e., a first-degree dependency), but also a number of features shared by the common attributes themselves (i.e., a second-degree dependency).

[0020] As an example, two or more companies can be said to have a first-degree dependency if they use the same web host. On the other hand, two or more companies may use

different web hosts, but the web hosts use software from the same upstream vendor in providing their services to the two or more companies. In that case, the two or more companies can be said to have a second-degree dependency because, while they do not use the same web host, they indirectly receive software from the same upstream vendor.

[0021] Analyzing degrees of dependency between a company that experienced a cybersecurity event and companies in a portfolio, or between companies in the portfolio yet to experience such an event, facilitates treating the portfolio itself as part of a network, where the impact of an occurrence of a cybersecurity event at one point in the network (e.g., at one company) can be measured by its likely propagation through the network (e.g., to other companies in the portfolio). This can directly depend on the degree of dependency between the company that experienced the cybersecurity event and the portfolio companies.

[0022] A machine learning model is utilized to identify the most significant cybersecurity events and the most significant interdependencies between companies to predict an occurrence of a cybersecurity risk event. According to an embodiment, a supervised machine learning model is trained over a time period where, during the training period, cybersecurity events and statistically significant shared features and interdependencies are identified, prioritized, ranked, and/or assigned corresponding weight. This data can be aggregated to form feature sets and one or more algorithms can be executed to generate a multiplier, which mathematically correlates to a likelihood that one or more portfolio companies will experience a cybersecurity risk event based on their relationship to a company or companies that experienced such an event. This relationship can be characterized by shared features e.g., common vendors, common security protocols, etc.). The multiplier can be used in real-time or near real-time to understand a portfolio's risk level and various steps can be enabled to reduce that risk.

[0023] The machine learning model operates to correlate a portfolio's risk of experiencing an adverse cybersecurity event. For example, consider the scenario where a company experiences a data breach. According to embodiments, in such case, data feeds of real-time reports on data breaches are analyzed, cybersecurity features most relevant to recent breach scenarios are identified, and a probability of a "catastrophic breach" occurring for one or more companies in the portfolio is predicted based on the prevalence of the identified cybersecurity features. Users are informed of the principal cybersecurity features that have been exploited in recent cybersecurity attacks and the like, and steps are enabled to mitigate the risk of those

attacks on portfolio companies. Further, instructions or recommendations to mitigate risk can be generated for display to the user or for automated execution by system components.

[0024] Embodiments also provide information and insight regarding a company's cybersecurity risk beyond tabulating individual risks associated with a company's cybersecurity posture (e.g. open ports, weak ciphers, malware infections, etc.). Accordingly, embodiments are particularly effective because they recognize that a portfolio of companies, while having relatively good tabulated cybersecurity risk scores on a per company basis, can also have a high correlated risk of experiencing a cybersecurity event. In any event, when a certain number or percentage of companies in the portfolio is at an increased risk, the portfolio itself can be considered at risk. This can be considered a correlated or systematic risk that can be mitigated by enabling a user or executing automated steps to optimize the portfolio's composition.

[0025] The foregoing features provide a system that quantifies a risk that multiple companies in a portfolio will experience a loss due to a cybersecurity event, and enables a user to take steps to mitigate that risk. This can be advantageous in a number of scenarios. For example, the inventive concepts can be utilized by a cyber insurance portfolio manager to gain quantitative insight into the probability of catastrophic loss due to multiple insured entities experiencing an adverse cybersecurity event. Also, where a user manages a portfolio of vendors (e.g., for vendor risk management), that user can assess the probability of multiple portfolio companies experiencing an adverse cybersecurity event.

[0026] FIGURE 1 shows aspects of system 100, which quantifies a cybersecurity risk level of a portfolio of companies using a risk multiplier and enables steps to reduce that risk. System 100 derives, compiles, or generates data sets and utilizes them to quantify a cybersecurity risk level for one or more portfolio companies, as well as an aggregate risk level for the portfolio itself. The quantified risk can be expressed using a multiplier, which can be a mathematical function or operator. According to an embodiment, the breach multiplier specifically quantifies the elevated risk due to a poorly diversified portfolio, which has an excess of common features, some of which are also shared with breached companies. It should be appreciated that the multiplier does not represent only a total amount of exposure across entities in a portfolio, but also is an expression of similarity of exposures across entities within a portfolio. The multiplier functions as a predictive value of the likelihood that a cybersecurity event (e.g., a catastrophic loss) will occur with respect to portfolio companies and can be used with a default, initial, or otherwise "standardized" cybersecurity risk level value (e.g., based on a randomly-sampled set

of companies or a set of companies specified according to certain criteria) to express the portfolio's cybersecurity risk level. Further, as discussed herein, system 100 can utilize different methods to derive the feature sets used to generate the multiplier.

[0027] Using the multiplier, system 100 executes steps, or directs a user to execute steps, to mitigate portfolio risk within a minimal or otherwise optimum number of steps. For example, a user can be directed to replace certain portfolio companies with companies not in the portfolio, which themselves can be randomly selected or selected according to predefined criteria. Also, a user can be directed to change certain interdependencies of portfolio companies. For example, if two or more portfolio companies use a problematic web host or share an upstream vendor, system 100 can flag that issue in its multiplier algorithm and direct a user to create a new portfolio composition where, e.g., the web host is not included as a vendor. In this way, system 100 can create a portfolio of companies that have dependencies (e.g., first-degree dependencies, second-degree dependencies, and so on) that optimizes the portfolio's aggregate cybersecurity risk level.

[0028] System 100 can comprise a server and/or cloud-based computing platform configured to execute the steps described herein. Accordingly, system 100 is a particular purpose computing system designed, configured, or adapted to perform the methods described herein and can be communicatively coupled with a number of end user devices 101a – 101n, which can be, e.g., a computer, tablet, Smartphone, or other similar end user computing device. Users can interact with system 100 using device 101 via one or more networks, such as network 102, which itself can comprise one or more of a local intranet, a LAN (Local Area Network), a WAN (Wide Area Network), a virtual private network (VPN), and the like. As will be apparent to those of skill in the art, communicative coupling can also be provided by, e.g., one or more of wireless connections, a synchronous optical network (SONET) connection, a digital Tl, TN, El or E3 line, Digital Data Service (DDS) connection, DSL (Digital Subscriber Line) connection, an Ethernet connection, and the like.

[0029] System 100 comprises processor 103 and memory 104, which stores instructions for executing steps according to methods described herein. These modules may locally reside in memory 104 or in a separate location. Further, as will be understood by those of skill in the art, a "module" can include an application-specific integrated circuit ("ASIC"), an electronic circuit, a processor (shared, dedicated, or group) that executes one or more of software or firmware, a

combinational logic circuit, and/or other suitable components that provide the described functionality.

[0030] A user can interact with system 100 at each end user station 101 using a graphical user interface (GUI) or the like, which itself can comprise one or more of dashboards, displays, notification centers, tables, and or other means to convey information relating to a portfolio, individual companies, cybersecurity events, risk levels, attributes, and user recommendations and action items, and the like.

[0031] During operation of system 100, one or more attributes of companies can be input into attribute module 105. The term "attribute" can be used synonymously with the term "attribute data" and each refers to data related to characteristics or features of an entity of interest. The attributes can relate to certain technologies utilized by a company such as email, website, social media, cloud services, servers, operation systems, and data storage (including, e.g., storage of website traffic, customer profiles, etc.). Also, non-technical attributes relating to a company can be input to attribute module 105. In some instances, it can be useful to utilize information relating to a company's products and services, financial history, employment characteristics, and the like. System 100 can determine what attributes to search for and use, or a user of system 100 can define or specify attributes of interest.

[0032] Attributes of a company can be collected directly from that company's network using previously existing network devices or new devices placed on the network or across different networks. This allows collection of proprietary, technical, and non-technical data relating to a company. System 100 can also gather attributes of interest for one or more companies by transmitting a query to each company, scraping online information from, e.g., websites, corporate filings, news sources, and public record databases and resources. In another embodiment, system 100 can also collect data from third party commercial sources and the like. To gather attribute information and input same to attribute module 105, data can be collected using a server or cloud-based device operating one or more software routines.

[0033] Attribute module 105 can rank or apply a weight to one or more attributes according to their influence on cybersecurity risk level. In an embodiment, an attribute weight is selected by an end user. For example, a portfolio manager working on behalf of an insurance company can determine that certain attributes, such as a company's technology area, technology vendors, and geographic region are important attributes for analyzing individual and aggregate cybersecurity risk. Accordingly, the user can assign a greater weight to such attributes.

[0034] System 100 can also determine how to weight attributes across different industries and the like. For example, if system 100 determines that the portfolio companies are hospitals, it can select attribute weights determined to be meaningful for medical practice. In any event, attribute weights can be adjusted and/or otherwise specified by system 100 or a user according to particular circumstances, preferences, and the like.

[0035] As mentioned, system 100 can utilize a machine learning model to quantity a portfolio's cybersecurity risk. Accordingly, company attribute information can be input to attribute module 105 during both a training period and an analysis period. In operation, system 100 can "learn" during a training period by, e.g., identifying patterns, categories, statistical relationships, etc., exhibited by training data. The result of the learning is then used to monitor whether new data exhibits the same patterns, categories, statistical relationships.

[0036] In operation of system 100, attribute module 105 can assign weights to certain attributes using information gathered during a training period. Based on attribute data relating to portfolio and/or non-portfolio companies analyzed during the training period, system 100 then makes informed decisions on the importance of different attributes. Accordingly, a description of an exemplary machine learning platform is helpful in understanding the inventive concepts described herein.

[0037] According to an embodiment, common attributes are identified and the significance of the identified common attributes can be expressed as a weight, ranking, prioritization, etc. By discovering patterns in historical and current data , machine learning can be utilized to make decisions in real-time about which attributes are indicative of a cybersecurity threat or a cybersecurity threat signature. For example, an increased likelihood of a cybersecurity threat may be discovered from one or more attributes even though the cybersecurity threat has not been seen before and no signature for the cybersecurity threat existed previously.

[0038] According to an embodiment, an automated predictive model first processes or filters raw supervised and/or unsupervised training data. A model can then be applied to the filtered data where, e.g., attributes or data fields corresponding to certain attributes that have no influence on cybersecurity risk level are eliminated, and the most significant attributes are heavily weighted. A multiplier is then generated by leveraging the foregoing aspects of the machine learning techniques, which itself is used to express the predicted cybersecurity risk for the portfolio.

[0039] In an embodiment, attribute data from various data sources can be evaluated in two separate data paths: (1) a real-time processing path, and (2) a batch processing path. Preferably, the evaluation of attribute data in these two data paths occurs concurrently. The real-time processing path is configured to continuously monitor and analyze the incoming attribute data (e.g., in the form of an unbounded data stream). To operate in real-time, the evaluation is performed primarily or exclusively on attribute data contemporaneously received with the data being generated by and/or received from the data source(s). In an embodiment, the real-time processing path excludes historical data (i.e., stored data pertaining to attributes analyzed in the past) from its evaluation. Alternatively, in an embodiment, the real-time processing path excludes third-party data from the evaluation in the real-time processing path. These example types of data that are excluded from the real-time path can be evaluated in the batch processing path.

[0040] Historical data and third party data may be used to create and improve the machine learning models employed to evaluate attribute data. Practically, the amount of such historical data and/or third party data can be potentially much larger than the real-time data stream. As such, the actual evaluation of the historical data tends to be slower. Consequently, in an embodiment, the real-time processing path does not use either or both the historical data and third party data as inputs. In other embodiments, historical and third party data may be used as inputs but the majority of the data used for evaluation in the real-time processing path still pertains to contemporaneous incoming attribute data. This is a consequence of the need to process the voluminous incoming attribute data quickly to obtain actionable information.

[0041] In the batch processing path, historical data and third-party data are processed optionally with the incoming real-time attribute data to, e.g., identify subtle attribute data indicative of cybersecurity risk. Batch processing may occur synchronously with real-time processing or in accordance with a predefined schedule.

[0042] Historical data can include data from different instantiations of the real-time data sources and may span time and geography. In some implementations, only an abridged version of the incoming attribute data is analyzed in the real-time processing path while a more complete version is stored as historical data. Accordingly, the historical data may, in one or more of these implementations, include attribute data that has more attributes than the abridged attribute data presented to the real-time processing path.

[0043] As in the real-time data path, actionable or relevant attribute data discovered by the batch analyzer may be acted upon automatically or may be presented to a user for a decision to take action. The action ultimately taken by a user can validate or invalidate conclusions reached by the batch analyzer and may serve as a source of feedback to the machine learning platform to improve its evaluation of subsequently processed data.

[0044] Attribute information processed by attribute module 105 can be used by comparison module 106 to generate a degree of similarity between companies-of-interest. A company of interest can be a portfolio company or a company not in a portfolio. For example, a company that experienced a cybersecurity event during a certain time period may be of interest. While the company that experienced the cybersecurity event may or may not be in a given portfolio, its attributes can be compared to companies in a portfolio, which are also companies-of-interest.

[0045] Also, it may be of interest to determine how many portfolio companies have attributes common to a company that experienced a cybersecurity event during a time period. If several portfolio companies share attributes with a company that experienced a cybersecurity event, it can be inferred that an occurrence of the cybersecurity event is more likely to occur at a portfolio company. This is exacerbated when there are several attributes common to the portfolio companies and/or the shared attributes are heavily weighted, i.e., assigned a greater weight based on their indication of an occurrence of a cybersecurity event.

[0046] The degree of similarity can be expressed in terms of a number of attributes common to two or more companies and/or the n-degrees of dependency between the attributes (and, therefore, the companies). Accordingly, comparison module 106 compares the attributes collected by attribute module 105 to determine a number of attributes common to the companies-of-interest and their degrees of dependencies. According to different embodiments, attribute module 105 and/or comparison module 106 filter and otherwise process attributes and comparison data by, e.g., assigning weights to attributes or set of attributes and the like.

[0047] In an embodiment, comparison module 106 generates a similarity score between companies-of-interest. The similarity score represents how similar a group of entities is to one another in view of (1) the number of attributes shared by companies, (2) the weight or relevance of the shared attributes, and (3) the degree of mutuality of the shared attributes.

[0048] The comparison or similarity data processed by comparison module 106 can be used by multiplier module 107 to generate a cybersecurity risk multiplier for a portfolio. The multiplier is a mathematical function or operator used to express the probability that a portfolio will experience a significant cybersecurity risk event.

[0049] Cybersecurity Risk Level Module 108 quantifies a portfolio's cybersecurity risk level based on the multiplier generated by multiplier module 107. That is, Cybersecurity Risk Level Module 108 generates a cybersecurity risk level for the portfolio of companies, which can be expressed as a function of the multiplier generated by multiplier generator module 107. The portfolio cybersecurity risk level can be represented as a fraction, a decimal, a percentage, and/or a normalized number in a range defined by a user or otherwise predetermined.

[0050] Utilizing action module 109, the portfolio cybersecurity risk level can be displayed by a graphical user interface at any end user station 101. In some embodiments, the cybersecurity risk level can be represented as a graph that illustrates the correlation among portfolio companies, as well as portfolio companies and non-portfolio companies. Companies can be graphically connected based on their number of shared attributes, the type or weight of shared attributes, and the degree of mutuality of the attributes.

[0051] As discussed herein, output of Cybersecurity Risk Level Module 108 can be utilized by action module 109 to generate steps that, if executed, will change the portfolio's cybersecurity risk level. In response to calculating a portfolio Cybersecurity Risk Level (CRL), action module 109 can be executed to provide the end user with some type of actionable feedback. For example, action module 109 can provide the end user with one or more actions that, if performed, will improve the cybersecurity risk level of the portfolio.

[0052] In one example, action module 109 can automatically identify attributes that, if changed, would affect the portfolio's cybersecurity risk level. For example, if high risk companies utilize service providers that use a particular CDN, action module 109 can output a recommendation that removing companies which use such same service providers will reduce portfolio risk level.

[0053] Therefore, an embodiment of system 100 can automatically provide the risk level generated by Cybersecurity Risk Level Module 108, expressed as a function of the multiplier generated by module 107, or other information to an end user, who can utilize that information to reduce portfolio risk level. If, for example, a new company is considered for inclusion in the

portfolio, it may be unacceptable for inclusion if its attributes are high risk or otherwise similar to high risk companies.

[0054] Action module 109 can also identify attributes that are problematic or negatively impact portfolio cybersecurity risk level. For example, action module 109 can identify vendors, such as web service providers and cloud service providers as particularly problematic attributes. In some embodiments, action module 109 can also identify network parameters, such as firewall policies and the like, as problematic. Prompting the user to modify problematic shared attributes will likely decrease the cybersecurity risk level. Further, action module 109 can also determine key variables that, if changed, would negatively impact cybersecurity risk level, and accordingly, identify these variables to the end user as desirable.

[0055] User actions that can be taken in response to cybersecurity risk level information also includes replacing one or more portfolio companies with one or more companies that do not share problematic attributes. Likewise, an action item can require that a user add a new company to the portfolio that is determined to include positive attributes (i.e., attributes indicative of low cybersecurity risk), such as security personnel, strong information technology infrastructure and protocols, and the like. In one example, action module 109 provides an attribute profile of a company that, if added to the portfolio, would sufficiently reduce the portfolio cybersecurity risk level.

[0056] System 100 can also update portfolio cybersecurity risk level based on feedback received at module 110 from an end user. For example, if a user wants to determine what effect adding a proposed company to the portfolio will have on its current cybersecurity risk level, a profile of selected attributes of the proposed company can be input to system 100 via feedback module 110. Selected attributes of the proposed company are then utilized by system 100 to compile an updated (albeit hypothetical) portfolio cybersecurity risk level, which can be displayed to the user. Feedback module 110 can received feedback from a user or feedback automatically generated by components of system 100, such as devices 101.

[0057] Further, under different scenarios, the difference between a predicted cybersecurity risk level and a previous cybersecurity risk level can be compared to a threshold. In an embodiment, system 100 compares the predicted cybersecurity risk level change to a threshold to determine if inclusion of a proposed company in the portfolio is justified. There may be instances where a net change in cybersecurity risk level is required by system parameters and/or user requirements before a portfolio change is recommended.

[0058] System 100 can further indicate to a user why a portfolio cybersecurity risk level changes in a particular way or by a particular amount. That is, system 100 can analyze underlying system data and its impact on cybersecurity risk level. Accordingly, system 100 can construct a portfolio using data gathered from an analysis of variables for one or more companies.

[0059] For example, system 100 can generate a report that informs a user about the number and type of companies to include in a portfolio to satisfy a certain cybersecurity risk level. The generated report can indicate that a portfolio manager should include a certain percentage of clients in a first technology sector, a second technology sector, and so on. These sectors can be determined by comparing attributes of various companies across sectors that yield an acceptable portfolio cybersecurity risk level.

[0060] FIGURE 2 shows a flow chart of steps performed to quantify a cybersecurity risk level of a portfolio of companies using a risk multiplier and enable steps to reduce that risk. The steps shown in FIGURE 2 can be executed by a system for reducing a cybersecurity risk level of a portfolio of companies using a risk multiplier, such as system 100 shown in FIGURE 1. The steps can be performed by processing logic that may comprise hardware (e.g., circuitry, dedicated logic, etc.), software (such as is run on a general purpose computer system or a dedicated machine), or a combination of both.

[0061] At step 201, an initial cybersecurity risk level of a portfolio of companies is determined. The initial determination can be performed in different ways. For example, a default risk level can be assigned to the portfolio based on, e.g., statistical data obtained from randomly sampled companies. The statistical sampling can be performed by implementing the supervised machine learning concepts discussed above with respect to system 100. For example, during a time period such a training period, a default or baseline risk level can be approximated by analyzing occurrences of cybersecurity events across a random sampling of companies. Analyzing the occurrences can involve evaluating different attributes of companies that experience a cybersecurity event and weighting those attributes. In some instances, this can yield a more meaningful baseline or default risk level for the portfolio of companies.

[0062] The initial risk can also be determined by sampling companies over a time period that are known to have attributes common to a significant number of portfolio companies. For example, where a number of portfolio companies share a common web host, or utilize products or service offered by the same vendor(s), embodiments can limit a sampling to companies used

to approximate an initial or default risk level to companies that have the same attributes. As such, an initial cybersecurity risk level can be generated, at least in part, by comparing cybersecurity data (e.g., attributes and/or their n-degree dependencies) relating companies in a portfolio of interest to cybersecurity data relating to companies in a portfolio comprising randomly selected companies.

[0063] Certain attributes can also be weighted according to their determined influence on cybersecurity risk level. That is, the identified attributes that are shared by a portfolio company and a company that experienced a cybersecurity risk event can be weighted according to their correlation with the occurrence of the cybersecurity risk event. Subsequently, a probability that portfolio companies sharing the identified attributes will also experience a cybersecurity risk event will depend on the weights assigned to the identified common attributes. In this way, the initial cybersecurity risk level for the portfolio can have more context, and/or can provide a more meaningful value for which the multiplier is applied.

[0064] The weight assigned to an attribute can depend on a degree of dependency associated with that attribute. As discussed in more detail below, attributes can be analyzed according to their degree of dependency on or similarity to one another. According to an embodiment, a first-degree attribute can be defined as an attribute that is directly common to at least two companies in the portfolio, a second-degree attribute can be defined as an attribute not directly common to the at least two companies, but directly common to the first-degree attribute, a third-degree attribute can be defined as an attribute not directly common to the at least two companies or the first-degree attribute, but directly common to the second-degree attribute, and so on.

[0065] According to an embodiment, first-degree attributes can be assigned greater weight than second-degree attributes, second-degree attributes can be assigned a greater weight than third-degree attributes, and so on. Recognizing not only attributes shared by companies, e.g., first-degree attributes, but further removed commonalities such as higher degree attributes, allows more insight into relationships between portfolio companies and other companies and the likelihood that a cybersecurity risk event at one company will propagate to a portfolio company. Obviously, this provides a user with enriched information and more degrees of freedom in executing steps to reduce portfolio risk level. A user is not limited to replacing one company for another based on shared attributes, but is able to select one or more companies for inclusion in a portfolio that are determined to not, e.g., utilize a problematic or high risk vendor.

[0066] Further, the initial risk level can be based on attributes of the portfolio companies themselves. The attributes of the portfolio companies can be used alone, or in combination with the foregoing features, to establish an initial risk level. For example, in an embodiment, certain attributes can be analyzed and a comparison performed to estimate how the initial risk of the portfolio likely deviates from a randomly sampled group of companies, or a group of companies that have attributes known to be common to companies in the portfolio.

[0067] The attributes themselves can be thought of as "internal" to a company or "external" to a company. Examples of internal attributes include, e.g., a host that is identified as vulnerable, a browser or operating system determined to be obsolete, an incidence of malware events that exceeds a threshold during a given time period (e.g., a month or a year), a number and type of open ports, a slow patching cadence for updating software with known vulnerabilities, a cipher identified as being weak, a newly-added subdomain, inadequate use of firewalls and intrusion detection systems, and the like. Examples of external attributes include social network sentiment, improper use of social media accounts, as well as leaked passwords and the like.

[0068] The initial cybersecurity risk level can be expressed in different ways, depending on user preferences, end-use applications, and the like. In an embodiment, the initial cybersecurity risk level can be expressed as an absolute value, or score, to be used as a reference. In other embodiments, the initial risk level can be expressed in terms of its relationship to another standard or reference value. For example, the initial value can be expressed as a percentage or the like, e.g., .8(x), 1.2(x), etc., where a value (x) can represent a "neutral" or otherwise accepted reference risk level.

[0069] According to an embodiment, step 201 is optional, where a standardized value is used as a reference for subsequent calculations. Accordingly, a subsequently quantified risk level of a portfolio is expressed as a deviation (as determined by a multiplier) from the standardized value. The standardized value can be used as a starting point or reference in all instances.

[0070] At step 202, at least one company that experienced a cybersecurity risk event during a certain time period is identified. The identified company, and attributes of the company, can serve as a starting point for determining a multiplier used to quantify the cybersecurity risk level of the portfolio. The company can be a portfolio company, or a company not in the portfolio, while certain of its attributes will be compared to those of portfolio

companies. Also, the time period in which the company experienced the cybersecurity event can be all or part of a training period, as described herein. On the other hand, the time period can be randomly selected or selected about a window in which cybersecurity events occur or are thought to have occurred (e.g., a time window about a period in which cybersecurity events increase or peak). In any event, whether or not historical, the time period is preferably close enough in time to the performance of steps described herein to be relevant.

[0071] At step 203, at least one attribute that is common to the company identified at step 202 and at least one company in the portfolio is identified. The identified common attributes are compared in a meaningful way to determine their correlation with cybersecurity risk. According to inventive concepts it is recognized that some attributes have minimal impact on cybersecurity risk level, while other attributes clearly influence same. For example, the sophistication of a web service vendor, its gross revenue, and its technology sector may strongly influence cybersecurity risk level, while geographic location, state of incorporation, number of employees may not. Accordingly, attributes that strongly influence cybersecurity risk will be assigned a greater weight than those that do not.

[0072] At step 204, a degree of mutuality is generated for the attributes identified at step 203. Notably, the inventive concepts not only recognize a number and weight of attributes shared by companies, but a degree of mutuality of the shared attributes. Accordingly, embodiments provide greater insight to portfolio cybersecurity risk level and offer significantly more options for a user to reduce portfolio risk level. That is, in determining risk level, a user is not confined to comparing attributes shared by two or more companies, but can also compare attributes common to companies that, while not in the portfolio, influence cybersecurity risk level of the portfolio.

[0073] By way of example, consider defining a first-degree attribute as an attribute that is directly common to at least two companies in the portfolio, a second-degree attribute as an attribute not directly common to the at least two companies, but directly common to the first-degree attribute, a third-degree attribute as an attribute not directly common to the at least two companies or the first-degree attribute, but common to the second-degree attribute, and so on. In that case, further consider companies C1 – C4 in a portfolio, where Vendor V1 supplies certain functionality implemented in security software used by C1 and C2, Vendor V2 supplies the same functionality implemented in security software used by C3 and C4, and Vendor VV1 supplies web authentication services to Vendors V1 and V2. In this example, Vendor V1 (or the service

it provides) is a first-degree attribute for Companies C1 and C2, while Vendor V2 (or the service it provides) is a first-degree attribute for Companies C3 and C4. With respect to companies C1 – C4, Vendor VV1 is a second-degree attribute where companies C1 and C2 receive the functionality implemented their security software from a vendor different than companies C3 and C4, but Vendors V1 and V2, and therefore, indirectly, companies C1 – C4 share the same web authentication features supplied by Vendor VV1. It could also be said that Vendor VV1 is a first-degree attribute of Vendors V1 and V2.

[0074] At step 205, a cybersecurity risk multiplier is generated. The multiplier is a mathematical function or operator used to express the portfolio's cybersecurity risk level. The multiplier can be a factor used to arrive at a mathematical product, or can be expressed as a more complex function or operator comprising, e.g., logarithmic or exponent components. Further, according to an embodiment, the multiplier can be an operator capable of showing a rate of change or gradient in a portfolio's cybersecurity risk level with respect to time, portfolio composition, and other factors. In this way, the multiplier can be utilized to see what factors create the greatest change or most heavily influence portfolio risk level. Such factors will be different across portfolios, and as such, the multiplier can comprise different contributions in different embodiments to more clearly track a risk level for any given portfolio.

[0075] According to an embodiment, the multiplier represents a similarity between portfolio companies and companies that experienced a cybersecurity event within a predefined feature space (where the feature space is defined by a supervised learning model) that is scaled and can be measured against a benchmark. The multiplier can be based on one or more of the number of portfolio companies having attributes common to a company that experienced a cybersecurity risk event, the number of the shared attributes themselves, the generated weight assigned to the shared attributes, and the degrees of dependency of the shared attributes.

[0076] Further, the multiplier is generated from data gathered using machine learning techniques discussed herein. A statistical model can be trained by first estimating a degree of similarity between companies in randomly composed portfolios and analyzing the number of K identified or discovered cybersecurity events in those portfolios over a period of time. The K identified or discovered cybersecurity events can be a combination of significant cybersecurity events and dependencies, where K = 0, 1, 2, . . . n. Then, a distribution of the portfolio of interest and the number of identified cybersecurity events for the randomly composed portfolios are used to fit a Bayesian model of likelihood of multiple cybersecurity events.

[0077] In other words, to generate the multiplier, machine learning techniques are used to analyze both a portfolio of interest and companies that experienced a cybersecurity event in a certain time period (e.g., the past six (6) months). From this, an estimate of the risk that multiple companies will experience a cybersecurity event is generated. According to an embodiment, the value of the multiplier is constrained to vary between 0 and 2(x), where 1(x) is the probability that a randomly composed portfolio will experience a cybersecurity event.

[0078] According to an embodiment, the multiplier can be used to express a cybersecurity risk level where:

(1) CB_PROBABILITY (D-SCORE, N) = CATASTROPHIC_BREACH_PROBABILITY (D-SCORE, N) = PROBABILITY (NUMBER_OF_BREACH >1|D-SCORE, N),"

(2) MULTIPLIER (D-SCORE, N) = CB_PROBABILITY (D-SCORE, N) / CB_PROBABILITY (D-SCORE=BENCHMARK, N),

where:

"CB_PROBABILITY" represents the probability that a portfolio of interest will experience a cybersecurity risk event, and is a function of "D-SCORE," which is a quantitative measure of the diversification level of the portfolio of interest within the predefined feature space;

"N" represents the number of companies in the portfolio of interest;

"PROBABILITY (D-SCORE)" represents a probability density function of the quantitative measure of diversification level of the portfolio of interest (D-SCORE), which is estimated by sampling randomly generated portfolios. According to one embodiment, this conditional probability is estimated by fitting a Kernel density model on the d-scores of randomly generated portfolios;

"PROBABILITY (NUMBER_OF_BREACH > 1 | D-SCORE, N)" represents a probability of a number of breach events occurring in the portfolio of interest, which is conditioned on the quantitative measure of diversification level of the portfolio of interest (D-SCORE).

"PROBABILITY (NUMBER_OF_BREACH > 1 | D-SCORE, N)" is proportional to PROBABILITY(D-SCORE | NUMBER_OF_BREACH > 1, N)*PROBABILITY (NUMBER_OF_BREACH > 1, N)

"PROBABILITY(D-SCORE | NUMBER_OF_BREACH > 1)" represents a probability of the quantitative measure of diversification level of the portfolio of interest (D-SCORE), which is conditioned on a number of breach events occurring in the portfolio of interest. According to one embodiment, this conditional probability is estimated by fitting a Kernel density model on the d-scores of randomly generated portfolios;

"PROBABILITY(NUMBER_OF_BREACH, N)" represents a joint probability of the number of breaches in a portfolio of size N. According to one embodiment, this probability follows a binomial distribution as binomial (N,p),where p = a number of companies experiencing a cybersecurity event divided by N;

"NUMBER_OF_BREACH" represents the number of vendors that experience a cyber incident within a pre-defined time interval;

"MULTIPLIER" represents Breach Multiplier;

"CB_PROBABILITY (D-SCORE=BENCHMARK, N) represents a joint probability of D-SCORE and portfolio size N; and

"BENCHMARK" is the mean of D-SCORE for a set of randomly selected portfolios.

[0079] The model used to generate the multiplier can be validated using a training model. During a training period, a weight for each attribute, attribute type, cybersecurity event, or cybersecurity event type can be generated. The most heavily weighted attributes and/or events can be selected by weight (e.g., the top ten (10) percent). A sampling pool can then be obtained by querying a different number of common attributes and/or event types. A portfolio can then be composed by randomly selecting from the sampling pool. The model can be trained and tested using portfolios of different sizes, e.g., randomly selected between a size of ten (10) to one hundred (100) companies.

[0080] At step 206, a portfolio cybersecurity risk level is generated as a function of the multiplier generated at step 205. Practically, the generated portfolio cybersecurity risk corresponds to a probability that a cybersecurity risk event will occur with respect to one or more portfolio companies, and depends on the number of shared attributes previously identified and their degrees of dependency. In other words, the generated portfolio cybersecurity risk level represents the likelihood one or more companies in a portfolio will experience a cybersecurity event in view of its degree of similarity to a company or companies that experienced such an event. The degree of similarity is directly related to the shared attributes, the weight of the attributes, and degrees of mutuality of the shared attributes, as discussed herein. Again, as mentioned above, some attributes can have minimal or no impact on the cybersecurity risk level, and such variables may be assigned a correspondingly small weight. If, for example, a shared attribute is not included in the risk level calculation by the end user the variable has no impact on the portfolio cybersecurity risk level.

[0081] The portfolio cybersecurity risk level can be expressed as an absolute value or as a relative value. For example, using the multiplier generated at step 205, the portfolio cybersecurity risk level generated at step 206 can be thought of as a mathematical product of, e.g., (1) the multiplier, and (2) an initial portfolio risk level or some other default or standardized value. As discussed, the initial portfolio risk level can be generated by applying a certain value to the portfolio itself, or can be based upon, e.g., sampling companies over a time period – whether the sampling is random or constrained to a particular set of companies that satisfy certain criteria. In any event, the machine learning technique discussed herein can be utilized to provide a baseline or standard value, or otherwise assign an initial portfolio risk level.

[0082] At step 207, a tool is enabled for reducing the portfolio's cybersecurity risk level. For example, if a portfolio is determined to have a high multiplier, and as a result, an increased cybersecurity risk level, portfolio companies that use problematic vendors can be investigated and/or replaced. Consistent with the foregoing description, enabling a tool to reduce a portfolio's cybersecurity risk level may involve displaying variable data fields and/or tools that allow a user to implement a number of changes to reduce the risk level. As an example, an interactive tool can be displayed to a user that comprises a list or series of available actions the user can execute to reduce the risk level. As mentioned herein, the actions can include removing a company from the portfolio, as well as replacing it with one or more companies. The one or more replacement companies can be considered less problematic or less risky than the replaced company insomuch as the replacement companies may not share one or more attributes with a

company that experience a cybersecurity risk event. On the other hand, the replacement companies can be randomly selected, or selected based on their similarity (or shared attributes) with other portfolio companies that are determined to be less risky. Further, when the inventive concepts are used for vendor risk management, portfolio companies can be instructed to remediate shared issues (e.g. open ports, etc.) as a mechanism for reducing risk.

[0083] In some instances, a user may wish to remove one or more problematic or risky companies, thereby reducing the size of the portfolio and constraining it to companies that satisfy certain criteria or otherwise are determined to not have shared attributes or dependency (again, of any n-degree) with a company that experienced a cybersecurity risk event. By removing one or more companies that are at an increased risk from the portfolio, the aggregate risk level for the portfolio advantageously decreases.

[0084] A user can also view the effects of its actions have on the portfolio's risk level. After a user executes one or more steps enabled at step 207, an updated or refined portfolio risk level can be generated and displayed to the user along with a new set of enabled steps for execution. This can be thought of as a feedback loop operating with feedback input by the user to the system.

[0085] At step 208, feedback is received and further action is taken with respect to the generated portfolio cybersecurity risk level. The feedback can be received as an automated response generated by the system, or as a manually-entered response from a user. For example, feedback can be received from an individual, such as a portfolio manager, that is manually entered at one or more end user stations. On the other hand, the feedback can be received from a network or system device that generates the feedback. For example, an end user software routine can receive the output, compare the output to a determined threshold or series of metrics, and respond with feedback to yield an updated input that better conforms to the threshold or metrics. The end user software routine may require that a portfolio cybersecurity risk level be under a certain number and, if that condition is not satisfied, may transmit a proposed company profile for consideration in the portfolio. Should that proposed company's profile be considered and sufficient lower the portfolio cybersecurity risk level, the output may be accepted and passed along to other system companies for further analysis, and the like.

[0086] In view of the foregoing, feedback can be expressed in various forms, such as a suggestion, specifically required action(s), option, or report. In any event, an object can be to compare the portfolio cybersecurity risk level to a benchmark or other threshold over some

period of time. In this way, a portfolio manager (employed by, e.g., an insurance company) can track the portfolio's aggregated cybersecurity risk level across an adjustable time frame. Doing so enables longer term analysis of the portfolio's risk level over time, and the manager's exposure in view of same. This, of course, allows a manager to make meaningful business decisions regarding the composition of the portfolio, and cast, willingness, and ability to underwrite the portfolio.

[0087] FIGURES 3A and 3B graphically illustrate data provided by an embodiment with respect to randomly composed portfolios having between twenty (20) and one hundred and fifty (150) companies. The data illustrates trends derived from a comparison between portfolio companies and companies that experienced a cybersecurity event Attributes of interest included third party vendors and industry type, and the portfolios were composed by enforcing a number of attributes in the portfolio. As seen in FIGURE 3A, the normalized d-score decreases generally in linear fashion with an increase in the number of shared attributes. FIGURE 3B shows that the likelihood of a company experiencing a cybersecurity event increases as the number of shared attributes increases.

[0088] FIGURE 4A illustrates a probability density function of multiplier values for positive portfolio $B > 1$ vs. negative portfolio $B \leq 1$, in which B is the number of cybersecurity events over a two (2) year time period. FIGURE 4B illustrates a probability density function of multiplier values for positive portfolio $B > 1$ vs. negative portfolio $B \leq 1$, in which B is the number of cybersecurity events over a one (1) year time period. As seen, with respect to performance for a randomly composed portfolio, recall rate is 70% and accuracy rate is 68%.

[0089] FIGURE 5 illustrates multiplier values as a function of average score. As seen, portfolios with more common attributes tend to have lower total scores. An entity with a high total score has lower cybersecurity risk than an entity with a low total score. According to FIGURE 5, statistical multiplier values are partially correlated with total score. As the multiplier also depends on the mutuality between companies, the multiplier detects a portfolio of good total score with low diversification, as marked by the circle.

[0090] FIGURE 6A is a heat map of cybersecurity attributes of a portfolio comprised of companies that have a high multiplier value and a low total score and FIGURE 6B [INSERT] is heat map of cybersecurity attributes of portfolio comprised of companies that have a low multiplier value and a high total score. As seen, certain attributes are indicative of clusters of companies most likely to experience a cybersecurity risk event.

[0091] FIGURE 7 shows the probability density functions of multiplier values for a different number of common attributes. In other words, FIGURE 7 shows how multiplier values map to categorical levels of numbers of shared attributes among companies in a portfolio.

[0092] Certain units described in this specification have been labeled as modules in order to more particularly emphasize their implementation independence. A module is ''[a] self-contained hardware or software component that interacts with a larger system." Alan Freedman, "The Computer Glossary" 268 (8th ed. 1998). A module may comprise a machine- or machines-executable instructions. For example, a module may be implemented as a hardware circuit comprising custom VLSI circuits or gate arrays, off-the-shelf semiconductors such as logic chips, transistors, or other discrete components. A module may also be implemented in programmable hardware devices such as field programmable gate arrays, programmable array logic, programmable logic devices or the like.

[0093] Modules may also include software-defined units or instructions, that when executed by a processing machine or device, transform data stored on a data storage device from a first state to a second state. An identified module of executable code may, for example, comprise one or more physical or logical blocks of computer instructions that may be organized as an object, procedure, or function. Nevertheless, the executables of an identified module need not be physically located together, but may comprise disparate instructions stored in different locations that, when joined logically together, comprise the module, and when executed by the processor, achieve the stated data transformation. A module of executable code may be a single instruction, or many instructions, and may even be distributed over several different code segments, among different programs, and/or across several memory devices. Similarly, operational data may be identified and illustrated herein within modules, and may be embodied in any suitable form and organized within any suitable type of data structure. The operational data may be collected as a single data set, or may be distributed over different locations including over different storage devices.

[0094] In the foregoing description, numerous specific details are provided, such as examples of programming, software modules, user selections, network transactions, database queries, database structures, hardware modules, hardware circuits, hardware chips, etc., to provide a thorough understanding of the present embodiments. One skilled in the relevant art will recognize, however, that the disclosure may be practiced without one or more of the specific details, or with other methods, components, materials, and so forth. In other instances, well-

known structures, materials, or operations are not shown or described in detail to avoid obscuring aspects of the disclosure.

[0095] In the following description, numerous details are set forth to provide a thorough understanding of the present invention. It will be apparent, however, to one skilled in the art, that the present invention may be practiced without these specific details. In other instances, well-known structures and devices are shown in block diagram form, rather than in detail, in order to avoid obscuring the present invention.

[0096] Some portions of the detailed descriptions that follow are presented in terms of algorithms and symbolic representations of operations on data bits within a computer memory. These algorithmic descriptions and representations are the means used by those skilled in the data processing arts to most effectively convey the substance of their work to others skilled in the art. An algorithm is here, and generally, conceived to be a self-consistent sequence of steps leading to a desired result. The steps are those requiring physical manipulations of physical quantities. Usually, though not necessarily, these quantities take the form of electrical or magnetic signals capable of being stored, transferred, combined, compared, and otherwise manipulated. It has proven convenient at times, principally for reasons of common usage, to refer to these signals as bits, values, elements, symbols, characters, terms, numbers, or the like.

[0097] It should be borne in mind, however, that all of these and similar terms are to be associated with the appropriate physical quantities and are merely convenient labels applied to these quantities. Unless specifically stated otherwise as apparent from the following discussion, it is appreciated that throughout the description, discussions utilizing terms such as "processing" or "computing" or "calculating" or "determining" or "displaying" or the like, refer to the action and processes of a computer system, or similar electronic computing device, that manipulates and transforms data represented as physical (electronic) quantities within the computer system's registers and memories into other data similarly represented as physical quantities within the computer system memories or registers or other such information storage, transmission or display devices.

[0098] The present invention also relates to apparatus for performing the operations herein. This apparatus may be specially constructed for the required purposes, or it may comprise a general purpose computer selectively activated or reconfigured by a computer program stored in the computer. Such a computer program may be stored in a computer readable storage medium, such as, but is not limited to, any type of disk including floppy disks, optical disks, CD-

ROMs, and magnetic-optical disks, read-only memories (ROMs), random access memories (RAMs), EPROMs, EEPROMs, magnetic or optical cards, or any type of media suitable for storing electronic instructions, and each coupled to a computer system bus.

[0099] The algorithms and displays presented herein are not inherently related to any particular computer or other apparatus. Various general purpose systems may be used with programs in accordance with the teachings herein, or it may prove convenient to construct more specialized apparatus to perform the required method steps. The required structure for a variety of these systems will appear from the description below. In addition, the present invention is not described with reference to any particular programming language. It will be appreciated that a variety of programming languages may be used to implement the teachings of the invention as described herein.

[00100] A machine-readable medium includes any mechanism for storing or transmitting information in a form readable by a machine (e.g., a computer). For example, a machine-readable medium includes read only memory ("ROM"); random access memory ("RAM"); magnetic disk storage media; optical storage media; flash memory devices; electrical, optical, acoustical or other form of propagated signals (e.g., carrier waves, infrared signals, digital signals, etc.).

[00101] Although the present invention and its advantages have been described in detail, it should be understood that various changes, substitutions and alterations can be made herein without departing from the spirit and scope of the invention as defined by the appended claims. Moreover, the scope of the present application is not intended to be limited to the particular embodiments of the process, machine, manufacture, composition of matter, means, methods, and steps described in the specification. As one of ordinary skill in the art will readily appreciate from the disclosure of the present invention, processes, machines, manufacture, compositions of matter, means, methods, or steps, presently existing or later to be developed that perform substantially the same function or achieve substantially the same result as the corresponding embodiments described herein may be utilized according to the present invention. Accordingly, the appended claims are intended to include within their scope such processes, machines, manufacture, compositions of matter, means, methods, or steps. Moreover, the scope of the present application is not intended to be limited to the particular embodiments of the process, machine, manufacture, composition of matter, means, methods, and steps described in the specification.

CLAIMS

What is claimed is:

1. An interactive tool that dynamically determines and modifies a cybersecurity risk level of a portfolio of companies in response to a user selection, the interactive tool comprising:

a memory; and

one or more processors communicatively coupled to the memory, where the one or more processors are configured to:

determine an initial cybersecurity risk level for the portfolio;

identify:

at least one company that experienced a cybersecurity risk event during a certain time period;

at least one attribute common to the at least one identified company that experienced the cybersecurity risk event and a plurality of companies in the portfolio, and

a degree of mutuality of the at least one attributes;

determine a probability that another cybersecurity risk event will occur with respect to the plurality of companies in the portfolio, where the probability depends on:

the number of identified common attributes, and

degrees of mutuality of the number of identified attributes;

generate, from the determined probability, a cybersecurity risk multiplier for the portfolio;

generate a refined cybersecurity risk level that is a function of the initial cybersecurity risk level and the cybersecurity risk multiplier;

determine one or more actions to reduce the refined cybersecurity risk level; and

display, to a user:

the refined cybersecurity risk level for the portfolio,

the one or more actions that the user can take to reduce the refined cybersecurity risk level, and

the effect that the one or more actions have on the refined cybersecurity level, and

execute at least one action of the one or more actions to reduce the refined cybersecurity risk level in response to the user selection.

2. The interactive tool of claim 1, where the action the user can take to reduce the refined cybersecurity risk level comprises:

an action to remove a company from the portfolio of companies; and

an action to replace the removed company with a new company, where the new company was not previously included in the portfolio.

3. The interactive tool of claim 1 where the refined cybersecurity risk level is expressed as a product of the initial cybersecurity risk level and the cybersecurity risk multiplier.

4. A method for utilizing an interactive tool to dynamically determine and modify a cybersecurity risk level of a portfolio of companies in response to a user selection, the method comprising:

determining an initial cybersecurity risk level for the portfolio;

identifying at least one company that experienced a cybersecurity risk event during a certain time period;

identifying:

at least one attribute common to the at least one identified company that experienced the cybersecurity risk event and a plurality of companies in the portfolio, and

a degree of mutuality of the at least one attributes;

determining a probability that another cybersecurity risk event will occur with respect to the plurality of companies in the portfolio, where the probability depends on:

the number of identified common attributes, and

degrees of mutuality of the number of identified attributes;

generating, from the determined probability, a cybersecurity risk multiplier for the portfolio;

generating a refined cybersecurity risk level that is a function of the initial cybersecurity risk level and the cybersecurity risk multiplier;

determining one or more actions to reduce the refined cybersecurity risk level; and

displaying via the interactive tool to a user:

the refined cybersecurity risk level for the portfolio,

the one or more actions that the user can take to reduce the refined cybersecurity risk level, and

the effect that the one or more actions have on the refined cybersecurity level, and

executing at least one action of the one or more actions to reduce the refined cybersecurity risk level in response to the user selection.

5. The method of claim 4, where the one or more actions that the user can take to reduce the refined cybersecurity risk level comprise:

removing a company from the portfolio of companies;

replacing the removed company with a new company, where the new company was not previously included in the portfolio; and

identifying a critical cybersecurity attribute and remove the identified attribute from the portfolio.

6. The method of claim 14, where the refined cybersecurity risk level is expressed as a product of the initial cybersecurity risk level and the cybersecurity risk multiplier.

7. The method of claim 4, where the at least one identified company that experienced a cybersecurity risk event during the certain time period is in the portfolio.

8. The method of claim 8, where the certain time period is historical.

9. The method of claim 4, where the at least one identified company that experienced a cybersecurity risk event during the certain time period is not in the portfolio.

10. The method of claim 9, where the certain time period is historical.

11. The method of claim 4, where the initial cybersecurity risk level is generated, at least in part, from cybersecurity data relating to at least one company in the portfolio during the certain time period.

12. The method of claim 4, where the initial cybersecurity risk level is generated, at least in part, by comparing attributes indicative of cybersecurity risk level of companies in the portfolio to the attributes indicative of cybersecurity risk level of companies in another portfolio comprising randomly selected companies.

13. The method of claim 4, where the identified common attributes are weighted according to their correlation with an incidence of a cybersecurity risk event, and the determined probability further depends on the weights of the identified common attributes.

14. The method of claim 4, where the identified common attributes comprise an internal attribute that is shared by companies in the portfolio.

15. The method of claim 14, where the internal attribute comprises one or more of: vulnerable host, obsolete user agent, number of new malware events, open ports, slow patching cadence, and inadequate use of firewalls and inadequate use of intrusion detection system.

16. The method of claim 4, where the identified common attributes comprise an external attribute that is shared by companies in the portfolio and one or more companies not in the portfolio.

17. The method of claim 16, where the external attribute comprises one or more of: inadequate use of social media accounts, lost or stolen passwords, and inadequate social network sentiment.

18. The method of claim 4, where the identified common attributes comprises a first-degree common attribute, and where the first-degree common attribute comprises at least one vendor that is common to two or more companies in the portfolio.

19. The method of claim 4, where the identified common attributes comprises a second-degree common attribute, and where the second-degree common attribute comprises at least one vendor that is common to two or more vendors, where the two or more vendors are common to two or more companies in the portfolio.

20. A non-transitory computer-readable storage medium storing instructions that, when executed by one or more processors, cause the one or more processors to perform operations for providing an interactive tool to dynamically determine and modify a cybersecurity risk level of a portfolio of companies, the operations comprising:

determining an initial cybersecurity risk level for the portfolio;

identifying at least one company that experienced a cybersecurity risk event during a certain time period;

identifying:

at least one attribute common to the at least one identified company that experienced the cybersecurity risk event and a plurality of companies in the portfolio, and

a degree of mutuality of the at least one attributes;

determining a probability that another cybersecurity risk event will occur with respect to the plurality of companies in the portfolio, where the probability depends on:

the number of identified common attributes, and

degrees of mutuality of the number of identified attributes;

generating, from the determined probability, a cybersecurity risk multiplier for the portfolio;

generating a refined cybersecurity risk level that is a function of the initial cybersecurity risk level and the cybersecurity risk multiplier;

determining one or more actions to reduce the refined cybersecurity risk level; and

displaying, to a user, an interactive tool that enables the user to view:

the refined cybersecurity risk level for the portfolio;

the one or more actions that the user can take to reduce the refined cybersecurity risk level and the effect that the one or more actions have on the refined cybersecurity level, and

execute at least one action of the one or more actions to reduce the refined cybersecurity risk level.

Black Kite Ex. 1002, Page 253 of 1060

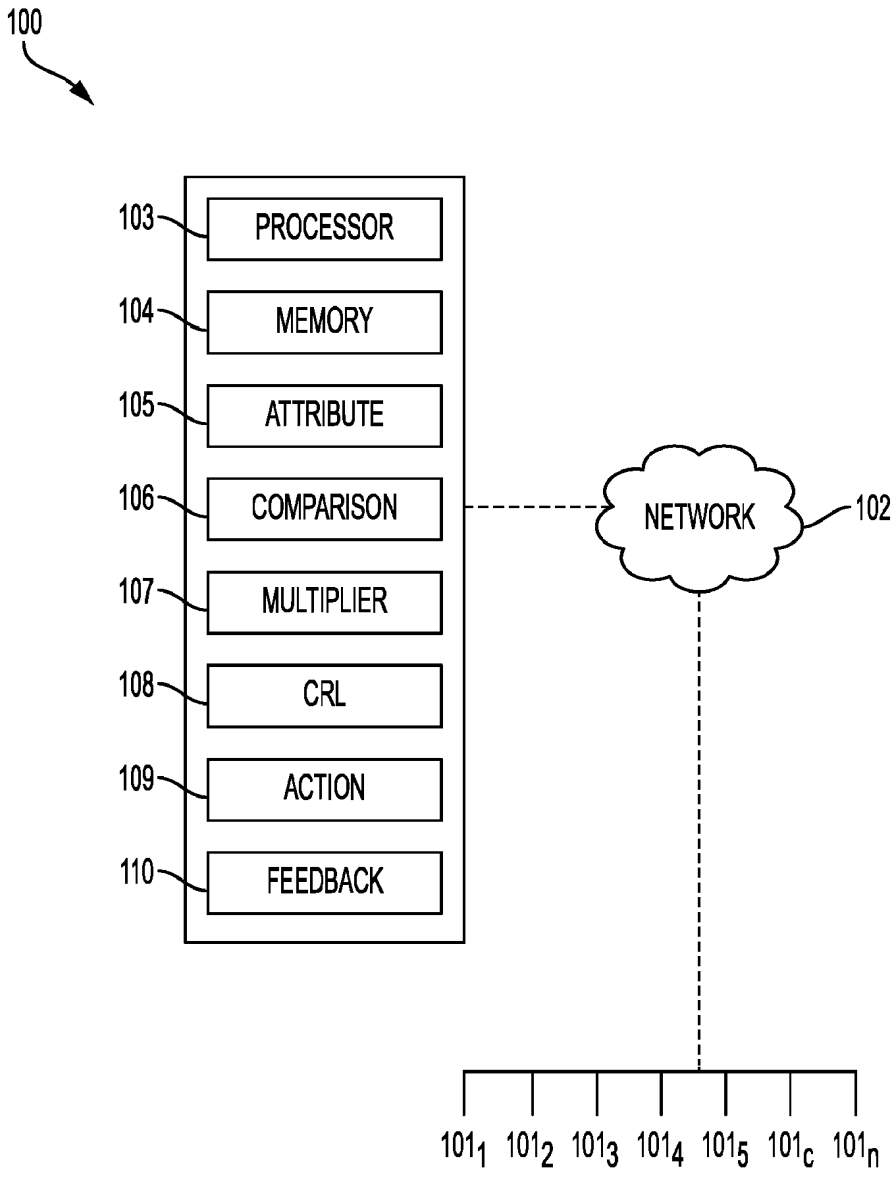


FIG. 1

Black Kite Ex. 1002, Page 254 of 1060

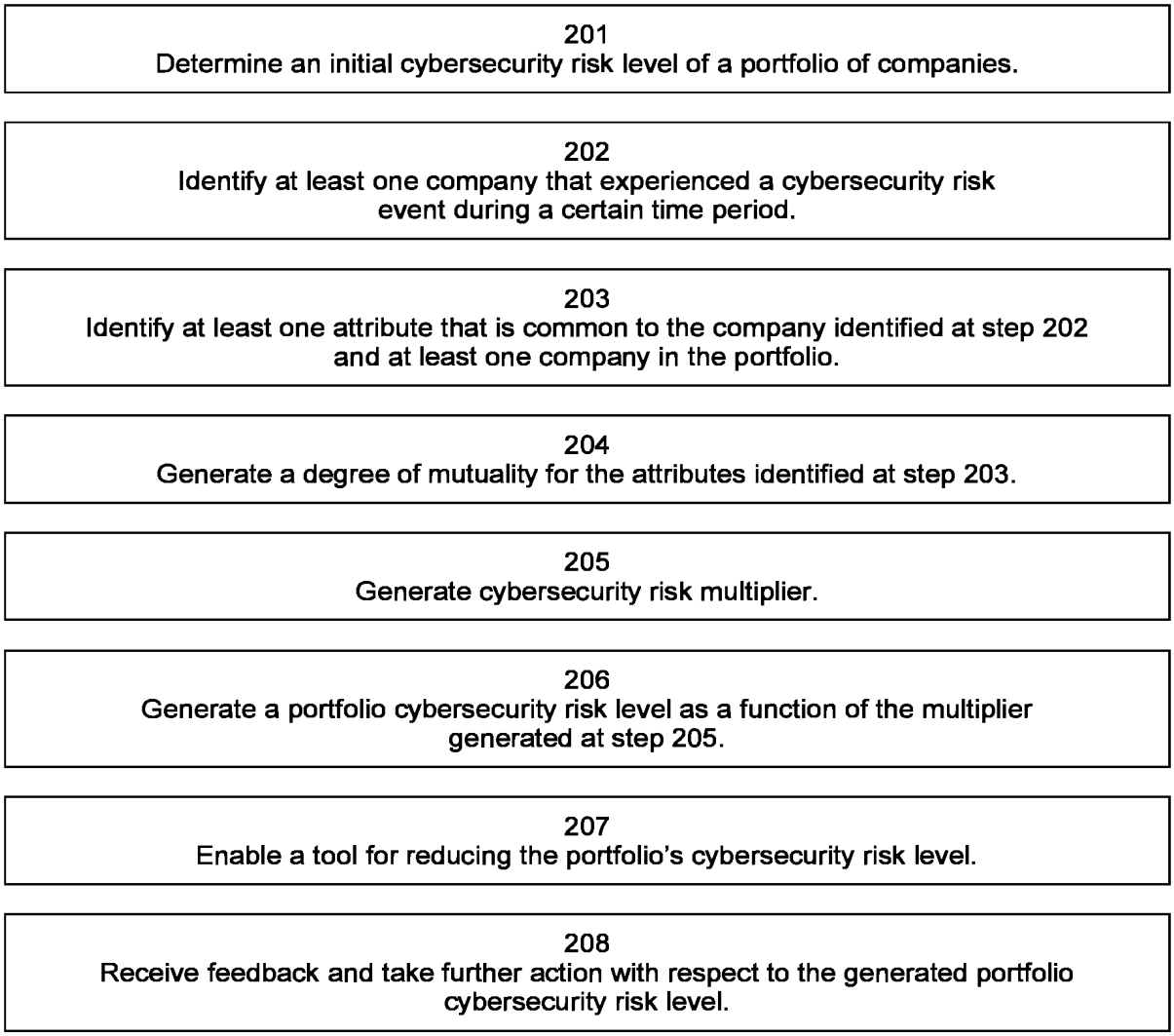

201
Determine an initial cybersecurity risk level of a portfolio of companies.
202
Identify at least one company that experienced a cybersecurity risk event during a certain time period.
203
Identify at least one attribute that is common to the company identified at step 202 and at least one company in the portfolio.
204
Generate a degree of mutuality for the attributes identified at step 203.
205
Generate cybersecurity risk multiplier.
206
Generate a portfolio cybersecurity risk level as a function of the multiplier generated at step 205.
207
Enable a tool for reducing the portfolio's cybersecurity risk level.
208
Receive feedback and take further action with respect to the generated portfolio cybersecurity risk level.

FIGURE 2

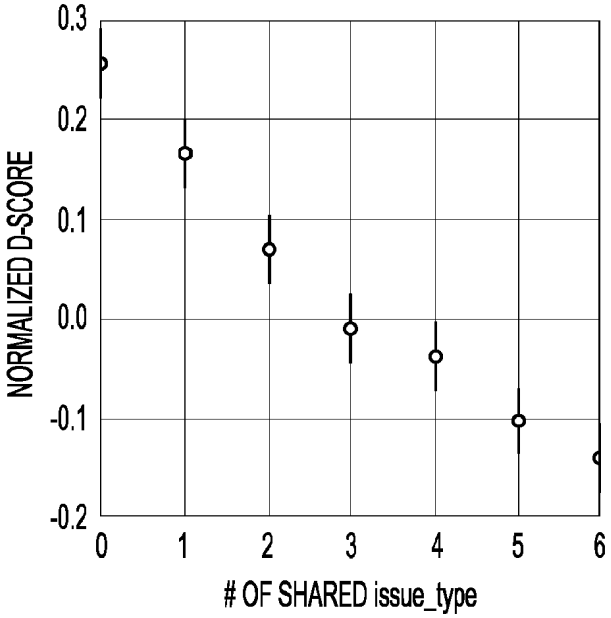


FIG. 3A

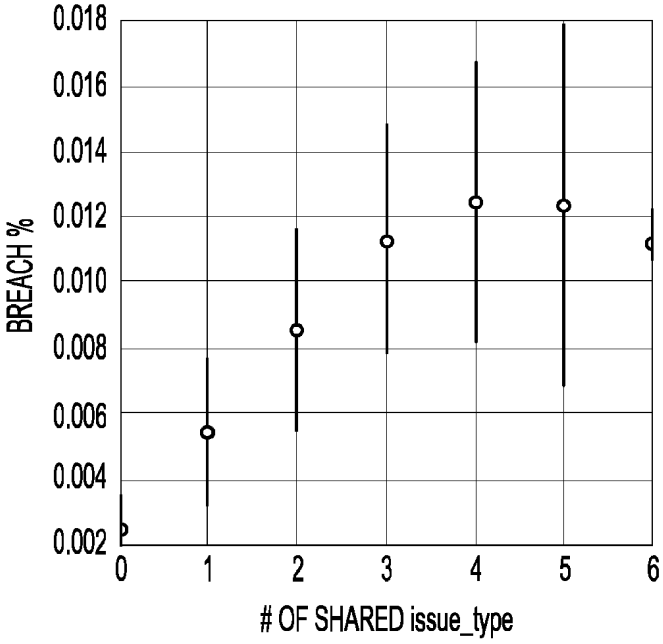


FIG. 3B

Black Kite Ex. 1002, Page 256 of 1060

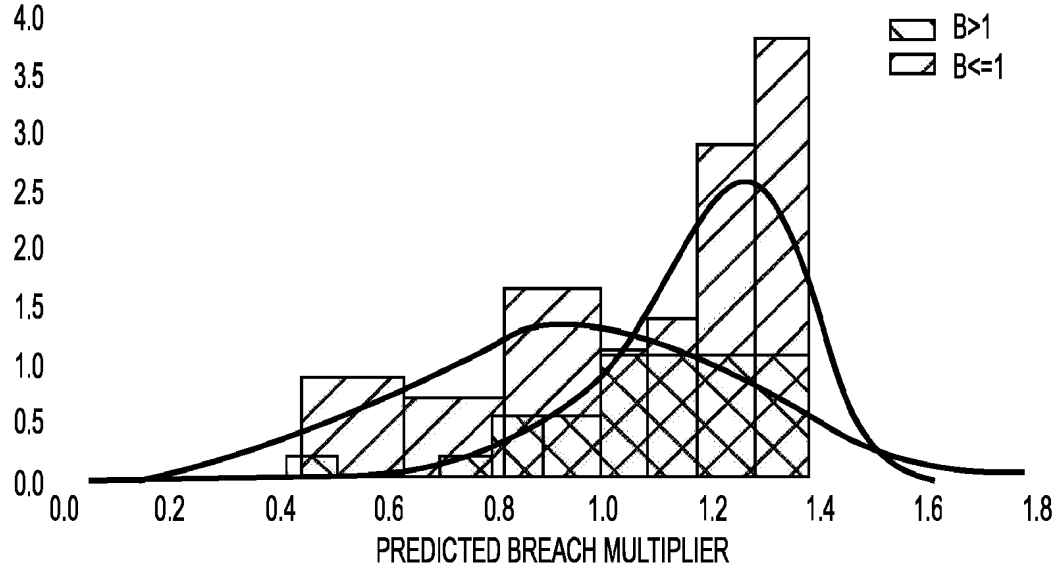


FIG. 4A

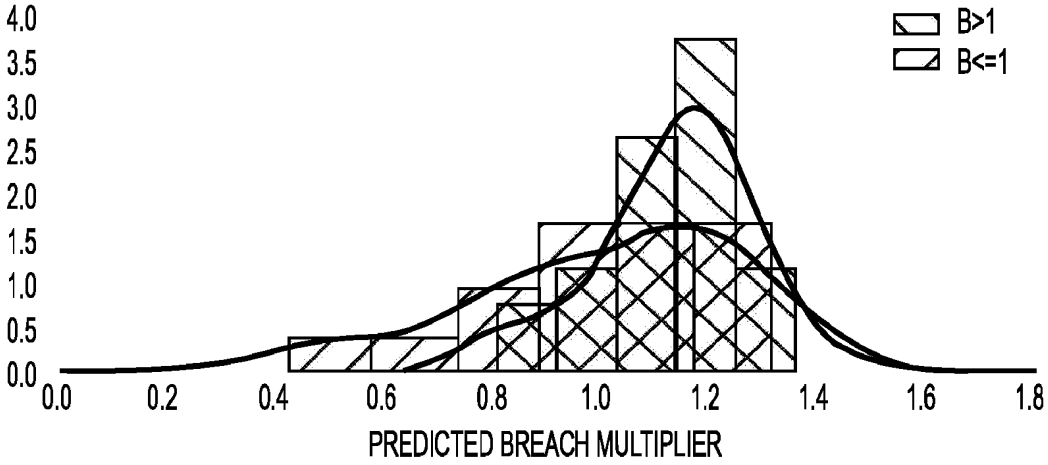


FIG. 4B

Black Kite Ex. 1002, Page 257 of 1060

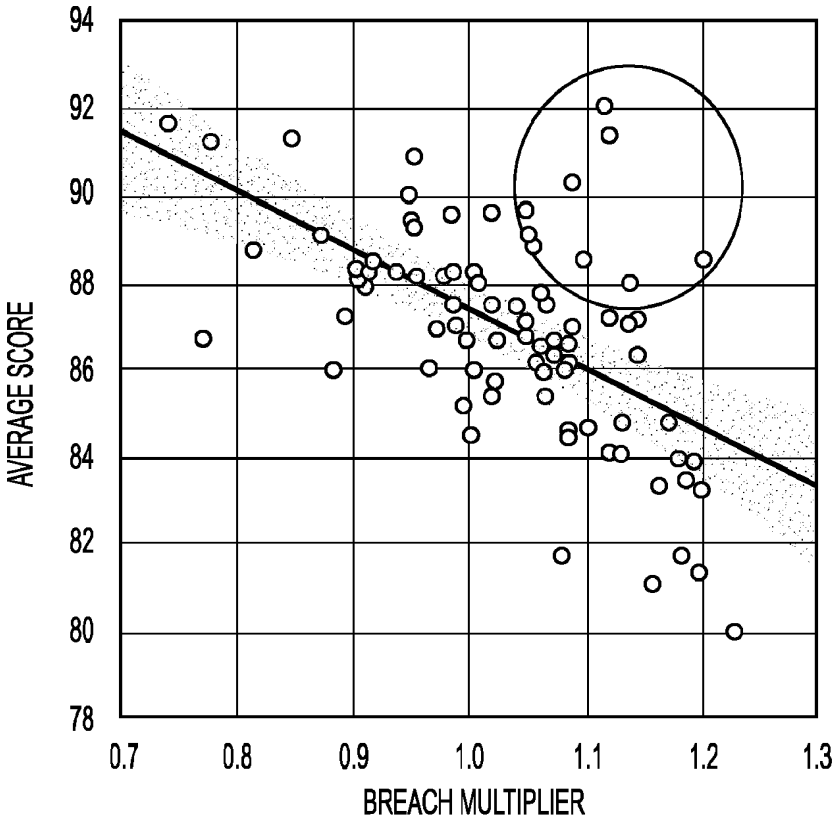


FIG. 5

Black Kite Ex. 1002, Page 258 of 1060

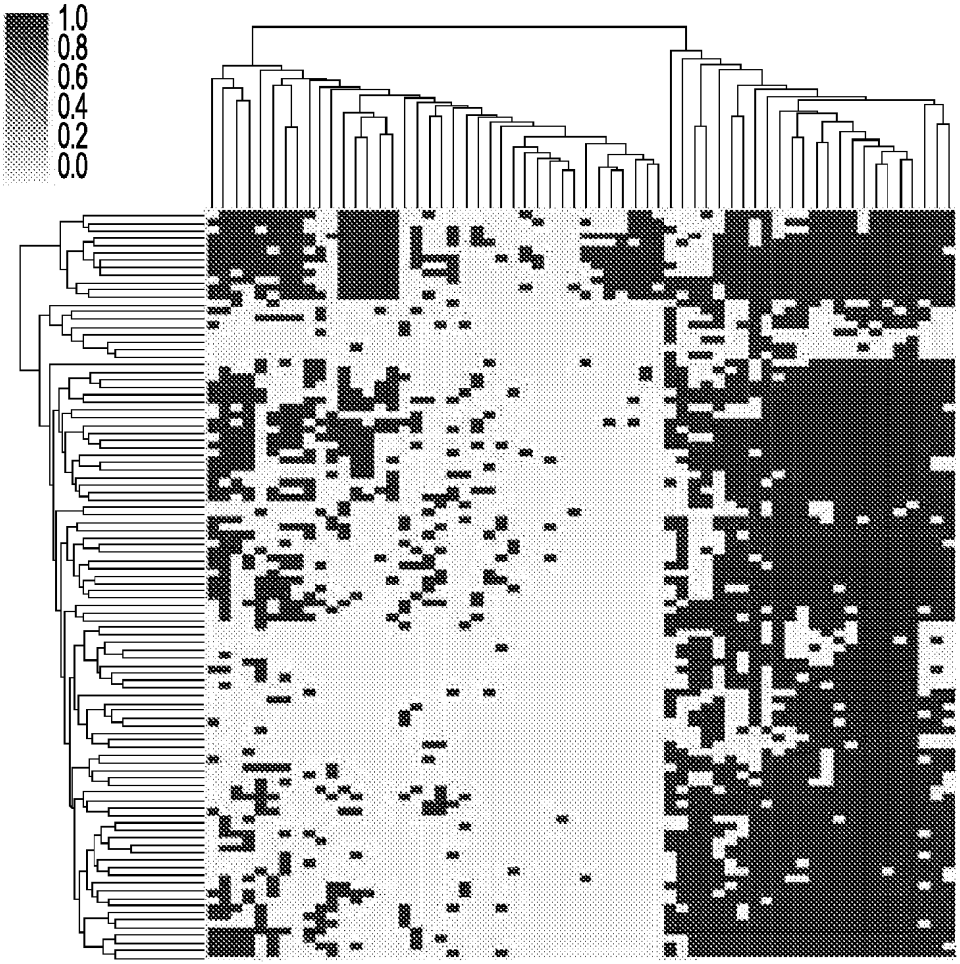


FIG. 6A

Black Kite Ex. 1002, Page 259 of 1060

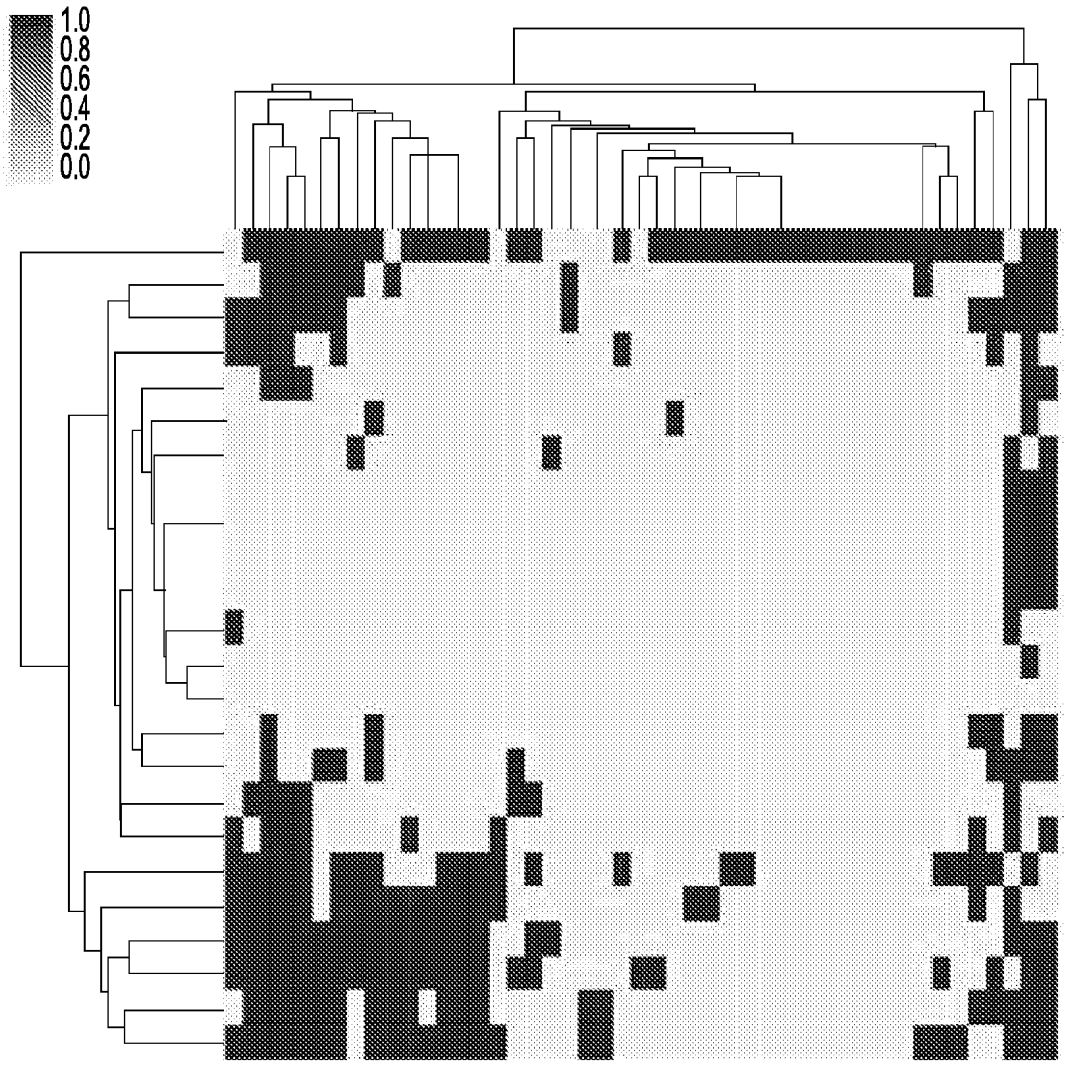


FIG. 6B

Black Kite Ex. 1002, Page 260 of 1060

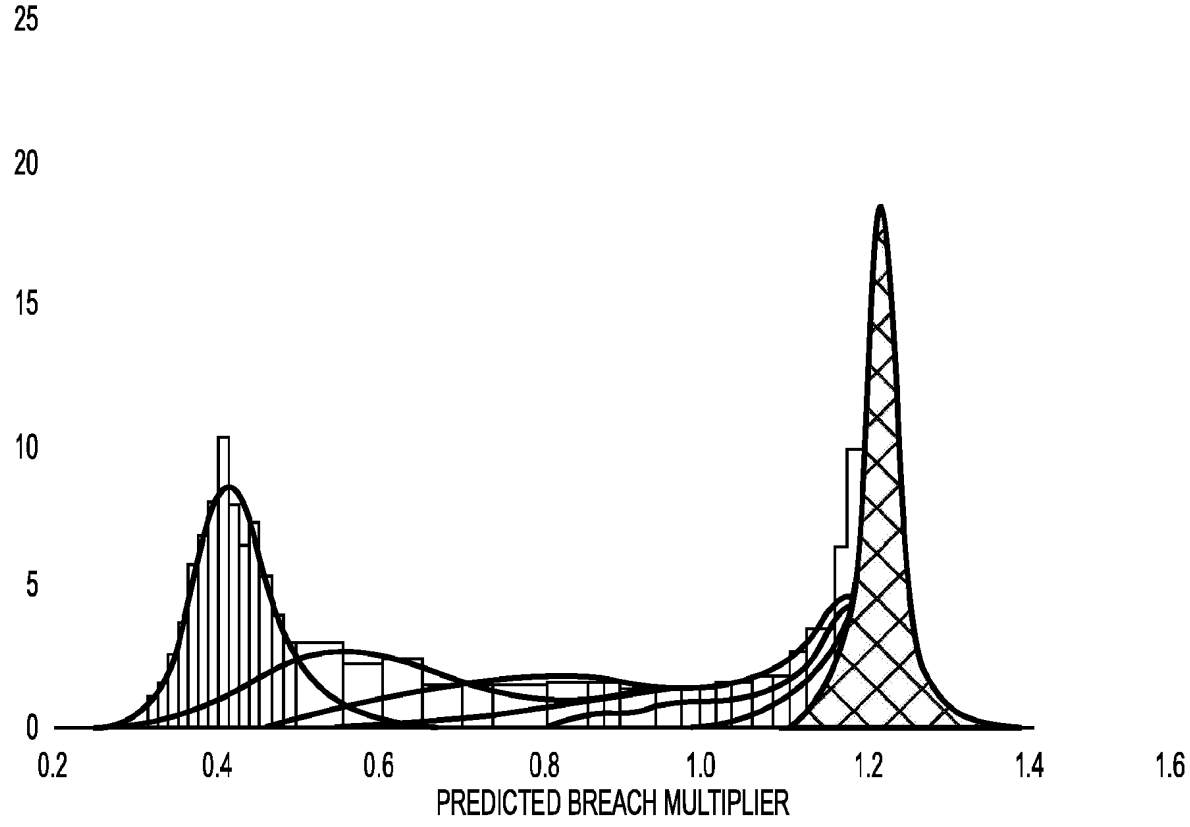


FIG. 7

Black Kite Ex. 1002, Page 261 of 1060

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US18/42957

A. CLASSIFICATION OF SUBJECT MATTER

IPC - G06F 15/16, 17/30, 21/57; G06Q 10/06; H04L 29/06 (2018.01)

CPC - G06F 15/16, 17/30, 21/577; G06Q 10/0635; H04L 29/06, 63/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

See Search History document

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

See Search History document

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

See Search History document

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2017/0048267 A1 (SECURITY SCORECARD, INC.) 16 February 2017; entire document	1-20
A	US 2015/0207813 A1 (VORSTACK, INC.) 23 July 2015; entire document	1 20
A	WO 2008/140683 A2 (SHELTONIX, INC.) 20 November 2008; entire document	1-20

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 August 2018 (23.08.2018)	19 SEP 2018
Name and mailing address of the ISA/ Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Authorized officer Shane Thomas PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (January 2015)

Docket No.: BST-004
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Stephen Wayne Boyer et al.

Application No.: 13/240,572 | Confirmation No.: 2423

Filed: September 22, 2011 | Art Unit: 2492

For: INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM | Examiner: S. P. Kanaan

Submitted via EFS-Web

INFORMATION DISCLOSURE STATEMENT (IDS)

Pursuant to 37 C.F.R. §§ 1.56, 1.97, and 1.98, the attention of the United States Patent and Trademark Office is hereby directed to the references listed on the attached PTO/SB/08. It is respectfully requested that the information be expressly considered during the prosecution of the above-identified application, and that the references be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Information Disclosure Statement is being submitted with a Request for Continued Examination.

In accordance with 37 CFR 1.98(a)(2)(ii), Applicant has not submitted copies of U.S. patents and U.S. patent applications.

In accordance with 37 C.F.R. § 1.97(g), the filing of this Information Disclosure Statement shall not be construed as a representation that a search has been made. In accordance with 37 C.F.R. § 1.97(h), the filing of this Information Disclosure Statement shall not be construed to be an admission that the information cited in this Information Disclosure Statement is, or is considered to be, material to patentability as defined in 37 C.F.R. § 1.56(b).

Applicant has cited for the Examiner's consideration certain co-pending U.S. patent applications that are owned at least in part by the assignee of this application, that describe subject matter that may be related to the present invention. The co-pending applications are listed herewith in accordance with M.P.E.P. 609.06 which states: "Applicant may wish to list U.S. patent application numbers on other than a form PTO/SB/08A and 08B format to avoid the application numbers of pending applications being published on the patent. If a citation is not printed on the patent but has been considered by the examiner, the patented file will reflect that fact as noted in MPEP § 609.05(b)."

No copies of the co-pending applications have been provided. If the Examiner wishes to have copies of the co-pending applications, Examiner should contact the Attorney or Agent of record. Applicant respectfully requests that the Examiner consider these listed documents and indicate that each was considered by making appropriate notations on this Information Disclosure Statement.

Docket No.	**U.S. Serial No.:**	**Title**	**Filing Date**
BST-002	15/377,574 9,705,932	METHODS AND SYSTEMS FOR CREATING, DE-DUPLICATING, AND ACCESSING DATA USING AN OBJECT STORAGE SYSTEM	December 13, 2016
BST-003	14/021,585 9,438,615 Published as: US2015/0074579	SECURITY RISK MANAGEMENT	September 9, 2013
BST-003C1	15/216,955 Published as: US2016/0330231	METHODS FOR USING ORGANIZATIONAL BEHAVIOR FOR RISK RATINGS	July 22, 2016
BST-003C2	15/239,063 Published as: US2017/0093901	SECURITY RISK MANAGEMENT	August 17, 2016

Docket No.	U.S. Serial No.:	Title	Filing Date
BST-004C1	14/944,484 9,973,524 Published as: US2016/0323308	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM	November 18, 2015
BST-004C1CP	15/142,677 9,830,569 Published as: US/2016/0239772	SECURITY ASSESSMENT USING SERVICE PROVIDER DIGITAL ASSET INFORMATION	April 29, 2016
BST-007	15/134,845 9,680,858	ANNOTATION PLATFORM FOR A SECURITY RISK SYSTEM	April 21, 2016
BST-008	15/044,952 Published as: US2017/0236077	RELATIONSHIPS AMONG TECHNOLOGY ASSETS AND SERVICES AND THE ENTITIES RESPONSIBLE FOR THEM	February 16, 2016
BST-008C2	15/089,375 10,176,445 Published as: US2017/0236079	RELATIONSHIPS AMONG TECHNOLOGY ASSETS AND SERVICES AND THE ENTITIES RESPONSIBLE FOR THEM	April 1, 2016
BST-009DA	29/598,298 D835,631	COMPUTER DISPLAY SCREEN WITH GRAPHICAL USER INTERFACE	March 24, 2017
BST-009DB	29/598,299 D818,475	COMPUTER DISPLAY WITH SECURITY RATINGS GRAPHICAL USER INTERFACE	March 24, 2017
BST-009DC	29/599,622	COMPUTER DISPLAY WITH SECURITY RATINGS GRAPHICAL USER INTERFACE	April 5, 2017

Docket No.	U.S. Serial No.:	Title	Filing Date
BST-009DD	29/599,620	COMPUTER DISPLAY WITH SECURITY RATINGS GRAPHICAL USER INTERFACE	April 5, 2017
BST-010	16/015,686	METHODS FOR MAPPING IP ADDRESSES AND DOMAINS TO ORGANIZATIONS USING USER ACTIVITY DATA	June 22, 2018
BST-011	15/918,286	CORRELATED RISK IN CYBERSECURITY	March 12, 2018
BST-011C1	16/292,956	CORRELATED RISK IN CYBERSECURITY	May 5, 2019
BST-011C2	16/795,056	CORRELATED RISK IN CYBERSECURITY	February 19, 2020
BST-012	16/170680	SYSTEMS AND METHODS FOR REMOTE DETECTION OF SOFTWARE THROUGH BROWSER WEBINJECTS	October 25, 2018
BST-012C1	16/688647	SYSTEMS AND METHODS FOR REMOTE DETECTION OF SOFTWARE THROUGH BROWSER WEBINJECTS	November 19, 2019
BST-013	15/954921	SYSTEMS AND METHODS FOR EXTERNAL DETECTION OF MISCONFIGURED SYSTEMS	April 17, 2018
BST-014	16/549764	SYSTEMS AND METHODS FOR INFERRING ENTITY RELATIONSHIPS VIA NETWORK COMMUNICATIONS OF USERS OR USER DEVICES	August 23, 2019
BST-014C1	16/787,650	SYSTEMS AND METHODS FOR INFERRING ENTITY RELATIONSHIPS VIA NETWORK COMMUNICATIONS OF USERS OR	February 11, 2020

Docket No.	U.S. Serial No.:	Title	Filing Date
		USER DEVICES	
BST-015	16/583991	SYSTEMS AND METHODS FOR NETWORK ASSET DISCOVERY AND ASSOCIATION THEREOF WITH ENTITIES	September 26, 2019
BST-016D	29/666942	COMPUTER DISPLAY WITH GRAPHICAL USER INTERFACE	October 17, 2018
BST-017	16/360,641	SYSTEMS AND METHODS FOR FORECASTING CYBERSECURITY RATINGS BASED ON EVENT-RATE SCENARIOS	March 21, 2019
BST-018	16/514,771	SYSTEMS AND METHODS FOR GENERATING SECURITY IMPROVEMENT PLANS FOR ENTITIES	July 17, 2019
BST-019D	29/677306	COMPUTER DISPLAY WITH CORPORATE HIERARCHY GRAPHICAL USER INTERFACE COMPUTER DISPLAY WITH CORPORATE HIERARCHY GRAPHICAL USER INTERFACE	January 18, 2019
BST-020	16/775840	SYSTEMS AND METHODS FOR ASSESSING CYBERSECURITY STATE OF ENTITIES BASED ON COMPUTER NETWORK CHARACTERIZATION	January 29, 2020
BST-021	16/779437	SYSTEMS AND METHODS FOR RAPIDLY GENERATING SECURITY RATINGS	January 31, 2020
BST-023	16/802232	SYSTEMS AND METHODS FOR IMPROVING A SECURITY PROFILE OF AN ENTITY BASED ON PEER SECURITY PROFILES	February 26, 2020

Docket No.	U.S. Serial No.:	Title	Filing Date
BST-023DA	29/725724	COMPUTER DISPLAY WITH RISK VECTORS GRAPHICAL USER INTERFACE	February 26, 2020

Additionally, Applicant hereby apprises the Examiner of the following patents and patent applications, including the contents of the file wrappers, the claims, any Office Actions issued therein, and any Notices of Allowance issued therefor:

1. U.S.S.N. 15/377,574 (Attorney Docket No. BST-002), now U.S. Patent No. 9,705,932, the Office Action mailed 03/02/2017 and the Notice of Allowance mailed 06/01/2017;

2. U.S.S.N. 14/021,585 (Attorney Docket No. BST-003), now U.S. Patent No. 9,438,615, the Office Action mailed 03/11/2016 and the Notice of Allowance mailed 08/09/2016;

3. U.S.S.N. 15/216,955 (Attorney Docket No. BST-003C1), the Office Actions mailed 11/04/2016, 03/09/2017, 06/06/2017, 12/05/2017, and 08/29/2018, and the Notice of Allowance mailed 02/06/2019;

4. U.S.S.N. 15/239,063 (Attorney Docket No. BST-003C2), the Office Action mailed 03/21/2018 and the Notice of Allowance mailed 01/14/2019;

5. U.S.S.N. 14/944,484 (Attorney Docket No. BST-004C1), now U.S. Patent No. 9,973,524, the Office Actions mailed 03/11/2016, 07/05/2016, and 01/17/2017 and the Notice of Allowance mailed 10/20/2017;

6. U.S.S.N. 15/142,677 (Attorney Docket No. BST-004C1CP), now U.S. Patent No. 9,830,569, the Office Actions mailed 07/26/2016, and 04/24/2017 and the Notice of Allowance mailed 10/11/2017;

7. U.S.S.N. 15/134,845 (Attorney Docket No. BST-007), now U.S. Patent No. 9,680,858, the Office Actions mailed 07/19/2016 and 01/26/2017, and the Notices of Allowance mailed 04/27/2017 and 05/09/2017;

8. U.S.S.N. 15/089,375 (Attorney Docket No. BST-008C2), now U.S. Patent No. 10,176,445, the Office Actions mailed 09/09/2016, 05/17/2017, and 11/17/2017 and the Notice of Allowance mailed 08/09/2018;

9. U.S.S.N. 29/598,298 (Attorney Docket No. BST-009DA), now U.S. Patent No. D835,631, the Notice of Allowance mailed 08/15/2018;

10. U.S.S.N. 29/598,299 (Attorney Docket No. BST-009DB), now U.S. Patent No. D818,475, the Notice of Allowance mailed 01/02/2018;

11. U.S.S.N. 29/599,622 (Attorney Docket No. BST-009DC), the Notice of Allowance mailed 12/11/2018;

12. U.S.S.N. 29/599,620 (Attorney Docket No. BST-009DD), the Notice of Allowance mailed 11/27/2018;

13. U.S.S.N. 16/015,686 (Attorney Docket No. BST-010), the Office Action mailed 11/16/2018; the Notice of Allowance mailed 05/10/2019;

14. U.S.S.N. 15/918,286 (Attorney Docket No. BST-011), the Office Action mailed 08/07/2018 and the Notice of Allowance mailed 11/29/2018; and

15. U.S.S.N. 16/292,956 (Attorney Docket No. BST-011C1), the Office Action mailed 07/10/2019; the Notices of Allowance mailed 01/08/2020 and 01/27/2020;

16. U.S.S.N. 16/795,056 (Attorney Docket No. BST-011C2), the Office Action mailed 05/01/2020;

17. U.S.S.N. 16/170,680 (Attorney Docket No. BST-012), the Office Action mailed 03/26/2019; the Notices of Allowance mailed 10/29/2019 and 08/27/2019;

18. U.S.S.N. 16/688,647 (Attorney Docket No. BST-012C1), the Office Action mailed 01/29/2020;

19. U.S.S.N. 15/954,921 (Attorney Docket No. BST-013), the Office Actions mailed 08/19/2019, 09/04/2018 and 01/03/2019; Advisory Action mailed 03/03/2020;

20. U.S.S.N. 16/787,650 (Attorney Docket No. BST-014C1), the Notice of Allowance mailed 04/07/2020;

21. U.S.S.N. 16/583,991 (Attorney Docket No. BST-015), the Office Action mailed 01/13/2020;

22. U.S.S.N. 29/666,942 (Attorney Docket No. BST-016D), the Notice of Allowance mailed 04/30/2020;

23. U.S.S.N. 16/360,641 (Attorney Docket No. BST-017), the Office Action mailed 08/07/2019 and 02/20/2020;

24. U.S.S.N. 16/514,771 (Attorney Docket No. BST-018), the Office Action mailed 12/04/2019; the Notice of Allowance mailed 03/18/2020; and

25. U.S.S.N. 16/802,232 (Attorney Docket No. BST-023), the Notice of Allowance mailed 04/24/2020.

As stated above, a Request for Continued Examination and related fee are being submitted with this paper. If any additional fees are due, the Director is hereby authorized to charge such fees to our Deposit Account No. 07-1700, under Order No. BST-004.

Dated: May 15, 2020

Respectfully submitted,

Electronic signature: /Gozde Guckaya/
Gozde Guckaya
Registration No.: 74,989
GOODWIN PROCTER LLP
100 Northern Avenue
Boston, Massachusetts 02210
(617) 305-6778
Agent for Applicant

Doc code: RCEX
Doc description: Request for Continued Examination (RCE)

PTO/SB/30EFS (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)

Application Number	13240572	Filing Date	2011-09-22	Docket Number (if applicable)	BST-004	Art Unit	2492
First Named Inventor	Stephen Wayne Boyer			Examiner Name	S. P. Kanaan		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

- ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
- ☐ Other _____

☒ Enclosed

- ☐ Amendment/Reply
- ☒ Information Disclosure Statement (IDS)
- ☐ Affidavit(s)/ Declaration(s)
- ☒ Other REQUEST TO REOPEN PROSECUTION IN RESPONSE TO NEW GROUND OF REJECTION UNDER 37 C.F.R. § 41.50(b)(1)

MISCELLANEOUS

☐ Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

☐ Other _____

FEES

The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.
☒ The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 07-1700

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

☒ Patent Practitioner Signature

Applicant Signature

PTO/SB/30EFS (02-18)
Approved for use through 11/30/2020. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Signature of Registered U.S. Patent Practitioner			
Signature	/Gozde Guckaya/	Date (YYYY-MM-DD)	2020-05-15
Name	Gozde Guckaya	Registration Number	74989

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Docket No.: BST-004
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant: Stephen Wayne Boyer et al.

Application No.: 13/240,572 | Confirmation No.: 2423

Filed: September 22, 2011 | Art Unit: 2492

For: INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM | Examiner: S. P. Kanaan

Submitted via EFS-Web

REQUEST TO REOPEN PROSECUTION IN RESPONSE TO NEW GROUND OF REJECTION UNDER 37 C.F.R. § 41.50(b)(1)

Applicant respectfully submits a request to reopen prosecution under 37 C.F.R. § 41.50(b)(1) in response to a new ground of rejection in the Decision on Appeal issued March 16, 2020 (the "Decision").

In response to the Decision, please consider amendments and remarks in support thereof for the above-identified U.S. patent application as follows:

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks begin on page 9 of this paper.

Appellant submits that this request is timely submitted, i.e., within two months of mailing of the Decision. The Office is authorized to charge any additional fees necessary for entry of this paper to Deposit Account No. 07-1700 (Order No. BST-004).

AMENDMENTS TO THE CLAIMS

1. (Currently amended) A method comprising:

collecting information about two or more organizations that have computer systems, network resources, and employees, the organizations posing risks through business relationships of the organizations with other parties, the information collected about the organizations being indicative of compromises, vulnerabilities or configurations of technology systems of the organizations and indicative of resiliencies of the organizations to recover from such compromises, vulnerabilities or configurations, the information indicative of durations of events associated with compromises or vulnerabilities or configurations,

at least some of the information about each of the organizations being collected automatically by computer using sensors on the Internet,

the information about each of the organizations being collected from two or more sources, one or more of the sources not being controlled by the organization, the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization,

at least partly automatically gathering information about assets that each of the organizations owns, controls, uses, or is affiliated with, including IP addresses and IP network address ranges, computer services residing within address ranges, or domain names,

at least one of the sources for each of the organizations comprising a public source or a commercial source,

processing by computer the information from the two or more sources for each of the organizations to form a composite rating of the organization that is indicative of a degree of risk to the organization or to a party through a business relationship with the organization, the composite rating comprising a calculated composite of metrics and data derived or collected from the sources, the processing comprising applying transformations to the data and metrics, and the processing comprising applying weights to the data and the metrics,

the metrics including a measure of the extent of, the frequency of, or duration of compromise of the technology systems of the organization, or of a configuration or vulnerability of the organization, and a measure of the resilience of the organization to recover from such

vulnerability, the measure of the resilience being inversely proportional to ~~one or more of~~ the duration of detected malicious activity ~~and the duration of the vulnerability~~, and

in connection with assessing a business risk to the organization or to a party through a business relationship with at least one of the organizations, delivering reports of the composite ratings of the organizations through a reporting facility to enable users of the reporting facility to monitor, assess, and mitigate the risks, based on the security vulnerabilities and resiliencies, in doing business with the organization and to compare the composite ratings of the organizations.

2-3. (Cancelled)

4. (Original) The method of claim 1, wherein the collected information is represented by at least two data types.

5. (Original) The method of claim 4, wherein the at least two data types include at least one of breach disclosures, block lists, configuration parameters, an identification of malware servers, an identification of a reputation, an identification of suspicious activity, an identification of spyware, white lists, an identification of compromised hosts, an identification of malicious activity, an identification of spam activity, an identification of vulnerable hosts, an identification of phishing activity, or an identification of e-mail viruses.

6. (Cancelled)

7. (Original) The method of claim 1, wherein the collected information evidences internal security controls.

8. (Original) The method of claim 1, wherein the collected information comprises outcomes of each of the organizations.

9. (Original) The method of claim 1, wherein the collected information evidences operational execution of security measures of each of the organizations.

10. (Original) The method of claim 1, wherein the collected information indicates whether a computer system of each of the organizations served malicious code to another system.

11. (Original) The method of claim 1, wherein the collected information indicates whether a computer system of each of the organizations communicated with a known attacker controlled network or sensor outside the control or network of the organization.

12. (Original) The method of claim 1, comprising: forming a series of the security ratings of each of the organizations.

13. (Original) The method of claim 12, comprising: determining a trend from the series of ratings.

14. (Original) The method of claim 12, comprising displaying the series of composite ratings.

15. (Cancelled)

16. (Original) The method of claim 14, wherein displaying the series of composite ratings for each of the organizations comprises posting the series of composite ratings for the organization to a web portal.

17-120. (Cancelled)

121. (Original) The method of claim 1, wherein the collected information represents externally observable outcome information.

122-123. (Cancelled)

124. (Original) The method of claim 1, comprising: determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information.

125. (Cancelled)

126. (Original) The method of claim 1, wherein: the collected information comprises at least two security characterizations of a computer system of each of the organizations.

127. (Original) The method of claim 1, wherein the collected information comprises a characterization of behavior of an employee of at least one of the organizations.

128. (Original) The method of claim 1, wherein the collected information comprises characterizations other than characterizations about a computer system of at least one of the organizations.

129. (Original) The method of claim 1, wherein the collected information comprises characterizations about policies of at least one of the organizations.

130. (Original) The method of claim 1, wherein the collected information comprises characterizations about information technology assets that at least one of the organizations owns, controls, uses, or is affiliated with.

131. (Original) The method of claim 1 in which collected information represents: (a) physical states, (b) technical states, (c) organizational states, or (d) cultural states of at least one of the organizations which can be exploited to create a security breach; or (e) the organization's ability to recover from a security breach; or any combination of two or more of these.

132. (Original) The method of claim 1 in which processing the information to form a composite rating comprises correlating data across the sources of information.

133. (Cancelled)

134. (Original) The method of claim 1 in which processing the information to form a composite rating comprises statistically correlating the composite rating with actual outcomes.

135. (Original) The method of claim 1 in which the vulnerability comprises physical, technical, organizational, or cultural states that can be exploited to create a security breach.

136. (Currently amended) A method comprising:

collecting, from at least two sources, information about two or more organizations, the collected information representing at least two data types, the collected information comprising outcomes of each of the organizations,

at least some of the information for each of the organizations being collected automatically by computer from at least two sources, one or more of the sources not controlled by the organization,

the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization, at least one of the sources including a commercial data source,

processing the information from both of the two sources for each of the organizations to form a composite rating of a security vulnerability of the organization and of a resilience of the organization to recover from a security breach, the resilience being inversely proportional to ~~one or more of~~ the duration of detected malicious activity ~~and the duration of the vulnerability, or both~~, the processing including applying models that account for differences in the respective sources,

normalizing the composite rating of each of the organizations based on a size characteristic of the organization to enable comparisons of composite ratings between the two or more organizations,

forming a series of the security ratings of each of the organizations, determining a trend from the series of ratings, and displaying the series of composite ratings through a portal,

determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information, and

reporting the composite ratings of the organizations through a portal to enable customers to monitor, assess, and mitigate risk in doing business with the organizations and to compare the composite ratings across the organizations.

137. (Currently amended) The system of claim 136, determining a confidence range of the composite rating, the size of the range varying inversely with the level of confidence in the composite rating.

138. (Original) The system of claim 137, wherein the confidence range is based on redundancy of the security characterizations.

139. (Original) The system of claim 137, wherein the confidence range is based on a size of the third party computer system.

140. (Original) The method of claim 1 comprising ranking the organization and other organizations within sectors or peer-groups or globally.

141. (Currently amended) A method comprising:

collecting information about an organization that has computer systems, network resources, and employees, the organization posing risks to itself or to other parties through business relationships of the organization with the other parties,

the information collected about the organization including (a) information collected automatically by computer on the Internet without permission of the organization, and (b) information indicative of resiliencies of the organization to recover from a security breach associated with a compromise or a vulnerability, the resiliencies being inversely proportional to ~~one or more of~~ the duration of detected malicious activity ~~and the duration of the compromise or vulnerability~~,

processing the information by computer to form a composite rating of the organization that is indicative of a degree of risk based on a business relationship with the organization, the composite rating comprising a measure of the resiliencies of the organization to recover from a security breach, and

in connection with assessing the degree of risk, delivering a report of the composite rating of the organization through a reporting facility to enable a user of the reporting facility to assess the risks, based at least in part on the resiliencies.

REMARKS

Claims 1, 136, 137, and 141 are amended. No claims are added or cancelled. Therefore, claims 1, 4, 5, 7-14, 16, 121, 124, 126-132, and 134-141 are pending. Claim 137 has been amended to correct a typographical error. Support for the amendments to claims 1, 136, and 141 can be found in at least page 13, lines 14-24 of the instant Application. No new matter has been added.

New Ground of Rejection under 35 U.S.C. § 112

Claims 1, 4, 5, 7-14, 16, 121, 124, 126-132, and 134-141 were rejected under 35 U.S.C. § 112, paragraph 1, for purportedly lacking adequate written description. Applicant has amended independent claim 1, without disclaimer or prejudice, to recite, in part, as follows:

> A method comprising:
> ...
> the metrics including a measure of the extent of, the frequency of, or duration of compromise of the technology systems of the organization, or of a configuration or vulnerability of the organization, and a measure of the resilience of the organization to recover from such vulnerability, **the measure of the resilience being inversely proportional to the duration of detected malicious activity**, ...
> (Emphasis added.)

Applicant respectfully submits that claim 1 as amended overcomes the rejection under § 112, paragraph 1. In particular, support for the amendment can be found in at least page 13 (lines 14-24), reproduced below:

> Organizational security risk may be measured along two vectors: vulnerability and resilience. An entity's vulnerability is defined as its "physical, technical, organizational, and cultural states," which can be exploited to create a security breach. An entity's resilience is defined to be its ability to recover from a security breach.
>
> The system 10 uses the concepts of vulnerability and resilience by examining externally observable proxies for them. An example proxy for entity vulnerability is the number of entity-owned IP addresses,' which are reported to be malicious. The higher the number of reports the more likely the entity was vulnerable and had been compromised. **Resilience is inversely proportional to**

> **the duration of detected malicious activity.** The shorter the duration of the malicious activity, the higher level of resilience the entity demonstrates as it can quickly identify and remove malicious infections.
> (Emphasis added.)

Applicant respectfully submits that independent claim 1, as amended, is patentable for at least the above reason. Independent claims 136 and 141 have been amended in an analogous manner and are therefore also patentable for at least the above reason. Claims 4, 5, 7-14, 16, 121, 124, 126-132, 134, 135, and 137-140 depend, directly or indirectly, on independent claim 1 or independent claim 136 and therefore also are patentable for at least the above reason.

Conclusion

In view of the foregoing, Applicant respectfully submit that claims 1, 4, 5, 7-14, 16, 121, 124, 126-132, and 134-141 are in condition for allowance. If the Examiner believes that another telephone conversation with Applicant's representatives would expedite the allowance of this application or would be helpful in resolving any outstanding issue, the Examiner is invited to call the undersigned at the telephone number set forth below.

Dated: May 15, 2020

Respectfully submitted,

Electronic signature: /Gozde Guckaya/
Gozde Guckaya
Registration No.: 74,989
Agent for Applicant
GOODWIN PROCTER LLP
100 Northern Avenue
Boston, Massachusetts 02210
(617) 305-6778

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/240,572	Filing Date 09/22/2011	☐ To be Mailed

ENTITY: ☐ LARGE ☑ SMALL ☐ MICRO

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A		N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A		N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*		x $26 =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*		x $110 =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).				
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))					
* If the difference in column 1 is less than zero, enter "0" in column 2.				TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT	05/15/2020	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 29	Minus	** 31	= 0		x $50 =	0
	Independent (37 CFR 1.16(h))	* 3	Minus	*** 3	= 0		x $230 =	0
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	0

		(Column 1)		(Column 2)	(Column 3)			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=		x $0 =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=		x $0 =	
	☐ Application Size Fee (37 CFR 1.16(s))							
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							
							TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.	SLIE
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".	/DIANIECE M JACOBS/
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".	
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.	

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/240,572	09/22/2011	Stephen Wayne Boyer	BST-004	2423

51414 7590 03/16/2020

GOODWIN PROCTER LLP
PATENT ADMINISTRATOR
100 NORTHERN AVENUE
BOSTON, MA 02210

EXAMINER	
KANAAN, SIMON P	

ART UNIT	PAPER NUMBER
2492	

NOTIFICATION DATE	DELIVERY MODE
03/16/2020	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JGoodwin@goodwinlaw.com
PSousa-Atwood@goodwinlaw.com
US-PatentBos@goodwinlaw.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte STEPHEN WAYNE BOYER, NAGARJUNA VENNA, and MEGUMI ANDO

Appeal 2019-001684
Application 13/240,572
Technology Center 2400

BEFORE JAMES B. ARPIN, STACEY G. WHITE, and JON M. JURGOVAN, *Administrative Patent Judges*.

ARPIN, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellant[1] appeals under 35 U.S.C. § 134(a), the Examiner's final rejections of claims 1, 4, 5, 7–14, 16, 121, 124, 126–132, and 134–141. Final Act. 4.[2] Claim 2, 3, 6, 15, 17–120, 122, 123, 125, and 133 are

---

[1] "Appellant" here refers to "applicant" as defined in 37 C.F.R. § 1.42. Appellant identifies the real party-in-interest as BitSight Technologies Inc. Appeal Br. 2. According to the Specification, because Appellant's work was supported by an award from the National Science Foundation, the U.S. Government has certain rights to the claimed invention. Spec., 1:4–5.

[2] In this Decision, we refer to Appellant's Appeal Brief ("Appeal Br.," filed December 21, 2017) and Reply Brief ("Reply Br.," filed July 27, 2018); the Final Office Action ("Final Act.," mailed February 13, 2017) and the Examiner's Answer ("Ans.," mailed May 16, 2018); and the originally-filed Specification ("Spec.," filed September 22, 2011). Rather than repeat the

canceled. Amdt., 3–8 (Nov. 9, 2016). We have jurisdiction under 35 U.S.C. § 6(b).

Because the claims lack adequate written description, we enter a new ground of rejection under 35 U.S.C. § 112, ¶ 1, and procedurally reverse the rejection under 35 U.S.C. § 103(a).

STATEMENT OF THE CASE

Appellant's claimed methods are "for creating a composite security rating from security characterization data of a third party computer system." Spec., 1:30–31.

As noted above, claims 1, 4, 5, 7–14, 16, 121, 124, 126–132, and 134–141 stand rejected. Claims 1, 136, and 141 are independent. Appeal Br. 15–16 (claim 1), 18–19 (claim 136), 20 (claim 141), (Claims App.). Claims 4, 5, 7–14, 16, 121, 124, and 137–140 depend directly or indirectly from claim 1. *Id.* at 16–20.

The Examiner relies on the same references and substantially similar arguments in rejecting claims 1, 136, and 141 (Final Act. 4–7, 14–16, 18–20), and Appellant does not contest the rejection of claims 4, 5, 7–14, 16, 121, 124, and 137–140 separately from claim 1 (Appeal Br. 11–13). Therefore, we focus our analysis on independent claim 1 and the disputed and overlapping limitations recited in independent claims 136 and 141.

Claim 1, reproduced below with disputed limitations emphasized, is representative.

1. A method comprising:

Examiner's findings and determinations and Appellant's contentions in their entirety, we refer to these documents.

collecting information about two or more organizations that have computer systems, network resources, and employees, the organizations posing risks through business relationships of the organizations with other parties, the information collected about the organizations being indicative of compromises, vulnerabilities or configurations of technology systems of the organizations and indicative of resiliencies of the organizations to recover from such compromises, vulnerabilities or configurations, the information indicative of durations of events associated with compromises or vulnerabilities or configurations,

at least some of the information about each of the organizations being collected automatically by computer using sensors on the Internet,

the information about each of the organizations being collected from two or more sources, one or more of the sources not being controlled by the organization, the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization,

at least partly automatically gathering information about assets that each of the organizations owns, controls, uses, or is affiliated with, including IP addresses and IP network address ranges, computer services residing within address ranges, or domain names,

at least one of the sources for each of the organizations comprising a public source or a commercial source,

processing by computer the information from the two or more sources for each of the organizations to form a composite rating of the organization that is indicative of a degree of risk to the organization or to a party through a business relationship with the organization, the composite rating comprising a calculated composite of metrics and data derived or collected from the sources, the processing comprising applying transformations to the data and metrics, and the processing comprising applying weights to the data and the metrics,

> *the metrics including a measure of the extent of, the frequency of, or duration of compromise of the technology systems of the organization, or of a configuration or vulnerability of the organization, and a measure of the resilience of the organization to recover from such vulnerability, the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability*, and
>
> in connection with assessing a business risk to the organization or to a party through a business relationship with at least one of the organizations, delivering reports of the composite ratings of the organizations through a reporting facility to enable users of the reporting facility to monitor, assess, and mitigate the risks, based on the security vulnerabilities and resiliencies, in doing business with the organization and to compare the composite ratings of the organizations.

Id. at 15–16 (emphasis added).

REFERENCES AND REJECTION

The Examiner relies upon the following references in rejecting the claims:

Name[3]	**Number**	**Published**	**Filed**
Newton	US 2004/0250122 A1	Dec. 9, 2004	May 9, 2003
Shull	US 2006/0212925 A1	Sept. 21, 2006	Mar. 2, 2006

Specifically, claims 1, 4, 5, 7–14, 16, 121, 124, 126–132, and 134–141 stand rejected as unpatentable under 35 U.S.C. § 103(a) over the combined teachings of Newton and Shull. Final Act. 4–20.

Appellant contests the obviousness rejection of independent claim 1 (Appeal Br. 4–7) and relies on the alleged deficiencies in that rejection to overcome the rejection of the independent claims 136 and 141 and of the

[3] All reference citations are to the first named inventor only.

Black Kite Ex. 1002, Page 290 of 1060

dependent claims (*id.* at 7–20). Because we determine that reversal of the rejection of independent claim 1 is dispositive, except for our ultimate decision, we do not discuss the merits of the rejections of claims 4, 5, 7–14, 16, 121, 124, 126–132, and 134–141 further herein. We review the appealed rejection of independent claim 1 for error based upon the issues identified by Appellant, and in light of the arguments and evidence produced thereon. *Ex parte Frye*, 94 USPQ2d 1072, 1075 (BPAI 2010) (precedential). We address the rejection of claim 1 below.

ANALYSIS

1. Obviousness of Claim 1 Over Newton and Shull

As noted above, the Examiner rejects independent claim 1 as obvious over the combined teachings of Newton and Shull. Final Act. 3–7. In particular, the Examiner finds that Newton teaches or suggests all of the limitations of claim 1, except for

> the composite rating comprising a calculated composite of metrics and data derived or collected from the sources, the processing comprising applying transformations to the data and metrics, and the processing comprising applying weights to the data and the metrics,
>
> the metrics including a measure of the extent of the frequency of, or the duration of compromise of the technology systems of the organization, or of a configuration or vulnerability of the organization, and a measure of the resilience of the organization to recover from such vulnerability, the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability.

Id. at 7 (emphasis omitted); *see* Appeal Br. 15–16 (Claims App.). However, the Examiner finds,

> Shull [0058] and figure 8, item 812, teaches creating a score for

> an entity from multiple sources which is similar to a credit score which informs requester of the trust of the entity, this score is received by the requester where activities are accounted for both legitimate (i.e.[,] positive) and illegitimate (i.e.[,] negative) and [0069] and [0073], teaches giving an overall trust score between 1 and 5 i.e.[,] a normalized composite score where 1 is *a reputable business* and 5 is likely engaged in illicit activity.).

Final Act. 7 (emphasis added). The Examiner concludes that a person of ordinary skill in the art would have had reason "to modify the method of collecting security characteristics from multiple sources as taught by Newton by creating a score representative of the different collected data as taught by Shull because it would aid the requester in determining whether the entity is trusted or not." *Id.*

Appellant notes that the Examiner fails to show where Shull teaches measuring "the resilience of the organization to recover from such vulnerability, the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability." Appeal Br. 8; *see* Reply Br. 5–7 (citing Shull ¶¶ 59, 68). Further, Appellant notes,

> Newton provides a list of exemplary properties that it *does* consider - seventeen to be exact - and the claimed resiliency is unsurprisingly absent. [*See* Newton ¶¶ 12–29.] As such, Appellant[] fail[s] to see how either Newton or Shull address[es] the claimed resiliency as claimed and as such disagree[s] with the Examiner's rejection.

Appeal Br. 8. We agree with Appellant.

Shull explains:

> Merely by way of example, a scoring system from 1 to 5 may be implemented. A score of 1 may indicate the online entity has been verified and/or certified reliable by a provider of the trust evaluation system, such as through a certification process. A

> score of 2 may indicate that the entity is relatively likely to be reputable (that is, to be engaged only in legitimate activities), while a score of 3 may indicate that the identification *and/or reputation of an entity* is doubtful and/or cannot be authenticated, and scores of 4 or 5 indicate that the entity is known to be disreputable (e.g., engage in and/or facilitate illicit activity).

Shull ¶ 58 (emphasis added). Shull, however, does not link an entity's reputation to a measure of its resilience. The Examiner finds,

> *Newton, [0012] teaches that every network in the world would have a rating in the database and [0030] teaches establishing a reputation for a network, and a reputation/rating is indicative on how trust worthy a network is and the information gathered would be indicative on the resilience a network would likely be due to a compromise as a larger organization with more resources that has existed longer is more likely to be resilient than a smaller organization with less resources and age.* Thus Newton [0012]-[0030] to show that all ORs of the limitation are actually disclosed and Shull [0059], [0068] as well teaches some of the alternative limitations.

Ans. 4 (emphasis added); *see* Final Act. 3. We are not persuaded that the Examiner's findings regarding Newton's teachings of *reputational* ratings databases together with Shull's teachings of scores evidencing *reputation* teach or suggest measuring *resilience*, as recited in claim 1.

Finally, Appellant contends that, in combining the teachings of Newton and Shull to achieve the recitations of claim 1, "the Examiner appears to be relying on hindsight to connect the dots from the network properties considered by Newton and Applicant['s] resiliency metric, however, impermissible hindsight must be avoided and the legal conclusion must be reached on the basis of the facts gleaned from the prior art." Appeal Br. 9.

> Any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning, but so long as it

> takes into account only knowledge which was within the level of ordinary skill [in the art] at the time the claimed invention was made and does not include knowledge gleaned only from applicant's disclosure, such a reconstruction is proper.

In re McLaughlin, 443 F.2d 1392, 1395, (CCPA 1971). Nevertheless, in view of the lack of evidence supporting the Examiner's finding that Newton's and Shull's teachings regarding reputation together teach or suggest "the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability," this finding appears to be based on nothing more than improper hindsight gleaned from Appellant's claim. *See Alza Corp. v. Mylan Labs., Inc.*, 464 F.3d 1286, 1290 (Fed. Cir. 2006) ("At its core, our anti-hindsight jurisprudence is a test that rests on the unremarkable premise that legal determinations of obviousness, as with such determinations generally, should be based on evidence rather than on mere speculation or conjecture.").

Consequently, we are persuaded that the Examiner erred in rejecting claim 1 as obvious over Newton and Shull, and we do not sustain the obviousness rejection of claim 1.

2. *The Remaining Claims*

As noted above, Appellant challenges the rejection of independent claim 136 and 141 for the same reasons as claim 1. Appeal Br. 11–13. Each of claims 4, 5, 7–14, 16, 121, 124, 126–132, 134, 135, and 137–140 depends directly from independent claim 1. *Id.* at 16–20 (Claims App.). Appellant does not challenge the rejection of the independent claims 136 and 141 or of the dependent claims separately from its challenge to the rejection of independent claim 1. *Id.* at 11–13; *see* Reply Br. 9. Because we are

Black Kite Ex. 1002, Page 294 of 1060

persuaded the Examiner erred with respect to the obviousness rejection of claim 1, we also are persuaded the Examiner erred with respect to the obviousness rejections of claims 4, 5, 7–14, 16, 121, 124, 126–132, and 134–141. For this reason, we do not sustain the rejection of those claims.

NEW GROUND OF REJECTION OF CLAIMS 26–49 UNDER 37 C.F.R. § 41.50(B)

We make the following new ground of rejection:

- Claims 1, 4, 5, 7–14, 16, 121, 124, 126–132, and 134–141 are rejected under 35 U.S.C. § 112, ¶ 1,[4] as lacking adequate written description.

35 U.S.C. § 112, ¶ 1, provides:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor . . . of carrying out his invention.

As our reviewing court has explained,

> The 'written description' requirement implements the principle that a patent must describe the technology that is sought to be patented; the requirement serves both to satisfy the inventor's obligation to disclose the technologic knowledge upon which the patent is based, and to demonstrate that the patentee was in possession of the invention that is claimed.

Capon v. Eshhar, 418 F.3d 1349, 1357 (Fed. Cir. 2005).

Claim 1 was amended to recite a method wherein:

[4] Final Act. 2; *see* MPEP § 2159.01.

> *the measure of the resilience being inversely proportional to* one or more of the duration of detected malicious activity and *the duration of the vulnerability*.

Appeal Br. 16 (Claims App.) (emphases added); *see* Amdt. After Final, 2 (Sept. 9, 2016). Claims 136 and 141 were amended to recite corresponding limitations. Appeal Br. 19, 20 (Claims App.); *see* Amdt. After Final at 7, 8. In the Amendment, Appellant stated, "[s]upport for the amendments may be found at least at paragraphs [0077] and [0078] of the application as published." Amdt. After Final at 9; *see* Appeal Br. 3 (citing Spec., 13:14–24 (Specification text corresponding to published paragraphs)).

The Specification discloses:

> *Organizational security risk may be measured along two vectors: vulnerability and resilience.* An entity's vulnerability is defined as its "physical, technical, organizational, and cultural states," which can be exploited to create a security breach. An entity's resilience is defined to be its ability to recover from a security breach.
>
> The system 10 uses the concepts of vulnerability and resilience by examining externally observable proxies for them. An example proxy for entity vulnerability is the number of entity-owned IP addresses, which are reported to be malicious. The higher the number of reports the more likely the entity was vulnerable and had been compromised. Resilience is inversely proportional to the duration of detected malicious activity. *The shorter the duration of the malicious activity, the higher level of resilience the entity demonstrates as it can quickly identify and remove malicious infections.*

Spec., 13:14–24 (emphases added). Thus, the Specification describes vulnerability and resilience as two separate vectors. *Id.* Further, the Specification describes resilience as inversely related to the duration of malicious activity. *Id.* However, apart from amended claims 1, 136, and 141, we do not find where the Specification describes "the measure of the

resilience being inversely proportional to . . . *the duration of the vulnerability*." *See* Spec., 29 (Claim 88 recites, "the resilience is inversely proportional to a duration of the malicious behavior."). Therefore, we reject independent claims 1, 136, and 141, and the claims dependent therefrom, under 35 U.S.C. § 112, ¶ 1, for lack of adequate written description.

DECISIONS

1. The Examiner erred in rejecting claims 1, 4, 5, 7–14, 16, 121, 124, 126–132, and 134–141 under 35 U.S.C. § 103(a) as obvious over the combined teachings of Newton and Shull; and.
2. We determine that claims 1, 4, 5, 7–14, 16, 121, 124, 126–132, and 134–141 are unpatentable under 35 U.S.C. § 112, ¶ 1, as lacking of adequate written description.
3. Thus, on this record, claims 1, 4, 5, 7–14, 16, 121, 124, 126–132, and 134–141 are unpatentable.

CONCLUSION

For the above reasons, we reverse the Examiner's decision rejecting claims 1, 4, 5, 7–14, 16, 121, 124, 126–132, and 134–141 as obvious over the combined teachings of Newton and Shull, but we determine claims 1, 4, 5, 7–14, 16, 121, 124, 126–132, and 134–141 are unpatentable as lacking adequate written description.

In summary:

Claims Rejected	35 U.S.C. §	References/Basis	Affirmed	Reversed	New Ground
1, 4, 5, 7–14, 16, 121, 124, 126–132, 134–141	103(a)	Newton, Shull		1, 4, 5, 7–14, 16, 121, 124, 126–132, 134–141	
1, 4, 5, 7–14, 16, 121, 124, 126–132, 134–141	112, ¶ 1	Written Description			1, 4, 5, 7–14, 16, 121, 124, 126–132, 134–141
Overall Outcome				1, 4, 5, 7–14, 16, 121, 124, 126–132, 134–141	1, 4, 5, 7–14, 16, 121, 124, 126–132, 134–141

This decision contains a new ground of rejection pursuant to 37 C.F.R. § 41.50(b). 37 C.F.R. § 41.50(b) provides "[a] new ground of rejection pursuant to this paragraph shall not be considered final for judicial review."

37 C.F.R. § 41.50(b) also provides that Appellant, WITHIN TWO MONTHS FROM THE DATE OF THE DECISION, must exercise one of the following two options with respect to the new ground of rejection to avoid termination of the appeal as to the rejected claims:

> (1) *Reopen prosecution.* Submit an appropriate amendment of the claims so rejected or new Evidence relating to the claims so rejected, or both, and have the matter reconsidered by the examiner, in which event the prosecution will be remanded to the examiner. . . .

> (2) *Request rehearing*. Request that the proceeding be reheard under § 41.52 by the Board upon the same Record. . . .

Further guidance on responding to a new ground of rejection can be found in the Manual of Patent Examining Procedure § 1214.01. No time for taking any action connected with this appeal may be extended under 37 C.F.R. § 1.136(a)(1).

REVERSED; 37 C.F.R. § 41.50(b)

Black Kite Ex. 1002, Page 299 of 1060

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/240,572	09/22/2011	Stephen Wayne Boyer	BST-004	2423

51414 7590 12/28/2018

GOODWIN PROCTER LLP
PATENT ADMINISTRATOR
100 Northern Avenue
BOSTON, MA 02210
UNITED STATES OF AMERICA

EXAMINER
KANAAN, SIMON P

ART UNIT	PAPER NUMBER
2492	

NOTIFICATION DATE	DELIVERY MODE
12/28/2018	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATENTBOS@GOODWINPROCTER.COM
PSOUSA-ATWOOD@GOODWINPROCTER.COM
GLENN.WILLIAMS@GOODWINPROCTER.COM

United States Patent and Trademark Office

Under Secretary of Commerce for Intellectual Property and
Director of the United States Patent and Trademark Office
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

GOODWIN PROCTER LLP
PATENT ADMINISTRATOR
100 NORTHERN AVENUE
BOSTON, MA 02210

Appeal No: 2019-001684
Application: 13/240,572
Appellant: Stephen Wayne Boyer et al.

Patent Trial and Appeal Board Docketing Notice

Application 13/240,572 was received from the Technology Center at the Board on December 21, 2018 and has been assigned Appeal No: 2019-001684.

In all future communications regarding this appeal, please include both the application number and the appeal number.

The mailing address for the Board is:

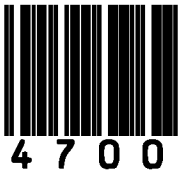
PATENT TRIAL and APPEAL BOARD
UNITED STATES PATENT AND TRADEMARK OFFICE
P.O. BOX 1450
ALEXANDRIA, VIRGINIA 22313-1450

Telephone inquiries can be made by calling 571-272-9797 and referencing the appeal number listed above.

By order of the Patent Trial and Appeal Board.

DAG

Office of Petitions: Routing Sheet



Application No. 13240572

This application is being forwarded to your office for further processing. A decision has been rendered on a petition filed in this application, as indicated below. For details of this decision, please see the document PET.OP.DEC filed on the same date as this document.

- [X] **GRANTED**
- [ ] **DISMISSED**
- [ ] **DENIED**

Office of Petitions: Decision Count Sheet

Mailing Month: 12

Application No.: 13240572

13240572

For US serial numbers: enter number only, no slashes or commas. Ex: 10123456
For PCT: enter "51+single digit of year of filing+last 5 numbers", Ex. for PCT/US05/12345, enter 51512345

Deciding Official: Hall, Dale

Count (1) - Palm Credit 13240572

Decision: GRANT

FINANCE WORK NEEDED
☐ Select Check Box for YES

GRANT

Decision Type: 502 - 37 CFR 1.137(b) - REVIVAL BASED ON UNINTENTI

502

Notes:

Count (2)

Decision: n/a

FINANCE WORK NEEDED
☐ Select Check Box for YES

Decision Type: NONE

Notes:

Count (3)

Decision: n/a

FINANCE WORK NEEDED
☐ Select Check Box for YES

Decision Type: NONE

Notes:

Initials of Approving Official (if required)

If more than 3 decisions, attach 2nd count sheet & mark this box ☐

Printed on: 12/7/2018

Office of Petitions Internal Document - Ver. 5.0

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/240,572	09/22/2011	Stephen Wayne Boyer	BST-004	2423

51414 7590 12/14/2018

GOODWIN PROCTER LLP
PATENT ADMINISTRATOR
100 Northern Avenue
BOSTON, MA 02210
UNITED STATES OF AMERICA

EXAMINER
KANAAN, SIMON P

ART UNIT	PAPER NUMBER
2492	

NOTIFICATION DATE	DELIVERY MODE
12/14/2018	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATENTBOS@GOODWINPROCTER.COM
PSOUSA-ATWOOD@GOODWINPROCTER.COM
GLENN.WILLIAMS@GOODWINPROCTER.COM

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

In re Application of	:	
BOYER, STEPHEN WAYNE, et al.	:	
Application No.: 13/240,572	:	DECISISON ON PETITION
Filing Date: September 22, 2011	:	
Attorney Docket No.: BST-004	:	

This is a decision on the petition filed July 27, 2018, under the unintentional provisions 37 CFR 1.137(a), to revive the above-identified application.

The petition is **GRANTED.**

This application became abandoned as a result of petitioner's failure to pay an appeal forwarding fee required by 37 CFR 41.45(b). As an appeal forwarding fee was not filed within the time period set forth in 37 CFR 41.45(a), the appeal was dismissed and the proceedings as to the rejected claims were terminated. See 37 CFR 37 41.45(b). As no claim was allowed, the application became abandoned July 17, 2018.

The petition satisfies the requirements of 37 CFR 1.137(a) in that petitioner has supplied (1) the reply in the form of an appeal forwarding fee of $1,120; (2) the petition fee of $1,000, and (3) a proper statement of unintentional delay.

Telephone inquiries concerning this decision should be directed to Dale Hall at (571) 272-3586.

This application is being referred to Technology Center AU 2492 for appropriate action by the Examiner on the reply received in accordance with this decision on petition.

/Irvin Dingle/
Irvin Dingle
Lead Paralegal Specialist
Office of Petitions

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/240,572	09/22/2011	Stephen Wayne Boyer	BST-004	2423

51414 7590 07/27/2018

GOODWIN PROCTER LLP
PATENT ADMINISTRATOR
100 Northern Avenue
BOSTON, MASSACHUSETTS 02210
UNITED STATES OF AMERICA

EXAMINER	
KANAAN, SIMON P	

ART UNIT	PAPER NUMBER
2492	

NOTIFICATION DATE	DELIVERY MODE
07/27/2018	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

GLENN.WILLIAMS@GOODWINPROCTER.COM
PATENTBOS@GOODWINPROCTER.COM
PSOUSA-ATWOOD@GOODWINPROCTER.COM

Notice of Abandonment	Application No.	Applicant(s)
	13/240,572	Boyer et al.
	Examiner	Art Unit
	SIMON P KANAAN	2492

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

This application is abandoned in view of:

1. ☑ Applicant's failure to timely file a proper reply to the Office letter mailed on 13 February 2017.
   (a) ☐ A reply was received on _____ (with a Certificate of Mailing or Transmission dated _____), which is after the expiration of the period for reply (including a total extension of time of _____ month(s)) which expired on _____.
   (b) ☐ A proposed reply was received on _____, but it does not constitute a proper reply under 37 CFR 1.113 to the final rejection. (A proper reply under 37 CFR 1.113 to a final rejection consists only of:(1) a timely filed amendment which places the application in condition for allowance; (2) a timely filed Notice of Appeal (with appeal fee); or (3) if this is utility or plant application, a timely filed Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. Note that RCEs are not permitted in design applications.)
   (c) ☐ A reply was received on _____ but it does not constitute a proper reply, or a bona fide attempt at a proper reply, to the non-final rejection. See 37 CFR 1.85(a) and 1.111. (See explanation in box 7 below).
   (d) ☑ No reply has been received.

2. ☐ Applicant's failure to timely pay the required issue fee and publication fee, if applicable, within the statutory period of three months from the mailing date of the Notice of Allowance (PTOL-85).
   (a) ☐ The issue fee and publication fee, if applicable, was received on _____ (with a Certificate of Mailing or Transmission dated _____), which is after the expiration of the statutory period for payment of the issue fee (and publication fee) set in the Notice of Allowance (PTOL-85).
   (b) ☐ The submitted fee of $ _____ is insufficient. A balance of $ _____ is due.
   The issue fee required by 37CFR 1.18 is $ _____ . The publication fee, if required by 37 CFR 1.18(d), is $ _____ .
   (c) ☐ The issue fee and publication fee, if applicable, has not been received.

3. ☐ Applicant's failure to timely file corrected drawings as required by, and within the three-month period set in, the Notice of Allowability (PTO-37).
   (a) ☐ Proposed corrected drawings were received on _____ (with a Certificate of Mailing or Transmission dated _____), which is after the expiration of the period for reply.
   (b) ☐ No corrected drawings have been received.

4. ☐ The letter of express abandonment which is signed by the attorney or agent of record or other party authorized under 37 CFR 1.33 (b). See 37 CFR 1.138(b).

5. ☐ The letter of express abandonment which is signed by an attorney or agent (acting in a representative capacity under 37 CFR 1.34) upon the filing of a continuing application.

6. ☐ The decision by the Board of Patent Appeals and Interference rendered on _____ and because the period for seeking court review of the decision has expired and there are no allowed claims.

7. ☑ The reason(s) below:

failure to pay appeal forwarding fee See CFR 41.45(b), spoke to applicant's representative on 7/23/2018 and they expressed interest in reviving application and needed me to formally abandon it in order to be able to do so.

/SIMON P KANAAN/
Examiner, Art Unit 2492

Petitions to revive under 37 CFR 1.137, or requests to withdraw the holding of abandonment under 37 CFR 1.181, should be promptly filed to minimize any negative effects on patent term.

Docket No.: BST-004
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Design Application of:
Stephen Wayne Boyer et al.

Application No.: 13/240,572	Confirmation No.: 2423
Filed: September 22, 2011	Art Unit: 2492
For: Information Technology Security Assessment System	Examiner: S. P. Kanaan

Mail Stop Petition
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PETITION FOR REVIVAL OF AN APPLICATION FOR PATENT ABANDONED UNINTENTIONALLY UNDER 37 C.F.R. § 1.137(a)

The above-identified application became unintentionally abandoned for failure to pay an Appeal Forwarding Fee in compliance with the Examiner's Answer dated May 16, 2018. To fully respond to the Examiner's Answer, filed concurrently herewith is the Appeal Forwarding Fee of $1,120.00 (for a small entity).

Factual Background

A. The Notification Date of the Examiner's Answer was May 16, 2018.

B. On July 16, 2018, a Reply Brief was filed within two months from the Notification Date of the Examiner's Answer. The Reply Brief itself required no fees per 37 CFR § 41.20(b)(2)(i).

C. On July 19, 2018, a Communication Re: Appeal was received, notifying that the appeal in the application is dismissed because of a "Failure to Pay Appeal Forwarding Fee – See CFR 41.45(b)."

For all these reasons, Applicant respectfully requests that the application be revived on the basis of unintentional delay pursuant to 37 C.F.R. § 1.137(a). In accordance with the requirements of 37 C.F.R. § 1.137(b), Applicant submits herewith:

1. Appeal Forwarding Fee of $1,120.00, for a small entity, as set forth in 37 C.F.R. § 41.20(b)(4);
2. The petition fee of $1,000.00, for a small entity, as set forth in 37 C.F.R. § 1.17(m);
3. A copy of the Reply Brief, in response to the Examiner's Answer, timely filed on July 16, 2018; and
4. A statement that the entire delay in filing the required reply from the due date for the reply until the filing of a grantable petition pursuant to 37 CFR 1.137(a) was unintentional.

Applicant wishes to draw the Office's attention to the filing of a Reply Brief on July 16, 2018, attached herein for convenience and timely filed within two months from the Notification Date of the Examiner's Answer, and respectfully requests that that the Reply Brief be considered upon reinstatement of the Appeal.

Please charge our credit card covering the fees set forth in 37 C.F.R. § 41.20(b)(4) and 37 C.F.R. § 1.17(m). Should any other fees be required for consideration of this paper, the Commissioner is hereby authorized to consider this paper a petition to charge such fees to our Deposit Account No. 07-1700 referencing docket no. BST-004.

Dated: July 27, 2018

Respectfully submitted,

Electronic signature: /Joel E. Lehrer/
Joel E. Lehrer
Registration No.: 56,401
GOODWIN PROCTER LLP
100 Northern Avenue
Boston, Massachusetts 02210
(617) 570-1000
Attorney for Applicant

Electronic Acknowledgement Receipt

EFS ID:	33182901
Application Number:	13240572
International Application Number:	
Confirmation Number:	2423
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Customer Number:	51414
Filer:	Gozde Guckaya/Andrea Borden
Filer Authorized By:	Gozde Guckaya
Attorney Docket Number:	BST-004
Receipt Date:	16-JUL-2018
Filing Date:	22-SEP-2011
Time Stamp:	13:19:38
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Reply Brief Filed	BST-004_Reply_Brief.pdf	124902 9d226c673eb5aca0bc175944dca3661a8f08103b	no	16

Warnings:

Information:	
Total Files Size (in bytes):	124902

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Docket No.: BST-004
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant: Stephen Wayne Boyer et al.

Application No.: 13/240,572 | Confirmation No.: 2423

Filed: September 22, 2011 | Art Unit: 2492

For: INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM | Examiner: S.P. Kanaan

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF

This Reply Brief under 37 C.F.R. § 41.41 is responsive to the Examiner's Answer mailed May 16, 2018 (the "Answer"). Appellant submits that the Reply Brief is timely submitted, i.e., within two months of mailing of the Answer.

The Office is authorized to charge any additional fees necessary for entry of this paper to Deposit Account No. 07-1700 (Order No. BST-004).

ARGUMENT

Appellant stands by the arguments presented in the Appeal Brief filed December 21, 2017, as modified and supplemented below. Appellant also offers the following additional observations based on the positions taken in the "Response to Arguments" section of the Answer.

Status of Amendments

The Answer at page 3 states: "On page 3 of the brief, Appellant states that there are amendments filed with RCE October 17, 2017; however no such amendments were filed on that date." However, looking to page 3 of the Appeal Brief filed on December 21, 2017 (as acknowledged by the Answer in "(2) Response to Argument" section as "the Brief"), there is **no** mention of amendments filed with a Request for Continued Examination ("RCE") on October 17, 2017. Appellant respectfully requests clarification or withdrawal of this statement.

The rejection of claims 1, 4, 5, 7-14, 16, 121, 122, 124, 126-132 and 134-141 under pre-AIA 35 U.S.C. § 103(a) is improper and should be reversed

The Examiner's rejection on pages 4-19 of the Office action, alleging that claims 1, 4, 5, 7-14, 16, 121, 122, 124, 126-132 and 134-141 are unpatentable under pre-AIA 35 U.S.C. § 103(a) over U.S. Publication No. 2004/0250122 to Newton ("Newton") in view of U.S. Publication No. 2006/0212925 to Shull et al. ("Shull"), is improper and should be reversed. Applicant respectfully disagrees with the arguments in the Answer and aims to address each argument below.

As an initial matter, under the "Definition of terms" section of the Answer on pages 3-4, the Examiner states that "Appellants define the term 'resiliency' by way of providing examples," and supplies a definition of "infrastructure resilience" provided by the National Infrastructure Advisory Council ("NIAC"). However, the Application provides the definition for "resilience" in the Specification at page 13, lines 16-17:

> An entity's resilience is defined to be its ability to recover from a security breach.

It is noted that the MPEP at sub-sections 2111.01(I), (IV), and (V) (including the flowchart) address the use of definitions of terms outside the Specification. Specifically, at MPEP 2111.01(IV)(A):

> **An applicant is entitled to be their own lexicographer and may rebut the presumption that claim terms are to be given their ordinary and customary meaning by clearly setting forth a definition of the term** that is different from its ordinary and customary meaning(s) in the specification at the time of filing. See In re Paulsen, 30 F.3d 1475, 1480, 31 USPQ2d 1671, 1674 (Fed. Cir. 1994)…

Thus, there is no need to rely on the external definition provided on page 4 of the Answer.

Next, at issue is whether the following limitation of independent claim 1 is obviated by Newton in view of Shull:

> the metrics including a measure of the extent of, the frequency of, or duration of compromise of the technology systems of the organization, or of a configuration or vulnerability of the organization, and a measure of the resilience of the organization to recover from such vulnerability, the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability

The Answer rejects this limitation by focusing on the "or" language (see Answer, page 4). However, not all of the terms of the above limitation are in the alternative. For the purposes of illustration and explanation, the above claim limitation is broken down and emphasized as in the following:

> the metrics including

(sub-limitation 1):

> a measure of the extent of, the frequency of, or duration of compromise of the technology systems of the organization, or of a configuration or vulnerability of the organization, **and**

(sub-limitation 2):

> a measure of the resilience of the organization to recover from such vulnerability, the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability

Contrary to the Answer at page 4 ("[a]lthough Newton need not teach all the elements listed in the measurement as they are listed with an "OR" so Newton need only teach one of the items"), to obviate this claim limitation, Newton in view of Shull are required to teach both sub-limitations (labeled "1" and "2") on either side of the term "AND". The following discussion explains why Newton in view of Shull does not teach both of these sub-limitations.

To reject the above limitation, the Answer cites paragraphs [0012]-[0030] of Newton, reproduced here:

> [0012] These questions, and many more, can be answered, with the present invention, a Network Intelligence Database. Every network in the world would have a record in the database, with a large number of properties. Some properties might be:
> [0013] Hostility level on the Internet;
> [0014] Security event history;
> [0015] Spam levels;
> [0016] Hosted services (web servers, email servers);
> [0017] Public wireless;
> [0018] Organization type: educational, enterprise, military;
> [0019] Organization associations: owned by, partnered with whom;
> [0020] Peer ISPs;
> [0021] Bandwidth connection to the Internet;
> [0022] Active security measures, firewalls, IDSs;
> [0023] Number of users, employees, people on this network;
> [0024] Age of the network;
> [0025] Inappropriate content served (hate sites, porn, pirated software);
> [0026] Industry: industrial, computers;
> [0027] Geographic placement;
> [0028] Open proxy servers; and
> [0029] Address, contact information.
> [0030] Accordingly, system and method of the present invention establish respective reputations for networks and allow a given network to determine whether to communicate with a particular network in dependence upon its reputation.

The Answer at page 4 states that:

> Newton, [0012] teaches that every network in the world would have a rating in the database and [0030] teaches establishing a reputation for a network, and a reputation/rating is indicative on how trust worthy a network is and the information gathered would be indicative on the resilience a network would likely

> be due to a compromise as a larger organization with more resources that has existed longer is more likely to be resilient than a smaller organization with less resources and age.

First, contrary to the Answer, Newton does not say that "every network in the world would have a **rating** in the database." Newton in paragraph [0012] states that "[e]very network in the world would have a **record** in the database, with a large number of properties" and proceeds to list the properties in paragraphs [0013]-[0029]. Thus, there is no **rating** taught or suggested by Newton in paragraph [0012]. Second, paragraph [0030] of Newton simply states "[a]ccordingly, system and method … establish respective reputations for networks" without making reference to any of the preceding properties. Paragraph [0030] does not even define the term "respective reputations for networks." Therefore, it cannot be inferred, as set forth in the Answer, that paragraph [0030] of Newton "**teaches** establishing a reputation for a network, and a reputation/rating is indicative on how trust worthy a network is and the information gathered would be indicative on the resilience a network would likely be due to a compromise as a larger organization with more resources that has existed longer is more likely to be resilient than a smaller organization with less resources and age."

Specifically taking "sub-limitation 2": Newton in the above cited portions does not teach or suggest the term "resilience" as used in claim 1 and/or as defined by the Specification. Specifically, in claim 1 "the measure of the resilience" is "inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability." Thus, Newton does not teach at least sub-limitation 2.

The Answer also cites Shull at paragraphs [0059] and [0068], which respectively state:

> [0059] This exemplary scoring scheme is designed to be extensible, in that a plurality of scores may be accorded to any given entity, based perhaps on various characteristics and/or categories of activities. Merely by way of example, an entity may be accorded a number of scores based on that entity's likelihood of being involved in phishing and/or other fraudulent activities, brand abuse, pornography, e-commerce, online transactions, consumer targeting, preferred programs, service expedition, etc. (It may be noted from the above list that not all activities need to be illegitimate activities. Merely by way of example, a score indicating that an entity is likely to be engaged in e-commerce may allow a user to infer that a transaction with that entity is relatively more likely to be a legitimate transaction and/or may be used by a security system on a client and/or a

> border device (including those described below, for example) to make a determination that a transaction with such an entity is an allowable communication.
>
> [0068] Another type of derived score that that may be calculated by scoring engine for an online entity is a secure infrastructure score 232. Secure infrastructure scores 232 may be used to evaluate and score an online entity's use of security features, such as certificates. Other exemplary types of derived scores include trusted record scores 233 (evaluating and scoring entities based on the respective online entity's history with trusted data sources), change scores 234 (evaluating and scoring the frequency with which an online entity changes domain registrations), whitelist and/or blacklist scores 235 (evaluating and scoring an online entity's suitability for a whitelist (very high repute) or blacklist (disreputable)), history scores 236 (evaluating historical data to determine an entity's online history, lack of history and/or a quality of that history), portfolio scores 237 (evaluating and scoring the online entity based on whether an online portfolio (domain names owned, activities performed, etc.) associated with the online entity is compatible (makes sense) with the nature and character of the online entity), and/or any other type of derived score which evaluates a factor of correlated data associated with an online entity. Other scores can include application scores and virus scores, which can evaluate the trustworthiness of particular applications and/or malicious code (such that, when a user attempts to install such applications and/or code, the scores can be used to either advise the user on whether the application should be installed and/or make a determination (e.g., at an operating system and/or domain policy level) whether to allow or prohibit such installation).

None of the above cited portions teach or suggest the concept of "a measure of resilience" nor the concept of the measure of resilience "being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability." Looking closer at paragraphs [0059] and [0068], Shull describes scoring of an entity based on:

(a) "that entity's likelihood of being involved in phishing and/or other fraudulent activities, brand abuse, pornography, e-commerce, online transactions, consumer targeting, preferred programs, service expedition, etc." [0059]

(b) "an online entity's use of security features, such as certificates" [0068]

(c) "the respective online entity's history with trusted data sources" [0068]

(d) "the frequency with which an online entity changes domain registrations" [0068]

(e) "an online entity's suitability for a whitelist (very high repute) or blacklist (disreputable)" [0068]

(f) "historical data to determine an entity's online history, lack of history and/or a quality of that history" [0068]

(g) "the online entity based on whether an online portfolio (domain names owned, activities performed, etc.) associated with the online entity is compatible (makes sense) with the nature and character of the online entity" [0068]

(h) "a factor of correlated data associated with an online entity" [0068]

(i) "the trustworthiness of particular applications and/or malicious code (such that, when a user attempts to install such applications and/or code, the scores can be used to either advise the user on whether the application should be installed and/or make a determination (e.g., at an operating system and/or domain policy level) whether to allow or prohibit such installation" [0068]

Note that the above quotations are labeled "(a)" - "(i)" to facilitate explanation. None of the above paragraphs of Shull teach or suggest sub-limitation 2. For example, in "(b)" above, an entity's use of security features does not relate an entity's resilience in recovering from a vulnerability. Security features such as certificates may prevent a vulnerability from occurring but would not aid the entity in recovery from the vulnerability. In another example, in "(i)" above, the trustworthiness of a particular application or code does not indicate any measure of resilience of the organization. Therefore, Appellant submit that Newton and Shull, whether taken individually or together, fail to teach or suggest the claimed subject matter, as is required for a rejection under 35 U.S.C. § 103(a) for at least these reasons.

Next, with respect to the following limitation: "the information indicative of durations of events associated with compromises or vulnerabilities or configurations," the Answer cites paragraphs [0041]-[0042] of Newton:

> [0041] The Master NID 12 includes information on networks through properties 22 of those networks and applies both a weighting system to those properties and time sensitivity (how things become less or more important over time).
>
> [0042] The Customer NID (C-NID) 14 includes information on networks, receives real-time updates from the Master-NID 12 that include properties, and has a multi-user weighting system and time sensitivity. The C-NID (Custom-NID)

> includes a real-time interface for receiving live remote updates from the Mater-NID. It also includes data mining and searching capability.

Newton in paragraphs [0041]-[0042] do not teach the above claim limitation. Simply because the word "time" is used in these paragraphs does not make their disclosures relevant to the claim limitation. Specifically, the term "time sensitivity" has to do with how the properties themselves become less or more important over time. For the sake of argument, and without disclaimer, if one assumes that "properties 22" include those listed in Fig. 1 under element "24" (which is not defined anywhere in Newton), whether any of these properties "become less or more important over time" is not related to "durations of events associated with compromises or vulnerabilities or configurations."

Additionally, the Answer cites paragraph [0057] of Shull, reproduced here:

> [0057] Trust evaluation system 102 may also provide a historical view of an entity's activities. Merely by way of example, if it is discovered that a given entity is engaging in an illicit activity, such as phishing, a record of the activity may be made with respect to that entity. Further, a record may be made with respect to each of the enabling parties associated with that entity, thereby tagging and/or labeling such enablers as being relatively more likely to facilitate illicit activities. Each time an enabling party is discovered to be a facilitator of such activity (and/or refuses to take corrective action when notified of such activity), a trust score may be adjusted. Trust score(s) may allow interested parties to determine quickly whether a given enabling party is relatively more or less likely to act as a facilitator of illicit activity, which can provide insight into the likelihood of a entity associated with such an enabling party to be engaged in an illicit activity and/or can allow the preparation of a complaint against an enabling party, etc.

Again, no disclosure in the above paragraph of Shull teaches or suggests "information indicative of durations of events associated with compromises or vulnerabilities or configurations." It is noted that the term "time" is used in the above paragraph when discussing instances in which an enabling party is discovered facilitating illicit activities. However, as before, this is entirely unrelated to "information indicative of durations of events…" as claimed. Thus, Newton in view of Shull fail to teach or suggest the claimed subject matter, as is required for a rejection under 35 U.S.C. § 103(a).

Finally, on pages 5-6, the Answer returns again to the definition of "infrastructure resilience" supplied on page 4 of the Answer. Specifically, the Answer states that:

> [t]he limitation "the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability" is no more than rewording of provided by Examiner definition of resilience. Because resilience is the ability to reduce the magnitude and/or duration of disruptive events, the higher the resilience the low is the magnitude and/or duration of disruptive events, which in mathematics well known as inversely proportional functionality.

To reiterate, the definition provided in the Answer cannot be used to define an already-defined term in the Specification (see above). Moreover, for the sake of argument, even if the claim limitation was a "rewording" of the provided definition (which it is not), the Answer explicitly states at page 4 that "NIAC cited ONLY as source of the term definition, and should NOT be considered as prior art reference." Therefore, it has no bearing on the patentability of the limitation in view of the claim as a whole.

The remainder of the Answer quotes the rejections of the Final Office Action dated February 13, 2017 and have been addressed in the Appeal Brief dated December 21, 2018. In summary, Appellants submit that Newton and Shull, either alone or in combination, fail to teach or suggest the claimed invention, when taken as a whole, as is required for a rejection under 35 U.S.C. § 103(a).

CONCLUSION

In view of the arguments above, and those articulated in the Appeal Brief, Appellant respectfully submit that claims 1, 4, 5, 7-14, 16, 121, 122, 124, 126-132, and 134-141 are patentable and urge the Board to reverse all of the Examiner's rejections as to each of these claims.

Dated: July 16, 2018

Respectfully submitted,

Electronic signature: /Gozde Guckaya/
Gozde Guckaya
Registration No.: 74,989
Agent for Applicant
GOODWIN PROCTER LLP
100 Northern Avenue
Boston, Massachusetts 02210
(617) 570-1000

CLAIMS APPENDIX

1. A method comprising:

collecting information about two or more organizations that have computer systems, network resources, and employees, the organizations posing risks through business relationships of the organizations with other parties, the information collected about the organizations being indicative of compromises, vulnerabilities or configurations of technology systems of the organizations and indicative of resiliencies of the organizations to recover from such compromises, vulnerabilities or configurations, the information indicative of durations of events associated with compromises or vulnerabilities or configurations,

at least some of the information about each of the organizations being collected automatically by computer using sensors on the Internet,

the information about each of the organizations being collected from two or more sources, one or more of the sources not being controlled by the organization, the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization,

at least partly automatically gathering information about assets that each of the organizations owns, controls, uses, or is affiliated with, including IP addresses and IP network address ranges, computer services residing within address ranges, or domain names,

at least one of the sources for each of the organizations comprising a public source or a commercial source,

processing by computer the information from the two or more sources for each of the organizations to form a composite rating of the organization that is indicative of a degree of risk to the organization or to a party through a business relationship with the organization, the composite rating comprising a calculated composite of metrics and data derived or collected from the sources, the processing comprising applying transformations to the data and metrics, and the processing comprising applying weights to the data and the metrics,

the metrics including a measure of the extent of, the frequency of, or duration of compromise of the technology systems of the organization, or of a configuration or vulnerability of the organization, and a measure of the resilience of the organization to recover from such

vulnerability, the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability, and

in connection with assessing a business risk to the organization or to a party through a business relationship with at least one of the organizations, delivering reports of the composite ratings of the organizations through a reporting facility to enable users of the reporting facility to monitor, assess, and mitigate the risks, based on the security vulnerabilities and resiliencies, in doing business with the organization and to compare the composite ratings of the organizations.

4. The method of claim 1, wherein the collected information is represented by at least two data types.

5. The method of claim 4, wherein the at least two data types include at least one of breach disclosures, block lists, configuration parameters, an identification of malware servers, an identification of a reputation, an identification of suspicious activity, an identification of spyware, white lists, an identification of compromised hosts, an identification of malicious activity, an identification of spam activity, an identification of vulnerable hosts, an identification of phishing activity, or an identification of e-mail viruses.

7. The method of claim 1, wherein the collected information evidences internal security controls.

8. The method of claim 1, wherein the collected information comprises outcomes of each of the organizations.

9. The method of claim 1, wherein the collected information evidences operational execution of security measures of each of the organizations.

10. The method of claim 1, wherein the collected information indicates whether a computer system of each of the organizations served malicious code to another system.

11. The method of claim 1, wherein the collected information indicates whether a computer system of each of the organizations communicated with a known attacker controlled network or sensor outside the control or network of the organization.

12. The method of claim 1, comprising: forming a series of the security ratings of each of the organizations.

13. The method of claim 12, comprising: determining a trend from the series of ratings.

14. The method of claim 12, comprising displaying the series of composite ratings.

16. The method of claim 14, wherein displaying the series of composite ratings for each of the organizations comprises posting the series of composite ratings for the organization to a web portal.

121. The method of claim 1, wherein the collected information represents externally observable outcome information.

124. The method of claim 1, comprising: determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information.

126. The method of claim 1, wherein: the collected information comprises at least two security characterizations of a computer system of each of the organizations.

127. The method of claim 1, wherein the collected information comprises a characterization of behavior of an employee of at least one of the organizations.

128. The method of claim 1, wherein the collected information comprises characterizations other than characterizations about a computer system of at least one of the organizations.

129. The method of claim 1, wherein the collected information comprises characterizations about policies of at least one of the organizations.

130. The method of claim 1, wherein the collected information comprises characterizations about information technology assets that at least one of the organizations owns, controls, uses, or is affiliated with.

131. The method of claim 1 in which collected information represents: (a) physical states, (b) technical states, (c) organizational states, or (d) cultural states of at least one of the organizations which can be exploited to create a security breach; or (e) the organization's ability to recover from a security breach; or any combination of two or more of these.

132. The method of claim 1 in which processing the information to form a composite rating comprises correlating data across the sources of information.

134. The method of claim 1 in which processing the information to form a composite rating comprises statistically correlating the composite rating with actual outcomes.

135. The method of claim 1 in which the vulnerability comprises physical, technical, organizational, or cultural states that can be exploited to create a security breach.

136. A method comprising

collecting, from at least two sources, information about two or more organizations, the collected information representing at least two data types, the collected information comprising outcomes of each of the organizations,

at least some of the information for each of the organizations being collected automatically by computer from at least two sources, one or more of the sources not controlled by the organization,

the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization, at least one of the sources including a commercial data source,

processing the information from both of the two sources for each of the organizations to form a composite rating of a security vulnerability of the organization and of a resilience of the organization to recover from a security breach, the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability, or both, the processing including applying models that account for differences in the respective sources,

normalizing the composite rating of each of the organizations based on a size characteristic of the organization to enable comparisons of composite ratings between the two or more organizations,

forming a series of the security ratings of each of the organizations, determining a trend from the series of ratings, and displaying the series of composite ratings through a portal,

determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information, and

reporting the composite ratings of the organizations through a portal to enable customers to monitor, assess, and mitigate risk in doing business with the organizations and to compare the composite ratings across the organizations.

137. The system of claim 1, determining a confidence range of the composite rating, the size of the range varying inversely with the level of confidence in the composite rating.

138. The system of claim 137, wherein the confidence range is based on redundancy of the security characterizations.

139. The system of claim 137, wherein the confidence range is based on a size of the third party computer system.

140. The method of claim 1 comprising ranking the organization and other organizations within sectors or peer-groups or globally.

141. A method comprising:

collecting information about an organization that has computer systems, network resources, and employees, the organization posing risks to itself or to other parties through business relationships of the organization with the other parties,

the information collected about the organization including (a) information collected automatically by computer on the Internet without permission of the organization, and (b) information indicative of resiliencies of the organization to recover from a security breach associated with a compromise or a vulnerability, the resiliencies being inversely proportional to one or more of the duration of detected malicious activity and the duration of the compromise or vulnerability,

processing the information by computer to form a composite rating of the organization that is indicative of a degree of risk based on a business relationship with the organization, the composite rating comprising a measure of the resiliencies of the organization to recover from a security breach, and in connection with assessing the degree of risk, delivering a report of the composite rating of the organization through a reporting facility to enable a user of the reporting facility to assess the risks, based at least in part on the resiliencies.

Electronic Patent Application Fee Transmittal

Application Number:	13240572
Filing Date:	22-Sep-2011
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Filer:	Joel E. Lehrer/Andrea Borden
Attorney Docket Number:	BST-004

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
PET. REVIVE ABANDON APP, DELAY PYMT-RESP	2453	1	1000	1000
Patent-Appeals-and-Interference:				
APPEAL FORWARDING FEE	2413	1	1120	1120

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**2120**

Electronic Acknowledgement Receipt

EFS ID:	33301144
Application Number:	13240572
International Application Number:	
Confirmation Number:	2423
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Customer Number:	51414
Filer:	Joel E. Lehrer/Andrea Borden
Filer Authorized By:	Joel E. Lehrer
Attorney Docket Number:	BST-004
Receipt Date:	27-JUL-2018
Filing Date:	22-SEP-2011
Time Stamp:	15:20:53
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Petition for review by the Office of Petitions	BST-004_Petition_to_Revive.pdf	82167 ff74675a588417603f7cc8df007fe76ad57ea8f7	no	2

Warnings:

Information:					
2	Reply Brief Filed	BST-004_Reply_Brief_as_filed.pdf	163390 0bf39aea934eed059bcfac629dc5d0894ac845be	no	18
Warnings:					
The PDF file has been signed with a digital signature and the legal effect of the document will be based on the contents of the file not the digital signature.					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	31746 31cddf97f3d623cce452d8909ebef78f861294a1	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	277303	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR/ PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
13/240,572	22 September 2011	Boyer et al.	BST-004

	EXAMINER	
GOODWIN PROCTER LLP PATENT ADMINISTRATOR **100 Northern Avenue** **BOSTON, MA 02210**	Everett R Williams	
	ART UNIT	PAPER
	OPAC	20180717

DATE MAILED: _____

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

See Attached

PTO-90C (Rev.04-03)

Communication Re: Appeal	Application No. 13/240,572	Applicant(s) Boyer et al.	
	Examiner KANAAN, SIMON P	Art Unit 2492	AIA Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

1. ☐ The Notice of Appeal filed on _____ is not acceptable because:

(a) ☐ it was not timely filed.

(b) ☐ the statutory fee for filing the appeal was not submitted. See 37 CFR 41.20(b)(1).

(c) ☐ the appeal fee received on_____ was not timely filed.

(d) ☐ the submitted fee of $ _____ is insufficient. The appeal fee required by 37 CFR 41.20(b)(1) is $ _____.

(e) ☐ the appeal is not in compliance with 37 CFR 41.31(a)(1) in that no claim has been twice rejected.

(f) ☐ a Notice of Allowability, PTO-37, was mailed by the Office on _____.

2. ☐ The appeal brief filed on _____ is NOT acceptable for the reason(s) indicated below:

(a) ☐ the brief and/or brief fee is untimely. See 37 CFR 41.37(a).

(b) ☐ the statutory fee for filing the brief has not been submitted. See 37 CFR 41.20(b)(2).

(c) ☐ the submitted brief fee of $ _____ is insufficient. The brief fee required by 37 CFR 41.20(b)(2) is $ _____.

The appeal in this application will be dismissed unless corrective action is taken to timely submit the brief and requisite fee. See 37CFR 41.37(a)(1). Extensions of time may be obtained under 37 CFR 1.136(a). See 37CFR 41.37(e).

3. ☑ The appeal in this application is DISMISSED because:

(a) ☐ the statutory fee for filing the brief as required under 37 CFR 41.20(b)(2) was not timely submitted and the period for obtaining an extension of time to file the brief under 37 CFR 1.136(a) has expired.

(b) ☐ the brief was not timely filed and the period for obtaining an extension of time to file the brief under 37 CFR 1.136(a) has expired.

(c) ☐ a Request for Continued Examination (RCE) under 37 CFR 1.114 was filed on _____.

(d) ☑ other: Failure to Pay Appeal Forwarding Fee- SeeCFR 41.45(b).

4. ☑ Because of the dismissal of the appeal, this application:

(a) ☐ is abandoned because there are no allowed claims.

(b) ☐ is before the examiner for final disposition because it contains allowed claims. Prosecution on the merits remains CLOSED.

(c) ☑ is before the examiner for consideration.

EVERETT R WILLIAMS (571)272-3619	

Docket No.: BST-004
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellant: Stephen Wayne Boyer et al.

Application No.: 13/240,572 | Confirmation No.: 2423

Filed: September 22, 2011 | Art Unit: 2492

For: INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM | Examiner: S.P. Kanaan

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF

This Reply Brief under 37 C.F.R. § 41.41 is responsive to the Examiner's Answer mailed May 16, 2018 (the "Answer"). Appellant submits that the Reply Brief is timely submitted, i.e., within two months of mailing of the Answer.

The Office is authorized to charge any additional fees necessary for entry of this paper to Deposit Account No. 07-1700 (Order No. BST-004).

ARGUMENT

Appellant stands by the arguments presented in the Appeal Brief filed December 21, 2017, as modified and supplemented below. Appellant also offers the following additional observations based on the positions taken in the "Response to Arguments" section of the Answer.

Status of Amendments

The Answer at page 3 states: "On page 3 of the brief, Appellant states that there are amendments filed with RCE October 17, 2017; however no such amendments were filed on that date." However, looking to page 3 of the Appeal Brief filed on December 21, 2017 (as acknowledged by the Answer in "(2) Response to Argument" section as "the Brief"), there is **no** mention of amendments filed with a Request for Continued Examination ("RCE") on October 17, 2017. Appellant respectfully requests clarification or withdrawal of this statement.

The rejection of claims 1, 4, 5, 7-14, 16, 121, 122, 124, 126-132 and 134-141 under pre-AIA 35 U.S.C. § 103(a) is improper and should be reversed

The Examiner's rejection on pages 4-19 of the Office action, alleging that claims 1, 4, 5, 7-14, 16, 121, 122, 124, 126-132 and 134-141 are unpatentable under pre-AIA 35 U.S.C. § 103(a) over U.S. Publication No. 2004/0250122 to Newton ("Newton") in view of U.S. Publication No. 2006/0212925 to Shull et al. ("Shull"), is improper and should be reversed. Applicant respectfully disagrees with the arguments in the Answer and aims to address each argument below.

As an initial matter, under the "Definition of terms" section of the Answer on pages 3-4, the Examiner states that "Appellants define the term 'resiliency' by way of providing examples," and supplies a definition of "infrastructure resilience" provided by the National Infrastructure Advisory Council ("NIAC"). However, the Application provides the definition for "resilience" in the Specification at page 13, lines 16-17:

> An entity's resilience is defined to be its ability to recover from a security breach.

It is noted that the MPEP at sub-sections 2111.01(I), (IV), and (V) (including the flowchart) address the use of definitions of terms outside the Specification. Specifically, at MPEP 2111.01(IV)(A):

> **An applicant is entitled to be their own lexicographer and may rebut the presumption that claim terms are to be given their ordinary and customary meaning by clearly setting forth a definition of the term** that is different from its ordinary and customary meaning(s) in the specification at the time of filing. See In re Paulsen, 30 F.3d 1475, 1480, 31 USPQ2d 1671, 1674 (Fed. Cir. 1994)…

Thus, there is no need to rely on the external definition provided on page 4 of the Answer.

Next, at issue is whether the following limitation of independent claim 1 is obviated by Newton in view of Shull:

> the metrics including a measure of the extent of, the frequency of, or duration of compromise of the technology systems of the organization, or of a configuration or vulnerability of the organization, and a measure of the resilience of the organization to recover from such vulnerability, the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability

The Answer rejects this limitation by focusing on the "or" language (see Answer, page 4). However, not all of the terms of the above limitation are in the alternative. For the purposes of illustration and explanation, the above claim limitation is broken down and emphasized as in the following:

> the metrics including

(sub-limitation 1):

> a measure of the extent of, the frequency of, or duration of compromise of the technology systems of the organization, or of a configuration or vulnerability of the organization, **and**

(sub-limitation 2):

> a measure of the resilience of the organization to recover from such vulnerability, the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability

Contrary to the Answer at page 4 ("[a]lthough Newton need not teach all the elements listed in the measurement as they are listed with an "OR" so Newton need only teach one of the items"), to obviate this claim limitation, Newton in view of Shull are required to teach both sub-limitations (labeled "1" and "2") on either side of the term "AND". The following discussion explains why Newton in view of Shull does not teach both of these sub-limitations.

To reject the above limitation, the Answer cites paragraphs [0012]-[0030] of Newton, reproduced here:

> [0012] These questions, and many more, can be answered, with the present invention, a Network Intelligence Database. Every network in the world would have a record in the database, with a large number of properties. Some properties might be:
> [0013] Hostility level on the Internet;
> [0014] Security event history;
> [0015] Spam levels;
> [0016] Hosted services (web servers, email servers);
> [0017] Public wireless;
> [0018] Organization type: educational, enterprise, military;
> [0019] Organization associations: owned by, partnered with whom;
> [0020] Peer ISPs;
> [0021] Bandwidth connection to the Internet;
> [0022] Active security measures, firewalls, IDSs;
> [0023] Number of users, employees, people on this network;
> [0024] Age of the network;
> [0025] Inappropriate content served (hate sites, porn, pirated software);
> [0026] Industry: industrial, computers;
> [0027] Geographic placement;
> [0028] Open proxy servers; and
> [0029] Address, contact information.
> [0030] Accordingly, system and method of the present invention establish respective reputations for networks and allow a given network to determine whether to communicate with a particular network in dependence upon its reputation.

The Answer at page 4 states that:

> Newton, [0012] teaches that every network in the world would have a rating in the database and [0030] teaches establishing a reputation for a network, and a reputation/rating is indicative on how trust worthy a network is and the information gathered would be indicative on the resilience a network would likely

> be due to a compromise as a larger organization with more resources that has existed longer is more likely to be resilient than a smaller organization with less resources and age.

First, contrary to the Answer, Newton does not say that "every network in the world would have a **rating** in the database." Newton in paragraph [0012] states that "[e]very network in the world would have a **record** in the database, with a large number of properties" and proceeds to list the properties in paragraphs [0013]-[0029]. Thus, there is no **rating** taught or suggested by Newton in paragraph [0012]. Second, paragraph [0030] of Newton simply states "[a]ccordingly, system and method … establish respective reputations for networks" without making reference to any of the preceding properties. Paragraph [0030] does not even define the term "respective reputations for networks." Therefore, it cannot be inferred, as set forth in the Answer, that paragraph [0030] of Newton "**teaches** establishing a reputation for a network, and a reputation/rating is indicative on how trust worthy a network is and the information gathered would be indicative on the resilience a network would likely be due to a compromise as a larger organization with more resources that has existed longer is more likely to be resilient than a smaller organization with less resources and age."

Specifically taking "sub-limitation 2": Newton in the above cited portions does not teach or suggest the term "resilience" as used in claim 1 and/or as defined by the Specification. Specifically, in claim 1 "the measure of the resilience" is "inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability." Thus, Newton does not teach at least sub-limitation 2.

The Answer also cites Shull at paragraphs [0059] and [0068], which respectively state:

> [0059] This exemplary scoring scheme is designed to be extensible, in that a plurality of scores may be accorded to any given entity, based perhaps on various characteristics and/or categories of activities. Merely by way of example, an entity may be accorded a number of scores based on that entity's likelihood of being involved in phishing and/or other fraudulent activities, brand abuse, pornography, e-commerce, online transactions, consumer targeting, preferred programs, service expedition, etc. (It may be noted from the above list that not all activities need to be illegitimate activities. Merely by way of example, a score indicating that an entity is likely to be engaged in e-commerce may allow a user to infer that a transaction with that entity is relatively more likely to be a legitimate transaction and/or may be used by a security system on a client and/or a

> border device (including those described below, for example) to make a determination that a transaction with such an entity is an allowable communication.
>
> [0068] Another type of derived score that that may be calculated by scoring engine for an online entity is a secure infrastructure score 232. Secure infrastructure scores 232 may be used to evaluate and score an online entity's use of security features, such as certificates. Other exemplary types of derived scores include trusted record scores 233 (evaluating and scoring entities based on the respective online entity's history with trusted data sources), change scores 234 (evaluating and scoring the frequency with which an online entity changes domain registrations), whitelist and/or blacklist scores 235 (evaluating and scoring an online entity's suitability for a whitelist (very high repute) or blacklist (disreputable)), history scores 236 (evaluating historical data to determine an entity's online history, lack of history and/or a quality of that history), portfolio scores 237 (evaluating and scoring the online entity based on whether an online portfolio (domain names owned, activities performed, etc.) associated with the online entity is compatible (makes sense) with the nature and character of the online entity), and/or any other type of derived score which evaluates a factor of correlated data associated with an online entity. Other scores can include application scores and virus scores, which can evaluate the trustworthiness of particular applications and/or malicious code (such that, when a user attempts to install such applications and/or code, the scores can be used to either advise the user on whether the application should be installed and/or make a determination (e.g., at an operating system and/or domain policy level) whether to allow or prohibit such installation).

None of the above cited portions teach or suggest the concept of "a measure of resilience" nor the concept of the measure of resilience "being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability." Looking closer at paragraphs [0059] and [0068], Shull describes scoring of an entity based on:

(a) "that entity's likelihood of being involved in phishing and/or other fraudulent activities, brand abuse, pornography, e-commerce, online transactions, consumer targeting, preferred programs, service expedition, etc." [0059]

(b) "an online entity's use of security features, such as certificates" [0068]

(c) "the respective online entity's history with trusted data sources" [0068]

(d) "the frequency with which an online entity changes domain registrations" [0068]

(e) "an online entity's suitability for a whitelist (very high repute) or blacklist (disreputable)" [0068]

(f) "historical data to determine an entity's online history, lack of history and/or a quality of that history" [0068]

(g) "the online entity based on whether an online portfolio (domain names owned, activities performed, etc.) associated with the online entity is compatible (makes sense) with the nature and character of the online entity" [0068]

(h) "a factor of correlated data associated with an online entity" [0068]

(i) "the trustworthiness of particular applications and/or malicious code (such that, when a user attempts to install such applications and/or code, the scores can be used to either advise the user on whether the application should be installed and/or make a determination (e.g., at an operating system and/or domain policy level) whether to allow or prohibit such installation" [0068]

Note that the above quotations are labeled "(a)" - "(i)" to facilitate explanation. None of the above paragraphs of Shull teach or suggest sub-limitation 2. For example, in "(b)" above, an entity's use of security features does not relate an entity's resilience in recovering from a vulnerability. Security features such as certificates may prevent a vulnerability from occurring but would not aid the entity in recovery from the vulnerability. In another example, in "(i)" above, the trustworthiness of a particular application or code does not indicate any measure of resilience of the organization. Therefore, Appellant submit that Newton and Shull, whether taken individually or together, fail to teach or suggest the claimed subject matter, as is required for a rejection under 35 U.S.C. § 103(a) for at least these reasons.

Next, with respect to the following limitation: "the information indicative of durations of events associated with compromises or vulnerabilities or configurations," the Answer cites paragraphs [0041]-[0042] of Newton:

> [0041] The Master NID 12 includes information on networks through properties 22 of those networks and applies both a weighting system to those properties and time sensitivity (how things become less or more important over time).
>
> [0042] The Customer NID (C-NID) 14 includes information on networks, receives real-time updates from the Master-NID 12 that include properties, and has a multi-user weighting system and time sensitivity. The C-NID (Custom-NID)

> includes a real-time interface for receiving live remote updates from the Mater-NID. It also includes data mining and searching capability.

Newton in paragraphs [0041]-[0042] do not teach the above claim limitation. Simply because the word "time" is used in these paragraphs does not make their disclosures relevant to the claim limitation. Specifically, the term "time sensitivity" has to do with how the properties themselves become less or more important over time. For the sake of argument, and without disclaimer, if one assumes that "properties 22" include those listed in Fig. 1 under element "24" (which is not defined anywhere in Newton), whether any of these properties "become less or more important over time" is not related to "durations of events associated with compromises or vulnerabilities or configurations."

Additionally, the Answer cites paragraph [0057] of Shull, reproduced here:

> [0057] Trust evaluation system 102 may also provide a historical view of an entity's activities. Merely by way of example, if it is discovered that a given entity is engaging in an illicit activity, such as phishing, a record of the activity may be made with respect to that entity. Further, a record may be made with respect to each of the enabling parties associated with that entity, thereby tagging and/or labeling such enablers as being relatively more likely to facilitate illicit activities. Each time an enabling party is discovered to be a facilitator of such activity (and/or refuses to take corrective action when notified of such activity), a trust score may be adjusted. Trust score(s) may allow interested parties to determine quickly whether a given enabling party is relatively more or less likely to act as a facilitator of illicit activity, which can provide insight into the likelihood of a entity associated with such an enabling party to be engaged in an illicit activity and/or can allow the preparation of a complaint against an enabling party, etc.

Again, no disclosure in the above paragraph of Shull teaches or suggests "information indicative of durations of events associated with compromises or vulnerabilities or configurations." It is noted that the term "time" is used in the above paragraph when discussing instances in which an enabling party is discovered facilitating illicit activities. However, as before, this is entirely unrelated to "information indicative of durations of events…" as claimed. Thus, Newton in view of Shull fail to teach or suggest the claimed subject matter, as is required for a rejection under 35 U.S.C. § 103(a).

Finally, on pages 5-6, the Answer returns again to the definition of "infrastructure resilience" supplied on page 4 of the Answer. Specifically, the Answer states that:

> [t]he limitation "the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability" is no more than rewording of provided by Examiner definition of resilience. Because resilience is the ability to reduce the magnitude and/or duration of disruptive events, the higher the resilience the low is the magnitude and/or duration of disruptive events, which in mathematics well known as inversely proportional functionality.

To reiterate, the definition provided in the Answer cannot be used to define an already-defined term in the Specification (see above). Moreover, for the sake of argument, even if the claim limitation was a "rewording" of the provided definition (which it is not), the Answer explicitly states at page 4 that "NIAC cited ONLY as source of the term definition, and should NOT be considered as prior art reference." Therefore, it has no bearing on the patentability of the limitation in view of the claim as a whole.

The remainder of the Answer quotes the rejections of the Final Office Action dated February 13, 2017 and have been addressed in the Appeal Brief dated December 21, 2018. In summary, Appellants submit that Newton and Shull, either alone or in combination, fail to teach or suggest the claimed invention, when taken as a whole, as is required for a rejection under 35 U.S.C. § 103(a).

CONCLUSION

In view of the arguments above, and those articulated in the Appeal Brief, Appellant respectfully submit that claims 1, 4, 5, 7-14, 16, 121, 122, 124, 126-132, and 134-141 are patentable and urge the Board to reverse all of the Examiner's rejections as to each of these claims.

Dated: July 16, 2018

Respectfully submitted,

Electronic signature: /Gozde Guckaya/
Gozde Guckaya
Registration No.: 74,989
Agent for Applicant
GOODWIN PROCTER LLP
100 Northern Avenue
Boston, Massachusetts 02210
(617) 570-1000

CLAIMS APPENDIX

1. A method comprising:

collecting information about two or more organizations that have computer systems, network resources, and employees, the organizations posing risks through business relationships of the organizations with other parties, the information collected about the organizations being indicative of compromises, vulnerabilities or configurations of technology systems of the organizations and indicative of resiliencies of the organizations to recover from such compromises, vulnerabilities or configurations, the information indicative of durations of events associated with compromises or vulnerabilities or configurations,

at least some of the information about each of the organizations being collected automatically by computer using sensors on the Internet,

the information about each of the organizations being collected from two or more sources, one or more of the sources not being controlled by the organization, the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization,

at least partly automatically gathering information about assets that each of the organizations owns, controls, uses, or is affiliated with, including IP addresses and IP network address ranges, computer services residing within address ranges, or domain names,

at least one of the sources for each of the organizations comprising a public source or a commercial source,

processing by computer the information from the two or more sources for each of the organizations to form a composite rating of the organization that is indicative of a degree of risk to the organization or to a party through a business relationship with the organization, the composite rating comprising a calculated composite of metrics and data derived or collected from the sources, the processing comprising applying transformations to the data and metrics, and the processing comprising applying weights to the data and the metrics,

the metrics including a measure of the extent of, the frequency of, or duration of compromise of the technology systems of the organization, or of a configuration or vulnerability of the organization, and a measure of the resilience of the organization to recover from such

vulnerability, the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability, and

in connection with assessing a business risk to the organization or to a party through a business relationship with at least one of the organizations, delivering reports of the composite ratings of the organizations through a reporting facility to enable users of the reporting facility to monitor, assess, and mitigate the risks, based on the security vulnerabilities and resiliencies, in doing business with the organization and to compare the composite ratings of the organizations.

4. The method of claim 1, wherein the collected information is represented by at least two data types.

5. The method of claim 4, wherein the at least two data types include at least one of breach disclosures, block lists, configuration parameters, an identification of malware servers, an identification of a reputation, an identification of suspicious activity, an identification of spyware, white lists, an identification of compromised hosts, an identification of malicious activity, an identification of spam activity, an identification of vulnerable hosts, an identification of phishing activity, or an identification of e-mail viruses.

7. The method of claim 1, wherein the collected information evidences internal security controls.

8. The method of claim 1, wherein the collected information comprises outcomes of each of the organizations.

9. The method of claim 1, wherein the collected information evidences operational execution of security measures of each of the organizations.

10. The method of claim 1, wherein the collected information indicates whether a computer system of each of the organizations served malicious code to another system.

11. The method of claim 1, wherein the collected information indicates whether a computer system of each of the organizations communicated with a known attacker controlled network or sensor outside the control or network of the organization.

12. The method of claim 1, comprising: forming a series of the security ratings of each of the organizations.

13. The method of claim 12, comprising: determining a trend from the series of ratings.

14. The method of claim 12, comprising displaying the series of composite ratings.

16. The method of claim 14, wherein displaying the series of composite ratings for each of the organizations comprises posting the series of composite ratings for the organization to a web portal.

121. The method of claim 1, wherein the collected information represents externally observable outcome information.

124. The method of claim 1, comprising: determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information.

126. The method of claim 1, wherein: the collected information comprises at least two security characterizations of a computer system of each of the organizations.

127. The method of claim 1, wherein the collected information comprises a characterization of behavior of an employee of at least one of the organizations.

128. The method of claim 1, wherein the collected information comprises characterizations other than characterizations about a computer system of at least one of the organizations.

129. The method of claim 1, wherein the collected information comprises characterizations about policies of at least one of the organizations.

130. The method of claim 1, wherein the collected information comprises characterizations about information technology assets that at least one of the organizations owns, controls, uses, or is affiliated with.

131. The method of claim 1 in which collected information represents: (a) physical states, (b) technical states, (c) organizational states, or (d) cultural states of at least one of the organizations which can be exploited to create a security breach; or (e) the organization's ability to recover from a security breach; or any combination of two or more of these.

132. The method of claim 1 in which processing the information to form a composite rating comprises correlating data across the sources of information.

134. The method of claim 1 in which processing the information to form a composite rating comprises statistically correlating the composite rating with actual outcomes.

135. The method of claim 1 in which the vulnerability comprises physical, technical, organizational, or cultural states that can be exploited to create a security breach.

136. A method comprising

collecting, from at least two sources, information about two or more organizations, the collected information representing at least two data types, the collected information comprising outcomes of each of the organizations,

at least some of the information for each of the organizations being collected automatically by computer from at least two sources, one or more of the sources not controlled by the organization,

the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization, at least one of the sources including a commercial data source,

processing the information from both of the two sources for each of the organizations to form a composite rating of a security vulnerability of the organization and of a resilience of the organization to recover from a security breach, the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability, or both, the processing including applying models that account for differences in the respective sources,

normalizing the composite rating of each of the organizations based on a size characteristic of the organization to enable comparisons of composite ratings between the two or more organizations,

forming a series of the security ratings of each of the organizations, determining a trend from the series of ratings, and displaying the series of composite ratings through a portal,

determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information, and

reporting the composite ratings of the organizations through a portal to enable customers to monitor, assess, and mitigate risk in doing business with the organizations and to compare the composite ratings across the organizations.

137. The system of claim 1, determining a confidence range of the composite rating, the size of the range varying inversely with the level of confidence in the composite rating.

138. The system of claim 137, wherein the confidence range is based on redundancy of the security characterizations.

139. The system of claim 137, wherein the confidence range is based on a size of the third party computer system.

140. The method of claim 1 comprising ranking the organization and other organizations within sectors or peer-groups or globally.

141. A method comprising:

collecting information about an organization that has computer systems, network resources, and employees, the organization posing risks to itself or to other parties through business relationships of the organization with the other parties,

the information collected about the organization including (a) information collected automatically by computer on the Internet without permission of the organization, and (b) information indicative of resiliencies of the organization to recover from a security breach associated with a compromise or a vulnerability, the resiliencies being inversely proportional to one or more of the duration of detected malicious activity and the duration of the compromise or vulnerability,

processing the information by computer to form a composite rating of the organization that is indicative of a degree of risk based on a business relationship with the organization, the composite rating comprising a measure of the resiliencies of the organization to recover from a security breach, and in connection with assessing the degree of risk, delivering a report of the composite rating of the organization through a reporting facility to enable a user of the reporting facility to assess the risks, based at least in part on the resiliencies.

Electronic Acknowledgement Receipt

EFS ID:	33182901
Application Number:	13240572
International Application Number:	
Confirmation Number:	2423
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Customer Number:	51414
Filer:	Gozde Guckaya/Andrea Borden
Filer Authorized By:	Gozde Guckaya
Attorney Docket Number:	BST-004
Receipt Date:	16-JUL-2018
Filing Date:	22-SEP-2011
Time Stamp:	13:19:38
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Reply Brief Filed	BST-004_Reply_Brief.pdf	124902 9d226c673eb5aca0bc175944dca3661a8f08103b	no	16

Warnings:

Information:	
Total Files Size (in bytes):	124902

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/240,572	09/22/2011	Stephen Wayne Boyer	BST-004	2423

51414 7590 05/16/2018

GOODWIN PROCTER LLP
PATENT ADMINISTRATOR
100 Northern Avenue
BOSTON, MASSACHUSETTS 02210
UNITED STATES OF AMERICA

EXAMINER	
KANAAN, SIMON P	

ART UNIT	PAPER NUMBER
2492	

NOTIFICATION DATE	DELIVERY MODE
05/16/2018	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

GLENN.WILLIAMS@GOODWINPROCTER.COM
PATENTBOS@GOODWINPROCTER.COM
PSOUSA-ATWOOD@GOODWINPROCTER.COM

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Application Number: 13/240,572
Filing Date: 22 Sep 2011
Appellant(s): Boyer et al.

Joel Lehrer
Reg. No: 56,401
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed December 21st 2017.

(1) Grounds of Rejection to be Reviewed on Appeal

Every ground of rejection set forth in the Office action dated February 13, 2017 from which the appeal is taken is being maintained by the examiner except for the grounds of rejection (if any) listed under the subheading "WITHDRAWN REJECTIONS." New grounds of rejection (if any) are provided under the subheading "NEW GROUNDS OF REJECTION."

The following ground(s) of rejection are applicable to the appealed claims.

Claims 1, 4, 5, 7-14, 16, 121, 122, 124, 126-132 and 134-141 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chris Newton (US Pre-Grant Publication No: 2004/0250122 A1) in view of Shull et al. (US Pre-Grant Publication No: 2006/0212925 A1)

(2) Response to Argument

The Examiner will show that contrary to Appellant's arguments in the Appeal Brief filed on 21st December 2018 (hereinafter referred to as "the Brief'), the Office Action mailed February 13 2017 has met the requirements of law necessary to show nonpatentability of the appealed claims. The Examiner will show that Appellant has failed to overcome the rejections under their respective titles and thus must be sustained.

To enable the reader to more easily follow which rebuttals are meant to address Appellant's arguments, the Examiner applies the heading scheme relied upon in the Brief.

Status of Amendments:

On page 3 of the brief, Appellant states that there are amendments filed with RCE October 17, 2017; however no such amendments were filed on that date.

Definitions of terms

According to Appellants: "discovery that the claimed "resiliency" is in fact a critical metric to consider" (Appeal Brief, 10). Further Appellants define the term "resiliency" by way of providing examples.

However the definition of Infrastructure resilience is well known in the art. Examiner relies on definition provided by NATIONAL INFRASTRUCTURE ADVISORY COUNCIL on page 8 of CRITICAL INFRASTRUCTURE RESILIENCE FINAL REPORT AND RECOMMENDATIONS (2009, 54 pages):

> ***Infrastructure resilience*** *is the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event.*

NIAC cited ONLY as source of the term definition, and should NOT be considered as prior art reference.

A. The rejection of claims 1, 4, 5, 7-14, 16, 121, 122, 124, 126-132 and 134-141 under pre-AIA 35 U.S.C. § 103(a) as unpatentable over Newton in view of Shull is improper and should be reversed.

Appellant argues **that the cited prior art does not teach : "the metrics including a measure of the extent of the frequency, or of the duration, or compromise of the technology systems of the organization, or of a configuration or vulnerability of the organization, and a measure of the resilience of the organization to recover from such vulnerability, the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability,".**

However examiner respectfully disagrees Although Newton need not teach all the elements listed in the measurement as they are listed with an "OR" so Newton need only teach one of the items. However Newton, [0012] teaches that every network in the world would have a rating in the database and [0030] teaches establishing a reputation for a network, and a reputation/rating is indicative on how trust worthy a network is and the information gathered would be indicative on the resilience a network would likely be due to a compromise as a larger organization with more resources that has existed longer is more likely to be resilient than a smaller organization with less resources and age. Thus Newton [0012]-[0030] to show that all ORs of the limitation are actually disclosed and Shull [0059], [0068] as well teaches some of the alternative limitations.

Also please note that resilience is defined to be "Infrastructure resilience is the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event."

Appellant argument related to: "**the information indicative of durations of events associated with compromises or vulnerabilities or configurations,**" in addition to Newton [0012] , see "[0041] The Master NID 12 includes information on networks through properties 22 of those networks and applies both a weighting system to those properties and time sensitivity (how things become less or more important over time)." Newton [0041]. Also [0042]. You have also mentioned *Shull [0058], [0057] is also relevant: "a record of the activity may be made with respect to that entity… Each time an enabling party is discovered to be a facilitator of such activity (and/or refuses to take corrective action when notified of such activity), a trust score may be adjusted. Trust score(s) may allow interested parties to determine quickly whether a given enabling party is relatively more or less likely to act as a facilitator of illicit activity, which can provide insight into the likelihood of a entity associated with such an enabling party to be engaged in an illicit activity and/or can allow the preparation of a complaint against an enabling party, etc."*

The limitation "the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability" is no more than rewording of provided by Examiner definition of resilience. Because resilience is the ability to reduce the magnitude and/or duration of disruptive events, the higher the

resilience the low is the magnitude and/or duration of disruptive events, which in mathematics well known as inversely proportional functionality.

For clarification examiner is including the rejection set forth in the final office action:

As per **claim 1**, Newton discloses **a method comprising: collecting information about two or more organizations** *(Newton, [0018])* **that have computer systems, network resources** *(Newton, [0022])*, **and employees** *(Newton, [0023])*, **the organizations posing risks through business relationships of the organizations with other parties,** *(Newton, [0025]. [0019])* **the information collected about the organizations being indicative of compromises, vulnerabilities or configurations of technology systems of the organizations and indicative of resiliencies of the organizations to recover from such compromises, vulnerabilities or configurations, the information indicative of durations of events associated with compromises or vulnerabilities or configurations,** *(: Although Newton need not teach all the elements listed in the measurement as they are listed with an "OR" so Newton need only teach one of the items. However Newton, [0012] teaches that every network in the world would have a rating in the database and [0030] teaches establishing a reputation for a network, and a reputation/rating is indicative on how trust worthy a network is and the information gathered would be indicative on the resilience a network would likely be due to a compromise as a larger organization with more resources that has existed longer is more likely to be resilient than a smaller organization with less resources and age. Thus Newton [0012]-[0030] to show that all ORs of the limitation are actually disclosed and Shull [0059], [0068] as well teaches some of the alternative limitations.)*

at least some of the information about each of the organizations being collected automatically by computer using sensors on the Internet, the information about each of the organizations being collected from two or more sources, one or more of the sources not being controlled by the

organization, the information format least the one or more sources that are not controlled by the organization being collected without permission of the organization, *(Newton, [0031] teaches having multiple agents gathering data and [0044]-[0048] teaches different agent types i.e. different network characterization as each agent type gathers different type of data in regards to the security and reputation of network, among these agents include data mining internet which is public information and data mining newsgroups and forums which are also public knowledge and externally observable information not controlled by an organization)*

at least partly automatically gathering information about assets that each of the organizations owns, controls, uses, or is affiliated with, including IP addresses and IP network address ranges, computer services residing within address ranges, or domain names, *(Newton, [0022]-[0023])*

at least one of the sources for each of the organizations comprising a public source or a commercial source, *(Newton, [0044]-[0048] and [0029], teaches information gathered externally from multiple sources including proxy information and data mining internet which is public information.)*

processing by computer the information from the two or more sources for each of the organizations to form a composite rating of the organization that is indicative of a degree of risk to the organization or to a party through a business relationship with the organization, *(Newton, [0016], teaches "Hosted services (web servers, email servers)" and [0044]-[0048] and [0029], teaches information gathered externally from multiple sources including proxy information and data mining internet which is public information.)*

in connection with a assessing a business risk to the organization or to a party through a business relationship with at least one of the organizations, delivering reports of the composite ratings of the organizations through a reporting facility to enable users of the reporting facility to monitor, assess, and mitigate the risks, based on the security vulnerabilities and resiliencies, in doing

business with the organization and to compare the composite ratings of the organizations. *(Newton, figure 3 item 14, teaches a database which stores information about the organizations i.e. portal.)*

But Newton does not teach **the composite rating comprising a calculated composite of metrics and data derived or collected from the sources, the processing comprising applying transformations to the data and metrics, and the processing comprising applying weights to the data and the metrics, the metrics including a measure of the extent of the frequency of, or the duration of compromise of the technology systems of the organization, or of a configuration or vulnerability of the organization, and a measure of the resilience of the organization to recover from such vulnerability, the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability,**

However, *(Shull [0058] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score which informs requester of the trust of the entity, this score is received by the requester where activities are accounted for both legitimate (i.e. positive) and illegitimate (i.e. negative) and [0069] and [0073], teaches giving an overall trust score between 1 and 5 i.e. a normalized composite score where 1 is a reputable business and 5 is likely engaged in illicit activity.)*

It would have been obvious at the time of the invention for one of the ordinary skill in the art to modify the method of collecting security characteristics from multiple sources as taught by Newton by creating a score representative of the different collected data as taught by Shull because it would aid the requester in determining whether the entity is trusted or not.

As per **claim 4**, Newton in view of Shull discloses **the method of Claim 1, wherein the collected information is represented by at least two data types.** *(Newton, [0044]-[0048] teaches different agent types.)*

As per **claim 5**, Newton in view of Shull discloses the method of Claim 4, wherein the at least two data types include at least one of breach disclosures, block lists, configuration parameters, an identification of malware servers, an identification of a reputation, an identification of suspicious activity, an identification of spyware, white lists, an identification of compromised hosts, an identification of malicious activity, an identification of spam activity, an identification of vulnerable hosts, an identification of phishing activity, or an identification of e-mail viruses. *(Newton, [0013]-[0029] teaches security measures etc.)*

As per **claim 7**, Newton in view of Shull discloses **the method of Claim 1, wherein the collected information evidences internal security controls.** *(Newton, [0013]-[0029] teaches security measures etc.)*

As per **claim 8**, Newton in view of Shull discloses **the method of Claim 1, wherein the collected information comprises outcomes of each of the organizations.** *(Newton, [0013]-[0029] teaches security measures and [0044]-[0048] teaches checking for information already available to the public about network.)*

As per **claim 9**, Newton in view of Shull discloses **the method of Claim 1, wherein the collected information evidences operational execution of security measures of the organizations.** *(Newton, [0013]-[0029] teaches security measures.)*

As per **claim 10**, Newton in view of Shull **discloses the method of Claim 1, wherein the collected information indicates whether a computer system of the organizations served malicious code to another system.** *(Newton, [0013], teaches hostility level and page 4, claim 6, teaches spam levels.)*

As per **claim 11**, Newton in view of Shull discloses **the method of Claim 1, wherein the collected information indicates whether a computer system of the organizations communicated with a known attacker controlled network or sensor outside the control network of the organization**. *(Newton, [0013] teaches hostility level.)*

As per **claim 12**, Newton in view of Shull discloses **the method of Claim 1, comprising: forming a series of the security ratings of the organizations**. *(Newton, [0042], teaches live remote updates i.e. continually computing rating and page 4, claim 6 teaches security information has multiple ratings and [0041], teaches the different information having different weight.)*

As per **claim 13**, Newton in view of Shull discloses **the method of Claim 12, comprising determining a trend from the series of ratings.** *(Newton, [0042], teaches live remote updates i.e. continually computing rating.)*

As per **claim 14**, Newton in view of Shull discloses **the method of Claim 12, comprising displaying the series of composite ratings**. *(Newton, [0033], teaches a master database for collecting and storing the network ratings and page 4, claim 6 teaches security information has multiple ratings and [0041], teaches the different information having different weight and Shull, [0058], [0076] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit*

score with informs requester of the trust of the entity, this score is received by the requester and a display device would display score as to help user determine whether to trust entity or not.)

As per **claim 16**, Newton in view of Shull **teaches the method of Claim 14, wherein displaying the series of composite ratings for each of the organizations comprises posting the series of composite ratings for each of the organizations to a web portal.** *(Newton, [0033], teaches a master database for collecting and storing the network ratings which includes information as listed in [0013]-[0029] which serve as warnings and Shull, [0058], [0076] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score with informs requester of the trust of the entity, this score is received by the requester and a display device would display score as to help user determine whether to trust entity or not.)*

As per **claim 121**, Newton in view of Shull teaches **the method of Claim 1, wherein the collected information represents externally observable outcome information**. - Newton, [0054], teaches agents getting information from news groups or sending packets and checking their responses.

As per **claim 122**, Newton in view of Shull teaches **the method of Claim 121, wherein the outcome information comprises outcome information associated with security vulnerability or resilience of each of the organizations. (***Shull, [0058] and Newton, page 4, claim 6, both teach that the information is associated with entity security and Newton even looks into active security systems as well.)*

As per **claim 124**, Newton in view of Shull teaches **the method of Claim 1, comprising: determining a badness score that corresponds to an intensity or duration of malicious activity**

determined from the collected information. *(Newton, page 4, claim 6, teaches having spam levels etc. Which are a badness score.)*

As per **claim 126**, Newton in view of Shull teaches **the method of Claim 1, wherein: the collected information comprises at least two security characterizations of a computer system of the entity.** *(Newton, page 4, claim 6, teaches checking open proxy servers and desktop security measures which are multiple characterizations of a system of the entity.)*

As per **claim 127**, Newton in view of Shull teaches **the method of Claim 1, wherein the collected information comprises a characterization of behavior of an employee of at least one of the organizations.** *(Newton, page 4, claim 6, inappropriate content served, spam levels, language spoken, geographic placement, industry, which are characterizations of employees in the network and the employees' behavior.)*

As per **claim 128**, Newton in view of Shull teaches **the method of Claim 1, wherein the collected information comprises characterizations other than characterizations about a computer system of at least one of the organizations.** *(Newton, page 4, claim 6, teaches security characterization includes security personnel.)*

As per **claim 129**, Newton in view of Shull teaches **the method of Claim 1, wherein the collected information comprises characterizations about policies of at least one of the organizations.** *(Newton, page 4, claim 6, teaches organization association, active security measures, desktop security measures, etc. which are policies see also [0059] and [0060].)*

As per **claim 130**, Newton in view of Shull teaches **the method of Claim 1, wherein the collected information comprises characterizations about information technology assets that at least one of the organizations owns, controls, uses, or is affiliated with.** *(Newton, page 4, claim 6, teaches organization associations see also [0043] and [0053].)*

As per **claim 131**, Newton in view of Shull **teaches the method of Claim 1 in which collected information represents: (a) physical states, (b) technical states, (c) organizational states, or (d) cultural states of at least one of the organizations which can be exploited to create a security breach; or (e) the organization's ability to recover from a security breach; or any combination of two or more of these.** *(Newton, page 4, claim 6, teaches active security measures and desktop security measures among other information collected about the organization.)*

As per claim 132, Newton in view of Shull teaches **the method of claim 1 in which processing the information to form a composite rating comprises correlating data across the sources of information.** *(Shull, [0058], teaches creating a score based on the different data received i.e. correlating the different data.)*

As per claim 134, Newton in view of Shull **teaches the method of claim 1 in which processing the information to form a composite rating comprises statistically correlating the composite rating with actual outcomes.** *(Newton, [0041], teaches giving different information different weight where less weight given to information as it becomes less important over time which is a statistical correlation with the information collected.)*

As per claim 135, Newton in view of Shull **teaches the method of claim 1 in which the vulnerability comprises physical, technical, organizational, or cultural states that can be exploited to create a security breach.** *(Newton, figure 1, item 24 and page 4, claim 6.)*

As **per claim 136**, Newton teaches **a method comprising collecting, from at least two sources, information about two or more organizations, the collected information representing at least two data types, the collected information comprising outcomes of each of the organizations, at least some of the information for each of the organizations being collected automatically by computer from at least two sources, one or more of the sources not controlled by the organization, the information from at least the one or more sources that are not controlled by the organization being collected without permission of the-organization, at least one of the sources including a commercial data source,** *(Newton, [0012] teaches that every network in the world would have a rating in the database and [0030] teaches establishing a reputation for a network, and [0031] teaches having multiple agents gathering data and [0044]-[0048] teaches different agent types i.e. different network characterization as each agent type gathers different type of data in regards to the security and reputation of network, among these agents include data mining internet which is public information and data mining newsgroups and forums which are also public knowledge and externally observable information not controlled by an organization and figure 1, items 24 include information about the network which towards the bottom of item 24 states "company info resources" i.e. network is associated with a company, and [0022] and [0072], teaches taking into account size of the network and number of employees.)*

at least partly automatically gathering information about assets that each of the organizations owns, controls, uses, or is affiliated with, including IP network address ranges, computer services

residing within address ranges, or domain names, *(Newton, [0029] teaches "Address, contact information." And [0019] teaches "Organization associations: owned by, partnered with whom")*

and displaying the series of ratings through a portal and reporting the ratings of the organizations through a portal to enable customers to monitor, assess, and mitigate risk in doing business with the organizations and to compare the composite ratings across the organizations. *(Newton, figure 3 item 14, teaches a database which stores information about the organizations i.e. portal.)*

But Newton does not teach **processing the information from both of the two sources for each of the organizations to form a composite rating of a security vulnerability of the organization and of a resilience of the organization to recover from a security breach, the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability, or both, the processing including applying models that account for differences in the respective sources,, normalizing the composite rating of each of the organizations based on a size characteristic of the organization to enable comparisons of composite ratings between the two or more organizations, forming a series of the security ratings of each of the organizations, determining a trend from the series of ratings, determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information.**

However, *(Shull [0058] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score which informs requester of the trust of the entity, this score is received by the requester where activities are accounted for both legitimate (i.e. positive) and illegitimate (i.e. negative) and [0069] and [0073], teaches giving an overall trust score between 1 and 5 i.e. a normalized composite score where 1 is a reputable business and 5 is likely engaged in illicit activity.)*

It would have been obvious at the time of the invention for one of the ordinary skill in the art to modify the method of collecting security characteristics from multiple sources as taught by Newton by creating a score representative of the different collected data as taught by Shull because it would aid the requester in determining whether the entity is trusted or not.

As per **claim 137**, Newton in view of Shull **teaches the method of claim 1, determining a confidence range of the composite rating, the size of the range varying inversely with the level of confidence in the composite rating.** *(Shull, [0069] and [0073], teaches giving an overall trust score between 1 and 5 i.e. a normalized composite score where 1 is a reputable business and 5 is likely engaged in illicit activity.)*

As per **claim 138**, Newton in view of Shull **teaches the system of claim 137, wherein the confidence range is based on redundancy of the security characterizations.** *(Shull, [0081], teaches taking into account consistency which is redundancy.)*

As per **claim 139**, Newton in view of Shull teaches **the method of claim 137, wherein the confidence range is based on a size of the third party computer system.** *(Newton, [0072], teaches taking into account size of the network.)*

As per **claim 140**, Newton in view of Shull teaches **the method of claim 1 comprising ranking the organization and other organizations within sectors or peer-groups or globally.** *(Shull, [0123]-[0124], teaches listing entities with similar scores together such as ones that scored a 3 or 4 so these would be ranked below ones which were listed as part of white list which ranked 1 or 2, see [0068], which teaches having white list, black list and grey lists.)*

As **per claim 141**, Newton teaches **a method comprising: collecting information about an organization** *(Newton, [0018])* **that has computer systems,** *(Newton, [0022])* **network resources, and employees,** *(Newton, [0023])* **the organization posing risks to itself or to other parties through business relationships of the organization with the other parties, the information collected about the organization** *(Newton, [0012] teaches that every network in the world would have a rating in the database and [0030] teaches establishing a reputation for a network)* **including (a) information collected automatically by computer on the Internet without permission of the organization, and** *(Newton, [0031] teaches having multiple agents gathering data and [0044]-[0048] teaches different agent types i.e. different network characterization as each agent type gathers different type of data in regards to the security and reputation of network, among these agents include data mining internet which is public information and data mining newsgroups and forums which are also public knowledge and externally observable information not controlled by an organization)* **(b) information indicative of resiliencies of the organization to recover from a security breach associated with a compromise or a vulnerability, the resiliencies being inversely proportional to one or more of the duration of detected malicious activity and the duration of the compromise or vulnerability,** *(Newton, [0030] teaches establishing a reputation for a network, and a reputation/rating is indicative on how trust worthy a network is and the information gathered would be indicative on the resilience a network would likely be due to a compromise as a larger organization with more resources that has existed longer is more likely to be resilient than a smaller organization with less resources and age)* **processing the information by computer to form a composite rating of the organization that is indicative of a degree of risk based on a business relationship with the organization,** *(Newton, [0016], teaches "Hosted services (web servers, email servers)" and [0044]-[0048] and [0029], teaches information gathered externally from multiple sources including proxy information and data mining internet which is public information.)*

delivering a report of the composite rating of the organization through a reporting facility to enable a user of the reporting facility to assess the risks, based at least in part on the resiliencies. *(Newton, figure 3 item 14, teaches a database which stores information about the organizations i.e. portal.)*

but Newton does not teach **the composite rating comprising a measure of the resiliencies of the organization to recover from a security breach, and in connection with assessing a the degree of risk** .

However, *(Shull [0058] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score which informs requester of the trust of the entity, this score is received by the requester where activities are accounted for both legitimate (i.e. positive) and illegitimate (i.e. negative) and [0069] and [0073], teaches giving an overall trust score between 1 and 5 i.e. a normalized composite score where 1 is a reputable business and 5 is likely engaged in illicit activity.)*

It would have been obvious at the time of the invention for one of the ordinary skill in the art to modify the method of collecting security characteristics from multiple sources as taught by Newton by creating a score representative of the different collected data as taught by Shull because it would aid the requester in determining whether the entity is trusted or not.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/SIMON P KANAAN/
Examiner, Art Unit 2492

/OLEG KORSAK/
Primary Examiner, Art Unit 2492

/SALEH NAJJAR/
Supervisory Patent Examiner, Art Unit 2492

Requirement to pay appeal forwarding fee. In order to avoid dismissal of the instant appeal in any application or ex parte reexamination proceeding, 37 CFR 41.45 requires payment of an appeal forwarding fee within the time permitted by 37 CFR 41.45(a), unless appellant had timely paid the fee for filing a brief required by 37 CFR 41.20(b) in effect on March 18, 2013.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Stephan Wayne Boyer *et al.*

Application No.: 13/240,572 | Confirmation No.: 2423

Filed: September 22, 2011 | Art Unit: 2492

For: INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM | Examiner: Kanaan, Simon P.

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLACEMENT APPEAL BRIEF

This Replacement Appeal Brief is responsive to the non-final Office action of February 13, 2017 (the "Office action") and the notice of defective appeal brief of December 1, 2017, and is being submitted pursuant to the Notice of Appeal filed April 12, 2017. A petition for a four-month extension of time for filing the Appeal Brief, to November 22, 2017, was submitted with the original Appeal Brief.

Appellants believe that no other fees are due in connection with this submission. However, please consider this a conditional authorization to charge any fees necessary for entry of these papers to our Deposit Account No. 07-1700, under Order No. BST-004.

I. REAL PARTY IN INTEREST

The real party in interest is BitSight Technologies Inc., the named Applicants and assignees of record of the present patent application, as indicated in the assignment recorded at Reel/Frame 027658/0906 of the USPTO's assignment records.

II. RELATED APPEALS, INTERFERENCES, AND TRIALS

There are no related appeals, interferences, or trials to report.

III. SUMMARY OF CLAIMED SUBJECT MATTER

Claims 1, 136 and 141 are the only independent claims, and each is directed to a method for assessing the risks associated with doing business with a particular entity based, at least in part, on a composite security rating.[1]

With regard to claim 1, information is collected about two or more organizations that have computer systems, network resources, and employees that, due to business relationships of the organizations with other parties, pose risks to the organization.[2] The information collected about the organizations is indicative of compromises, vulnerabilities or configurations of technology systems of the organizations, and of resiliencies of the organizations to recover from such compromises, vulnerabilities or configurations.[3] The information is also indicative of durations of events associated with compromises or vulnerabilities or configurations.[4] Some of the information is collected automatically by computers using sensors on the Internet.[5] The information about the organizations is collected from two or more sources, one or more of which is not controlled by the organization and collected without permission of the organization.[6] Information is gathered about assets that each of the organizations owns, controls, uses, or is affiliated with, including IP addresses and IP network address ranges, computer services residing within address ranges, or domain names.[7] At least one of the sources of such information is a public or commercial source.[8] The information is

[1] *See, e.g.*, Specification, page 2, lines 9-10.
[2] *See, e.g.*, Specification, page 7, line 28 – page 8, line 1; page 9, lines 14-16.
[3] *See, e.g.*, Specification, page 3, lines 11-14; page 9 line 28 – page 10, line 2; page 13, lines 15-17.
[4] *See, e.g.*, Specification, page 3, lines 11-14; page 13, lines 22-24.
[5] *See, e.g.*, Specification, page 10, lines 4-7, Figure 2.
[6] *See, e.g.*, Specification, page 2, lines 13-14; page 8, lines 4-5, page 9, lines 13-16.
[7] *See, e.g.*, Specification, page 7, lines 30-32.
[8] *See, e.g.*, Specification, page 8, lines 13-14.

processed to form a composite rating of the organization that is indicative of a degree of risk to the organization or to a party through a business relationship with the organization.[9] The composite rating comprises a calculated composite of metrics and data derived or collected from the sources.[10] The processing includes applying transformations and weights to the data and metrics.[11] The metrics include a measure of the extent of, the frequency of, or duration of compromise of the technology systems of the organization, or of a configuration or vulnerability of the organization, and a measure of the resilience of the organization to recover from such vulnerability, where the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability.[12] In connection with assessing a business risk to the organization through a business relationship with at least one of the organizations, reports of the composite ratings of the organizations are provided through a reporting facility to enable users of the reporting facility to monitor, assess, and mitigate the risks, based on the security vulnerabilities and resiliencies, in doing business with the organization and to compare the composite ratings of the organizations.[13]

With regard to claim 136, information about two or more organizations is collected from at least two sources.[14] The information represents at least two data types and comprising outcomes of each of the organizations.[15] At least some of the information for each of the organizations is collected automatically by computer from at least two sources.[16] One or more of the sources is not controlled by the organization (i.e., a commercial data source), and the information from at the sources that are not controlled by the organization is collected without permission of the organization.[17] The information from the two sources is processed for each of the organizations to form a composite rating of a security vulnerability of the organization and of a resilience of the

[9] *See, e.g.*, Specification, page 4, lines 2-3; page 4, lines 4-5; page 9, lines 14-18.
[10] *See, e.g.*, Specification, page 3, lines 15-19; page 4, lines 2-3; page 19, lines 12-14.
[11] *See, e.g.*, Specification, page 19, lines 17-20.
[12] *See, e.g.*, Specification, page 3, lines 11-14; page 13, lines 14-24.
[13] *See, e.g.*, Specification, page 7, lines 16-23; page 9, lines 14-19; page 22, lines 7-12.
[14] *See, e.g.*, Specification, page 7, line 28 – page 8, line 1; page 9, lines 14-16.
[15] *See, e.g.*, Specification, page 2, lines 16-19.
[16] *See, e.g.*, Specification, page 2, lines 12-15; page 8, lines 2-3; page 9, lines 13-14; page 10, lines 4-8.
[17] *See, e.g.*, Specification, page 2, lines 12-15; page 8, lines 2-3; page 9, lines 3-4.

organization to recover from a security breach.[18] The resilience is inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability, or both.[19] The processing includes applying models that account for differences in the respective sources.[20] The composite rating of each of the organizations is normalized based on a size characteristic of the organization to enable comparisons of composite ratings between the two or more organizations.[21] A series of security ratings is formed for each of the organizations[22]. A trend is determined from the series of ratings and displayed through a portal.[23] A badness score is determined that corresponds to an intensity or duration of malicious activity determined from the collected information.[24] The composite ratings of the organizations are displayed through a portal to enable customers to monitor, assess, and mitigate risk in doing business with the organizations and to compare the composite ratings across the organizations.[25]

With regard to claim 141, information is collected about an organization that has computer systems, network resources, and employees.[26] Through business relationships of the organization with the other parties, the organization poses risks to itself or to other parties.[27] The information collected about the organization includes information collected automatically by computer on the Internet without permission of the organization.[28] The information collected also includes information indicative of resiliencies of the organization to recover from a security breach associated with a compromise or a vulnerability.[29] The resiliencies are inversely proportional to one or more of the duration of detected malicious activity and the duration of the compromise or vulnerability.[30] The information is processed by a computer to form a composite rating of the organization that is indicative of a degree of risk based on a business

---

[18] *See, e.g.*, Specification, page 3, lines 11-14; page 13, lines 14-24.
[19] *See, e.g.*, Specification, page 3, lines 11-14; page 13, lines 14-24.
[20] *See, e.g.*, Specification, page 8, lines 25-29.
[21] *See, e.g.*, Specification, page 4, lines 2-3; page 4, lines 6-10; page 16, lines 22-26.
[22] *See, e.g.*, Specification, page 2, lines 25-26.
[23] *See, e.g.*, Specification, page 18, lines 17-20.
[24] *See, e.g.*, Specification, page 13, line 32 – page 14, line 10.
[25] *See, e.g.*, Specification, page 9, lines 11-18.
[26] *See, e.g.*, Specification, page 7, line 28 – page 8, line 1; page 9, lines 14-16.
[27] *See, e.g.*, Specification, page 7, line 28 – page 8, line 1; page 9, lines 14-16.
[28] *See, e.g.*, Specification, page 2, line 13-14; page 8 lines 4-5; page 9, lines 3-16.
[29] *See, e.g.*, Specification, page 3, lines 11-14; page 13, lines 14-21.
[30] *See, e.g.*, Specification, page 3, lines 11-14; page 13, lines 14-21.

relationship with the organization.[31] The composite rating comprises a measure of the resiliencies of the organization to recover from a security breach.[32] In connection with assessing the degree of risk, a report of the composite rating of the organization is delivered through a reporting facility to enable a user of the reporting facility to assess the risks, based at least in part on the resiliencies.[33]

IV. ARGUMENT

Appellants' technique for assessing the potential security risks of engaging with a particular organization of independent claims 1, 136 and 141 each require at least one feature that distinguishes their methods from other cyber-security rating techniques in the prior art. Specifically, each claim recites using "resiliencies of the organization to recover from a security breach associated with a compromise or a vulnerability" where that resiliency is "inversely proportional to one or more of the duration of detected malicious activity and the duration of the compromise or vulnerability" as an input into a security rating.[34]

In the Office action, the Examiner simply refers to these features without any clear indication of how any particular prior art reference teaches or suggests these limitations. In fact, the Examiner first expressly admits that Newton fails to disclose such capabilities, instead suggesting that Shull teaches this approach, but the Examiner does not point to any specific language in Shull – because no such language exists, and in fact the limitation is completely ignored in the discussion of Shull.[35] In an attempt to cure this deficiency, the Examiner returns to Newton, and claims that the measuring of resilience of a network is inherent in any rating.

A. The rejection of claims 1, 4, 5, 7-14, 16, 121, 122, 124, 126-132 and 134-141 under pre-AIA 35 U.S.C. § 103(a) as unpatentable over Newton in view of Shull is improper and should be reversed.

The Examiner's rejection on pages 4-19 of the Office action, alleging that claims 1, 4, 5, 7-14, 16, 121, 122, 124, 126-132 and 134-141 are unpatentable under pre-AIA 35 U.S.C. § 103(a) over U.S. Patent Publication No. 2004/0250122 to Newton

[31] *See, e.g.*, Specification, page 4, lines 2-5; page 9, lines 14-18; page 21, lines 11-24.
[32] *See, e.g.*, Specification, page 13, line 14-21.
[33] *See, e.g.*, Specification, page 9, lines 11-18.
[34] *See, e.g.*, Specification, page 3, lines 11-14; page 13, lines 14-21.
[35] *S*ee, Final Office Action, p. 7.

("Newton") in view of U.S. Patent Publication No. 2006/0212925 to Shull et al. ("Shull"), is improper and should be reversed.

Newton appears to discuss systems and methods for establishing reputations among networks.[36] More specifically, Newton describes examples of information agents that may be used to "gather information [about networks] from a number of sources."[37] Separately, a set of high level policies are applied against the gathered information to create specific rules sets, which in turn determine whether traffic from certain sites will be permitted.[38] Newton's system simply provides a means for turning policies into rule sets that can be executed by network agents – Newton does not, however, provide specific metrics used, and certainly does not contemplate that "durations of events associated with compromises or vulnerabilities or configurations" are used to influence the policies, let alone contribute to a rating.

Shull generally describes methods for implementing trust policies among entities based on a trust score. Again, like Newton, nowhere does Shull contemplate that "durations of events associated with compromises or vulnerabilities or configurations" should be used as a component of his trust score – and in fact, the Examiner simply cites to Shull's score calculations based on general entity size and a rating from 1-5.[39]

(i) Claims 1, 4, 5, 7-14, 16, 121, 124, 126-132, 134, 135, 138, 139 and 140

Appellants submit that the Examiner when relying on the teachings of Newton in view of Shull, has failed to establish a *prima facie* case of obviousness.[40] A *prima facie* case of obviousness under 35 U.S.C. § 103(a) requires, among other things, a showing that the applied references, either alone or in combination, teach or suggest each and every element of the claimed invention, when taken as a whole.[41] Moreover, "[r]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational

[36] *See*, Newton ¶ [0030].
[37] *See*, Newton ¶¶ [0043] – [0048].
[38] *See*, Newton ¶ [0053].
[39] *See*, Final Office Action, p. 8.
[40] *See In re Oetiker*, 977 F.2d 1443, 1445 (Fed. Cir. 1992) ("[T]he examiner bears the initial burden, on review of the prior art or on any other ground, of presenting a *prima facie* case of unpatentability.").
[41] *See* MPEP § 2141.02(I).

underpinning to support the legal conclusion of obviousness."[42] Appellants submit that the Examiner has failed to meet these requirements and request that the rejection be reversed.

As noted above, the claimed capture system requires, among other things:

- collecting information about two or more organizations that have computer systems, network resources, and employees, the organizations posing risks through business relationships of the organizations with other parties, the information collected about the organizations being indicative of compromises, vulnerabilities or configurations of technology systems of the organizations, and indicative of resiliencies of the organizations to recover from such compromises, or vulnerabilities or configurations;
- processing by computer the information from the two or more sources for each of the organizations to form a composite rating of the organization that is indicative of a degree of risk to the organization or to a party through a business relationship with the organization, the composite rating comprising a calculated composite of metrics and data derived or collected from the sources, the processing comprising applying transformations to the data and metrics, and the processing comprising applying weights to the data and the metrics; and
- the metrics including a measure of the extent of, the frequency of, or duration of compromise of the technology systems of the organization, or of a configuration or vulnerability of the organization, and a measure of the resilience of the organization to recover from such vulnerability, the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability.

Appellants submit that these features are not disclosed in the applied references.

[42] *KSR v. Teleflex, Inc.*, 550 U.S. 398, 418 (2007) (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)) (emphasis added).

The Examiner appears to rely on Newton for teaching certain elements of the claimed ratings system in claim 1 but then acknowledges that Newton does not teach or disclose:

> "the composite rating comprising a calculated composite of metrics and data derived or collected from the sources, the processing comprising applying transformations to the data and metrics, and the processing comprising applying weights to the data and the metrics, the metrics including a measure of the extent of the frequency of, or the duration of compromise of the technology systems of the organization, or of a configuration or vulnerability of the organization, and a measure of the resilience of the organization to recover from such vulnerability, the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability"

and attempts to remedy this admitted shortcoming by citing to Shull.[43] The Examiner then suggests that Shull "teaches creating a score for an entity from multiple sources which is similar to a credit score which informs requester of the trust of the entity, this score is received by the requester where activities are accounted for both legitimate (i.e. positive) and illegitimate (i.e. negative)" and also "teaches giving an overall trust score between 1 and 5 i.e. a normalized composite score where 1 is a reputable business and 5 is likely engaged in illicit activity.)".[44] Nowhere does the Examiner provide any evidence, either expressly or inherently, that cures the admitted inadequacies of Newton. In fact, Newton provides a list of exemplary properties that it *does* consider – seventeen to be exact – and the claimed resiliency is unsurprisingly absent.[45] As such, Appellants fail to see how either Newton or Shull address the claimed resiliency as claimed and as such disagree with the Examiner's rejection.

In addressing Appellants' arguments, the Examiner suggests that the claimed resilience is somehow inherent in the ratings described by Newton and/or Shull.

---

[43] *See* Final Office action, p. 7.
[44] *See* Final Office action, p. 7.
[45] *See*, Newton ¶¶ [0013] – [0029].

Specifically, the Examiner notes "a reputation/rating is indicative on how trust worthy a network is and the information gathered would be indicative on the resilience a network would likely be due to a compromise as a larger organization with more resources that has existed longer is more likely to be resilient than a smaller organization with less resources and age."[46] In making this statement, the Examiner appears to be relying on hindsight to connect the dots from the network properties considered by Newton and Applicants' resiliency metric, however, impermissible hindsight must be avoided and the legal conclusion must be reached on the basis of the facts gleaned from the prior art.[47] Even if, arguendo, the Examiner is suggesting that the claimed resiliency is somehow inherently implied by Newton's network properties, it is well settled that inherency may not be established by probabilities or possibilities. In order to make a proper rejection based on inherency, the Office "must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic necessarily flows from the teachings of the applied prior art."[48] In applying this standard, the Board has previously required that the Office provide "cogent technical reasoning and/or objective evidence" to support its rejection.[49] The Federal Circuit has further stated that "[t]o establish inherency, the extrinsic evidence must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill."[50] "Inherency … may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient."[51]

The Office bears the initial burden or presenting a *prima facie* case of unpatentability.[52] For a rejection based on inherency, this includes the burden to show

---

[46] *See* Final Office action, p. 3.
[47] *See* MPEP § 2142.
[48] *See* MPEP § 2112(IV), underlining added.
[49] *See Ex Parte Levy*, 17 U.S.P.Q. 2d 1461, 1464 (Bd. Pat. App. & Inter. 1990) (underlining added) (citing, *inter alia*, *In re King*, 801 F.2d 1324, 231 (Fed. Cir. 1986); *W.L. Gore & Assocs., Inc. v. Garlock, Inc.*, 721 F.2d 1540 (Fed. Cir. 1983); *In re Oelrich*, 666 F.2d 578 (CCPA 1981)).
[50] *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999) (quoting *Continental Can Co. v. Monsanto Co.*, 948 F.2d 1264, 1268 (Fed. Cir. 1991)).
[51] *In re Oelrich*, 666 F.2d at 581.
[52] *In re Oetiker*, 977 F.2d at 1445.

that the above standard is satisfied.[53] Only after a *prima facie* case has been established, does the burden shift to the applicant to rebut the finding of inherency.[54]

Under the above standard, the Office has failed to carry its burden to establish a *prima facie* case of unpatentability based on inherency. In particular, the Office fails to provide any basis in fact and/or technical reasoning why the purportedly inherent features of Appellants' claimed rating methods necessarily flow from the teachings of Newton or Shull. Further, the Office presents no evidence that makes clear that the purportedly inherent features are not mere probabilities or possibilities, but necessarily present in the teachings of Newton or Shull, and that such features would be recognized as being present by persons skilled in the art.

Appellants' discovery that the claimed "resiliency" is in fact a critical metric to consider when deriving a rating for an organization is best realized through an example. Consider a first entity such as a high-profile government agency or technology company that is routinely targeted by cyber-criminals. Such an entity might experience dozens, if not hundreds of such attacks on a daily basis. However, due to its sophistication and experience, the *impact* of these events may be (but is not necessarily) minimal because the duration of each is so short – that is the entity may have teams of people and complex systems in place to quickly recognize, counter and recover from these attacks. Such an entity may therefore receive a good rating using Appellants' approach, regardless of its consistent targeting.

Conversely, a retail store or state agency may rarely be targeted, but, due to its relative lack of sophistication an attack may last much longer before it is recognized and remedied, resulting in serious ramifications such as customer data breaches, financial loss, and fraud. Such an entity may receive a poor rating using Appellants' methods due specifically to its lack of ability to recover from an attack. Such considerations, and therefore any means for addressing how to incorporate an entity's resiliency are completely absent from the teachings of both Newton and Shull.

---

[53] *In re Mousa*, 479 Fed. Appx. 348 (Fed. Cir. 2012) ("Examiner has the burden of providing reasonable proof that a claim limitation is an inherent characteristic of the prior art.").
[54] *In re Oetiker*, 977 F.2d at 1445; *see also In re Schreiber*, 128 F.3d 1473, 1478 (Fed. Cir. 1997) (holding that the burden of proof shifted to the inventor to rebut the finding of inherency only after the Examiner established a *prima facie* case).

In view of the foregoing, Appellants submit that Newton, in light of Shull, fails to teach or suggest the claimed subject matter, when taken as a whole, as is required for a rejection under 35 U.S.C. § 103(a). Accordingly, no *prima facie* case of obviousness has been established, and the rejection of independent claim 1, and all claims depending therefrom, should be reversed for at least the reasons set forth above.

(ii) Claims 136, 138 and 139

Appellants submit that the rejection of claim 136 should be reversed for at least the same reasons that the rejection of claim 1 should be reversed.

Claim 136 recites, in relevant part:

- collecting, from at least two sources, information about two or more organizations, the collected information representing at least two data types, the collected information comprising outcomes of each of the organizations, and
- processing the information from both of the two sources for each of the organizations to form a composite rating of a security vulnerability of the organization and of a resilience of the organization to recover from a security breach, the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability, or both, the processing including applying models that account for differences in the respective sources.

In rejecting claim 136, the Examiner made no reference to, and did not cite any specific language from either Newton or Shull regarding an organization's resiliency, and certainly did not identify any teachings in either reference of a resiliency that is "inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability" as claimed.

Therefore, Appellants submit that Newton and Shull, whether taken individually or together, fail to teach or suggest the claimed subject matter, as is required for a rejection under 35 U.S.C. § 103(a). Accordingly, no *prima facie* case of obviousness has been established, and the rejection of claim 136 and each claim that depends

therefrom should be reversed for the same reasons why the rejection of claim 1 should be reversed.

(iii) Claim 141

Appellants submit that the rejection of claim 141 should be reversed for at least the same reasons that the rejection of claim 1 should be reversed.

Claim 141 recites, in relevant part:

- collecting information about an organization that has computer systems, network resources, and employees, the organization posing risks to itself or to other parties through business relationships of the organization with the other parties,
- the information collected about the organization including … information indicative of resiliencies of the organization to recover from a security breach associated with a compromise or a vulnerability, the resiliencies being inversely proportional to one or more of the duration of detected malicious activity and the duration of the compromise or vulnerability, and
- processing the information by computer to form a composite rating of the organization that is indicative of a degree of risk based on a business relationship with the organization, the composite comprising a measure of the resiliencies of the organization to recover from a security breach, and
- in connection with assessing the degree of risk, delivering a report of the composite rating of the organization through a reporting facility to enable a user of the reporting facility to assess the risks, based at least in part on the resiliencies.

Regarding the claimed “resiliency” metric, the Examiner suggests “Newton, teaches establishing a reputation for a network, and a reputation/rating is indicative on how trust worthy a network is and the information gathered would be indicative on the resilience a network would likely be due to a compromise as a larger organization with more resources that has existed longer is more likely to be resilient than a smaller

organization with less resources and age."[55] Such a statement not only requires a significant leap of faith, it is unsupported by any fact.

As noted above with regard to claims 1 and 136, the Examiner impermissibly relies on hindsight – only making the connection between the network parameters listed by Newton and the claimed resiliency *after* he has read Appellants' claims. Moreover, the Examiner's suggestion that a larger organization that has existed longer is somehow, by default, more resilient than a smaller organization with less resources relies on probabilities – a classic example of a logical fallacy where a statement is assumed to be true because it might be the case. Certainly there are numerous examples of large, long-standing organizations that have suffered significant and extended security breaches (e.g., Yahoo, Equifax, TJX Companies, etc.) – which using Appellants' techniques might rate poorly, while many smaller, new organizations have been able to identify and recover from potential breaches quickly, resulting in a better risk profile.

Appellants submit that Newton and Shull, either alone or in combination, fail to teach or suggest the claimed invention, when taken as a whole, as is required for a rejection under 35 U.S.C. § 103(a). Accordingly, no *prima facie* case of obviousness has been established, and the rejection of claim 141 should be reversed.

[55] *See,* Final Office action, pp. 18-19.

CONCLUSION

For the foregoing reasons, Appellants respectfully request that all the rejections of claims 1, 4, 5, 7-14, 16, 121, 122, 124, 126-132, and 134-141 be reversed.

Dated: December 21, 2017

Respectfully submitted,

Electronic signature: /Joel E. Lehrer/
Joel E. Lehrer
Registration No.: 56,401
GOODWIN PROCTER LLP
100 Northern Avenue
Boston, MA 02210
(617) 570-1836
Attorney for Appellants
Customer No. 051414

V. CLAIMS APPENDIX

1. A method comprising:

collecting information about two or more organizations that have computer systems, network resources, and employees, the organizations posing risks through business relationships of the organizations with other parties, the information collected about the organizations being indicative of compromises, vulnerabilities or configurations of technology systems of the organizations and indicative of resiliencies of the organizations to recover from such compromises, vulnerabilities or configurations, the information indicative of durations of events associated with compromises or vulnerabilities or configurations,

at least some of the information about each of the organizations being collected automatically by computer using sensors on the Internet,

the information about each of the organizations being collected from two or more sources, one or more of the sources not being controlled by the organization, the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization,

at least partly automatically gathering information about assets that each of the organizations owns, controls, uses, or is affiliated with, including IP addresses and IP network address ranges, computer services residing within address ranges, or domain names,

at least one of the sources for each of the organizations comprising a public source or a commercial source,

processing by computer the information from the two or more sources for each of the organizations to form a composite rating of the organization that is indicative of a degree of risk to the organization or to a party through a business relationship with the organization, the composite rating comprising a calculated composite of metrics and data derived or collected from the sources, the processing comprising applying transformations to the data and metrics, and the processing comprising applying weights to the data and the metrics,

the metrics including a measure of the extent of, the frequency of, or duration of compromise of the technology systems of the organization, or of a configuration or vulnerability of the organization, and a measure of the resilience of the organization to recover from such vulnerability, the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability, and

in connection with assessing a business risk to the organization or to a party through a business relationship with at least one of the organizations, delivering reports of the composite ratings of the organizations through a reporting facility to enable users of the reporting facility to monitor, assess, and mitigate the risks, based on the security vulnerabilities and resiliencies, in doing business with the organization and to compare the composite ratings of the organizations.

4. The method of claim 1, wherein the collected information is represented by at least two data types.

5. The method of claim 4, wherein the at least two data types include at least one of breach disclosures, block lists, configuration parameters, an identification of malware servers, an identification of a reputation, an identification of suspicious activity, an identification of spyware, white lists, an identification of compromised hosts, an identification of malicious activity, an identification of spam activity, an identification of vulnerable hosts, an identification of phishing activity, or an identification of e-mail viruses.

7. The method of claim 1, wherein the collected information evidences internal security controls.

8. The method of claim 1, wherein the collected information comprises outcomes of each of the organizations.

9. The method of claim 1, wherein the collected information evidences operational execution of security measures of each of the organizations.

10. The method of claim 1, wherein the collected information indicates whether a computer system of each of the organizations served malicious code to another system.

11. The method of claim 1, wherein the collected information indicates whether a computer system of each of the organizations communicated with a known attacker controlled network or sensor outside the control or network of the organization.

12. The method of claim 1, comprising: forming a series of the security ratings of each of the organizations.

13. The method of claim 12, comprising: determining a trend from the series of ratings.

14. The method of claim 12, comprising displaying the series of composite ratings.

16. The method of claim 14, wherein displaying the series of composite ratings for each of the organizations comprises posting the series of composite ratings for the organization to a web portal.

121. The method of claim 1, wherein the collected information represents externally observable outcome information.

124. The method of claim 1, comprising: determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information.

126. The method of claim 1, wherein: the collected information comprises at least two security characterizations of a computer system of each of the organizations.

127. The method of claim 1, wherein the collected information comprises a characterization of behavior of an employee of at least one of the organizations.

128. The method of claim 1, wherein the collected information comprises characterizations other than characterizations about a computer system of at least one of the organizations.

129. The method of claim 1, wherein the collected information comprises characterizations about policies of at least one of the organizations.

130. The method of claim 1, wherein the collected information comprises characterizations about information technology assets that at least one of the organizations owns, controls, uses, or is affiliated with.

131. The method of claim 1 in which collected information represents: (a) physical states, (b) technical states, (c) organizational states, or (d) cultural states of at least one of the organizations which can be exploited to create a security breach; or (e) the organization's ability to recover from a security breach; or any combination of two or more of these.

132. The method of claim 1 in which processing the information to form a composite rating comprises correlating data across the sources of information.

134. The method of claim 1 in which processing the information to form a composite rating comprises statistically correlating the composite rating with actual outcomes.

135. The method of claim 1 in which the vulnerability comprises physical, technical, organizational, or cultural states that can be exploited to create a security breach.

136. A method comprising

collecting, from at least two sources, information about two or more organizations, the collected information representing at least two data types, the collected information comprising outcomes of each of the organizations,

at least some of the information for each of the organizations being collected automatically by computer from at least two sources, one or more of the sources not controlled by the organization,

the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization, at least one of the sources including a commercial data source,

processing the information from both of the two sources for each of the organizations to form a composite rating of a security vulnerability of the organization and of a resilience of the organization to recover from a security breach, the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability, or both, the processing including applying models that account for differences in the respective sources,

normalizing the composite rating of each of the organizations based on a size characteristic of the organization to enable comparisons of composite ratings between the two or more organizations,

forming a series of the security ratings of each of the organizations, determining a trend from the series of ratings, and displaying the series of composite ratings through a portal,

determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information, and

reporting the composite ratings of the organizations through a portal to enable customers to monitor, assess, and mitigate risk in doing business with the organizations and to compare the composite ratings across the organizations.

137. The system of claim 1, determining a confidence range of the composite rating, the size of the range varying inversely with the level of confidence in the composite rating.

138. The system of claim 137, wherein the confidence range is based on redundancy of the security characterizations.

139. The system of claim 137, wherein the confidence range is based on a size of the third party computer system.

140. The method of claim 1 comprising ranking the organization and other organizations within sectors or peer-groups or globally.

141. A method comprising:

collecting information about an organization that has computer systems, network resources, and employees, the organization posing risks to itself or to other parties through business relationships of the organization with the other parties,

the information collected about the organization including (a) information collected automatically by computer on the Internet without permission of the organization, and (b) information indicative of resiliencies of the organization to recover from a security breach associated with a compromise or a vulnerability, the resiliencies being inversely proportional to one or more of the duration of detected malicious activity and the duration of the compromise or vulnerability,

processing the information by computer to form a composite rating of the organization that is indicative of a degree of risk based on a business relationship with the organization, the composite rating comprising a measure of the resiliencies of the organization to recover from a security breach, and in connection with assessing the degree of risk, delivering a report of the composite rating of the organization through a reporting facility to enable a user of the reporting facility to assess the risks, based at least in part on the resiliencies.

Electronic Acknowledgement Receipt

EFS ID:	31300573
Application Number:	13240572
International Application Number:	
Confirmation Number:	2423
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Customer Number:	51414
Filer:	Joel E. Lehrer/Susan Cannon
Filer Authorized By:	Joel E. Lehrer
Attorney Docket Number:	BST-004
Receipt Date:	21-DEC-2017
Filing Date:	22-SEP-2011
Time Stamp:	15:39:48
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Appeal Brief Filed	BST-004_Supp_AppealBrief.pdf	118133 28dd904319ff72f1a206ff75c39d81d05d24f66f	no	20

Warnings:

Information:	
Total Files Size (in bytes):	118133

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

51414 e 2017-12-01
GOODWIN PROCTER LLP
PATENT ADMINISTRATOR
100 Northern Avenue
BOSTON,MA 02210

Paper No. 20171120

Application No.:	13/240,572	**Date Mailed:**	2017-12-01 ELECTRONIC
First Named Inventor:	Stephen Wayne Boyer	Examiner:	KANAAN, SIMON P
Attorney Docket No.:	BST-004	Art Unit:	2492
Confirmation No.:	2423	Filing Date:	09/22/2011

Please find attached an Office communication concerning this application or proceeding.

Commissioner for Patents

PTO-90c (Rev.08-06)

Notification of Non-Compliant Appeal Brief (37 CFR 41.37)	Application No. 13/240,572	Applicant(s) Boyer et al.	
	Examiner KANAAN, SIMON P	Art Unit 2492	AIA Status No

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

The Appeal Brief filed on 02 November 2017 is defective for failure to comply with one or more provisions of 37 CFR 41.37(c).

To avoid dismissal of the appeal, applicant must file an amended brief or other appropriate correction (see MPEP 1205.03) within **ONE MONTH or THIRTY DAYS** from the mailing date of this Notification, whichever is longer. **EXTENSIONS OF THIS TIME PERIOD MAY BE GRANTED UNDER 37 CFR 1.136.**

1. ☐ The brief does not contain the items required under 37 CFR 41.37(c), or the items are not under the proper heading or in the proper order.

2. ☑ (a) The brief does not contain a concise explanation of the subject matter defined in each of the rejected independent claims, referring to the specification in the Record by page and line number or by paragraph number and to the drawings, if any, by reference characters; and/or (b) the brief fails to identify, for each rejected independent claim and for each dependent claim argued separately that contains a means plus function or step plus function recitation under 35 U.S.C. 112, sixth paragraph, the structure, material, or acts described in the specification as corresponding to each claimed function with reference to the specification in the Record by page and line number or paragraph number, and to the drawings, if any, by reference characters (37 CFR 41.37(c)(1)(iii)).

3. ☐ The brief does not contain a correct copy of the appealed claims as an appendix thereto (37 CFR 41.37(c)(1)(v)).

4. ☐ Other (including any explanation in support of the above items):

The Summary of Claimed Subject Matter is deficient as it maps the claims to the specification by paragraph numbers and page and line numbers were used in the original specification.

The entire Appeal Brief is not necessary only the corrected section(s)..

/LORENDA M HOOD/ 571-272-1751

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Stephan Wayne Boyer *et al.*

Application No.: 13/240,572 Confirmation No.: 2423

Filed: September 22, 2011 Art Unit: 2492

For: INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM Examiner: Kanaan, Simon P.

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

This Appeal Brief is responsive to the non-final Office action of February 13, 2017 (the "Office action"), and is being submitted pursuant to the Notice of Appeal filed April 12, 2017. A petition for a four-month extension of time for filing this Appeal Brief, to November 22, 2017, is being submitted herewith.

Appellants believe that no other fees are due in connection with this submission. However, please consider this a conditional authorization to charge any fees necessary for entry of these papers to our Deposit Account No. 07-1700, under Order No. BST-004.

I. REAL PARTY IN INTEREST

The real party in interest is BitSight Technologies Inc., the named Applicants and assignees of record of the present patent application, as indicated in the assignment recorded at Reel/Frame 027658/0906 of the USPTO's assignment records.

II. RELATED APPEALS, INTERFERENCES, AND TRIALS

There are no related appeals, interferences, or trials to report.

III. SUMMARY OF CLAIMED SUBJECT MATTER

Claims 1, 136 and 141 are the only independent claims, and each is directed to a method for assessing the risks associated with doing business with a particular entity based, at least in part, on a composite security rating.[1]

With regard to claim 1, information is collected about two or more organizations that have computer systems, network resources, and employees that, due to business relationships of the organizations with other parties, pose risks to the organization.[2] The information collected about the organizations is indicative of compromises, vulnerabilities or configurations of technology systems of the organizations, and of resiliencies of the organizations to recover from such compromises, vulnerabilities or configurations.[3] The information is also indicative of durations of events associated with compromises or vulnerabilities or configurations.[4] Some of the information is collected automatically by computers using sensors on the Internet.[5] The information about the organizations is collected from two or more sources, one or more of which is not controlled by the organization and collected without permission of the organization.[6] Information is gathered about assets that each of the organizations owns, controls, uses, or is affiliated with, including IP addresses and IP network address ranges, computer services residing within address ranges, or domain names.[7] At least one of the sources of such information is a public or commercial source.[8] The information is

---

[1] *See, e.g.*, Specification, ¶ [0007].
[2] *See, e.g.*, Specification, ¶¶ [0044], [0047], [0057].
[3] *See, e.g.*, Specification, ¶¶ [0015], [0060], [0077].
[4] *See, e.g.*, Specification, ¶¶ [0015], [0078].
[5] *See, e.g.*, Specification, ¶ [0061], Figure 2.
[6] *See, e.g.*, Specification, ¶¶ [0008], [0045], [0057].
[7] *See, e.g.*, Specification, ¶ [0044].
[8] *See, e.g.*, Specification, ¶¶ [0008], [0127].

processed to form a composite rating of the organization that is indicative of a degree of risk to the organization or to a party through a business relationship with the organization.[9] The composite rating comprises a calculated composite of metrics and data derived or collected from the sources.[10] The processing includes applying transformations and weights to the data and metrics.[11] The metrics include a measure of the extent of, the frequency of, or duration of compromise of the technology systems of the organization, or of a configuration or vulnerability of the organization, and a measure of the resilience of the organization to recover from such vulnerability, where the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability.[12] In connection with assessing a business risk to the organization through a business relationship with at least one of the organizations, reports of the composite ratings of the organizations are provided through a reporting facility to enable users of the reporting facility to monitor, assess, and mitigate the risks, based on the security vulnerabilities and resiliencies, in doing business with the organization and to compare the composite ratings of the organizations.[13]

With regard to claim 136, information about two or more organizations is collected from at least two sources.[14] The information represents at least two data types and comprising outcomes of each of the organizations.[15] At least some of the information for each of the organizations is collected automatically by computer from at least two sources.[16] One or more of the sources is not controlled by the organization (i.e., a commercial data source), and the information from at the sources that are not controlled by the organization is collected without permission of the organization.[17] The information from the two sources is processed for each of the organizations to form a composite rating of a security vulnerability of the organization and of a resilience of the

[9] *See, e.g.*, Specification, ¶¶ [0021], [0022], [0077].
[10] *See, e.g.*, Specification, ¶¶ [0016], [0021], [0122].
[11] *See, e.g.*, Specification, ¶ [0124].
[12] *See, e.g.*, Specification, ¶¶ [0015], [0077], [0078].
[13] *See, e.g.*, Specification, ¶¶ [0042], [0057], [0139], [0143].
[14] *See, e.g.*, Specification, ¶¶ [0044], [0047], [0057].
[15] *See, e.g.*, Specification, ¶ [0009].
[16] *See, e.g.*, Specification, ¶¶ [0008], [0045], [0057], [0061].
[17] *See, e.g.*, Specification, ¶¶ [0008], [0045], [0057].

organization to recover from a security breach.[18] The resilience is inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability, or both.[19] The processing includes applying models that account for differences in the respective sources.[20] The composite rating of each of the organizations is normalized based on a size characteristic of the organization to enable comparisons of composite ratings between the two or more organizations.[21] A series of security ratings is formed for each of the organizations[22]. A trend is determined from the series of ratings and displayed through a portal.[23] A badness score is determined that corresponds to an intensity or duration of malicious activity determined from the collected information.[24] The composite ratings of the organizations are displayed through a portal to enable customers to monitor, assess, and mitigate risk in doing business with the organizations and to compare the composite ratings across the organizations.[25]

With regard to claim 141, information is collected about an organization that has computer systems, network resources, and employees.[26] Through business relationships of the organization with the other parties, the organization poses risks to itself or to other parties.[27] The information collected about the organization includes information collected automatically by computer on the Internet without permission of the organization.[28] The information collected also includes information indicative of resiliencies of the organization to recover from a security breach associated with a compromise or a vulnerability.[29] The resiliencies are inversely proportional to one or more of the duration of detected malicious activity and the duration of the compromise or vulnerability.[30] The information is processed by a computer to form a composite rating of the organization that is indicative of a degree of risk based on a business

---

[18] *See, e.g.*, Specification, ¶¶ [0015], [0077], [0078].
[19] *See, e.g.*, Specification, ¶¶ [0015], [0077], [0078].
[20] *See, e.g.*, Specification, ¶ [0052].
[21] *See, e.g.*, Specification, ¶¶ [0021], [0024], [0096].
[22] *See, e.g.*, Specification, ¶¶ [0011], [0110].
[23] *See, e.g.*, Specification, ¶¶ [0011], [0110].
[24] *See, e.g.*, Specification, ¶ [0080].
[25] *See, e.g.*, Specification, ¶ [0057].
[26] *See, e.g.*, Specification, ¶¶ [0044], [0047], [0057].
[27] *See, e.g.*, Specification, ¶¶ [0044], [0047], [0057].
[28] *See, e.g.*, Specification, ¶¶ [0008], [0045], [0057]
[29] *See, e.g.*, Specification, ¶¶ [0015], [0077], [0078].
[30] *See, e.g.*, Specification, ¶¶ [0015], [0077], [0078].

relationship with the organization.[31] The composite rating comprises a measure of the resiliencies of the organization to recover from a security breach.[32] In connection with assessing the degree of risk, a report of the composite rating of the organization is delivered through a reporting facility to enable a user of the reporting facility to assess the risks, based at least in part on the resiliencies.[33]

IV. ARGUMENT

Appellants' technique for assessing the potential security risks of engaging with a particular organization of independent claims 1, 136 and 141 each require at least one feature that distinguishes their methods from other cyber-security rating techniques in the prior art. Specifically, each claim recites using "resiliencies of the organization to recover from a security breach associated with a compromise or a vulnerability" where that resiliency is "inversely proportional to one or more of the duration of detected malicious activity and the duration of the compromise or vulnerability" as an input into a security rating.[34]

In the Office action, the Examiner simply refers to these features without any clear indication of how any particular prior art reference teaches or suggests these limitations. In fact, the Examiner first expressly admits that Newton fails to disclose such capabilities, instead suggesting that Shull teaches this approach, but the Examiner does not point to any specific language in Shull – because no such language exists, and in fact the limitation is completely ignored in the discussion of Shull.[35] In an attempt to cure this deficiency, the Examiner returns to Newton, and claims that the measuring of resilience of a network is inherent in any rating.

A. The rejection of claims 1, 4, 5, 7-14, 16, 121, 122, 124, 126-132 and 134-141 under pre-AIA 35 U.S.C. § 103(a) as unpatentable over Newton in view of Shull is improper and should be reversed.

The Examiner's rejection on pages 4-19 of the Office action, alleging that claims 1, 4, 5, 7-14, 16, 121, 122, 124, 126-132 and 134-141 are unpatentable under pre-AIA 35 U.S.C. § 103(a) over U.S. Patent Publication No. 2004/0250122 to Newton

[31] *See, e.g.*, Specification, ¶¶ [0033], [0034], [0134].
[32] *See, e.g.*, Specification, ¶¶ [0077], [0078].
[33] *See, e.g.*, Specification, ¶ [0057].
[34] *See, e.g.*, Specification, ¶¶ [0015], [0077], [0078].
[35] *S*ee, Final Office Action, p. 7.

("Newton") in view of U.S. Patent Publication No. 2006/0212925 to Shull et al. ("Shull"), is improper and should be reversed.

Newton appears to discuss systems and methods for establishing reputations among networks.[36] More specifically, Newton describes examples of information agents that may be used to "gather information [about networks] from a number of sources."[37] Separately, a set of high level policies are applied against the gathered information to create specific rules sets, which in turn determine whether traffic from certain sites will be permitted.[38] Newton's system simply provides a means for turning policies into rule sets that can be executed by network agents – Newton does not, however, provide specific metrics used, and certainly does not contemplate that "durations of events associated with compromises or vulnerabilities or configurations" are used to influence the policies, let alone contribute to a rating.

Shull generally describes methods for implementing trust policies among entities based on a trust score. Again, like Newton, nowhere does Shull contemplate that "durations of events associated with compromises or vulnerabilities or configurations" should be used as a component of his trust score – and in fact, the Examiner simply cites to Shull's score calculations based on general entity size and a rating from 1-5.[39]

(i) Claims 1, 4, 5, 7-14, 16, 121, 124, 126-132, 134, 135, 138, 139 and 140

Appellants submit that the Examiner when relying on the teachings of Newton in view of Shull, has failed to establish a *prima facie* case of obviousness.[40] A *prima facie* case of obviousness under 35 U.S.C. § 103(a) requires, among other things, a showing that the applied references, either alone or in combination, teach or suggest each and every element of the claimed invention, when taken as a whole.[41] Moreover, "[r]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational

[36] *See*, Newton ¶ [0030].
[37] *See*, Newton ¶¶ [0043] – [0048].
[38] *See*, Newton ¶ [0053].
[39] *See*, Final Office Action, p. 8.
[40] *See In re Oetiker*, 977 F.2d 1443, 1445 (Fed. Cir. 1992) ("[T]he examiner bears the initial burden, on review of the prior art or on any other ground, of presenting a *prima facie* case of unpatentability.").
[41] *See* MPEP § 2141.02(I).

underpinning to support the legal conclusion of obviousness."[42] Appellants submit that the Examiner has failed to meet these requirements and request that the rejection be reversed.

As noted above, the claimed capture system requires, among other things:

- collecting information about two or more organizations that have computer systems, network resources, and employees, the organizations posing risks through business relationships of the organizations with other parties, the information collected about the organizations being indicative of compromises, vulnerabilities or configurations of technology systems of the organizations, and indicative of resiliencies of the organizations to recover from such compromises, or vulnerabilities or configurations;
- processing by computer the information from the two or more sources for each of the organizations to form a composite rating of the organization that is indicative of a degree of risk to the organization or to a party through a business relationship with the organization, the composite rating comprising a calculated composite of metrics and data derived or collected from the sources, the processing comprising applying transformations to the data and metrics, and the processing comprising applying weights to the data and the metrics; and
- the metrics including a measure of the extent of, the frequency of, or duration of compromise of the technology systems of the organization, or of a configuration or vulnerability of the organization, and a measure of the resilience of the organization to recover from such vulnerability, the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability.

Appellants submit that these features are not disclosed in the applied references.

[42] *KSR v. Teleflex, Inc.*, 550 U.S. 398, 418 (2007) (quoting *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)) (emphasis added).

The Examiner appears to rely on Newton for teaching certain elements of the claimed ratings system in claim 1 but then acknowledges that Newton does not teach or disclose:

> "the composite rating comprising a calculated composite of metrics and data derived or collected from the sources, the processing comprising applying transformations to the data and metrics, and the processing comprising applying weights to the data and the metrics, the metrics including a measure of the extent of the frequency of, or the duration of compromise of the technology systems of the organization, or of a configuration or vulnerability of the organization, and a measure of the resilience of the organization to recover from such vulnerability, the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability"

and attempts to remedy this admitted shortcoming by citing to Shull.[43] The Examiner then suggests that Shull "teaches creating a score for an entity from multiple sources which is similar to a credit score which informs requester of the trust of the entity, this score is received by the requester where activities are accounted for both legitimate (i.e. positive) and illegitimate (i.e. negative)" and also "teaches giving an overall trust score between 1 and 5 i.e. a normalized composite score where 1 is a reputable business and 5 is likely engaged in illicit activity.)".[44] Nowhere does the Examiner provide any evidence, either expressly or inherently, that cures the admitted inadequacies of Newton. In fact, Newton provides a list of exemplary properties that it *does* consider – seventeen to be exact – and the claimed resiliency is unsurprisingly absent.[45] As such, Appellants fail to see how either Newton or Shull address the claimed resiliency as claimed and as such disagree with the Examiner's rejection.

In addressing Appellants' arguments, the Examiner suggests that the claimed resilience is somehow inherent in the ratings described by Newton and/or Shull.

---

[43] *See* Final Office action, p. 7.
[44] *See* Final Office action, p. 7.
[45] *See*, Newton ¶¶ [0013] – [0029].

Specifically, the Examiner notes "a reputation/rating is indicative on how trust worthy a network is and the information gathered would be indicative on the resilience a network would likely be due to a compromise as a larger organization with more resources that has existed longer is more likely to be resilient than a smaller organization with less resources and age."[46] In making this statement, the Examiner appears to be relying on hindsight to connect the dots from the network properties considered by Newton and Applicants' resiliency metric, however, impermissible hindsight must be avoided and the legal conclusion must be reached on the basis of the facts gleaned from the prior art.[47] Even if, arguendo, the Examiner is suggesting that the claimed resiliency is somehow inherently implied by Newton's network properties, it is well settled that inherency may not be established by probabilities or possibilities. In order to make a proper rejection based on inherency, the Office "must provide a basis in fact and/or technical reasoning to reasonably support the determination that the allegedly inherent characteristic necessarily flows from the teachings of the applied prior art."[48] In applying this standard, the Board has previously required that the Office provide "cogent technical reasoning and/or objective evidence" to support its rejection.[49] The Federal Circuit has further stated that "[t]o establish inherency, the extrinsic evidence must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill."[50] "Inherency … may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient."[51]

The Office bears the initial burden or presenting a *prima facie* case of unpatentability.[52] For a rejection based on inherency, this includes the burden to show

---

[46] *See* Final Office action, p. 3.
[47] *See* MPEP § 2142.
[48] *See* MPEP § 2112(IV), underlining added.
[49] *See Ex Parte Levy*, 17 U.S.P.Q. 2d 1461, 1464 (Bd. Pat. App. & Inter. 1990) (underlining added) (citing, *inter alia*, *In re King*, 801 F.2d 1324, 231 (Fed. Cir. 1986); *W.L. Gore & Assocs., Inc. v. Garlock, Inc.*, 721 F.2d 1540 (Fed. Cir. 1983); *In re Oelrich*, 666 F.2d 578 (CCPA 1981)).
[50] *In re Robertson*, 169 F.3d 743, 745 (Fed. Cir. 1999) (quoting *Continental Can Co. v. Monsanto Co.*, 948 F.2d 1264, 1268 (Fed. Cir. 1991)).
[51] *In re Oelrich*, 666 F.2d at 581.
[52] *In re Oetiker*, 977 F.2d at 1445.

that the above standard is satisfied.[53] Only after a *prima facie* case has been established, does the burden shift to the applicant to rebut the finding of inherency.[54]

Under the above standard, the Office has failed to carry its burden to establish a *prima facie* case of unpatentability based on inherency. In particular, the Office fails to provide any basis in fact and/or technical reasoning why the purportedly inherent features of Appellants' claimed rating methods necessarily flow from the teachings of Newton or Shull. Further, the Office presents no evidence that makes clear that the purportedly inherent features are not mere probabilities or possibilities, but necessarily present in the teachings of Newton or Shull, and that such features would be recognized as being present by persons skilled in the art.

Appellants' discovery that the claimed "resiliency" is in fact a critical metric to consider when deriving a rating for an organization is best realized through an example. Consider a first entity such as a high-profile government agency or technology company that is routinely targeted by cyber-criminals. Such an entity might experience dozens, if not hundreds of such attacks on a daily basis. However, due to its sophistication and experience, the *impact* of these events may be (but is not necessarily) minimal because the duration of each is so short – that is the entity may have teams of people and complex systems in place to quickly recognize, counter and recover from these attacks. Such an entity may therefore receive a good rating using Appellants' approach, regardless of its consistent targeting.

Conversely, a retail store or state agency may rarely be targeted, but, due to its relative lack of sophistication an attack may last much longer before it is recognized and remedied, resulting in serious ramifications such as customer data breaches, financial loss, and fraud. Such an entity may receive a poor rating using Appellants' methods due specifically to its lack of ability to recover from an attack. Such considerations, and therefore any means for addressing how to incorporate an entity's resiliency are completely absent from the teachings of both Newton and Shull.

---

[53] *In re Mousa*, 479 Fed. Appx. 348 (Fed. Cir. 2012) ("Examiner has the burden of providing reasonable proof that a claim limitation is an inherent characteristic of the prior art.").
[54] *In re Oetiker*, 977 F.2d at 1445; *see also In re Schreiber*, 128 F.3d 1473, 1478 (Fed. Cir. 1997) (holding that the burden of proof shifted to the inventor to rebut the finding of inherency only after the Examiner established a *prima facie* case).

In view of the foregoing, Appellants submit that Newton, in light of Shull, fails to teach or suggest the claimed subject matter, when taken as a whole, as is required for a rejection under 35 U.S.C. § 103(a). Accordingly, no *prima facie* case of obviousness has been established, and the rejection of independent claim 1, and all claims depending therefrom, should be reversed for at least the reasons set forth above.

(ii) Claims 136, 138 and 139

Appellants submit that the rejection of claim 136 should be reversed for at least the same reasons that the rejection of claim 1 should be reversed.

Claim 136 recites, in relevant part:

- collecting, from at least two sources, information about two or more organizations, the collected information representing at least two data types, the collected information comprising outcomes of each of the organizations, and
- processing the information from both of the two sources for each of the organizations to form a composite rating of a security vulnerability of the organization and of a resilience of the organization to recover from a security breach, the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability, or both, the processing including applying models that account for differences in the respective sources.

In rejecting claim 136, the Examiner made no reference to, and did not cite any specific language from either Newton or Shull regarding an organization's resiliency, and certainly did not identify any teachings in either reference of a resiliency that is "inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability" as claimed.

Therefore, Appellants submit that Newton and Shull, whether taken individually or together, fail to teach or suggest the claimed subject matter, as is required for a rejection under 35 U.S.C. § 103(a). Accordingly, no *prima facie* case of obviousness has been established, and the rejection of claim 136 and each claim that depends

therefrom should be reversed for the same reasons why the rejection of claim 1 should be reversed.

(iii) Claim 141

Appellants submit that the rejection of claim 141 should be reversed for at least the same reasons that the rejection of claim 1 should be reversed.

Claim 141 recites, in relevant part:

- collecting information about an organization that has computer systems, network resources, and employees, the organization posing risks to itself or to other parties through business relationships of the organization with the other parties,
- the information collected about the organization including … information indicative of resiliencies of the organization to recover from a security breach associated with a compromise or a vulnerability, the resiliencies being inversely proportional to one or more of the duration of detected malicious activity and the duration of the compromise or vulnerability, and
- processing the information by computer to form a composite rating of the organization that is indicative of a degree of risk based on a business relationship with the organization, the composite comprising a measure of the resiliencies of the organization to recover from a security breach, and
- in connection with assessing the degree of risk, delivering a report of the composite rating of the organization through a reporting facility to enable a user of the reporting facility to assess the risks, based at least in part on the resiliencies.

Regarding the claimed “resiliency” metric, the Examiner suggests “Newton, teaches establishing a reputation for a network, and a reputation/rating is indicative on how trust worthy a network is and the information gathered would be indicative on the resilience a network would likely be due to a compromise as a larger organization with more resources that has existed longer is more likely to be resilient than a smaller

organization with less resources and age."[55] Such a statement not only requires a significant leap of faith, it is unsupported by any fact.

As noted above with regard to claims 1 and 136, the Examiner impermissibly relies on hindsight – only making the connection between the network parameters listed by Newton and the claimed resiliency *after* he has read Appellants' claims. Moreover, the Examiner's suggestion that a larger organization that has existed longer is somehow, by default, more resilient than a smaller organization with less resources relies on probabilities – a classic example of a logical fallacy where a statement is assumed to be true because it might be the case. Certainly there are numerous examples of large, long-standing organizations that have suffered significant and extended security breaches (e.g., Yahoo, Equifax, TJX Companies, etc.) – which using Appellants' techniques might rate poorly, while many smaller, new organizations have been able to identify and recover from potential breaches quickly, resulting in a better risk profile.

Appellants submit that Newton and Shull, either alone or in combination, fail to teach or suggest the claimed invention, when taken as a whole, as is required for a rejection under 35 U.S.C. § 103(a). Accordingly, no *prima facie* case of obviousness has been established, and the rejection of claim 141 should be reversed.

[55] *See,* Final Office action, pp. 18-19.

CONCLUSION

For the foregoing reasons, Appellants respectfully request that all the rejections of claims 1, 4, 5, 7-14, 16, 121, 122, 124, 126-132, and 134-141 be reversed.

Dated: November 2, 2017

Respectfully submitted,

Electronic signature: /Joel E. Lehrer/
Joel E. Lehrer
Registration No.: 56,401
GOODWIN PROCTER LLP
100 Northern Avenue
Boston, MA 02210
(617) 570-1836
Attorney for Appellants
Customer No. 051414

V. CLAIMS APPENDIX

1. A method comprising:

collecting information about two or more organizations that have computer systems, network resources, and employees, the organizations posing risks through business relationships of the organizations with other parties, the information collected about the organizations being indicative of compromises, vulnerabilities or configurations of technology systems of the organizations and indicative of resiliencies of the organizations to recover from such compromises, vulnerabilities or configurations, the information indicative of durations of events associated with compromises or vulnerabilities or configurations,

at least some of the information about each of the organizations being collected automatically by computer using sensors on the Internet,

the information about each of the organizations being collected from two or more sources, one or more of the sources not being controlled by the organization, the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization,

at least partly automatically gathering information about assets that each of the organizations owns, controls, uses, or is affiliated with, including IP addresses and IP network address ranges, computer services residing within address ranges, or domain names,

at least one of the sources for each of the organizations comprising a public source or a commercial source,

processing by computer the information from the two or more sources for each of the organizations to form a composite rating of the organization that is indicative of a degree of risk to the organization or to a party through a business relationship with the organization, the composite rating comprising a calculated composite of metrics and data derived or collected from the sources, the processing comprising applying transformations to the data and metrics, and the processing comprising applying weights to the data and the metrics,

the metrics including a measure of the extent of, the frequency of, or duration of compromise of the technology systems of the organization, or of a configuration or vulnerability of the organization, and a measure of the resilience of the organization to recover from such vulnerability, the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability, and

in connection with assessing a business risk to the organization or to a party through a business relationship with at least one of the organizations, delivering reports of the composite ratings of the organizations through a reporting facility to enable users of the reporting facility to monitor, assess, and mitigate the risks, based on the security vulnerabilities and resiliencies, in doing business with the organization and to compare the composite ratings of the organizations.

4. The method of claim 1, wherein the collected information is represented by at least two data types.

5. The method of claim 4, wherein the at least two data types include at least one of breach disclosures, block lists, configuration parameters, an identification of malware servers, an identification of a reputation, an identification of suspicious activity, an identification of spyware, white lists, an identification of compromised hosts, an identification of malicious activity, an identification of spam activity, an identification of vulnerable hosts, an identification of phishing activity, or an identification of e-mail viruses.

7. The method of claim 1, wherein the collected information evidences internal security controls.

8. The method of claim 1, wherein the collected information comprises outcomes of each of the organizations.

9. The method of claim 1, wherein the collected information evidences operational execution of security measures of each of the organizations.

10. The method of claim 1, wherein the collected information indicates whether a computer system of each of the organizations served malicious code to another system.

11. The method of claim 1, wherein the collected information indicates whether a computer system of each of the organizations communicated with a known attacker controlled network or sensor outside the control or network of the organization.

12. The method of claim 1, comprising: forming a series of the security ratings of each of the organizations.

13. The method of claim 12, comprising: determining a trend from the series of ratings.

14. The method of claim 12, comprising displaying the series of composite ratings.

16. The method of claim 14, wherein displaying the series of composite ratings for each of the organizations comprises posting the series of composite ratings for the organization to a web portal.

121. The method of claim 1, wherein the collected information represents externally observable outcome information.

124. The method of claim 1, comprising: determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information.

126. The method of claim 1, wherein: the collected information comprises at least two security characterizations of a computer system of each of the organizations.

127. The method of claim 1, wherein the collected information comprises a characterization of behavior of an employee of at least one of the organizations.

128. The method of claim 1, wherein the collected information comprises characterizations other than characterizations about a computer system of at least one of the organizations.

129. The method of claim 1, wherein the collected information comprises characterizations about policies of at least one of the organizations.

130. The method of claim 1, wherein the collected information comprises characterizations about information technology assets that at least one of the organizations owns, controls, uses, or is affiliated with.

131. The method of claim 1 in which collected information represents: (a) physical states, (b) technical states, (c) organizational states, or (d) cultural states of at least one of the organizations which can be exploited to create a security breach; or (e) the organization's ability to recover from a security breach; or any combination of two or more of these.

132. The method of claim 1 in which processing the information to form a composite rating comprises correlating data across the sources of information.

134. The method of claim 1 in which processing the information to form a composite rating comprises statistically correlating the composite rating with actual outcomes.

135. The method of claim 1 in which the vulnerability comprises physical, technical, organizational, or cultural states that can be exploited to create a security breach.

136. A method comprising

collecting, from at least two sources, information about two or more organizations, the collected information representing at least two data types, the collected information comprising outcomes of each of the organizations,

at least some of the information for each of the organizations being collected automatically by computer from at least two sources, one or more of the sources not controlled by the organization,

the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization, at least one of the sources including a commercial data source,

processing the information from both of the two sources for each of the organizations to form a composite rating of a security vulnerability of the organization and of a resilience of the organization to recover from a security breach, the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability, or both, the processing including applying models that account for differences in the respective sources,

normalizing the composite rating of each of the organizations based on a size characteristic of the organization to enable comparisons of composite ratings between the two or more organizations,

forming a series of the security ratings of each of the organizations, determining a trend from the series of ratings, and displaying the series of composite ratings through a portal,

determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information, and

reporting the composite ratings of the organizations through a portal to enable customers to monitor, assess, and mitigate risk in doing business with the organizations and to compare the composite ratings across the organizations.

137. The system of claim 1, determining a confidence range of the composite rating, the size of the range varying inversely with the level of confidence in the composite rating.

138. The system of claim 137, wherein the confidence range is based on redundancy of the security characterizations.

139. The system of claim 137, wherein the confidence range is based on a size of the third party computer system.

140. The method of claim 1 comprising ranking the organization and other organizations within sectors or peer-groups or globally.

141. A method comprising:

collecting information about an organization that has computer systems, network resources, and employees, the organization posing risks to itself or to other parties through business relationships of the organization with the other parties,

the information collected about the organization including (a) information collected automatically by computer on the Internet without permission of the organization, and (b) information indicative of resiliencies of the organization to recover from a security breach associated with a compromise or a vulnerability, the resiliencies being inversely proportional to one or more of the duration of detected malicious activity and the duration of the compromise or vulnerability,

processing the information by computer to form a composite rating of the organization that is indicative of a degree of risk based on a business relationship with the organization, the composite rating comprising a measure of the resiliencies of the organization to recover from a security breach, and in connection with assessing the degree of risk, delivering a report of the composite rating of the organization through a reporting facility to enable a user of the reporting facility to assess the risks, based at least in part on the resiliencies.

Electronic Patent Application Fee Transmittal

Application Number:	13240572
Filing Date:	22-Sep-2011
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Filer:	Joel E. Lehrer/Susan Cannon
Attorney Docket Number:	BST-004

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 4 months with $0 paid	2254	1	1100	1100
Miscellaneous:				
			Total in USD ($)	**1100**

Electronic Acknowledgement Receipt

EFS ID:	30838022
Application Number:	13240572
International Application Number:	
Confirmation Number:	2423
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Customer Number:	51414
Filer:	Joel E. Lehrer/Susan Cannon
Filer Authorized By:	Joel E. Lehrer
Attorney Docket Number:	BST-004
Receipt Date:	02-NOV-2017
Filing Date:	22-SEP-2011
Time Stamp:	16:17:05
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$1100
RAM confirmation Number	110317INTEFSW16184500
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Extension of Time	BST_004_EOT.pdf	22795 92b59a65854f24069c070b743ba54042d527f80b	no	1
Warnings:					
Information:					
2	Appeal Brief Filed	BST-004_Appeal_Brief.pdf	115599 606ad5b59cebd3bd479c23b463913b3d506b946a	no	20
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30281 de74fba422fc117c54d06fc65a144661ada0498d	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	168675		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/22 (03-13)
Approved for use through 07/31/2017. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)

Docket Number (Optional): BST-004

Application Number	13/240,572-Conf. #2423	Filed	September 22, 2011

For: INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM

Art Unit	2492	Examiner	S. P. Kanaan

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	Micro Entity Fee	
☐ One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☐ Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$
☐ Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$
☒ Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$ 1,100.00
☐ Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☒ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☒ Payment by credit card.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 07-1700 .

☒ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71. 37 CFR 3.73(b) statement is enclosed (Form PTO/SB/96).

☒ attorney or agent of record. Registration number 56,401 .

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____ .

/Joel E. Lehrer/	November 2, 2017
Signature	Date
Joel E. Lehrer	(617) 570-1057
Typed or printed name	Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☐ * Total of 1 forms are submitted.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/240,572	09/22/2011	Stephen Wayne Boyer	BST-004	2423

51414 7590 06/22/2017

GOODWIN PROCTER LLP
PATENT ADMINISTRATOR
100 Northern Avenue
BOSTON, MA 02210

EXAMINER	
KANAAN, SIMON P	

ART UNIT	PAPER NUMBER
2492	

NOTIFICATION DATE	DELIVERY MODE
06/22/2017	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATENTBOS@GOODWINPROCTER.COM
PSOUSA-ATWOOD@GOODWINPROCTER.COM
GLENN.WILLIAMS@GOODWINPROCTER.COM

Notice of Panel Decision from Pre-Appeal Brief Review	Application No. 13/240,572	Applicant(s) BOYER ET AL.
	Examiner SIMON KANAAN	Art Unit 2492

This is in response to the Pre-Appeal Brief Request for Review filed 12 April, 2017.

1. ☐ **Improper Request** – The Request is improper and a conference will not be held for the following reason(s):

☐ The Notice of Appeal has not been filed concurrent with the Pre-Appeal Brief Request.
☐ The request does not include reasons why a review is appropriate.
☐ A proposed amendment is included with the Pre-Appeal Brief request.
☐ Other: .

The time period for filing a response continues to run from the receipt date of the Notice of Appeal or from the mail date of the last Office communication, if no Notice of Appeal has been received.

2. ☒ **Proceed to Board of Patent Appeals and Interferences** – A Pre-Appeal Brief conference has been held. The application remains under appeal because there is at least one actual issue for appeal. Applicant is required to submit an appeal brief in accordance with 37 CFR 41.37. The time period for filing an appeal brief will be reset to be one month from mailing this decision, or the balance of the two-month time period running from the receipt of the notice of appeal, whichever is greater. Further, the time period for filing of the appeal brief is extendible under 37 CFR 1.136 based upon the mail date of this decision or the receipt date of the notice of appeal, as applicable.

☐ The panel has determined the status of the claim(s) is as follows:
Claim(s) allowed: _____.
Claim(s) objected to: _____.
Claim(s) rejected: *1,4-5,7-14, 16, 121, 124, 126-132, 134-141*.
Claim(s) withdrawn from consideration: _____.

3. ☐ **Allowable application** – A conference has been held. The rejection is withdrawn and a Notice of Allowance will be mailed. Prosecution on the merits remains closed. No further action is required by applicant at this time.

4. ☐ **Reopen Prosecution** – A conference has been held. The rejection is withdrawn and a new Office action will be mailed. No further action is required by applicant at this time.

All participants:

(1) *SIMON KANAAN*.	(3) *Saleh Najjar*.
(2) *Oleg Korsak*.	(4)_____.

/OLEG KORSAK/ Primary Examiner, Art Unit 2492	/SIMON KANAAN/ Examiner, Art Unit 2492	/SALEH NAJJAR/ Supervisory Patent Examiner, Art Unit 2492

Docket No.: BST-004
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Stephen Wayne Boyer, et al.

Application No.: 13/240,572 | Confirmation No.: 2423

Filed: September 22, 2011 | Art Unit: 2492

For: INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM | Examiner: Kanaan, Simon P.

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

COMMENTS ACCOMPANYING REQUEST FOR PRE-APPEAL BRIEF CONFERENCE

This paper is submitted along with a Pre-Appeal Brief Request for Review, in accordance with the Official Gazette Notice dated July 12, 2005 (the "Gazette Notice"), and a Notice of Appeal in response to the Office action transmitted by the U.S. Patent and Trademark Office on February 13, 2017. The fee for filing the Notice of Appeal is submitted herewith. Appellant believes that no additional fees are required, but if additional fees are necessary for entry of this paper, please charge any such fees to Deposit Account No. 07-1700, with reference to Attorney Docket No. BST-004.

Appellant's **Remarks** begin on page 2 of this paper.

REMARKS

The Examiner has improperly rejected pending claims 1, 4, 5, 7-14, 16, 121, 122, 124, 126-132, and 134-141 under 35 U.S.C. §103(a) as being unpatentable over U.S. Publication No. 2004/0250122 (hereinafter "Newton") in view of U.S. Publication No. 2006/0212925 (hereinafter "Shull"). Appellant submits that the applied references, even if combined in the manner proposed in the Office action, fail to teach each and every limitation of the claimed invention, when taken as a whole, as is required for a *prima facie* rejection under 35 U.S.C. § 103.

Accordingly, Appellant submits that these rejections are "improper and without basis," and therefore satisfy the standards for pre-appeal review set forth in the Gazette Notice. Also consistent with the Gazette Notice, we submit that the error is "based upon a clear legal or factual deficiency … rather than an interpretation of the claims or prior art teachings."

Rejections Under §103

Regarding the rejection of the independent claims under 35 U.S.C. § 103 in the final Office action dated February 13, 2017 (the "Office action"), the Examiner fails to make a *prima facie* case of obviousness because he does not fully address the following limitations:

> collecting information about two or more companies or other organizations that have computer systems, network resources, and employees, the organizations posing risks to themselves or to other parties through business relationships of the organizations with the other parties, the information collected about the organizations being indicative of compromises or of vulnerabilities or of configurations of technology systems, data, or other information of the organizations, and indicative of resiliencies of the organizations to recover from security breaches including compromises or vulnerabilities or configurations, **the information indicative of durations of events associated with compromises or vulnerabilities or configurations**…

> the metrics including a measure of the extent of, the frequency of, or the duration of compromise of the computer systems or data of the organization, or of a configuration or vulnerability of the organization, and a measure of the resilience of the organization to recover from a security breach or vulnerability, **the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability**…

Black Kite Ex. 1002, Page 423 of 1060

These limitations are merely restated in the Office action (pages 4 and 7), without a clear indication of how or if a particular prior art reference has been used to teach or suggest the limitation. Further, the Examiner has failed to fully consider Appellant's arguments submitted in the Office action response filed November 9, 2016 (the "Response").

In fact, the Examiner admits on page 7 that Newton does not teach "the metrics including a measure of the extent of the frequency, or of the duration, or compromise of the technology systems of the organization, or of a configuration or vulnerability of the organization, a measure of the resilience of the organization to recover from such vulnerability, the measure of resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability." Instead, the Office action appears to rely on Shull for this limitation. However, Shull is silent on the use or definition of a measure of resilience, and the Office action completely ignores this limitation with regards to Shull, only using Shull for its description of "creating a score for an entity from multiple sources which is similar to a credit score which informs requester of the trust of the entity where activities are accounted for both legitimate (i.e., positive) and illegitimate (i.e., negative)." Instead, the Office action improperly returns to Newton to address those elements missing from Shull.

Specifically, the Office action attempts to address the Appellant's argument that Newton does not teach "the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability," by citing to generic language of Newton and then assuming, improperly and without any support whatsoever, that measuring resilience of a network is inherent in a rating. It is well settled that inherency may not be established by probabilities or possibilities - the mere fact that a certain thing may result from or could possibly be included in a given set of circumstances is not sufficient. The cited language is completely silent with respect to any measure of resilience. In fact, nowhere does Newton teach or define a measurement of resilience, as admitted later in the Office action on page 7, and therefore a prima facie case of obviousness has not been established.

Accordingly, because the rejections of the claims under § 103 in the Office action is deficient for at least the reasons described above, Appellant submits that the rejections are based on clear factual and legal deficiencies and should be withdrawn.

Black Kite Ex. 1002, Page 424 of 1060

CONCLUSION

As set forth in the foregoing remarks, Appellant respectfully submits that there are clear errors in the Examiner's rejections. Appellant requests allowance of all pending claims or, in the alternative, reopening of prosecution on the merits with a proposed amendment to place any presently unpatentable claims in condition for allowance.

Dated: April 12, 2017

Respectfully submitted,

Electronic signature: /Joel E. Lehrer/
Joel E. Lehrer
Registration No.: 56,401
GOODWIN PROCTER LLP
100 Northern Avenue
Boston, Massachusetts 02210
(617) 570-1057
Attorney for Applicant

Doc Code: AP.PRE.REQ

USED IN LIEU OF PTO/SB/33 (07-09)

PRE-APPEAL BRIEF REQUEST FOR REVIEW	Docket Number (Optional) BST-004	
	Application Number 13/240,572-Conf. #2423	Filed September 22, 2011
	First Named Inventor Stephen Boyer et al.	
	Art Unit 2492	Examiner S. P. Kanaan

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request.

This request is being filed with a notice of appeal.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

☐ applicant /inventor.

☐ assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed.
(Form PTO/SB/96)

☒ attorney or agent of record.
Registration number 56,401.

☐ attorney or agent acting under 37 CFR 1.34.
Registration number if acting under 37 CFR 1.34 _____

/Joel E. Lehrer/
Signature

Joel E. Lehrer
Typed or printed name

(617) 570-1057
Telephone number

April 12, 2017
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☐ *Total of 1 forms are submitted.

NOTICE OF APPEAL FROM THE EXAMINER TO THE PATENT TRIAL AND APPEAL BOARD	Docket Number (Optional) BST-004

In re Application of	Stephen Boyer et al.
Application Number	13/240,572-Conf. #2423
Filed	September 22, 2011
For	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
Art Unit	2492
Examiner	S. P. Kanaan

Applicant hereby **appeals** to the Patent Trial and Appeal Board from the last decision of the examiner.

The fee for this Notice of Appeal is (37 CFR 41.20(b)(1)) $ 800.00

[x] Applicant claims small entity status. See 37 CFR 1.27. Therefore, the fee shown above is reduced by half, and the resulting fee is: $ 400.00

[ ] A check in the amount of the fee is enclosed.

[x] Payment by credit card. Form PTO-2038 is attached.

[x] The Director is hereby authorized to charge any fees which may be required, or credit any overpayment to Deposit Account No. 07-1700 .

[ ] A petition for an extension of time under 37 CFR 1.136(a) (PTO/SB/22) is enclosed.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

[ ] applicant/inventor.

[ ] assignee of record of the entire interest. See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96)

[x] attorney or agent of record. Registration number 56,401 .

[ ] attorney or agent acting under 37 CFR 1.34. Registration number if acting under 37 CFR 1.34. _____

/Joel E. Lehrer/
Signature

Joel E. Lehrer
Typed or printed name

(617) 570-1057
Telephone number

April 12, 2017
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

[ ] *Total of 1 forms are submitted.

Electronic Patent Application Fee Transmittal

Application Number:	13240572
Filing Date:	22-Sep-2011
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Filer:	Joel E. Lehrer/Tricia Ayube
Attorney Docket Number:	BST-004

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
NOTICE OF APPEAL	2401	1	400	400
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**400**

Electronic Acknowledgement Receipt

EFS ID:	28893347
Application Number:	13240572
International Application Number:	
Confirmation Number:	2423
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Customer Number:	51414
Filer:	Joel E. Lehrer/Tricia Ayube
Filer Authorized By:	Joel E. Lehrer
Attorney Docket Number:	BST-004
Receipt Date:	12-APR-2017
Filing Date:	22-SEP-2011
Time Stamp:	11:50:15
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$400
RAM confirmation Number	041217INTEFSW11510900
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Pre-Brief Conference request	Comments_Accompanying_Pre-Appeal_Conference_Request.pdf	30740 23d05bdc673aa713a92d0c7e8c1f1e62b6583609	no	4
Warnings:					
Information:					
2	Pre-Brief Conference request	PreAppeal_Brief_request.pdf	17282 8b52cafa11613e25eea5fe231dba1fc5d9cf323a	no	1
Warnings:					
Information:					
3	Notice of Appeal Filed	Notice_of_Appeal.pdf	19669 74a3848bac621cc0e3c76bbabc351f8daa1bf134	no	1
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	30234 1d9c68c833d21e6f6406959bba497b7f75fa9e75	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	97925		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/240,572	09/22/2011	Stephen Wayne Boyer	BST-004	2423

51414 7590 02/13/2017

GOODWIN PROCTER LLP
PATENT ADMINISTRATOR
100 Northern Avenue
BOSTON, MA 02210

EXAMINER
KANAAN, SIMON P

ART UNIT	PAPER NUMBER
2492	

NOTIFICATION DATE	DELIVERY MODE
02/13/2017	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATENTBOS@GOODWINPROCTER.COM
PSOUSA-ATWOOD@GOODWINPROCTER.COM
GLENN.WILLIAMS@GOODWINPROCTER.COM

Office Action Summary	Application No. 13/240,572	Applicant(s) BOYER ET AL.	
	Examiner SIMON KANAAN	Art Unit 2492	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11/9/2019*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1,4,5,7-14,16,121,124,126-132 and 134-141* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1,4,5,7-14,16,121,124,126-132 and 134-141* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *9/22/2014* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date *11/28/2016*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

Office Action Summary

1. Instant office action is in response to applicant's argument/amendments filed 11/28/2016. Claims 1, 4, 5, 7-14, 16, 121,124, 126-132 and 134-141 are pending in the instant application.

2. Claims 1, 4, 5, 7-14, 16, 121, 124, 126-132 and 134-141 are rejected (Claim Rejections - 35 USC § 103).

3. Applicant's arguments/amendments filed 11/28/2016 have been considered but are not persuasive.

Notice of Pre-AIA or AIA Status

4. The present application is being examined under the pre-AIA first to invent provisions

5. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

Applicant's Amendments and Examiner's Response

6. Applicant's arguments/amendments filed 11/9/2016 have been considered but are not persuasive. As for applicant's arguments,

a. Applicant argues that the cited prior art does not teach: "**the metrics including a measure of the extent of the frequency, or of the duration, or compromise of the technology systems of the organization, or of a configuration or vulnerability of the organization, and a measure of the resilience of the organization to recover from such vulnerability, the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability,**".

However, the examiner disagrees Newton, [0012] teaches that every network in the world would have a rating in the database and [0030] teaches establishing a reputation for a network, and a reputation/rating is indicative on how trust worthy a network is and the information gathered would be indicative on the resilience a network would likely be due to a compromise as a larger organization with more resources that has existed longer is more likely to be resilient than a smaller organization with less resources and age.

b. Applicant argues: The Office action cites to Shull in an attempt to show Shull teaches the use of confidence intervals when reporting a cyber-security score or rating. Neither the cited text, nor Shull generally teach providing such a confidence interval.

However, the examiner disagrees as Shull, [0069] and [0073], teaches giving an overall trust score between 1 and 5 i.e. a normalized composite score where 1 is a reputable business and 5 is likely engaged in illicit activity. Claim

137 states "determining a confidence range of the composite rating" and the range is 1 to 5.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1, 4, 5, 7-14, 16, 121, 122, 124, 126-132 and 134-141 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chris Newton (US Pre-Grant Publication No: 2004/0250122 A1) hereinafter referred to as Newton in view of in view of Shull et al. (US Pre-Grant Publication No: 2006/0212925 A1) hereinafter referred to as Shull.

As per **claim 1**, Newton discloses **a method comprising: collecting information about two or more organizations** *(Newton, [0018])* **that have computer systems, network resources** *(Newton, [0022])***, and employees** *(Newton, [0023])***, the organizations posing risks through business relationships of the organizations with other parties,** *(Newton, [0025]. [0019])* **the information collected about the organizations being indicative of compromises, vulnerabilities or configurations of technology systems of the organizations and indicative of resiliencies of the organizations to recover from such compromises, vulnerabilities or configurations, the information indicative of durations of events associated with**

compromises or vulnerabilities or configurations, *(Newton, [0012] teaches that every network in the world would have a rating in the database and [0030] teaches establishing a reputation for a network, and a reputation/rating is indicative on how trust worthy a network is and the information gathered would be indicative on the resilience a network would likely be due to a compromise as a larger organization with more resources that has existed longer is more likely to be resilient than a smaller organization with less resources and age)*

at least some of the information about each of the organizations being collected automatically by computer using sensors on the Internet, the information about each of the organizations being collected from two or more sources, one or more of the sources not being controlled by the organization, the information format least the one or more sources that are not controlled by the organization being collected without permission of the organization, *(Newton, [0031] teaches having multiple agents gathering data and [0044]-[0048] teaches different agent types i.e. different network characterization as each agent type gathers different type of data in regards to the security and reputation of network, among these agents include data mining internet which is public information and data mining newsgroups and forums which are also public knowledge and externally observable information not controlled by an organization)*

at least partly automatically gathering information about assets that each of the organizations owns, controls, uses, or is affiliated with, including IP

addresses and IP network address ranges, computer services residing within address ranges, or domain names, *(Newton, [0022]-[0023])*

at least one of the sources for each of the organizations comprising a public source or a commercial source, *(Newton, [0044]-[0048] and [0029], teaches information gathered externally from multiple sources including proxy information and data mining internet which is public information.)*

processing by computer the information from the two or more sources for each of the organizations to form a composite rating of the organization that is indicative of a degree of risk to the organization or to a party through a business relationship with the organization, *(Newton, [0016], teaches "Hosted services (web servers, email servers)" and [0044]-[0048] and [0029], teaches information gathered externally from multiple sources including proxy information and data mining internet which is public information.)*

in connection with a assessing a business risk to the organization or to a party through a business relationship with at least one of the organizations, delivering reports of the composite ratings of the organizations through a reporting facility to enable users of the reporting facility to monitor, assess, and mitigate the risks, based on the security vulnerabilities and resiliencies, in doing business with the organization and to compare the composite ratings of the organizations. *(Newton, figure 3 item 14, teaches a database which stores information about the organizations i.e. portal.)*

But Newton does not teach **the composite rating comprising a calculated composite of metrics and data derived or collected from the sources, the processing comprising applying transformations to the data and metrics, and the processing comprising applying weights to the data and the metrics, the metrics including a measure of the extent of the frequency of, or the duration of compromise of the technology systems of the organization, or of a configuration or vulnerability of the organization, and a measure of the resilience of the organization to recover from such vulnerability, the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability,**

However, *(Shull [0058] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score which informs requester of the trust of the entity, this score is received by the requester where activities are accounted for both legitimate (i.e. positive) and illegitimate (i.e. negative) and [0069] and [0073], teaches giving an overall trust score between 1 and 5 i.e. a normalized composite score where 1 is a reputable business and 5 is likely engaged in illicit activity.)*

It would have been obvious at the time of the invention for one of the ordinary skill in the art to modify the method of collecting security characteristics from multiple sources as taught by Newton by creating a score representative of the different collected data as taught by Shull because it would aid the requester in determining whether the entity is trusted or not.

As per **claim 4**, Newton in view of Shull discloses **the method of Claim 1, wherein the collected information is represented by at least two data types.** *(Newton, [0044]-[0048] teaches different agent types.)*

As per **claim 5**, Newton in view of Shull discloses the method of Claim 4, wherein the at least two data types include at least one of breach disclosures, block lists, configuration parameters, an identification of malware servers, an identification of a reputation, an identification of suspicious activity, an identification of spyware, white lists, an identification of compromised hosts, an identification of malicious activity, an identification of spam activity, an identification of vulnerable hosts, an identification of phishing activity, or an identification of e-mail viruses. *(Newton, [0013]-[0029] teaches security measures etc.)*

As per **claim 7**, Newton in view of Shull discloses **the method of Claim 1, wherein the collected information evidences internal security controls.** *(Newton, [0013]-[0029] teaches security measures etc.)*

As per **claim 8**, Newton in view of Shull discloses **the method of Claim 1, wherein the collected information comprises outcomes of each of the organizations.** *(Newton, [0013]-[0029] teaches security measures and [0044]-[0048] teaches checking for information already available to the public about network.)*

As per **claim 9**, Newton in view of Shull discloses **the method of Claim 1, wherein the collected information evidences operational execution of security measures of the organizations.** *(Newton, [0013]-[0029] teaches security measures.)*

As per **claim 10**, Newton in view of Shull **discloses the method of Claim 1, wherein the collected information indicates whether a computer system of the organizations served malicious code to another system.** *(Newton, [0013], teaches hostility level and page 4, claim 6, teaches spam levels.)*

As per **claim 11**, Newton in view of Shull discloses **the method of Claim 1, wherein the collected information indicates whether a computer system of the organizations communicated with a known attacker controlled network or sensor outside the control network of the organization**. *(Newton, [0013] teaches hostility level.)*

As per **claim 12**, Newton in view of Shull discloses **the method of Claim 1, comprising: forming a series of the security ratings of the organizations**. *(Newton, [0042], teaches live remote updates i.e. continually computing rating and page 4, claim 6 teaches security information has multiple ratings and [0041], teaches the different information having different weight.)*

As per **claim 13**, Newton in view of Shull discloses **the method of Claim 12, comprising determining a trend from the series of ratings.** *(Newton, [0042], teaches live remote updates i.e. continually computing rating.)*

As per **claim 14**, Newton in view of Shull discloses **the method of Claim 12, comprising displaying the series of composite ratings**. *(Newton, [0033], teaches a master database for collecting and storing the network ratings and page 4, claim 6 teaches security information has multiple ratings and [0041], teaches the different information having different weight and Shull, [0058], [0076] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score with informs requester of the trust of the entity, this score is received by the requester and a display device would display score as to help user determine whether to trust entity or not.)*

As per **claim 16**, Newton in view of Shull **teaches the method of Claim 14, wherein displaying the series of composite ratings for each of the organizations comprises posting the series of composite ratings for each of the organizations to a web portal.** *(Newton, [0033], teaches a master database for collecting and storing the network ratings which includes information as listed in [0013]-[0029] which serve as warnings and Shull, [0058], [0076] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score with informs requester*

of the trust of the entity, this score is received by the requester and a display device would display score as to help user determine whether to trust entity or not.)

As per **claim 121**, Newton in view of Shull teaches **the method of Claim 1, wherein the collected information represents externally observable outcome information**. - Newton, [0054], teaches agents getting information from news groups or sending packets and checking their responses.

As per **claim 122**, Newton in view of Shull teaches **the method of Claim 121, wherein the outcome information comprises outcome information associated with security vulnerability or resilience of each of the organizations.** *(Shull, [0058] and Newton, page 4, claim 6, both teach that the information is associated with entity security and Newton even looks into active security systems as well.)*

As per **claim 124**, Newton in view of Shull teaches **the method of Claim 1, comprising: determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information.** *(Newton, page 4, claim 6, teaches having spam levels etc. Which are a badness score.)*

As per **claim 126**, Newton in view of Shull teaches **the method of Claim 1, wherein: the collected information comprises at least two security characterizations of a computer system of the entity.** *(Newton, page 4, claim 6,*

teaches checking open proxy servers and desktop security measures which are multiple characterizations of a system of the entity.)

As per **claim 127**, Newton in view of Shull teaches **the method of Claim 1, wherein the collected information comprises a characterization of behavior of an employee of at least one of the organizations.** *(Newton, page 4, claim 6, inappropriate content served, spam levels, language spoken, geographic placement, industry, which are characterizations of employees in the network and the employees' behavior.)*

As per **claim 128**, Newton in view of Shull teaches **the method of Claim 1, wherein the collected information comprises characterizations other than characterizations about a computer system of at least one of the organizations.** *(Newton, page 4, claim 6, teaches security characterization includes security personnel.)*

As per **claim 129**, Newton in view of Shull teaches **the method of Claim 1, wherein the collected information comprises characterizations about policies of at least one of the organizations.** *(Newton, page 4, claim 6, teaches organization association, active security measures, desktop security measures, etc. which are policies see also [0059] and [0060].)*

As per **claim 130**, Newton in view of Shull teaches **the method of Claim 1, wherein the collected information comprises characterizations about information technology assets that at least one of the organizations owns, controls, uses, or is affiliated with.** *(Newton, page 4, claim 6, teaches organization associations see also [0043] and [0053].)*

As per **claim 131**, Newton in view of Shull **teaches the method of Claim 1 in which collected information represents: (a) physical states, (b) technical states, (c) organizational states, or (d) cultural states of at least one of the organizations which can be exploited to create a security breach; or (e) the organization's ability to recover from a security breach; or any combination of two or more of these.** *(Newton, page 4, claim 6, teaches active security measures and desktop security measures among other information collected about the organization.)*

As per claim 132, Newton in view of Shull teaches **the method of claim 1 in which processing the information to form a composite rating comprises correlating data across the sources of information.** *(Shull, [0058], teaches creating a score based on the different data received i.e. correlating the different data.)*

As per claim 134, Newton in view of Shull **teaches the method of claim 1 in which processing the information to form a composite rating comprises statistically correlating the composite rating with actual outcomes.** *(Newton,*

[0041], teaches giving different information different weight where less weight given to information as it becomes less important over time which is a statistical correlation with the information collected.)

As per claim 135, Newton in view of Shull **teaches the method of claim 1 in which the vulnerability comprises physical, technical, organizational, or cultural states that can be exploited to create a security breach.** *(Newton, figure 1, item 24 and page 4, claim 6.)*

As **per claim 136**, Newton teaches **a method comprising collecting, from at least two sources, information about two or more organizations, the collected information representing at least two data types, the collected information comprising outcomes of each of the organizations, at least some of the information for each of the organizations being collected automatically by computer from at least two sources, one or more of the sources not controlled by the organization, the information from at least the one or more sources that are not controlled by the organization being collected without permission of the-organization, at least one of the sources including a commercial data source,** *(Newton, [0012] teaches that every network in the world would have a rating in the database and [0030] teaches establishing a reputation for a network, and [0031] teaches having multiple agents gathering data and [0044]-[0048] teaches different agent types i.e. different network characterization as each agent type gathers different type of*

data in regards to the security and reputation of network, among these agents include data mining internet which is public information and data mining newsgroups and forums which are also public knowledge and externally observable information not controlled by an organization and figure 1, items 24 include information about the network which towards the bottom of item 24 states "company info resources" i.e. network is associated with a company, and [0022] and [0072], teaches taking into account size of the network and number of employees.)

at least partly automatically gathering information about assets that each of the organizations owns, controls, uses, or is affiliated with, including IP network address ranges, computer services residing within address ranges, or domain names, *(Newton, [0029] teaches "Address, contact information." And [0019] teaches "Organization associations: owned by, partnered with whom")*

and displaying the series of ratings through a portal and reporting the ratings of the organizations through a portal to enable customers to monitor, assess, and mitigate risk in doing business with the organizations and to compare the composite ratings across the organizations. *(Newton, figure 3 item 14, teaches a database which stores information about the organizations i.e. portal.)*

But Newton does not teach **processing the information from both of the two sources for each of the organizations to form a composite rating of a security vulnerability of the organization and of a resilience of the organization to recover from a security breach, the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability,**

or both, the processing including applying models that account for differences in the respective sources,, normalizing the composite rating of each of the organizations based on a size characteristic of the organization to enable comparisons of composite ratings between the two or more organizations, forming a series of the security ratings of each of the organizations, determining a trend from the series of ratings, determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information.

However, *(Shull [0058] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score which informs requester of the trust of the entity, this score is received by the requester where activities are accounted for both legitimate (i.e. positive) and illegitimate (i.e. negative) and [0069] and [0073], teaches giving an overall trust score between 1 and 5 i.e. a normalized composite score where 1 is a reputable business and 5 is likely engaged in illicit activity.)*

It would have been obvious at the time of the invention for one of the ordinary skill in the art to modify the method of collecting security characteristics from multiple sources as taught by Newton by creating a score representative of the different collected data as taught by Shull because it would aid the requester in determining whether the entity is trusted or not.

As per **claim 137**, Newton in view of Shull **teaches the method of claim 1, determining a confidence range of the composite rating, the size of the range varying inversely with the level of confidence in the composite rating.** *(Shull, [0069] and [0073], teaches giving an overall trust score between 1 and 5 i.e. a normalized composite score where 1 is a reputable business and 5 is likely engaged in illicit activity.)*

As per **claim 138**, Newton in view of Shull **teaches the system of claim 137, wherein the confidence range is based on redundancy of the security characterizations.** *(Shull, [0081], teaches taking into account consistency which is redundancy.)*

As per **claim 139**, Newton in view of Shull teaches **the method of claim 137, wherein the confidence range is based on a size of the third party computer system.** *(Newton, [0072], teaches taking into account size of the network.)*

As per **claim 140**, Newton in view of Shull teaches **the method of claim 1 comprising ranking the organization and other organizations within sectors or peer-groups or globally.** *(Shull, [0123]-[0124], teaches listing entities with similar scores together such as ones that scored a 3 or 4 so these would be ranked below ones which were listed as part of white list which ranked 1 or 2, see [0068], which teaches having white list, black list and grey lists.)*

As **per claim 141**, Newton teaches **a method comprising: collecting information about an organization** *(Newton, [0018])* **that has computer systems,** *(Newton, [0022])* **network resources, and employees,** *(Newton, [0023])* **the organization posing risks to itself or to other parties through business relationships of the organization with the other parties, the information collected about the organization** *(Newton, [0012] teaches that every network in the world would have a rating in the database and [0030] teaches establishing a reputation for a network)* **including (a) information collected automatically by computer on the Internet without permission of the organization, and** *(Newton, [0031] teaches having multiple agents gathering data and [0044]-[0048] teaches different agent types i.e. different network characterization as each agent type gathers different type of data in regards to the security and reputation of network, among these agents include data mining internet which is public information and data mining newsgroups and forums which are also public knowledge and externally observable information not controlled by an organization)* **(b) information indicative of resiliencies of the organization to recover from a security breach associated with a compromise or a vulnerability, the resiliencies being inversely proportional to one or more of the duration of detected malicious activity and the duration of the compromise or vulnerability,** *(Newton, [0030] teaches establishing a reputation for a network, and a reputation/rating is indicative on how trust worthy a network is and the information gathered would be indicative on the resilience a network would likely be due to a compromise as a larger*

organization with more resources that has existed longer is more likely to be resilient than a smaller organization with less resources and age) **processing the information by computer to form a composite rating of the organization that is indicative of a degree of risk based on a business relationship with the organization,** *(Newton, [0016], teaches "Hosted services (web servers, email servers)" and [0044]-[0048] and [0029], teaches information gathered externally from multiple sources including proxy information and data mining internet which is public information.)*

delivering a report of the composite rating of the organization through a reporting facility to enable a user of the reporting facility to assess the risks, based at least in part on the resiliencies. *(Newton, figure 3 item 14, teaches a database which stores information about the organizations i.e. portal.)*

but Newton does not teach **the composite rating comprising a measure of the resiliencies of the organization to recover from a security breach, and in connection with assessing a the degree of risk** .

However, *(Shull [0058] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score which informs requester of the trust of the entity, this score is received by the requester where activities are accounted for both legitimate (i.e. positive) and illegitimate (i.e. negative) and [0069] and [0073], teaches giving an overall trust score between 1 and 5 i.e. a normalized composite score where 1 is a reputable business and 5 is likely engaged in illicit activity.)*

It would have been obvious at the time of the invention for one of the ordinary skill in the art to modify the method of collecting security characteristics from multiple sources as taught by Newton by creating a score representative of the different collected data as taught by Shull because it would aid the requester in determining whether the entity is trusted or not.

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SIMON KANAAN whose telephone number is (571)270-3906. The examiner can normally be reached on Mon-Thurs 7:30-5:00 EST.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Saleh Najjar can be reached on 5712724006. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/SIMON KANAAN/
Examiner, Art Unit 2492

/SALEH NAJJAR/

Supervisory Patent Examiner, Art Unit 2492

Notice of References Cited	Application/Control No. 13/240,572	Applicant(s)/Patent Under Reexamination BOYER ET AL.	
	Examiner SIMON KANAAN	Art Unit 2492	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-2008/0262895 A1	10-2008	Hofmeister; Douglas F.	G06Q10/04	705/7.17
*	B	US-2009/0094265 A1	04-2009	VLACHOS; MICHAIL	G06F21/16	1/1
*	C	US-2009/0132861 A1	05-2009	Costa; Manuel	G06F11/0748	714/45
	D	US-				
	E	US-				
	F	US-				
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

PTO/SB/08a (07-09)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 4

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Boyer
Art Unit	2492
Examiner Name	S. Kanaan
Attorney Docket Number	BST-004

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A45	US-2001/0044798-A1	11-22-2001	Nagral et al.	
	A46	US-2002/0083077-A1	06-27-2002	Vardi	
	A47	US-2003/0050862-A1	03-13-2003	Bleicken et al.	
	A48	US-2003/0123424-A1	07-03-2003	Jung	
	A49	US-2004/0024859-A1	02-05-2004	Bloch et al.	
	A50	US-2004/0133561-A1	07-08-2004	Burke	
	A51	US-2004/0193918-A1	09-30-2004	Green et al.	
	A52	US-2004/0199791-A1	10-07-2004	Poletto et al.	
	A53	US-2004/0199792-A1	10-07-2004	Tan et al.	
	A54	US-2004/0250122-A1	12-09-2004	Newton	
	A55	US-2004/0250134-A1	12-09-2004	Kohler et al.	
	A56	US-2005/0071450-A1	03-31-2005	Allen et al.	
	A57	US-2005/0108415-A1	05-19-2005	Turk et al.	
	A58	US-2005/0131830-A1	06-16-2005	Juarez et al.	
	A59	US-2006/0173992-A1	08-03-2006	Weber et al.	
	A60	US-2007/0143851-A1	06-21-2007	Nicodemus et al.	
	A61	US-2007/0282730-A1	12-06-2007	Carpenter et al.	
	A62	US-2008/0162931-A1	07-03-2008	Lord et al.	
	A63	US-2009/0044272-A1	02-12-2009	Jarrett	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/SIMON P KANAAN/	Date Considered	02/06/2017

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

PTO/SB/08a (07-09)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 4

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Boyer
Art Unit	2492
Examiner Name	S. Kanaan
Attorney Docket Number	BST-004

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A64	US-2009/0193054-A1	07-30-2009	Karimisetty et al.	
	A65	US-2010/0262444-A1	10-14-2010	Atwal et al.	
	A66	US-2011/0185403-A1	07-28-2011	DOLAN et al.	
	A67	US-2014/0108474-A1	04-17-2014	David et al.	
	A68	US-2015/0310188-A1	10-29-2015	Ford et al.	
	A69	US-6,792,401	09-14-2004	Nigro et al.	
	A70	US-8,429,630	04-23-2013	Nickolov et al.	
	A71	US-8,504,556	08-06-2013	Rice et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/SIMON P KANAAN/	Date Considered	02/06/2017

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

PTO/SB/08b (07-09)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	3	of	4

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Boyer
Art Unit	2492
Examiner Name	S. Kanaan
Attorney Docket Number	BST-004

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	C72	Computer Network Graph-Bees, http://bioteams.com/2007/04/30/visualizing_complex_networks.html, date accessed September 28, 2016	
	C73	Computer Network Graph-Univ. of Michigan, http://people.cst.cmich.edu/liao1q/research.shtml, date accessed September 28, 2016	
	C74	Hacking Exposed 6, S. McClure et al., copyright 2009, 37 pages.	
	C75	MaxMind, https://www.maxmind.com/en/about-maxmind, https://www.maxmind.com/en/geoip2-isp-database, date accessed September 28, 20116, 3 pages.	
	C76	Netcraft, www.netcraft.com, date accessed September 28, 2016, 2 pages.	
	C77	NetScanTools Pro, http://www.netscantools.com/nstpromain.html, date accessed September 28, 2016, 2 pages.	
	C78	Network Security Assessment, C. McNab, copyright 2004, 13 pages.	
	C79	RFC 781, https://tools.ietf.org/html/rfc781, date accessed September 28, 2016, 3 pages.	
	C80	RFC 950, https://tools.ietf.org/html/rfc950, date accessed September 28, 2016, 19 pages.	
	C81	RFC 954, https://tools.ietf.org/html/rfc954, date accessed September 28, 2016, 5 pages.	

Examiner Signature	/SIMON P KANAAN/	Date Considered	02/06/2017

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

PTO/SB/08b (07-09)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	4	of	4	Attorney Docket Number	BST-004

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Boyer
Art Unit	2492
Examiner Name	S. Kanaan

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	C82	RFC 1834, https://tools.ietf.org/html/rfc1834, date accessed September 28, 2016, 7 pages.	
	C83	SamSpade Network Inquiry Utility, https://www.sans.org/reading-room/whitepapers/tools/sam-spade-934, date accessed September 28, 2016, 19 pages.	
	C84	Security Warrior, Cyrus Peikari, Anton, Chapter 8: Reconnaissance, 6 pages.	
	C85	Snort Intrusion Monitoring System, http://archive.oreilly.com/pub/h/1393, date accessed September 28, 2016, 3 pages.	
	C86	Wikipedia, https://en.wikipedia.org/wiki/Crowdsourcing, date accessed September 28, 2016	

Examiner Signature	/SIMON P KANAAN/	Date Considered	02/06/2017

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.P.K/

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	Art Unit
	SIMON KANAAN	2432

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor and Assignee Search (PALM)	4/18/2013	SK
class/subclass search + text (EAST: 726/1,2,22,25+text)	3/7/2016	SK
CPC + text (EAST: H04L63/20,145,14,0236,1433,104 OR H04L67/306 OR H04L51/12 OR H04L61/1511 OR H04L9/321 OR G06F21/00,577 + text)	2/7/2017	SK

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/SIMON KANAAN/ Examiner.Art Unit 2492	

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	12	(US-20040193918-$ or US-20050080720-$ or US-20040221296-$ or US-20050108415-$ or US-20040250122-$ or US-20080091834-$ or US-20120253890-$ or US-20140019196-$).did. or (US-5867799-$ or US-6016475-$ or US-7100195-$ or US-7748038-$).did.	US-PGPUB; USPAT	ADJ	ON	2017/02/07 05:13
L3	12	portfolio with business with reputation	US-PGPUB; USPAT	ADJ	ON	2017/02/07 05:39
L4	3	L3 AND ((705/26.7 OR 705/38 OR 705/7.28 OR 705/7.29 OR 705/7.33 OR 705/7.39).CCLS.)	US-PGPUB; USPAT	ADJ	ON	2017/02/07 05:39
L5	125	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.) and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2017/02/07 05:39
L6	133	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2017/02/07 05:39
L7	10	network reputation with (rat$3 or assess$4) and public	US-PGPUB; USPAT	ADJ	ON	2017/02/07 05:39
L8	24	(resilien$3) with (malicious or vulnerability) with (duration or time)	US-PGPUB; USPAT	ADJ	ON	2017/02/07 05:41
L9	160	reputation and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2017/02/07 05:50
L10	82	reputation and domain and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2017/02/07 05:50

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L2	1	"Term Removed"	US-PGPUB	ADJ	ON	2017/02/07 05:13

2/ 7/ 2017 5:50:45 AM
C:\ Users\ skanaan\ Documents\ EAST\ Workspaces\ 13240572.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	**Art Unit**
	SIMON KANAAN	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/18/2013	11/07/2013	06/04/2014	02/22/2015	05/28/2015	09/25/2015	03/07/2016	02/07/2017	
	1	✓	✓	✓	✓	✓	✓	✓	✓	
	2	✓	✓	-	-	-	-	-	-	
	3	✓	✓	✓	✓	✓	-	-	-	
	4	✓	✓	✓	✓	✓	✓	✓	✓	
	5	✓	✓	✓	✓	✓	✓	✓	✓	
	6	✓	✓	-	-	-	-	-	-	
	7	✓	✓	✓	✓	✓	✓	✓	✓	
	8	✓	✓	✓	✓	✓	✓	✓	✓	
	9	✓	✓	✓	✓	✓	✓	✓	✓	
	10	✓	✓	✓	✓	✓	✓	✓	✓	
	11	✓	✓	✓	✓	✓	✓	✓	✓	
	12	✓	✓	✓	✓	✓	✓	✓	✓	
	13	✓	✓	✓	✓	✓	✓	✓	✓	
	14	✓	✓	✓	✓	✓	✓	✓	✓	
	15	✓	✓	-	-	-	-	-	-	
	16	✓	✓	✓	✓	✓	✓	✓	✓	
	17	✓	✓	-	-	-	-	-	-	
	18	✓	✓	-	-	-	-	-	-	
	19	✓	✓	-	-	-	-	-	-	
	20	✓	✓	-	-	-	-	-	-	
	21	-	-	-	-	-	-	-	-	
	22	-	-	-	-	-	-	-	-	
	23	-	-	-	-	-	-	-	-	
	24	-	-	-	-	-	-	-	-	
	25	-	-	-	-	-	-	-	-	
	26	-	-	-	-	-	-	-	-	
	27	-	-	-	-	-	-	-	-	
	28	-	-	-	-	-	-	-	-	
	29	-	-	-	-	-	-	-	-	
	30	-	-	-	-	-	-	-	-	
	31	-	-	-	-	-	-	-	-	
	32	-	-	-	-	-	-	-	-	
	33	-	-	-	-	-	-	-	-	
	34	-	-	-	-	-	-	-	-	
	35	-	-	-	-	-	-	-	-	
	36	-	-	-	-	-	-	-	-	

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	**Art Unit**
	SIMON KANAAN	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/18/2013	11/07/2013	06/04/2014	02/22/2015	05/28/2015	09/25/2015	03/07/2016	02/07/2017	
	37	-	-	-	-	-	-	-	-	
	38	-	-	-	-	-	-	-	-	
	39	-	-	-	-	-	-	-	-	
	40	-	-	-	-	-	-	-	-	
	41	-	-	-	-	-	-	-	-	
	42	-	-	-	-	-	-	-	-	
	43	-	-	-	-	-	-	-	-	
	44	-	-	-	-	-	-	-	-	
	45	-	-	-	-	-	-	-	-	
	46	-	-	-	-	-	-	-	-	
	47	-	-	-	-	-	-	-	-	
	48	-	-	-	-	-	-	-	-	
	49	-	-	-	-	-	-	-	-	
	50	-	-	-	-	-	-	-	-	
	51	-	-	-	-	-	-	-	-	
	52	-	-	-	-	-	-	-	-	
	53	-	-	-	-	-	-	-	-	
	54	-	-	-	-	-	-	-	-	
	55	-	-	-	-	-	-	-	-	
	56	-	-	-	-	-	-	-	-	
	57	-	-	-	-	-	-	-	-	
	58	-	-	-	-	-	-	-	-	
	59	-	-	-	-	-	-	-	-	
	60	-	-	-	-	-	-	-	-	
	61	-	-	-	-	-	-	-	-	
	62	-	-	-	-	-	-	-	-	
	63	-	-	-	-	-	-	-	-	
	64	-	-	-	-	-	-	-	-	
	65	-	-	-	-	-	-	-	-	
	66	-	-	-	-	-	-	-	-	
	67	-	-	-	-	-	-	-	-	
	68	-	-	-	-	-	-	-	-	
	69	-	-	-	-	-	-	-	-	
	70	-	-	-	-	-	-	-	-	
	71	-	-	-	-	-	-	-	-	
	72	-	-	-	-	-	-	-	-	

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	**Art Unit**
	SIMON KANAAN	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/18/2013	11/07/2013	06/04/2014	02/22/2015	05/28/2015	09/25/2015	03/07/2016	02/07/2017	
	73	-	-	-	-	-	-	-	-	
	74	-	-	-	-	-	-	-	-	
	75	-	-	-	-	-	-	-	-	
	76	-	-	-	-	-	-	-	-	
	77	-	-	-	-	-	-	-	-	
	78	-	-	-	-	-	-	-	-	
	79	-	-	-	-	-	-	-	-	
	80	-	-	-	-	-	-	-	-	
	81	-	-	-	-	-	-	-	-	
	82	-	-	-	-	-	-	-	-	
	83	-	-	-	-	-	-	-	-	
	84	-	-	-	-	-	-	-	-	
	85	-	-	-	-	-	-	-	-	
	86	-	-	-	-	-	-	-	-	
	87	-	-	-	-	-	-	-	-	
	88	-	-	-	-	-	-	-	-	
	89	-	-	-	-	-	-	-	-	
	90	-	-	-	-	-	-	-	-	
	91	-	-	-	-	-	-	-	-	
	92	-	-	-	-	-	-	-	-	
	93	-	-	-	-	-	-	-	-	
	94	-	-	-	-	-	-	-	-	
	95	-	-	-	-	-	-	-	-	
	96	-	-	-	-	-	-	-	-	
	97	-	-	-	-	-	-	-	-	
	98	-	-	-	-	-	-	-	-	
	99	-	-	-	-	-	-	-	-	
	100	-	-	-	-	-	-	-	-	
	101	-	-	-	-	-	-	-	-	
	102	-	-	-	-	-	-	-	-	
	103	-	-	-	-	-	-	-	-	
	104	-	-	-	-	-	-	-	-	
	105	-	-	-	-	-	-	-	-	
	106	-	-	-	-	-	-	-	-	
	107	-	-	-	-	-	-	-	-	
	108	-	-	-	-	-	-	-	-	

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	**Art Unit**
	SIMON KANAAN	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/18/2013	11/07/2013	06/04/2014	02/22/2015	05/28/2015	09/25/2015	03/07/2016	02/07/2017	
	109	-	-	-	-	-	-	-	-	
	110	-	-	-	-	-	-	-	-	
	111	-	-	-	-	-	-	-	-	
	112	-	-	-	-	-	-	-	-	
	113	-	-	-	-	-	-	-	-	
	114	-	-	-	-	-	-	-	-	
	115	-	-	-	-	-	-	-	-	
	116	-	-	-	-	-	-	-	-	
	117	-	-	-	-	-	-	-	-	
	118	-	-	-	-	-	-	-	-	
	119	-	-	-	-	-	-	-	-	
	120	-	-	-	-	-	-	-	-	
	121			✓	✓	✓	✓	✓	✓	
	122			✓	✓	✓	✓	✓	✓	
	123			✓	✓	✓	-	-	-	
	124			✓	✓	✓	✓	✓	✓	
	125			✓	-	-	-	-	-	
	126			✓	✓	✓	✓	✓	✓	
	127			✓	✓	✓	✓	✓	✓	
	128			✓	✓	✓	✓	✓	✓	
	129			✓	✓	✓	✓	✓	✓	
	130			✓	✓	✓	✓	✓	✓	
	131			✓	✓	✓	✓	✓	✓	
	132			✓	✓	✓	✓	✓	✓	
	133			✓	-	-	-	-	-	
	134			✓	✓	✓	✓	✓	✓	
	135			✓	✓	✓	✓	✓	✓	
	136				✓	✓	✓	✓	✓	
	137				✓	✓	✓	✓	✓	
	138				✓	✓	✓	✓	✓	
	139				✓	✓	✓	✓	✓	
	140				✓	✓	✓	✓	✓	
	141							✓	✓	

PTO/SB/08a (07-09)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	1	of	4

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Boyer
Art Unit	2492
Examiner Name	S. Kanaan
Attorney Docket Number	BST-004

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A45	US-2001/0044798-A1	11-22-2001	Nagral et al.	
	A46	US-2002/0083077-A1	06-27-2002	Vardi	
	A47	US-2003/0050862-A1	03-13-2003	Bleicken et al.	
	A48	US-2003/0123424-A1	07-03-2003	Jung	
	A49	US-2004/0024859-A1	02-05-2004	Bloch et al.	
	A50	US-2004/0133561-A1	07-08-2004	Burke	
	A51	US-2004/0193918-A1	09-30-2004	Green et al.	
	A52	US-2004/0199791-A1	10-07-2004	Poletto et al.	
	A53	US-2004/0199792-A1	10-07-2004	Tan et al.	
	A54	US-2004/0250122-A1	12-09-2004	Newton	
	A55	US-2004/0250134-A1	12-09-2004	Kohler et al.	
	A56	US-2005/0071450-A1	03-31-2005	Allen et al.	
	A57	US-2005/0108415-A1	05-19-2005	Turk et al.	
	A58	US-2005/0131830-A1	06-16-2005	Juarez et al.	
	A59	US-2006/0173992-A1	08-03-2006	Weber et al.	
	A60	US-2007/0143851-A1	06-21-2007	Nicodemus et al.	
	A61	US-2007/0282730-A1	12-06-2007	Carpenter et al.	
	A62	US-2008/0162931-A1	07-03-2008	Lord et al.	
	A63	US-2009/0044272-A1	02-12-2009	Jarrett	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08a (07-09)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 4

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Boyer
Art Unit	2492
Examiner Name	S. Kanaan
Attorney Docket Number	BST-004

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
	A64	US-2009/0193054-A1	07-30-2009	Karimisetty et al.	
	A65	US-2010/0262444-A1	10-14-2010	Atwal et al.	
	A66	US-2011/0185403-A1	07-28-2011	DOLAN et al.	
	A67	US-2014/0108474-A1	04-17-2014	David et al.	
	A68	US-2015/0310188-A1	10-29-2015	Ford et al.	
	A69	US-6,792,401	09-14-2004	Nigro et al.	
	A70	US-8,429,630	04-23-2013	Nickolov et al.	
	A71	US-8,504,556	08-06-2013	Rice et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08b (07-09)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	3	of	4	Attorney Docket Number	BST-004

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Boyer
Art Unit	2492
Examiner Name	S. Kanaan

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	C72	Computer Network Graph-Bees, http://bioteams.com/2007/04/30/visualizing_complex_networks.html, date accessed September 28, 2016	
	C73	Computer Network Graph-Univ. of Michigan, http://people.cst.cmich.edu/liao1q/research.shtml, date accessed September 28, 2016	
	C74	Hacking Exposed 6, S. McClure et al., copyright 2009, 37 pages.	
	C75	MaxMind, https://www.maxmind.com/en/about-maxmind, https://www.maxmind.com/en/geoip2-isp-database, date accessed September 28, 20116, 3 pages.	
	C76	Netcraft, www.netcraft.com, date accessed September 28, 2016, 2 pages.	
	C77	NetScanTools Pro, http://www.netscantools.com/nstpromain.html, date accessed September 28, 2016, 2 pages.	
	C78	Network Security Assessment, C. McNab, copyright 2004, 13 pages.	
	C79	RFC 781, https://tools.ietf.org/html/rfc781, date accessed September 28, 2016, 3 pages.	
	C80	RFC 950, https://tools.ietf.org/html/rfc950, date accessed September 28, 2016, 19 pages.	
	C81	RFC 954, https://tools.ietf.org/html/rfc954, date accessed September 28, 2016, 5 pages.	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08b (07-09)
Approved for use through 07/31/2016. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet	4	of	4

Complete if Known	
Application Number	13/240,572-Conf. #2423
Filing Date	September 22, 2011
First Named Inventor	Stephen Boyer
Art Unit	2492
Examiner Name	S. Kanaan
Attorney Docket Number	BST-004

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
	C82	RFC 1834, https://tools.ietf.org/html/rfc1834, date accessed September 28, 2016, 7 pages.	
	C83	SamSpade Network Inquiry Utility, https://www.sans.org/reading-room/whitepapers/tools/sam-spade-934, date accessed September 28, 2016, 19 pages.	
	C84	Security Warrior, Cyrus Peikari, Anton, Chapter 8: Reconnaissance, 6 pages.	
	C85	Snort Intrusion Monitoring System, http://archive.oreilly.com/pub/h/1393, date accessed September 28, 2016, 3 pages.	
	C86	Wikipedia, https://en.wikipedia.org/wiki/Crowdsourcing, date accessed September 28, 2016	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

Electronic Patent Application Fee Transmittal

Application Number:	13240572
Filing Date:	22-Sep-2011
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Filer:	Joel E. Lehrer/Tricia Ayube
Attorney Docket Number:	BST-004

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
SUBMISSION- INFORMATION DISCLOSURE STMT	2806	1	90	90
		Total in USD ($)		**90**

Electronic Acknowledgement Receipt

EFS ID:	27615906
Application Number:	13240572
International Application Number:	
Confirmation Number:	2423
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Customer Number:	51414
Filer:	Joel E. Lehrer/Tricia Ayube
Filer Authorized By:	Joel E. Lehrer
Attorney Docket Number:	BST-004
Receipt Date:	28-NOV-2016
Filing Date:	22-SEP-2011
Time Stamp:	15:41:12
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$90
RAM confirmation Number	112916INTEFSW15415000
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	Computer_Network_Graph-Bees.pdf	207194 3cc813ad9c99a15c7b4cdd1d921e5151619a1fa4	no	2
Warnings:					
Information:					
2	Non Patent Literature	Computer_Network_Graph-Univ_of_Michigan.pdf	1401588 5654d5b2092bd561913ee2c72411e00aa75229c3	no	5
Warnings:					
Information:					
3	Non Patent Literature	Hacking_Exposed_6.pdf	7778648 d64413fd9c277891c77430a183e00dd9ed7ca5de	no	37
Warnings:					
Information:					
4	Non Patent Literature	MaxMind-1.pdf	133758 5fc357d2d0dd11cf50f26cff7f7dd5ee5b5cea79	no	3
Warnings:					
Information:					
5	Non Patent Literature	netcraft.pdf	131825 5f176c8066bf3cf6c4f351818dde4c1c7c630047	no	2
Warnings:					
Information:					
6	Non Patent Literature	NetScantools.pdf	324744 e65971e76eb7f0cf039aa6939baabfffba89c577	no	2
Warnings:					
Information:					

7	Non Patent Literature	Network_Security_Assessment.pdf	1803210 8851b10c8673685c1ebb024df2d9d024cda8a0e7	no	13
Warnings:					
Information:					
8	Non Patent Literature	RFC_781.pdf	69980 1a73605238b4e6334b712d84b3f93eb8b9576e2a	no	3
Warnings:					
Information:					
9	Non Patent Literature	RFC_950.pdf	169354 681cc289d3e9b452e440586eaa748cbabdaab571	no	19
Warnings:					
Information:					
10	Non Patent Literature	RFC_954.pdf	85018 0a2126ca9a84163b1844d0899611744c4328b84d	no	5
Warnings:					
Information:					
11	Non Patent Literature	RFC_1834.pdf	158464 8c1d213719c09948c479153c9d88dcfe0eee1c18	no	7
Warnings:					
Information:					
12	Non Patent Literature	SamSpade.pdf	293552 46cbe14c8a00b793836dfe7ef4799f2a0012a8bf	no	19
Warnings:					
Information:					
13	Non Patent Literature	Security_Warrior.pdf	1084077 86e9779f8188529b9832a55870ab897b4884e4e2	no	6
Warnings:					
Information:					

14	Non Patent Literature	Snort_Intrusion.pdf	180052 8910cf0232ea438abab13a3977a68a5918c63489	no	3
Warnings:					
Information:					
15	Non Patent Literature	Wikipedia-Crowdsourcing.pdf	617990 2a7561636614883ba01bd57aad055ea4f5a4c647	no	25
Warnings:					
Information:					
16	Transmittal Letter	IDS.pdf	19094 dcee46f21c24e864b8f41efbc7ef589444f262dc	no	2
Warnings:					
Information:					
17	Information Disclosure Statement (IDS) Form (SB08)	SB08.pdf	54377 830b5e3cdd6b42247caadfd8458daee9ab316d2d	no	4
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
18	Fee Worksheet (SB06)	fee-info.pdf	30664 08afaab3101a46a4c4e38e9e14095aa3a38e54e9	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	14543589	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Docket No.: BST-004
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Stephen Boyer et al.

Application No.: 13/240,572 Confirmation No.: 2423

Filed: September 22, 2011 Art Unit: 2492

For: INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM Examiner: S. Kanaan

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT (IDS)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Pursuant to 37 C.F.R. § 1.56, 1.97 and 1.98, the attention of the United States Patent and Trademark Office is hereby directed to the references listed on the attached PTO/SB/08. It is respectfully requested that the information be expressly considered during the prosecution of the above-identified application, and that the references be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Supplemental Information Disclosure Statement is filed more than three months after the filing date of this application, OR more than three months after the date of entry of the national stage in the international application, AND after the mailing date of a first Office Action on the merits, but before the mailing date of any of a Final Action under 37 C.F.R.§ 1.113, a Notice of Allowance under 37 C.F.R. § 1.311 or an action that otherwise closes prosecution in this application (37 C.F.R. § 1.97(c)).

In accordance with 37 C.F.R. § 1.98(a)(2)(ii), copies of U.S. patents and U.S. patent application publications are not submitted. Submitted herewith are copies of foreign patents and non-patent literature in accordance with 37 C.F.R. § 1.98(a)(2).

In accordance with 37 C.F.R. § 1.97(g), the filing of this Supplemental Information Disclosure Statement shall not be construed as a representation that a search has been made. In accordance with 37 C.F.R. § 1.97(h), the filing of this Supplemental Information Disclosure Statement shall not be construed to be an admission that the information cited in this Information Disclosure Statement is, or is considered to be, material to the patentability as defined in 37 C.F.R. § 1.56(b).

It is submitted that the Supplemental Information Disclosure Statement is in compliance with 37 C.F.R. § 1.98, and the Examiner is respectfully requested to consider the listed references.

Please charge our Credit Card in the amount of $90.00 covering the fee set forth in 37 C.F.R. § 1.17(p). The Director is hereby authorized to charge any deficiency in the fees filed, asserted to be filed or which should have been filed herewith to our Deposit Account No. 07-1700, under Order No. **BST-004**.

Dated: November 28, 2016

Respectfully submitted,

Electronic signature: /Joel E. Lehrer/
Joel E. Lehrer
Registration No.: 56,401
GOODWIN PROCTER LLP
100 Northern Avenue
Boston, Massachusetts 02210
(617) 570-1000
Attorney for Applicant

ACTIVE/88704718.1

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of: Stephen Wayne Boyer et al.	
Application No.: 13/240,572	Confirmation No.: 2423
Filed: September 22, 2011	Art Unit: 2492
For: INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM	Examiner: Kanaan, Simon P.

MS Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PRELIMINARY AMENDMENT

In addition to the response to the non-final Office action mailed from the U.S. Patent and Trademark Office on March 10, 2016 filed on September 9, 2016, Applicant submits this Preliminary Amendment to further clarify that which the Applicant believes to be the invention. Applicant presumes entry of the amendments filed on September 9, and respectfully requests entry of the following additional amendments, reconsideration and withdrawal of all grounds of rejection, and passage of the claims to allowance. Please amend the above-identified application, without prejudice, as follows:

- Amendments to the Claims are reflected in the Listing of the Claims that begins on page 2 of this paper.
- Remarks begin on page 9 of this paper.

Applicant believes that no fees are due for entry and consideration of this paper and respectfully petitions therefor. However, in the event that any fees are due, the Commissioner is hereby authorized to charge such fees to Deposit Account No. 07-1700, Order No. BST-004.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims

1. (Currently amended) A method comprising:

collecting information about two or more ~~companies or other~~ organizations that have computer systems, network resources, and employees, the organizations posing risks ~~to themselves or to other parties~~ through business relationships of the organizations with ~~the~~ other parties, the information collected about the organizations being indicative of compromises, ~~or of~~ vulnerabilities or ~~of~~ configurations of technology systems~~, data, or other information~~ of the organizations~~,~~ and indicative of resiliencies of the organizations to recover from such ~~security breaches including~~ compromises, ~~or~~ vulnerabilities or configurations, the information indicative of durations of events associated with compromises or vulnerabilities or configurations,

at least some of the information about each of the organizations being collected automatically by computer using sensors on the Internet,

the information about each of the organizations being collected from two or more sources, one or more of the sources not being controlled by the organization, the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization,

at least partly automatically gathering information about assets that each of the organizations owns, controls, uses, or is affiliated with, including IP addresses and IP network address ranges, computer services residing within address ranges, or domain names,

at least one of the sources for each of the organizations comprising a public source or a commercial source,

processing by computer the information from the two or more sources for each of the organizations to form a composite rating of the organization that is indicative of a degree of risk to the organization or to a party through a business relationship with the organization, the

composite rating comprising a calculated composite of metrics and data derived or collected from the sources, the processing comprising applying transformations to the data and metrics, and the processing comprising applying weights to the data and the metrics,

the metrics including a measure of the extent of, the frequency of, or duration of compromise of the technology ~~computer~~ systems ~~or data~~ of the organization, or of a configuration or vulnerability of the organization, and a measure of the resilience of the organization to recover from ~~a security breach or~~ such vulnerability, the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability, and

in connection with assessing a business risk to the organization or to a party through a business relationship with at least one of the organizations, delivering reports of the composite ratings of the organizations through a reporting facility to enable users of the reporting facility to monitor, assess, and mitigate the risks, based on the security vulnerabilities and resiliencies, in doing business with the organization and to compare the composite ratings of the organizations.

2. (Canceled)

3. (Canceled)

4. (Original) The method of claim 1, wherein the collected information is represented by at least two data types.

5. (Original) The method of claim 4, wherein the at least two data types include at least one of breach disclosures, block lists, configuration parameters, an identification of malware servers, an identification of a reputation, an identification of suspicious activity, an identification of spyware, white lists, an identification of compromised hosts, an identification of malicious activity, an identification of spam activity, an identification of vulnerable hosts, an identification of phishing activity, or an identification of e-mail viruses.

6. (Canceled)

7. (Original) The method of claim 1, wherein the collected information evidences internal security controls.

8. (Original) The method of claim 1, wherein the collected information comprises outcomes of each of the organizations.

9. (Original) The method of claim 1, wherein the collected information evidences operational execution of security measures of each of the organizations.

10. (Original) The method of claim 1, wherein the collected information indicates whether a computer system of each of the organizations served malicious code to another system.

11. (Original) The method of claim 1, wherein the collected information indicates whether a computer system of each of the organizations communicated with a known attacker controlled network or sensor outside the control or network of the organization.

12. (Original) The method of claim 1, comprising: forming a series of the security ratings of each of the organizations.

13. (Original) The method of claim 12, comprising: determining a trend from the series of ratings.

14. (Original) The method of claim 12, comprising displaying the series of composite ratings.

15. (Canceled)

16. (Original) The method of claim 14, wherein displaying the series of composite ratings for each of the organizations comprises posting the series of composite ratings for the organization to a web portal.

17. (Canceled)

18. (Canceled)

19-120. (Canceled)

121. (Original) The method of claim 1, wherein the collected information represents externally observable outcome information.

122. (Cancelled)

123. (Canceled)

124. (Original) The method of claim 1, comprising: determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information.

125. (Canceled)

126. (Original) The method of claim 1, wherein: the collected information comprises at least two security characterizations of a computer system of each of the organizations.

127. (Original) The method of claim 1, wherein the collected information comprises a characterization of behavior of an employee of at least one of the organizations.

128. (Original) The method of claim 1, wherein the collected information comprises characterizations other than characterizations about a computer system of at least one of the organizations.

129. (Original) The method of claim 1, wherein the collected information comprises characterizations about policies of at least one of the organizations.

130. (Original) The method of claim 1, wherein the collected information comprises characterizations about information technology assets that at least one of the organizations owns, controls, uses, or is affiliated with.

131. (Original) The method of claim 1 in which collected information represents: (a) physical states, (b) technical states, (c) organizational states, or (d) cultural states of at least one of the organizations which can be exploited to create a security breach; or (e) the organization's ability to recover from a security breach; or any combination of two or more of these.

132. (Original) The method of claim 1 in which processing the information to form a composite rating comprises correlating data across the sources of information.

133. (Canceled)

134. (Original) The method of claim 1 in which processing the information to form a composite rating comprises statistically correlating the composite rating with actual outcomes.

135. (Original) The method of claim 1 in which the vulnerability comprises physical, technical, organizational, or cultural states that can be exploited to create a security breach.

136. (Currently amended) A method comprising

collecting, from at least two sources, information about two or more ~~companies or other~~ organizations, the collected information representing at least two data types, the collected information comprising outcomes of each of the organizations,

at least some of the information for each of the organizations being collected automatically by computer from at least two sources, one or more of the sources not controlled by the organization,

the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization, at least one of the sources including a commercial data source,

processing the information from both of the two sources for each of the organizations to form a composite rating of a security vulnerability of the organization ~~to creation of a security breach or a compromise of a system of the organization or~~ and of a resilience of the organization to recover from a security breach, the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability, or both, the processing including applying models that account for differences in the respective sources,

normalizing the composite rating of each of the organizations based on a size characteristic of the organization to enable comparisons of composite ratings between the two or more organizations,

forming a series of the security ratings of each of the organizations, determining a trend from the series of ratings, and displaying the series of composite ratings through a portal,

determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information, and

reporting the composite ratings of the organizations through a portal to enable customers to monitor, assess, and mitigate risk in doing business with the organizations and to compare the composite ratings across the organizations.

137. (Original) The system of claim 1, determining a confidence range of the composite rating, the size of the range varying inversely with the level of confidence in the composite rating.

138. (Original) The system of claim 137, wherein the confidence range is based on redundancy of the security characterizations.

139. (Original) The system of claim 137, wherein the confidence range is based on a size of the third party computer system.

140. (Original) The method of claim 1 comprising ranking the organization and other organizations within sectors or peer-groups or globally.

141. (Currently amended) A method comprising:

collecting information about an organization that has computer systems, network resources, and employees, the organization posing risks to itself or to other parties through business relationships of the organization with the other parties,

the information collected about the organization including (a) information collected automatically by computer on the Internet without permission of the organization, and (b) information indicative of resiliencies of the organization to recover from a security breach associated with a compromise or a vulnerability, the resiliencies being inversely proportional to one or more of the duration of detected malicious activity and the duration of the compromise or vulnerability~~, or a configuration~~,

processing the information by computer to form a composite rating of the organization that is indicative of a degree of risk ~~to the organization or to a party through~~ based on a business relationship with the organization, the composite rating ~~being based on metrics that include~~ comprising a measure of the resiliencies of the organization to recover from a security breach ~~associated with a compromise or a vulnerability or a configuration~~, and

in connection with assessing ~~a~~ the degree of risk, ~~business risk to the organization or to a party through a business relationship with the organization,~~ delivering a report of the composite rating of the organization through a reporting facility to enable a user of the reporting facility to assess the risks, based at least in part on the resiliencies~~, in doing business with the organization~~.

REMARKS

Applicant thanks Examiner Kanaan for conducting a telephonic interview on October 4, 2016. The participants included Examiner Holmes, Applicant's undersigned representative (Joel E. Lehrer). During the interview, the discussion focused on the amendments and arguments presented in the Amendment and Response filed on October 28, 2016 and further amendments presented herein. Accordingly, this paper is intended to constitute a proper recordation of the interview in accordance with M.P.E.P. § 713.04.

Claims 1, 4, 5, 7-14, 16, 121, 122, 124, 126-132, and 134-141 are currently pending. Claims 1, 4, 5, 7-14, 16, 121, 122, 124, 126 –132, and 124 –141 stand rejected under 35 U.S.C. § 103(a) based on the Office action issued on March 10, 2016. With this Preliminary Amendment, Applicant further amends claims 1, 136, and 141 and cancels claim 122. Support for the amendments may be found at least at paragraphs [0077] and [0078] of the application as published. No new matter has been added. Upon entry of this paper, claims 1, 4, 5, 7-14, 16, 121, 124, 126-132, and 134-141 will be pending. Applicant respectfully requests the consideration of these amendments in conjunction with the remarks set forth in the Amendment and Response filed on September 9, 2016.

CONCLUSION

In view of the foregoing, Applicant respectfully requests reconsideration, withdrawal of all grounds of rejection, and allowance of claims 1, 4, 5, 7-14, 16, 121, 122, 124, 126-132, and 134-141 in due course. The Examiner is invited to contact Applicant's undersigned representative by telephone at the number listed below to discuss any outstanding issues.

Dated: November 9, 2016

Respectfully submitted,

Electronic signature: /Joel E. Lehrer/
Joel E. Lehrer
Registration No.: 56,401
GOODWIN PROCTER LLP
100 Northern Avenue
Boston, Massachusetts 02210
(617) 570-1057
Attorney for Applicant

ACTIVE/88457348.1

Black Kite Ex. 1002, Page 488 of 1060

Electronic Acknowledgement Receipt

EFS ID:	27459699
Application Number:	13240572
International Application Number:	
Confirmation Number:	2423
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Customer Number:	51414
Filer:	Joel E. Lehrer/Meghan Breault
Filer Authorized By:	Joel E. Lehrer
Attorney Docket Number:	BST-004
Receipt Date:	09-NOV-2016
Filing Date:	22-SEP-2011
Time Stamp:	13:49:42
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		BST-004_PreliminaryAmendment.pdf	98685 66ab41dcf656cc28f17be09a8e3b343753543200	yes	10

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Preliminary Amendment	1	1
	Claims	2	8
	Applicant Arguments/Remarks Made in an Amendment	9	10
Warnings:			
Information:			
	Total Files Size (in bytes):	98685	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/240,572	Filing Date 09/22/2011	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT **11/09/2016**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 29	Minus	** 31	= 0	X $40 =	0
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $210 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
GOIGA DUCKETT

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/240,572	09/22/2011	Stephen Wayne Boyer	38879-0006001	2423

51414 7590 11/08/2016

GOODWIN PROCTER LLP
PATENT ADMINISTRATOR
100 Northern Avenue
BOSTON, MA 02210

EXAMINER
KANAAN, SIMON P

ART UNIT	PAPER NUMBER
2492	

NOTIFICATION DATE	DELIVERY MODE
11/08/2016	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATENTBOS@GOODWINPROCTER.COM
PSOUSA-ATWOOD@GOODWINPROCTER.COM
GLENN.WILLIAMS@GOODWINPROCTER.COM

Applicant-Initiated Interview Summary	Application No.	Applicant(s)	
	13/240,572	BOYER ET AL.	
	Examiner	Art Unit	
	SIMON KANAAN	2492	

All participants (applicant, applicant's representative, PTO personnel):

(1) *SIMON KANAAN*. (3)_____.

(2) *Joel Lehrer (Reg No 56401)*. (4)_____.

Date of Interview: *28 October 2016*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1*.

Identification of prior art discussed: *Newton (200402500122) and Shull (20060212925)*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Examiner and applicant's representative discussed the claim amendments filed 9/9/2016. Examiner appreciated the explanation from the applicant's representative that the focus of the amendments is for the resilience of the company. Examiner agreed that a clear definition of resilience is likely to overcome current art rejection however that the claims first limitation with the multiple or/and combination makes unclear whether resilience limitation is listed in the alternative. Examiner asked if claim could be clarified to help better show the positive recitation the resilience limitation .

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/SIMON KANAAN/ Examiner, Art Unit 2492	/SALEH NAJJAR/ Supervisory Patent Examiner, Art Unit 2492

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:

1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/240,572	09/22/2011	Stephen Wayne Boyer	38879-0006001

CONFIRMATION NO. 2423

POA ACCEPTANCE LETTER

51414
GOODWIN PROCTER LLP
PATENT ADMINISTRATOR
100 Northern Avenue
BOSTON, MA 02210

OC00000086430870

Date Mailed: 10/13/2016

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 10/07/2016.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/sleutchit/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/240,572	09/22/2011	Stephen Wayne Boyer	38879-0006001

CONFIRMATION NO. 2423

POWER OF ATTORNEY NOTICE

26161
FISH & RICHARDSON P.C. (BO)
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

OC000000086430857

Date Mailed: 10/13/2016

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 10/07/2016.

- The Power of Attorney to you in this application has been revoked by the applicant. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/sleutchit/

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82A (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FOR POWER OF ATTORNEY TO ONE OR MORE REGISTERED PRACTITIONERS

NOTE: This form is to be submitted with the Power of Attorney by Applicant form (PTO/AIA/82B) to identify the application to which the Power of Attorney is directed, in accordance with 37 CFR 1.5, unless the application number and filing date are identified in the Power of Attorney by Applicant form. If neither form PTO/AIA/82A nor form PTO/AIA82B identifies the application to which the Power of Attorney is directed, the Power of Attorney will not be recognized in the application.

Application Number	13/240,572
Filing Date	September 22, 2011
First Named Inventor	Stephen Boyer
Title	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
Art Unit	2492
Examiner Name	S. P. Kanaan
Attorney Docket Number	BST-004

SIGNATURE of Applicant or Patent Practitioner

Signature	/Joel E. Lehrer/	Date (Optional)	October 7, 2016
Name	Joel E. Lehrer	Registration Number	56,401
Title (if Applicant is a juristic entity)			
Applicant Name (if Applicant is a juristic entity)			

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4(d) for signature requirements and certifications. If more than one applicant, use multiple forms.

☐ *Total of 1 forms are submitted.

Doc Code: PA..
Document Description: Power of Attorney

PTO/AIA/82B (07-13)
Approved for use through 11/30/2014. OMB 0651-0051
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

POWER OF ATTORNEY BY APPLICANT

I hereby revoke all previous powers of attorney given in the application identified in either the attached transmittal letter or the boxes below.

Application Number	Filing Date

(Note: The boxes above may be left blank if information is provided on form PTO/AIA/62A.)

[X] I hereby appoint the Patent Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the application referenced in the attached transmittal letter (form PTO/AIA/62A) or identified above: 051414

OR

[ ] I hereby appoint Practitioner(s) named in the attached list (form PTO/AIA/82C) as my/our attorney(s) or agent(s), and to transact all business in the United States Patent and Trademark Office connected therewith for the patent application referenced in the attached transmittal letter (form PTO/AIA/82A) or identified above. (Note: Complete form PTO/AIA/82C.)

Please recognize or change the correspondence address for the application identified in the attached transmittal letter or the boxes above to:

[X] The address associated with the above-mentioned Customer Number

OR

[ ] The address associated with Customer Number:

OR

Firm or Individual Name					
Address					
City		State		Zip	
Country					
Telephone		Email			

I am the Applicant (if the Applicant is a juristic entity, list the Applicant name in the box):

BitSight Technologies, Inc.

[ ] Inventor or Joint Inventor (title not required below)

[ ] Legal Representative of a Deceased or Legally Incapacitated Inventor (title not required below)

[X] Assignee or Person to Whom the Inventor is Under an Obligation to Assign (provide signer's title if applicant is a juristic entity)

[ ] Person Who Otherwise Shows Sufficient Proprietary Interest (e.g., a petition under 37 CFR 1.46(b)(2) was granted in the application or is concurrently being filed with this document) (provide signer's title if applicant is a juristic entity)

SIGNATURE of Applicant for Patent

The undersigned (whose title is supplied below) is authorized to act on behalf of the applicant (e.g., where the applicant is a juristic entity).

Signature	[signature]	Date (Optional)	10/5/16
Name			
Title			

NOTE: Signature - This form must be signed by the applicant in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. If more than one applicant, use multiple forms.

[ ] Total of 1 forms are submitted.

PTO/SB/96 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: Stephen Boyer et al.

Application No./Patent No.: 13/240,572 Filed/Issue Date: September 22, 2011

Titled: INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM

BitSight Technologies, Inc. , a Corporation
(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.

states that it is:

1. [X] the assignee of the entire right, title, and interest in;
2. [ ] an assignee of less than the entire right, title, and interest in
(The extent (by percentage) of its ownership interest is _____ %); or
3. [ ] the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made)

the patent application/patent identified above, by virtue of either:

A. [X] An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 027658 , Frame 0906 , or for which a copy therefore is attached.

OR

B. [ ] A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: _____ To: _____
The document was recorded in the United States Patent and Trademark Office at
Reel _____ , Frame _____ , or for which a copy thereof is attached.

2. From: _____ To: _____
The document was recorded in the United States Patent and Trademark Office at
Reel _____ , Frame _____ , or for which a copy thereof is attached.

3. From: _____ To: _____
The document was recorded in the United States Patent and Trademark Office at
Reel _____ , Frame _____ , or for which a copy thereof is attached.

[ ] Additional documents in the chain of title are listed on a supplemental sheet(s).

[ ] As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (*i.e.*, a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3. to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Joel E. Lehrer/ October 7, 2016
Signature Date

Joel E. Lehrer Attorney for Assignee
Printed or Typed Name Title

Electronic Acknowledgement Receipt

EFS ID:	27137065
Application Number:	13240572
International Application Number:	
Confirmation Number:	2423
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Customer Number:	26161
Filer:	Joel E. Lehrer/Tricia Ayube
Filer Authorized By:	Joel E. Lehrer
Attorney Docket Number:	38879-0006001
Receipt Date:	07-OCT-2016
Filing Date:	22-SEP-2011
Time Stamp:	16:30:34
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		POA.pdf	632660 39d93abd2dee8039fbde8af2faa02dce38c123e3	yes	3

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Power of Attorney	1	2
	Assignee showing of ownership per 37 CFR 3.73	3	3
Warnings:			
Information:			
	Total Files Size (in bytes):	632660	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of: Stephen Wayne Boyer et al.	
Application No.: 13/240,572	Confirmation No.: 2423
Filed: September 22, 2011	Art Unit: 2492
For: INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM	Examiner: Kanaan, Simon P.

MS Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT AND RESPONSE

In response to the non-final Office action mailed from the U.S. Patent and Trademark Office on March 10, 2016, Applicant submits this Amendment and Response. Applicant respectfully requests entry of the following amendments, reconsideration and withdrawal of all grounds of rejection, and passage of the claims to allowance. Please amend the above-identified application, without prejudice, as follows:

- Amendments to the Claims are reflected in the Listing of the Claims that begins on page 2 of this paper.
- Remarks begin on page 9 of this paper.

Applicant believes that a surcharge for a three-month extension of time is due for entry and consideration of this paper and respectfully petitions therefor. A fee for one additional claim is also due in connection with the filing of this paper. No other fees are believed due; however, in the event that any fees are due, the Commissioner is hereby authorized to charge such fees to Deposit Account No. 07-1700, Order No. BST-004.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims

1. (Currently amended) A method comprising:

collecting information about two or more companies or other organizations that have computer systems, network resources, and employees, the organizations posing risks to themselves or to other parties through business relationships of the organizations with the other parties, the information collected about the organizations being indicative of compromises or of vulnerabilities or of configurations of technology systems, data, or other information of the organizations, and indicative of resiliencies of the organizations to recover from security breaches including compromises or vulnerabilities or configurations, the information indicative of durations of events associated with compromises or vulnerabilities or configurations,

at least some of the information about each of the organizations being collected automatically by computer using sensors on the Internet,

the information about each of the organizations being collected from two or more sources, one or more of the sources not being controlled by the organization, the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization,

at least partly automatically gathering information about assets that each of the organizations owns, controls, uses, or is affiliated with, including IP addresses and IP network address ranges, computer services residing within address ranges, or domain names,

at least one of the sources for each of the organizations comprising a public source or a commercial source,

processing by computer the information from the two or more sources for each of the organizations to form a composite rating of the organization that is indicative of a degree of risk to the organization or to a party through a business relationship with the organization, the

composite rating comprising a calculated composite of metrics and data derived or collected from the sources, the processing comprising applying transformations to the data and metrics, and the processing comprising applying weights to the data and the metrics,

the metrics including a measure of the extent of, ~~or~~ the frequency of, or the duration of compromise of the computer systems or data of the organization, or of a configuration or vulnerability of the organization, and a measure of the resilience of the organization to recover from a security breach or vulnerability, the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability, and

in connection with assessing a business risk to the organization or to a party through a business relationship with at least one of the organizations, delivering ~~a report~~ reports of the composite ratings of the organizations through a reporting facility to enable ~~a user~~ users of the reporting facility to monitor, assess, and mitigate the risks, based on the security vulnerabilities and resiliencies, in doing business with the organization and to compare the composite ratings of the organizations.

2. (Canceled)

3. (Canceled)

4. (Original) The method of claim 1, wherein the collected information is represented by at least two data types.

5. (Original) The method of claim 4, wherein the at least two data types include at least one of breach disclosures, block lists, configuration parameters, an identification of malware servers, an identification of a reputation, an identification of suspicious activity, an identification of spyware, white lists, an identification of compromised hosts, an identification of malicious activity, an identification of spam activity, an identification of vulnerable hosts, an identification of phishing activity, or an identification of e-mail viruses.

6. (Canceled)

7. (Original) The method of claim 1, wherein the collected information evidences internal security controls.

8. (Original) The method of claim 1, wherein the collected information comprises outcomes of each of the organizations.

9. (Original) The method of claim 1, wherein the collected information evidences operational execution of security measures of each of the organizations.

10. (Original) The method of claim 1, wherein the collected information indicates whether a computer system of each of the organizations served malicious code to another system.

11. (Original) The method of claim 1, wherein the collected information indicates whether a computer system of each of the organizations communicated with a known attacker controlled network or sensor outside the control or network of the organization.

12. (Original) The method of claim 1, comprising: forming a series of the security ratings of each of the organizations.

13. (Original) The method of claim 12, comprising: determining a trend from the series of ratings.

14. (Original) The method of claim 12, comprising displaying the series of composite ratings.

15. (Canceled)

16. (Original) The method of claim 14, wherein displaying the series of composite ratings for each of the organizations comprises posting the series of composite ratings for the organization to a web portal.

17. (Canceled)

18. (Canceled)

19-120. (Canceled)

121. (Original) The method of claim 1, wherein the collected information represents externally observable outcome information.

122. (Original) The method of claim 121, wherein the outcome information comprises outcome information associated with security vulnerability or resilience of each of the organizations.

123. (Canceled)

124. (Original) The method of claim 1, comprising: determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information.

125. (Canceled)

126. (Original) The method of claim 1, wherein: the collected information comprises at least two security characterizations of a computer system of each of the organizations.

127. (Original) The method of claim 1, wherein the collected information comprises a characterization of behavior of an employee of at least one of the organizations.

128. (Original) The method of claim 1, wherein the collected information comprises characterizations other than characterizations about a computer system of at least one of the organizations.

129. (Original) The method of claim 1, wherein the collected information comprises characterizations about policies of at least one of the organizations.

130. (Original) The method of claim 1, wherein the collected information comprises characterizations about information technology assets that at least one of the organizations owns, controls, uses, or is affiliated with.

131. (Original) The method of claim 1 in which collected information represents: (a) physical states, (b) technical states, (c) organizational states, or (d) cultural states of at least one of the organizations which can be exploited to create a security breach; or (e) the organization's ability to recover from a security breach; or any combination of two or more of these.

132. (Original) The method of claim 1 in which processing the information to form a composite rating comprises correlating data across the sources of information.

133. (Canceled)

134. (Original) The method of claim 1 in which processing the information to form a composite rating comprises statistically correlating the composite rating with actual outcomes.

135. (Original) The method of claim 1 in which the vulnerability comprises physical, technical, organizational, or cultural states that can be exploited to create a security breach.

136. (Currently amended) A method comprising

collecting, from at least two sources, information about two or more companies or other organizations, the collected information representing at least two data types, the collected information comprising outcomes of each of the organizations,

at least some of the information for each of the organizations being collected automatically by computer from at least two sources, one or more of the sources not controlled by the organization,

the information from at least the one or more sources that are not controlled by the organization being collected without permission of the-organization, at least one of the sources including a commercial data source,

processing the information from both of the two sources for each of the organizations to form a composite rating of a security vulnerability of the organization to creation of a security breach or a compromise of a system of the organization or of a resilience of the organization to recover from a security breach, the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability, or both, the processing including applying models that account for differences in the respective sources,

normalizing the composite rating of each of the organizations based on a size characteristic of the organization to enable comparisons of composite ratings between the two or more organizations,

forming a series of the security ratings of each of the organizations, determining a trend from the series of ratings, and displaying the series of composite ratings through a portal,

determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information, and

reporting the composite ratings of the organizations through a portal to enable customers to monitor, assess, and mitigate risk in doing business with the organizations and to compare the composite ratings across the organizations.

137. (Original) The system of claim 1, determining a confidence range of the composite rating, the size of the range varying inversely with the level of confidence in the composite rating.

138. (Original) The system of claim 137, wherein the confidence range is based on redundancy of the security characterizations.

139. (Original) The system of claim 137, wherein the confidence range is based on a size of the third party computer system.

140. (Original) The method of claim 1 comprising ranking the organization and other organizations within sectors or peer-groups or globally.

141. (Currently amended) A method comprising:

collecting information about an organization that has computer systems, network resources, and employees, the organization posing risks to itself or to other parties through business relationships of the organization with the other parties,

the information collected about the organization including (a) information collected automatically by computer on the Internet without permission of the organization, and (b) information indicative of resiliencies of the organization to recover from a security breach associated with a compromise or a vulnerability, the resiliencies being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability, or a configuration,

processing the information by computer to form a composite rating of the organization that is indicative of a degree of risk to the organization or to a party through a business relationship with the organization, the composite rating being based on metrics that include a measure of the resiliencies of the organization to recover from a security breach associated with a compromise or a vulnerability or a configuration, and

in connection with assessing a business risk to the organization or to a party through a business relationship with the organization, delivering a report of the composite rating of the organization through a reporting facility to enable a user of the reporting facility to assess the risks, based at least in part on the resiliencies, in doing business with the organization.

REMARKS

Claims 1, 4, 5, 7-14, 16, 121, 122, 124, 126-132, and 134-141 are currently pending. Claims 1, 4, 5, 7-14, 16, 121, 122, 124, 126 –132, and 124 –141 stand rejected under 35 U.S.C. § 103(a). With this Amendment and Response, Applicant hereby amends claims 1, 136, and 141. Support for the amendments may be found at least at paragraphs [0077] and [0078] of the application as published. No new matter has been added. Upon entry of this paper, claims 1, 4, 5, 7-14, 16, 121, 122, 124, 126-132, and 134-141 will be pending.

Rejection of claims under 35 U.S.C. § 103(a)

Claims 1, 4, 5, 7-14, 16, 121, 122, 124, 126 –132, and 124 –141 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Publication No. 2004/0250122 by Newton ("Newton") in view of U.S. Publication No. 2006/0212925 by Shull et al. ("Shull").

Independent Claims 1, 136, and 141

Claim 1 as amended recites, in part, "the metrics including a measure of the extent of, the frequency of, or the duration of compromise of the computer systems or data of the organization, or of a configuration or vulnerability of the organization, and a measure of the resilience of the organization to recover from a security breach or vulnerability, the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability." Independent claims 136 and 141 include similar limitations.

Briefly, Newton appears to describe a network intelligence database that use network information agents to gather information about individual networks (e.g., spam levels, hosted services, active security measures, etc.). See Newton at [0015], [0016], [0022], and [0031]. The network intelligence agents provide the gathered information to a network intelligence database, which may be accessed via a customer network security system. The network security system may then be used to secure a network based on the information collected by the network intelligence agents and stored in the database. Ibid. A Policy enforcer (PE) then translates conceptual rules for what networks may communicate with the customer's network into generic rules that are applied to all of the customer's devices. See id. at [0053] and [0055].

Nowhere does Newton teach or discuss resilience. Specifically, Newton is silent on the ability of the ratings to provide "a measure of the resilience of the organization to recover from a security breach or vulnerability, the measure of the resilience being inversely proportional to one or more of the duration of detected malicious activity and the duration of the vulnerability" as recited in independent claim 1 as amended, and as similarly recited in claims 136 and 141. It is advantageous to include the resiliency of an organization as a metric as it allows the user to evaluate an organization's preparedness for a security breach or other cyber-security threat. In practice, Applicants' invention provides users with actionable insights and ratings regarding an entity's capability to react to and recover from a cyber-security incident, whether it be an actual detected malicious act and/or the inherent system vulnerability exploited to cause the malicious act. An entity's resilience is a key metric when determining whether to do business with that entity.

Furthermore, because claims 4, 5, 7-14, 16, 121, 122, 124, 126 –132, 124-135, 137, and 140 depend from independent claim 1 and, therefore, include all of the limitations thereof, Applicant respectfully submits that dependent claims 4, 5, 7-14, 16, 121, 122, 124, 126 –132, 124-135, 137, and 140 are allowable as well, for at least the same reasons. Withdrawal of the grounds for rejection is respectfully requested.

Dependent Claim 137

The Office action cites to Shull in an attempt to show Shull teaches the use of confidence intervals when reporting a cyber-security score or rating. Neither the cited text, nor Shull generally teach providing such a confidence interval. As described in the office action, Shull "teaches giving an overall trust score between 1 and 5," meaning Shull teaches providing a single trust score of 1, or 2, or 3, or 4, or 5. See, Office action of May 5, 2016, at page 17. Selecting a number from a defined set is not analogous to providing a confidence range as recited in claim 137. Clearly, a range, such as 3 – 5, is different than a single value of, say, 4, and allows the user additional insights into the accuracy and confidence of the reported values. Shull does not contemplate such a feature.

CONCLUSION

In view of the foregoing, Applicant respectfully requests reconsideration, withdrawal of all grounds of rejection, and allowance of claims 1, 4, 5, 7-14, 16, 121, 122, 124, 126-132, and 134-141 in due course. The Examiner is invited to contact Applicant's undersigned representative by telephone at the number listed below to discuss any outstanding issues.

Dated: September 9, 2016

Respectfully submitted,

Electronic signature: /Joel E. Lehrer/
Joel E. Lehrer
Registration No.: 56,401
GOODWIN PROCTER LLP
100 Northern Avenue
Boston, Massachusetts 02210
(617) 570-1057
Attorney for Applicant

ACTIVE/87849703.2

Electronic Patent Application Fee Transmittal

Application Number:	13240572
Filing Date:	22-Sep-2011
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Filer:	Joel E. Lehrer/Tricia Ayube
Attorney Docket Number:	38879-0006001

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 3 months with $0 paid	2253	1	700	700
Miscellaneous:				
			Total in USD ($)	**700**

Electronic Acknowledgement Receipt

EFS ID:	26881316
Application Number:	13240572
International Application Number:	
Confirmation Number:	2423
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Customer Number:	26161
Filer:	Joel E. Lehrer/Tricia Ayube
Filer Authorized By:	Joel E. Lehrer
Attorney Docket Number:	38879-0006001
Receipt Date:	09-SEP-2016
Filing Date:	22-SEP-2011
Time Stamp:	16:31:02
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	CARD
Payment was successfully received in RAM	$700
RAM confirmation Number	091216INTEFSW16322900
Deposit Account	1096
Authorized User	Tricia Ayube

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Extension of Time	EOT.pdf	22889 2268e46d60a152d29fea8a41e9200ceafd86d197	no	1
Warnings:					
Information:					
2		Amendment_and_Response.pdf	41689 d489d4ce6d2e8c6bc1a22fa6dce688f3c5a82abd	yes	11

Multipart Description/PDF files in .zip description

Document Description	Start	End
Preliminary Amendment	1	1
Claims	2	8
Applicant Arguments/Remarks Made in an Amendment	9	11

Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30861 46cbcba96c288f70805b6949f6b0d312457f09c7	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	95439		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/22 (03-13)
Approved for use through 3/31/2013. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)	Docket Number (Optional) BST-004
Application Number 13/240,572-Conf. #2423	Filed September 22, 2011
For INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM	
Art Unit N/A	Examiner Not Yet Assigned

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above-identified application.

The requested extension and fee are as follows (check time period desired and enter the appropriate fee below):

	Fee	Small Entity Fee	Micro Entity Fee	
☐ One month (37 CFR 1.17(a)(1))	$200	$100	$50	$
☐ Two months (37 CFR 1.17(a)(2))	$600	$300	$150	$
☒ Three months (37 CFR 1.17(a)(3))	$1,400	$700	$350	$ 700.00
☐ Four months (37 CFR 1.17(a)(4))	$2,200	$1,100	$550	$
☐ Five months (37 CFR 1.17(a)(5))	$3,000	$1,500	$750	$

☐ Applicant asserts small entity status. See 37 CFR 1.27.

☐ Applicant certifies micro entity status. See 37 CFR 1.29.
Form PTO/SB/15A or B or equivalent must either be enclosed or have been submitted previously.

☐ A check in the amount of the fee is enclosed.

☒ Payment by credit card. Form PTO-2038 is attached.

☐ The Director has already been authorized to charge fees in this application to a Deposit Account.

☒ The Director is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 07-1700 .

☒ Payment made via EFS-Web.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the

☐ applicant/inventor.

☐ assignee of record of the entire interest. See 37 CFR 3.71. 37 CFR 3.73(b) statement is enclosed (Form PTO/SB/96).

☒ attorney or agent of record. Registration number 56,401 .

☐ attorney or agent acting under 37 CFR 1.34. Registration number _____ .

/Joel E. Lehrer/	September 9, 2016
Signature	Date
Joel E. Lehrer	(617) 570-1057
Typed or printed name	Telephone Number

NOTE: This form must be signed in accordance with 37 CFR 1.33. See 37 CFR 1.4 for signature requirements and certifications. Submit multiple forms if more than one signature is required, see below*.

☐ * Total of 1 forms are submitted.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/240,572	Filing Date 09/22/2011	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT **09/09/2016**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 30	Minus	** 31	= 0	X $40 =	0
Independent (37 CFR 1.16(h))	* 3	Minus	***3	= 0	X $210 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
HENRIETT K. DENDY

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/240,572	09/22/2011	Stephen Wayne Boyer	38879-0006001

CONFIRMATION NO. 2423

26161
FISH & RICHARDSON P.C. (BO)
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

PUBLICATION NOTICE

OC000000084368610

Title:INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM

Publication No.US-2016-0205126-A1
Publication Date:07/14/2016

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/240,572	09/22/2011	Stephen Wayne Boyer	38879-0006001

CONFIRMATION NO. 2423

26161
FISH & RICHARDSON P.C. (BO)
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

NONPUBLICATION RESCISSION LETTER



Date Mailed: 04/08/2016

Communication Regarding Rescission Of Nonpublication Request and/or Notice of Foreign Filing

Applicant's rescission of the previously-filed nonpublication request and/or notice of foreign filing is acknowledged. The paper has been reflected in the Patent and Trademark Office's (USPTO's) computer records so that the earliest possible projected publication date can be assigned.

The projected publication date is 07/14/2016.

If applicant rescinded the nonpublication request before or on the date of "foreign filing,"[1] then no notice of foreign filing is required.

If applicant foreign filed the application after filing the above application and before filing the rescission, and the rescission did not also include a notice of foreign filing, then a notice of foreign filing (not merely a rescission) is required to be filed within 45 days of the date of foreign filing. See 35 U.S.C. § 122(b)(2)(B)(iii), and Clarification of the United States Patent and Trademark Office's Interpretation of the Provisions of 35 U.S.C. § 122(b)(2)(B)(ii)-(iv), 1272 Off. Gaz. Pat. Office 22 (July 1, 2003).

If a notice of foreign filing is required and is not filed within 45 days of the date of foreign filing, then the application becomes abandoned pursuant to 35 U.S.C. § 122(b)(2)(B)(iii). In this situation, applicant should either file a petition to revive or notify the Office that the application is abandoned. See 37 CFR 1.137(f). Any such petition to revive will be forwarded to the Office of Petitions for a decision. Note that the filing of the petition will not operate to stay any period of reply that may be running against the application.

Questions regarding petitions to revive should be directed to the Office of Petitions at (571) 272-3282.

[1] Note, for purpose of this notice, that "foreign filing" means "filing an application directed to the same invention in another country, or under a multilateral international agreement, that requires publication of applications 18 months after filing".

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/byemane/

Substitute Disclosure Form	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. 38879-0006001	Application No. 13/240,572
Information Disclosure Statement by Applicant (Use several sheets if necessary)		Applicant Boyer et al.	
(37 CFR §1.98(b))		Filing Date September 22, 2011	Group Art Unit 2492

U.S. Patent Documents							
Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	1.	2012/0158725	06-2012	Molloy et al.			
	2.	2014/0204803	07-2014	Nguyen			
	3.	5,867,799	02-1999	Lang			
	4.	6,016,475	01-2000	Miller			
	5.	7,100,195	08-2006	Underwood			
	6.	2012/0166458	06-2012	Laudanski			
	7.	2005/0080720	04-2005	Betz			
	8.	2004/0221296	11-2004	Ogielski			
	9.	7,748,038	06-2010	Olivier			

Foreign Patent Documents or Published Foreign Patent Applications								
Examiner Initial	Desig. ID	Document Number	Publication Date	Country or Patent Office	Class	Subclass	Translation Yes	Translation No

Other Documents (include Author, Title, Date, and Place of Publication)		
Examiner Initial	Desig. ID	Document
	10.	PAIR transaction history of US application no. 14/021,585 and pending claims as of March 22, 2016.
	11.	PAIR transaction history of US application no. 14/944,484, application as filed and pending claims as of March 22, 2016.

Examiner Signature	Date Considered

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

RESCISSION OF PREVIOUS NONPUBLICATION REQUEST
(35 U.S.C. 122(b)(2)(B)(ii))
AND, IF APPLICABLE,
NOTICE OF FOREIGN FILING
(35 U.S.C. 122(b)(2)(B)(iii))

Send completed form to:
Mail Stop PG Pub
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450
FAX: (571) 273-8300

Application Number	13/240,572
Filing Date	September 22, 2011
First Named Inventor	Stephen Boyer
Title	Information Technology Security Assessment System
Atty Docket Number	38879-0006001
Art Unit	2492
Examiner	Simon P. Kanaan

A request that the above-identified application not be published under 35 U.S.C. 122(b) (nonpublication request) was included with the above-identified application on filing pursuant to 35 U.S.C 122(b)(2)(B)(i). I hereby **rescind** the previous nonpublication request.

If a notice of foreign or international filing is or will be required by 35 U.S.C. 122(b)(2)(B)(iii) and 37 CFR 1.213(c), I hereby provide such notice. This notice is being provided no later than forty-five (**45**) days after the date of such foreign or international filing.

*If a notice of subsequent foreign or international filing required by 35 U.S.C. 122(b)(2)(B)(iii) and 37 CFR 1.213(c) was not filed within forty-five (**45**) days after the date of filing of the foreign or international application, the application is ABANDONED, and a petition to revive under 37 CFR 1.137(b) is required. See 37 CFR 1.137(f).*

/David L. Feigenbaum/ — Signature
March 31, 2016 — Date

David L. Feigenbaum — Typed or printed name
30,378 — Registration Number, if applicable

(617) 542-5070
Telephone Number

This request must be signed in compliance with 37 CFR 1.33(b).

If information or assistance is needed in completing this form, please contact the Pre-Grant Publication Division at (703) 605-4283 or by e-mail at PGPub@USPTO.gov.

CERTIFICATE OF *MAILING* OR *TRANSMISSION*

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop PG Pub, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, or facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.

Signature			
Name (Print/Type)		Date	

23508139.doc

Electronic Patent Application Fee Transmittal

Application Number:	13240572
Filing Date:	22-Sep-2011
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Filer:	David L Feigenbaum
Attorney Docket Number:	38879-0006001

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	2806	1	90	90
		Total in USD ($)		**90**

Electronic Acknowledgement Receipt

EFS ID:	25363389
Application Number:	13240572
International Application Number:	
Confirmation Number:	2423
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Customer Number:	26161
Filer:	David L Feigenbaum
Filer Authorized By:	
Attorney Docket Number:	38879-0006001
Receipt Date:	31-MAR-2016
Filing Date:	22-SEP-2011
Time Stamp:	16:21:17
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$90
RAM confirmation Number	3214
Deposit Account	061050
Authorized User	FISH & RICHARDSON P C

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		6001-IDS-1449.pdf	132327 7d466a448dcbf6e3becd42aaecd5ae80bef7f170	yes	3
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Transmittal Letter		1	2	
	Information Disclosure Statement (IDS) Form (SB08)		3	3	
Warnings:					
Information:					
2	Non Patent Literature	6002-TH-PC-APP.pdf	869398 ee052e87a7e2497e460621441e87aae6c929ecf5	no	33
Warnings:					
Information:					
3	Rescind Nonpublication Request for Pre Grant Pub	6001-rescind.pdf	165749 50dcc7a1f326004e981dd5fc9ea9edf78fec8671	no	1
Warnings:					
Information:					
4	Non Patent Literature	4001-TH-.pdf	111418 af69019d5fc4eefe257fa7b4742c3d9ae7eb22bd	no	2
Warnings:					
Information:					
5	Fee Worksheet (SB06)	fee-info.pdf	30790 742469361fe5996a2aff535402d40f0ec56cdc50	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1309682		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor	:	Stephen Boyer	Art Unit	:	2492
Serial No.	:	13/240,572	Examiner	:	Simon P. Kanaan
Filed	:	September 22, 2011	Conf. No.	:	2423
Title	:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM			

MAIL STOP AMENDMENT
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT

Please consider the references listed on the attached PTO-1449 form.

A copy of the United States patent document will be provided upon request. Copies of all non-U.S. patent documents and other documents are enclosed.

The United States patent applications and/or patents listed below contain material related to material in this application. Copies of the applications and/or patents, their current claims (in the case of patents), and their transaction histories from the patent office public PAIR website are enclosed (or were provided previously with information disclosure statements identified in the table).

The applicant invites the examiner to consider the claims and claim amendments of these other applications and/or patents, and the positions of the examiners and the applicant that appear in their prosecution histories. The applicant understands that the examiner has direct access to these papers at the patent office, but will be happy to provide copies to the examiner upon request.

US serial number and filing date/ status	Examiner and group art unit	Is patent or application attached and listed on form 1449 and/or what is the date of a prior information disclosure statement with which it was submitted	In the case of an application, are claims attached or what is the date of a prior information disclosure statement with which they were submitted	Is current PAIR transaction history attached and listed on form 1449
61/386,156 9/24/2010 Expired	N/A	No	No	No – previously submitted on 10/8/15
61/492,287 6/1/2011 Issued	N/A	No	No	No - Unavailable in PAIR
14/021,585 9/9/2013 Pending	Omar R. Abdul-Ali GAU 2142	No – published application listed on 1449 form	Yes	Yes
14/944,484 11/18/15 Pending	Simon P. Kanaan GAU 2492	Yes	Yes	Yes

This statement is being filed after a first action on the merits, but before receipt of a final action or a notice of allowance. A late submission fee in the amount of $90, specified by 37 CFR §1.17(p), is being paid with this statement.

Apply any necessary charges or credits to deposit account 06-1050, referencing the above attorney docket number.

Please contact the undersigned if there are any questions regarding this Statement.

Respectfully submitted,

Date:/3/31/16/_____

/David L. Feigenbaum/_____
David L. Feigenbaum
Reg. No. 30,378

Customer Number 26161
Fish & Richardson P.C.
Telephone: (617) 542-5070
Facsimile: (877) 769-7945

23506691.doc

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/240,572	09/22/2011	Stephen Wayne Boyer	38879-0006001	2423

26161 7590 03/10/2016
FISH & RICHARDSON P.C. (BO)
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
KANAAN, SIMON P	

ART UNIT	PAPER NUMBER
2492	

NOTIFICATION DATE	DELIVERY MODE
03/10/2016	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATDOCTC@fr.com

Office Action Summary	Application No. 13/240,572	Applicant(s) BOYER ET AL.	
	Examiner SIMON KANAAN	Art Unit 2492	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *2/18/2016*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5)☒ Claim(s) *1,4,5,7-14,16,121,122,124,126-132 and 134-141* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1,4,5,7-14,16,121,122,124,126-132 and 134-141* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *9/22/2014* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date *10/8/2015*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions

2. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

Office Action Summary

3. Claims 1, 4, 5, 7-14, 16, 121, 122, 124, 126-132 and 134-141 are pending in the instant application.

4. Claims 1, 4, 5, 7-14, 16, 121, 122, 124, 126-132 and 134-141 are rejected (Claim Rejections - 35 USC § 103).

5. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 2/18/2016 has been entered.

6. Applicant's arguments/amendments filed 10/28/2015 have been considered but are not persuasive.

Applicant's Amendments and Examiner's Response

7. Applicant's arguments/amendments filed 10/28/2015 have been considered but are not persuasive. As for applicant's arguments,

a. Applicant argues that the cited prior art does not teach: rating "**an organization**".

However, the examiner disagrees as Newton [0007], teaches *"ones identity and hence ones reputation can hide behind a network address" and [0008], teaches "on a larger scale, such as a network, there is no way on knowing whom you are dealing with other than relying on anecdotal information", so a network is associated with an entity i.e. organization. Also [0011], teaches "University of XXX's student network, one of the most hostile networks in the world" i.e. a university which is an organization has a network associated with it so by computing the network score the score is for the organization. {0018], teaches " Organization type: educational, enterprise, military" [0019], teaches "Organization associations: owned by, partnered with whom" and [0023], teaches "Number of users, employees, people on this network;" so the network is itself an organization as it has associations, employees and even an address and contact information [0029]."* [0018]-[0020], teaches who organization is associated with, type of organization as well as number of employees, an entity having employees and is a type of an organization is an organization.

b. Applicant argues that the cited prior art does not teach "**organizations posing risks to themselves or to other parties through business relationships of the organizations with the other parties"**

However, the examiner disagrees as *(Newton [0030] teaches establishing a reputation for a network and [0011], teaches "risks associated with communicating with open university networks, or residential ISP networks" i.e. they are computing risk to determine whether to communicate with a network i.e. organization (see argument response to item a.).)*

c. Applicant *argues that the cited prior art does not teach "***and indicative of resiliencies of the organizations to recover from security breaches the information about each of the organizations being collected from two or more sources"**

However, the examiner disagrees as *(Newton, [0012] teaches that every network in the world would have a rating in the database, this rating as shown in [0013]-[0029], is comprised using multiple sources of information and would be indicative of how resilient a network is.*

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

> A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to

a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1, 4, 5, 7-14, 16, 121, 122, 124, 126-132 and 134-141 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chris Newton (US Pre-Grant Publication No: 2004/0250122 A1) hereinafter referred to as Newton in view of in view of Shull et al. (US Pre-Grant Publication No: 2006/0212925 A1) hereinafter referred to as Shull.

As per **claims 1 and 141**, Newton discloses a method comprising: **collecting information about two or more companies or other organizations, that have computer systems, network resources, and employees, the organizations posing risks to themselves or to other parties through business relationships of the organizations with the other parties, the information collected about the organizations being indicative of compromises or of vulnerabilities of technology systems, data, or other information of the organizations, and indicative of resiliencies of the organizations to recover from security breaches the information about each of the organizations being collected from two or more sources, one or more of the sources not being controlled by the organization, the information format least the one or more sources that are not controlled by the organization being collected without permission of the organization**, *(Newton, [0012] teaches that every network in the world would have a rating in the database and [0030] teaches establishing a reputation for a network, and [0031] teaches having multiple agents gathering data and [0044]-[0048] teaches different agent types i.e. different network characterization as each agent type gathers different type of data in*

regards to the security and reputation of network, among these agents include data mining internet which is public information and data mining newsgroups and forums which are also public knowledge and externally observable information not controlled by an organization and figure 1, items 24 include information about the network which towards the bottom of item 24 states "company info resources" i.e. network is associated with a company and [0022] and [0072], teaches taking into account size of the network and number of employees.)

at least one of the sources for each of the organizations comprising a public source or a commercial source, *(Newton, [0044]-[0048] and [0029], teaches information gathered externally from multiple sources including proxy information and data mining internet which is public information.)*

processing the information from the two or more sources for each of the organizations to form (A) security vulnerability of the organization (b) compromise of a technology system of the organization, (c) a resilience of the organization to recover from a security breach, the processing including applying models that account for differences in the respective sources, *(Newton, [0016], teaches "Hosted services (web servers, email servers)" and [0044]-[0048] and [0029], teaches information gathered externally from multiple sources including proxy information and data mining internet which is public information.)*

in connection with a assessing a business risk to the organization or to a party through a business relationship with at least one of the organizations, delivering a report of the composite ratings of the organizations through a

reporting facility to enable a user of the reporting facility to monitor, assess, and mitigate the risks, based on the security vulnerabilities and resiliencies, in doing business with the organization and to compare the composite ratings of the organizations. *(Newton, figure 3 item 14, teaches a database which stores information about the organizations i.e. portal.)*

But Newton does not **teach the composite rating comprising a composite of two or more of (a) security vulnerability of the organization, (b) of compromise of a technology system, data, or information of the organization: the forming of the composite rating for each of the organizations including (a) aggregating metrics associated with the computer system of the organization, the metrics including measures of the frequency of or durations of compromises of the computer system or the organization, and (b) taking account of positive information about the organization,**

However, *(Shull [0058] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score which informs requester of the trust of the entity, this score is received by the requester where activities are accounted for both legitimate (i.e. positive) and illegitimate (i.e. negative) and [0069] and [0073], teaches giving an overall trust score between 1 and 5 i.e. a normalized composite score where 1 is a reputable business and 5 is likely engaged in illicit activity.)*

It would have been obvious at the time of the invention for one of the ordinary skill in the art to modify the method of collecting security characteristics from multiple sources as taught by Newton by creating a score representative of the different collected data as taught by Shull because it would aid the requester in determining whether the entity is trusted or not.

As per **claim 4**, Newton in view of Shull discloses **the method of Claim 1, wherein the collected information is represented by at least two data types.** *(Newton, [0044]-[0048] teaches different agent types.)*

As per **claim 5**, Newton in view of Shull discloses the method of Claim 4, wherein the at least two data types include at least one of breach disclosures, block lists, configuration parameters, an identification of malware servers, an identification of a reputation, an identification of suspicious activity, an identification of spyware, white lists, an identification of compromised hosts, an identification of malicious activity, an identification of spam activity, an identification of vulnerable hosts, an identification of phishing activity, or an identification of e-mail viruses. *(Newton, [0013]-[0029] teaches security measures etc.)*

As per **claim 7**, Newton in view of Shull discloses **the method of Claim 1, wherein the collected information evidences internal security controls.** *(Newton, [0013]-[0029] teaches security measures etc.)*

As per **claim 8**, Newton in view of Shull discloses **the method of Claim 1, wherein the collected information comprises outcomes of each of the organizations.** *(Newton, [0013]-[0029] teaches security measures and [0044]-[0048] teaches checking for information already available to the public about network.)*

As per **claim 9**, Newton in view of Shull discloses **the method of Claim 1, wherein the collected information evidences operational execution of security measures of the organizations.** *(Newton, [0013]-[0029] teaches security measures.)*

As per **claim 10**, Newton in view of Shull **discloses the method of Claim 1, wherein the collected information indicates whether a computer system of the organizations served malicious code to another system.** *(Newton, [0013], teaches hostility level and page 4, claim 6, teaches spam levels.)*

As per **claim 11**, Newton in view of Shull discloses **the method of Claim 1, wherein the collected information indicates whether a computer system of the organizations communicated with a known attacker controlled network or sensor outside the control network of the organization**. *(Newton, [0013] teaches hostility level.)*

As per **claim 12**, Newton in view of Shull discloses **the method of Claim 1, comprising: forming a series of the security ratings of the organizations**. *(Newton, [0042], teaches live remote updates i.e. continually computing rating and page 4, claim 6 teaches security information has multiple ratings and [0041], teaches the different information having different weight.)*

As per **claim 13**, Newton in view of Shull discloses **the method of Claim 12, comprising determining a trend from the series of ratings.** *(Newton, [0042], teaches live remote updates i.e. continually computing rating.)*

As per **claim 14**, Newton in view of Shull discloses **the method of Claim 12, comprising displaying the series of composite ratings**. *(Newton, [0033], teaches a master database for collecting and storing the network ratings and page 4, claim 6 teaches security information has multiple ratings and [0041], teaches the different information having different weight and Shull, [0058], [0076] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score with informs requester of the trust of the entity, this score is received by the requester and a display device would display score as to help user determine whether to trust entity or not.)*

As per **claim 16**, Newton in view of Shull **teaches the method of Claim 14, wherein displaying the series of composite ratings for each of the organizations**

comprises posting the series of composite ratings for each of the organizations to a web portal. *(Newton, [0033], teaches a master database for collecting and storing the network ratings which includes information as listed in [0013]-[0029] which serve as warnings and Shull, [0058], [0076] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score with informs requester of the trust of the entity, this score is received by the requester and a display device would display score as to help user determine whether to trust entity or not.)*

As per **claim 121**, Newton in view of Shull teaches **the method of Claim 1, wherein the collected information represents externally observable outcome information**. - Newton, [0054], teaches agents getting information from news groups or sending packets and checking their responses.

As per **claim 122**, Newton in view of Shull teaches **the method of Claim 121, wherein the outcome information comprises outcome information associated with security vulnerability or resilience of each of the organizations.** *(Shull, [0058] and Newton, page 4, claim 6, both teach that the information is associated with entity security and Newton even looks into active security systems as well.)*

As per **claim 124**, Newton in view of Shull teaches **the method of Claim 1, comprising: determining a badness score that corresponds to an intensity or**

duration of malicious activity determined from the collected information.

(Newton, page 4, claim 6, teaches having spam levels etc. Which are a badness score.)

As per **claim 126**, Newton in view of Shull teaches **the method of Claim 1, wherein: the collected information comprises at least two security characterizations of a computer system of the entity.** *(Newton, page 4, claim 6, teaches checking open proxy servers and desktop security measures which are multiple characterizations of a system of the entity.)*

As per **claim 127**, Newton in view of Shull teaches **the method of Claim 1, wherein the collected information comprises a characterization of behavior of an employee of at least one of the organizations.** *(Newton, page 4, claim 6, inappropriate content served, spam levels, language spoken, geographic placement, industry, which are characterizations of employees in the network and the employees' behavior.)*

As per **claim 128**, Newton in view of Shull teaches **the method of Claim 1, wherein the collected information comprises characterizations other than characterizations about a computer system of at least one of the organizations.** *(Newton, page 4, claim 6, teaches security characterization includes security personnel.)*

As per **claim 129**, Newton in view of Shull teaches **the method of Claim 1, wherein the collected information comprises characterizations about policies of at least one of the organizations.** *(Newton, page 4, claim 6, teaches organization association, active security measures, desktop security measures, etc. which are policies see also [0059] and [0060].)*

As per **claim 130**, Newton in view of Shull teaches **the method of Claim 1, wherein the collected information comprises characterizations about information technology assets that at least one of the organizations owns, controls, uses, or is affiliated with.** *(Newton, page 4, claim 6, teaches organization associations see also [0043] and [0053].)*

As per **claim 131**, Newton in view of Shull **teaches the method of Claim 1 in which collected information represents: (a) physical states, (b) technical states, (c) organizational states, or (d) cultural states of at least one of the organizations which can be exploited to create a security breach; or (e) the organization's ability to recover from a security breach; or any combination of two or more of these.** *(Newton, page 4, claim 6, teaches active security measures and desktop security measures among other information collected about the organization.)*

As per claim 132, Newton in view of Shull teaches **the method of claim 1 in which processing the information to form a composite rating comprises**

correlating data across the sources of information. *(Shull, [0058], teaches creating a score based on the different data received i.e. correlating the different data.)*

As per claim 134, Newton in view of Shull **teaches the method of claim 1 in which processing the information to form a composite rating comprises statistically correlating the composite rating with actual outcomes.** *(Newton, [0041], teaches giving different information different weight where less weight given to information as it becomes less important over time which is a statistical correlation with the information collected.)*

As per claim 135, Newton in view of Shull **teaches the method of claim 1 in which the vulnerability comprises physical, technical, organizational, or cultural states that can be exploited to create a security breach.** *(Newton, figure 1, item 24 and page 4, claim 6.)*

As **per claim 136**, Newton teaches **a method comprising collecting, from at least two sources, information about two or more companies or other organizations, the collected information representing at least two data types, the collected information comprising outcomes of each of the organizations, at least some of the information for each of the organizations being collected automatically by computer from at least two sources, one or more of the sources not controlled by the organization, the information from at least the one or more**

sources that are not controlled by the organization being collected without permission of the-organization, at least one of the sources including a commercial data source, *(Newton, [0012] teaches that every network in the world would have a rating in the database and [0030] teaches establishing a reputation for a network, and [0031] teaches having multiple agents gathering data and [0044]-[0048] teaches different agent types i.e. different network characterization as each agent type gathers different type of data in regards to the security and reputation of network, among these agents include data mining internet which is public information and data mining newsgroups and forums which are also public knowledge and externally observable information not controlled by an organization and figure 1, items 24 include information about the network which towards the bottom of item 24 states "company info resources" i.e. network is associated with a company, and [0022] and [0072], teaches taking into account size of the network and number of employees.)*

at least partly automatically gathering information about assets that each of the organizations owns, controls, uses, or is affiliated with, including IP network address ranges, computer services residing within address ranges, or domain names, *(Newton, [0029] teaches "Address, contact information." And [0019] teaches "Organization associations: owned by, partnered with whom")*

and displaying the series of ratings through a portal and reporting the ratings of the organizations through a portal to enable customers to monitor, assess, and mitigate risk in doing business with the organizations and to

compare the composite ratings across the organizations. *(Newton, figure 3 item 14, teaches a database which stores information about the organizations i.e. portal.)*

But Newton does not **teach processing by computer the information from both of the two sources for each of the organizations to form a composite rating of the organization of a security vulnerability of the organization to creation of a security breach or a compromise of a system of the organization or of a resilience of the organization to recover from a security breach or both, the processing including applying models that account for differences in the respective sources, normalizing the composite rating of each of the organizations based on a size characteristic of the organization to enable comparisons of composite ratings between the two or more organizations, forming a series of the security ratings of each of the organizations, determining a trend from the series of ratings, determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information.**

However, *(Shull [0058] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score which informs requester of the trust of the entity, this score is received by the requester where activities are accounted for both legitimate (i.e. positive) and illegitimate (i.e. negative) and [0069] and [0073], teaches giving an overall trust score between 1 and 5 i.e. a normalized composite score where 1 is a reputable business and 5 is likely engaged in illicit activity.)*

It would have been obvious at the time of the invention for one of the ordinary skill in the art to modify the method of collecting security characteristics from multiple sources as taught by Newton by creating a score representative of the different collected data as taught by Shull because it would aid the requester in determining whether the entity is trusted or not.

As per **claim 137**, Newton in view of Shull **teaches the method of claim 1, determining a confidence range of the composite rating, the size of the range varying inversely with the level of confidence in the composite rating.** *(Shull, [0069] and [0073], teaches giving an overall trust score between 1 and 5 i.e. a normalized composite score where 1 is a reputable business and 5 is likely engaged in illicit activity.)*

As per **claim 138**, Newton in view of Shull **teaches the system of claim 137, wherein the confidence range is based on redundancy of the security characterizations.** *(Shull, [0081], teaches taking into account consistency which is redundancy.)*

As per **claim 139**, Newton in view of Shull teaches **the method of claim 137, wherein the confidence range is based on a size of the third party computer system.** *(Newton, [0072], teaches taking into account size of the network.)*

As per **claim 140**, Newton in view of Shull teaches **the method of claim 1 comprising ranking the organization and other organizations within sectors or peer-groups or globally.** *(Shull, [0123]-[0124], teaches listing entities with similar scores together such as ones that scored a 3 or 4 so these would be ranked below ones which were listed as part of white list which ranked 1 or 2, see [0068], which teaches having white list, black list and grey lists.)*

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Simon Kanaan whose telephone number is (571)270-3906. The examiner can normally be reached on Mon-Thurs 7:30-5:00 EST.

If attempts to reach the above noted Examiner by telephone are unsuccessful, the Examiner's supervisor, Saleh Najjar, can be reached at the following telephone number: (571) 272-4006.

The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.

/S. K./
Examiner, Art Unit 2432

/SALEH NAJJAR/
Supervisory Patent Examiner, Art Unit 2492

Notice of References Cited	Application/Control No. 13/240,572	Applicant(s)/Patent Under Reexamination BOYER ET AL.	
	Examiner SIMON KANAAN	Art Unit 2492	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	CPC Classification	US Classification
*	A	US-2008/0140495 A1	06-2008	Bhamidipaty; Anuradha	G06Q10/00	705/7.12
*	B	US-2012/0166458 A1	06-2012	Laudanski; Paul	H04L51/12	707/755
	C	US-				
	D	US-				
	E	US-				
	F	US-				
	G	US-				
	H	US-				
	I	US-				
	J	US-				
	K	US-				
	L	US-				
	M	US-				

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	CPC Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Substitute Disclosure Form / U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No.	Application No.
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))	38879-0006001	13/240,572
	Applicant: Boyer et al.	
	Filing Date: September 22, 2011	Group Art Unit: 2432

U.S. Patent Documents

Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	1.	2015/0074579	3-2015	Gladstone et al			

Foreign Patent Documents or Published Foreign Patent Applications

Examiner Initial	Desig. ID	Document Number	Publication Date	Country or Patent Office	Class	Subclass	Translation Yes	Translation No

Other Documents (include Author, Title, Date, and Place of Publication)

Examiner Initial	Desig. ID	Document
	2.	PAIR transaction history of US application no. 14/021,585 as of October 7, 2015 and application as filed.
	3.	PAIR transaction history of US application no. 61/386,156 as of October 7, 2015.

Examiner Signature	Date Considered
/Simon Kanaan/	03/07/2016

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /S.K./

Black Lotus Ex. 1002, Page 552 of 1060

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	**Art Unit**
	SIMON KANAAN	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/18/2013	11/07/2013	06/04/2014	02/22/2015	05/28/2015	09/25/2015	03/07/2016		
	1	✓	✓	✓	✓	✓	✓	✓		
	2	✓	✓	-	-	-	-	-		
	3	✓	✓	✓	✓	✓	-	-		
	4	✓	✓	✓	✓	✓	✓	✓		
	5	✓	✓	✓	✓	✓	✓	✓		
	6	✓	✓	-	-	-	-	-		
	7	✓	✓	✓	✓	✓	✓	✓		
	8	✓	✓	✓	✓	✓	✓	✓		
	9	✓	✓	✓	✓	✓	✓	✓		
	10	✓	✓	✓	✓	✓	✓	✓		
	11	✓	✓	✓	✓	✓	✓	✓		
	12	✓	✓	✓	✓	✓	✓	✓		
	13	✓	✓	✓	✓	✓	✓	✓		
	14	✓	✓	✓	✓	✓	✓	✓		
	15	✓	✓	-	-	-	-	-		
	16	✓	✓	✓	✓	✓	✓	✓		
	17	✓	✓	-	-	-	-	-		
	18	✓	✓	-	-	-	-	-		
	19	✓	✓	-	-	-	-	-		
	20	✓	✓	-	-	-	-	-		
	21	-	-	-	-	-	-	-		
	22	-	-	-	-	-	-	-		
	23	-	-	-	-	-	-	-		
	24	-	-	-	-	-	-	-		
	25	-	-	-	-	-	-	-		
	26	-	-	-	-	-	-	-		
	27	-	-	-	-	-	-	-		
	28	-	-	-	-	-	-	-		
	29	-	-	-	-	-	-	-		
	30	-	-	-	-	-	-	-		
	31	-	-	-	-	-	-	-		
	32	-	-	-	-	-	-	-		
	33	-	-	-	-	-	-	-		
	34	-	-	-	-	-	-	-		
	35	-	-	-	-	-	-	-		
	36	-	-	-	-	-	-	-		

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	**Art Unit**
	SIMON KANAAN	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/18/2013	11/07/2013	06/04/2014	02/22/2015	05/28/2015	09/25/2015	03/07/2016		
	37	-	-	-	-	-	-	-		
	38	-	-	-	-	-	-	-		
	39	-	-	-	-	-	-	-		
	40	-	-	-	-	-	-	-		
	41	-	-	-	-	-	-	-		
	42	-	-	-	-	-	-	-		
	43	-	-	-	-	-	-	-		
	44	-	-	-	-	-	-	-		
	45	-	-	-	-	-	-	-		
	46	-	-	-	-	-	-	-		
	47	-	-	-	-	-	-	-		
	48	-	-	-	-	-	-	-		
	49	-	-	-	-	-	-	-		
	50	-	-	-	-	-	-	-		
	51	-	-	-	-	-	-	-		
	52	-	-	-	-	-	-	-		
	53	-	-	-	-	-	-	-		
	54	-	-	-	-	-	-	-		
	55	-	-	-	-	-	-	-		
	56	-	-	-	-	-	-	-		
	57	-	-	-	-	-	-	-		
	58	-	-	-	-	-	-	-		
	59	-	-	-	-	-	-	-		
	60	-	-	-	-	-	-	-		
	61	-	-	-	-	-	-	-		
	62	-	-	-	-	-	-	-		
	63	-	-	-	-	-	-	-		
	64	-	-	-	-	-	-	-		
	65	-	-	-	-	-	-	-		
	66	-	-	-	-	-	-	-		
	67	-	-	-	-	-	-	-		
	68	-	-	-	-	-	-	-		
	69	-	-	-	-	-	-	-		
	70	-	-	-	-	-	-	-		
	71	-	-	-	-	-	-	-		
	72	-	-	-	-	-	-	-		

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	**Art Unit**
	SIMON KANAAN	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/18/2013	11/07/2013	06/04/2014	02/22/2015	05/28/2015	09/25/2015	03/07/2016		
	73	-	-	-	-	-	-	-		
	74	-	-	-	-	-	-	-		
	75	-	-	-	-	-	-	-		
	76	-	-	-	-	-	-	-		
	77	-	-	-	-	-	-	-		
	78	-	-	-	-	-	-	-		
	79	-	-	-	-	-	-	-		
	80	-	-	-	-	-	-	-		
	81	-	-	-	-	-	-	-		
	82	-	-	-	-	-	-	-		
	83	-	-	-	-	-	-	-		
	84	-	-	-	-	-	-	-		
	85	-	-	-	-	-	-	-		
	86	-	-	-	-	-	-	-		
	87	-	-	-	-	-	-	-		
	88	-	-	-	-	-	-	-		
	89	-	-	-	-	-	-	-		
	90	-	-	-	-	-	-	-		
	91	-	-	-	-	-	-	-		
	92	-	-	-	-	-	-	-		
	93	-	-	-	-	-	-	-		
	94	-	-	-	-	-	-	-		
	95	-	-	-	-	-	-	-		
	96	-	-	-	-	-	-	-		
	97	-	-	-	-	-	-	-		
	98	-	-	-	-	-	-	-		
	99	-	-	-	-	-	-	-		
	100	-	-	-	-	-	-	-		
	101	-	-	-	-	-	-	-		
	102	-	-	-	-	-	-	-		
	103	-	-	-	-	-	-	-		
	104	-	-	-	-	-	-	-		
	105	-	-	-	-	-	-	-		
	106	-	-	-	-	-	-	-		
	107	-	-	-	-	-	-	-		
	108	-	-	-	-	-	-	-		

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	**Art Unit**
	SIMON KANAAN	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/18/2013	11/07/2013	06/04/2014	02/22/2015	05/28/2015	09/25/2015	03/07/2016		
	109	-	-	-	-	-	-	-		
	110	-	-	-	-	-	-	-		
	111	-	-	-	-	-	-	-		
	112	-	-	-	-	-	-	-		
	113	-	-	-	-	-	-	-		
	114	-	-	-	-	-	-	-		
	115	-	-	-	-	-	-	-		
	116	-	-	-	-	-	-	-		
	117	-	-	-	-	-	-	-		
	118	-	-	-	-	-	-	-		
	119	-	-	-	-	-	-	-		
	120	-	-	-	-	-	-	-		
	121			✓	✓	✓	✓	✓		
	122			✓	✓	✓	✓	✓		
	123			✓	✓	✓	-	-		
	124			✓	✓	✓	✓	✓		
	125			✓	-	-	-	-		
	126			✓	✓	✓	✓	✓		
	127			✓	✓	✓	✓	✓		
	128			✓	✓	✓	✓	✓		
	129			✓	✓	✓	✓	✓		
	130			✓	✓	✓	✓	✓		
	131			✓	✓	✓	✓	✓		
	132			✓	✓	✓	✓	✓		
	133			✓	-	-	-	-		
	134			✓	✓	✓	✓	✓		
	135			✓	✓	✓	✓	✓		
	136				✓	✓	✓	✓		
	137				✓	✓	✓	✓		
	138				✓	✓	✓	✓		
	139				✓	✓	✓	✓		
	140				✓	✓	✓	✓		
	141							✓		

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	Art Unit
	SIMON KANAAN	2432

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor and Assignee Search (PALM)	4/18/2013	SK
class/subclass search + text (EAST: 726/1,2,22,25+text)	3/7/2016	SK
CPC + text (EAST: H04L63/20,145,14,0236,1433,104 OR H04L67/306 OR H04L51/12 OR H04L61/1511 OR H04L9/321 OR G06F21/00,577 + text)	3/7/2016	SK

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/SIMON KANAAN/ Examiner.Art Unit 2432	

Electronic Patent Application Fee Transmittal

Application Number:	13240572
Filing Date:	22-Sep-2011
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Filer:	David L Feigenbaum/jennifer franco
Attorney Docket Number:	38879-0006001

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 1 month with $0 paid	2251	1	100	100
Miscellaneous:				
			Total in USD ($)	**100**

Electronic Acknowledgement Receipt

EFS ID:	24961152
Application Number:	13240572
International Application Number:	
Confirmation Number:	2423
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Customer Number:	26161
Filer:	David L Feigenbaum/jennifer franco
Filer Authorized By:	David L Feigenbaum
Attorney Docket Number:	38879-0006001
Receipt Date:	19-FEB-2016
Filing Date:	22-SEP-2011
Time Stamp:	11:31:06
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$100
RAM confirmation Number	8911
Deposit Account	061050
Authorized User	FISH & RICHARDSON P C

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Fee Worksheet (SB06)	fee-info.pdf	31182 befbe5468ef4708a5fdb00a480d6aa739ac62b30	no	2

Warnings:	
Information:	
Total Files Size (in bytes):	31182

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/30 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995. no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Request for Continued Examination (RCE) Transmittal

Address to:
Mail Stop RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Application Number	13/240,572
Filing Date	September 22, 2011
First Named Inventor	Stephen Boyer
Art Unit	2492
Examiner Name	Simon P. Kanaan
Attorney Docket Number	38879-0006001

This is a Request for Continued Examination (RCE) under 37 CFR 1 .114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. See Instruction Sheet for RCEs (not to be submitted to the USPTO) on page 2.

1. Submission required under 37 CFR 1.114 Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

   a. ☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

      i. ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

      ii. ☐ Other _____

   b. ☐ Enclosed

      i. ☐ Amendment/Reply

      ii. ☐ Affidavit(s)/ Declaration(s)

      iii. ☐ Information Disclosure Statement (IDS)

      iv. ☐ Other _____

2. Miscellaneous

   Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a

   a. ☐ period of _____ months. (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

   b. ☐ Other _____

3. Fees The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.
   The Director is hereby authorized to charge the following fees any underpayment of fees or credit any overpayments to

   a. ☒ Deposit Account No. 06-1050 .

      i. ☒ RCE fee required under 37 CFR 1.17(e)

      ii ☐ Extension of time fee (37 CFR 1.136 and 1.17)

      iii ☒ Other any deficiencies

   b. ☐ Check in the amount of $ _____ enclosed

   c. ☐ Payment by credit card (Form PTO-2038 enclosed)

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Signature	/David L. Feigenbaum/	Date	February 18, 2016
Name (Print/Type)	David L. Feigenbaum	Registration No.	30,378

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop RCE, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450 or facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.

Signature			
Name (Print/Type)		Date	

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

American LegalNet, Inc.
www.FormsWorkFlow.com

Electronic Patent Application Fee Transmittal

Application Number:	13240572
Filing Date:	22-Sep-2011
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Filer:	David L Feigenbaum/jennifer franco
Attorney Docket Number:	38879-0006001

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
RCE- 2nd and Subsequent Request	2820	1	850	850
		Total in USD ($)		**850**

Electronic Acknowledgement Receipt

EFS ID:	24946473
Application Number:	13240572
International Application Number:	
Confirmation Number:	2423
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Customer Number:	26161
Filer:	David L Feigenbaum/jennifer franco
Filer Authorized By:	David L Feigenbaum
Attorney Docket Number:	38879-0006001
Receipt Date:	18-FEB-2016
Filing Date:	22-SEP-2011
Time Stamp:	11:06:49
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$850
RAM confirmation Number	11458
Deposit Account	061050
Authorized User	FISH & RICHARDSON P C

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	RCE.pdf	143861 91ab9e03c11ff38c3e8a4ec2121d792634fa5a49	no	1
Warnings:					
This is not a USPTO supplied RCE SB30 form.					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	31030 3f64285e5238eefb790ada78578052916e2b1837	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	174891		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/240,572	09/22/2011	Stephen Wayne Boyer	38879-0006001	2423

26161 7590 02/12/2016
FISH & RICHARDSON P.C. (BO)
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
KANAAN, SIMON P	

ART UNIT	PAPER NUMBER
2492	

NOTIFICATION DATE	DELIVERY MODE
02/12/2016	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATDOCTC@fr.com

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 13/240,572	**Applicant(s)** BOYER ET AL.	
	Examiner SIMON KANAAN	**Art Unit** 2492	**AIA (First Inventor to File) Status** No

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 28 December 2015 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

NO NOTICE OF APPEAL FILED

1. ☒ The reply was filed after a final rejection. No Notice of Appeal has been filed. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance;

(2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114 if this is a utility or plant application. Note that RCEs are not permitted in design applications. The reply must be filed within one of the following time periods:

a) ☒ The period for reply expires *3* months from the mailing date of the final rejection.

b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action; or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

c) ☐ A prior Advisory Action was mailed more than 3 months after the mailing date of the final rejection in response to a first after-final reply filed within 2 months of the mailing date of the final rejection. The current period for reply expires months from the mailing date of *the prior Advisory Action* or SIX MONTHS from the mailing date of the final rejection, whichever is earlier.

Examiner Note: If box 1 is checked, check either box (a), (b) or (c). ONLY CHECK BOX (b) WHEN THIS ADVISORY ACTION IS THE FIRST RESPONSE TO APPLICANT'S FIRST AFTER-FINAL REPLY WHICH WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. ONLY CHECK BOX (c) IN THE LIMITED SITUATION SET FORTH UNDER BOX (c). See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) or (c) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☒ The proposed amendments filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   a) ☒ They raise new issues that would require further consideration and/or search (see NOTE below);
   b) ☐ They raise the issue of new matter (see NOTE below);
   c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.
   NOTE: *See Continuation Sheet*. (See 37 CFR 1.116 and 41.33(a)).

4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).

5. ☐ Applicant's reply has overcome the following rejection(s): _____.

6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

7. ☒ For purposes of appeal, the proposed amendment(s): (a) ☒ will not be entered, or (b) ☐ will be entered, and an explanation of how the new or amended claims would be rejected is provided below or appended.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

9. ☐ The affidavit or other evidence filed after final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).

10. ☐ The affidavit or other evidence filed after the date of filing the Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).

11. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

12. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because:
Applicants amendments to independent claim 1 and newly added independent claim 141 raise new issues which require further search and consideration .

13. ☐ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____

14. ☐ Other: _____.

STATUS OF CLAIMS

15. The status of the claim(s) is (or will be) as follows:
Claim(s) allowed: .
Claim(s) objected to: .
Claim(s) rejected: 1,4,5,7-14,16,40,121,122,124,126-132 and 134.
Claim(s) withdrawn from consideration: .

/SALEH NAJJAR/ Supervisory Patent Examiner, Art Unit 2492	/SIMON KANAAN/ Examiner, Art Unit 2492

Continuation of 3. NOTE: Applicants amendments to independent claim 1 and newly added independent claim 141 raise new issues which require further search and consideration .

OPAP AKIMA-18
DEC 2 8 2015
PATENT & TRADEMARK OFFICE

Attorney Docket No.: 38879-0006001

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor	:	Stephen Boyer	Art Unit	:	2492
Serial No.	:	13/240,572	Examiner	:	Simon P. Kanaan
Filed	:	September 22, 2011	Conf. No.	:	2423

Title : INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM

MAIL STOP AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY TO ACTION DATED OCTOBER 26, 2015 AND INTERVIEW SUMMARY

DO NOT ENTER: /S.K./
02/07/2016

CERTIFICATE OF (A) MAILING BY FIRST CLASS MAIL OR (B) TRANSMISSION
I hereby certify under 37 CFR §1.8(a) that this correspondence is either (A) addressed as set out in 37 CFR §1.1(a) and being deposited with the United States Postal Service as first class mail with sufficient postage, or (B) being transmitted by facsimile in accordance with 37 CFR § 1.6(d) or via the Office electronic filing system in accordance with 37 CFR § 1.6(a)(4), on the date indicated below.

December 23, 2015
Date of Deposit or Transmission

Apply S signature
Signature

Lesley P. Arciniega
Typed or Printed Name of Person Signing Certificate

OPAP AKIMA-18
DEC 2 8 2015
PATENT & TRADEMARK OFFICE

Attorney Docket No.: 38879-0006001

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor	:	Stephen Boyer	Art Unit	:	2492
Serial No.	:	13/240,572	Examiner	:	Simon P. Kanaan
Filed	:	September 22, 2011	Conf. No.	:	2423

Title : INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM

MAIL STOP AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY TO ACTION DATED OCTOBER 26, 2015 AND INTERVIEW SUMMARY

CERTIFICATE OF (A) MAILING BY FIRST CLASS MAIL OR (B) TRANSMISSION
I hereby certify under 37 CFR §1.8(a) that this correspondence is either (A) addressed as set out in 37 CFR §1.1(a) and being deposited with the United States Postal Service as first class mail with sufficient postage, or (B) being transmitted by facsimile in accordance with 37 CFR § 1.6(d) or via the Office electronic filing system in accordance with 37 CFR § 1.6(a)(4), on the date indicated below.

December 23, 2015
Date of Deposit or Transmission

Apply S signature
Signature

Lesley P. Arciniega
Typed or Printed Name of Person Signing Certificate

List of claims (replacing prior versions):

1. (currently amended) A method comprising:

collecting information about two or more companies or other organizations that have computer systems, network resources, and employees, the organizations posing risks to themselves or to other parties through business relationships of the organizations with the other parties, the information collected about the organizations being indicative of compromises or ~~indicative~~ of vulnerabilities of technology systems, data, or other information of the organizations, ~~or~~ and indicative of resiliencies of the organizations to recover from security breaches including compromises or vulnerabilities or configurations,

at least some of the information about each of the organizations being collected automatically by computer using sensors on the Internet,

the information about each of the organizations being collected from two or more sources, one or more of the sources not being controlled by the organization, the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization,

at least partly automatically gathering information about assets that each of the organizations owns, controls, uses, or is affiliated with, including IP network address ranges, computer services residing within address ranges, or domain names,

at least one of the sources for each of the organizations comprising a public source or a commercial source,

processing by computer the information from the two or more sources for each of the organizations to form a composite rating of the organization that is indicative of a degree of risk to the organization or to a party through a business relationship with the organization, the composite rating comprising a calculated composite of metrics and data derived or collected from the sources, the processing comprising applying transformations to the data and metrics, and the processing comprising applying weights to the data and the metrics,

the metrics including a measure of the extent of or the frequency of or duration of compromise of the computer systems or data of the organization, or of a configuration or

vulnerability of the organization, ~~or~~ and a measure of the resilience of the organization to recover from a security breach or vulnerability, and

in connection with ~~a~~ assessing a business risk to the organization or to a party through a business relationship with ~~or with~~ at least one of the organizations, delivering a report of the composite ratings of the organizations through a reporting facility to enable a user of the reporting facility to monitor, assess, and mitigate the risks, based on the security vulnerabilities ~~or~~ and resiliencies ~~or both~~, in doing business with the organization and to compare the composite ratings of the organizations.

2. (canceled)

3. (canceled)

4. (previously presented) The method of claim 1, wherein the collected information is represented by at least two data types.

5. (previously presented) The method of claim 4, wherein the at least two data types include at least one of breach disclosures, block lists, configuration parameters, an identification of malware servers, an identification of a reputation, an identification of suspicious activity, an identification of spyware, white lists, an identification of compromised hosts, an identification of malicious activity, an identification of spam activity, an identification of vulnerable hosts, an identification of phishing activity, or an identification of e-mail viruses.

6. (canceled)

7. (previously presented) The method of claim 1, wherein the collected information evidences internal security controls.

8. (previously presented) The method of claim 1, wherein the collected information comprises outcomes of each of the organizations.

9. (previously presented) The method of claim 1, wherein the collected information evidences operational execution of security measures of each of the organizations.

10. (previously presented) The method of claim 1, wherein the collected information indicates whether a computer system of each of the organizations served malicious code to another system.

11. (previously presented) The method of claim 1, wherein the collected information indicates whether a computer system of each of the organizations communicated with a known attacker controlled network or sensor outside the control or network of the organization.

12. (previously presented) The method of claim 1, comprising:
forming a series of the security ratings of each of the organizations.

13. (previously presented) The method of claim 12, comprising:
determining a trend from the series of ratings.

14. (previously presented) The method of claim 12, comprising:
displaying the series of composite ratings.

15. (canceled)

16. (previously presented) The method of claim 14, wherein displaying the series of composite ratings for each of the organizations comprises posting the series of composite ratings for the organization to a web portal.

17. (canceled)

18. (canceled)

19-120. (canceled)

121. (previously presented) The method of claim 1, wherein the collected information represents externally observable outcome information.

122. (previously presented) The method of claim 121, wherein the outcome information comprises outcome information associated with security vulnerability or resilience of each of the organizations.

123. (canceled)

124. (previously presented) The method of claim 1, comprising:

determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information.

125. (canceled)

126. (previously presented) The method of claim 1, wherein:

the collected information comprises at least two security characterizations of a computer system of each of the organizations.

127. (previously presented) The method of claim 1, wherein the collected information comprises a characterization of behavior of an employee of at least one of the organizations.

128. (previously presented) The method of claim 1, wherein the collected information comprises characterizations other than characterizations about a computer system of at least one of the organizations.

129. (previously presented) The method of claim 1, wherein the collected information comprises characterizations about policies of at least one of the organizations.

130. (previously presented) The method of claim 1, wherein the collected information comprises characterizations about information technology assets that at least one of the organizations owns, controls, uses, or is affiliated with.

131. (previously presented) The method of claim 1 in which collected information represents: (a) physical states, (b) technical states, (c) organizational states, or (d) cultural states of at least one of the organizations which can be exploited to create a security breach; or (e) the organization's ability to recover from a security breach; or any combination of two or more of these.

132. (previously presented) The method of claim 1 in which processing the information to form a composite rating comprises correlating data across the sources of information.

133. (canceled)

134. (previously presented) The method of claim 1 in which processing the information to form a composite rating comprises statistically correlating the composite rating with actual outcomes.

135. (previously presented) The method of claim 1 in which the vulnerability comprises physical, technical, organizational, or cultural states that can be exploited to create a security breach.

136. (previously presented) A method comprising

collecting, from at least two sources, information about two or more companies or other organizations, the collected information representing at least two data types, the collected information comprising outcomes of each of the organizations,

at least some of the information for each of the organizations being collected automatically by computer from at least two sources, one or more of the sources not controlled by the organization,

the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization, at least one of the sources including a commercial data source,

processing the information from both of the two sources for each of the organizations to form a composite rating of a security vulnerability of the organization to creation of a security breach or a compromise of a system of the organization or of a resilience of the organization to recover from a security breach or both, the processing including applying models that account for differences in the respective sources,

normalizing the composite rating of each of the organizations based on a size characteristic of the organization to enable comparisons of composite ratings between the two or more organizations,

forming a series of the security ratings of each of the organizations, determining a trend from the series of ratings, and displaying the series of composite ratings through a portal,

determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information, and

reporting the composite ratings of the organizations through a portal to enable customers to monitor, assess, and mitigate risk in doing business with the organizations and to compare the composite ratings across the organizations.

137. (previously presented) The system of claim 1, determining a confidence range of the composite rating, the size of the range varying inversely with the level of confidence in the composite rating.

138. (previously presented) The system of claim 137, wherein the confidence range is based on redundancy of the security characterizations.

139. (previously presented) The system of claim 137, wherein the confidence range is based on a size of the third party computer system.

140. (previously presented) The method of claim 1 comprising ranking the organization and other organizations within sectors or peer-groups or globally.

141. (new) A method comprising:

collecting information about an organization that has computer systems, network resources, and employees, the organization posing risks to itself or to other parties through business relationships of the organization with the other parties,

the information collected about the organization including (a) information collected automatically by computer on the Internet without permission of the organization, and (b) information indicative of resiliencies of the organization to recover from a security breach associated with a compromise or a vulnerability or a configuration,

processing the information by computer to form a composite rating of the organization that is indicative of a degree of risk to the organization or to a party through a business relationship with the organization, the composite rating being based on metrics that include a measure of the resiliencies of the organization to recover from a security breach associated with a compromise or a vulnerability or a configuration, and

in connection with assessing a business risk to the organization or to a party through a business relationship with the organization, delivering a report of the composite rating of the organization through a reporting facility to enable a user of the reporting facility to assess the risks, based at least in part on the resiliencies, in doing business with the organization.

INTERVIEW SUMMARY

The applicant thanks the examiner for the telephone interview on September 24, 2015, that included Examiner Samson Lemma, the inventor Stephen Boyer, and the undersigned. The interview included a discussion of claim 1, possible amendments to claim 1, and the patentability of the claims with respect to the Newton and Shull references.

REMARKS

The comments of the applicant below are each preceded by related comments of the examiner (in small, bold type).

> **6. ... applicant argues that the cited prior art does not teach:**
>
> **a. giving an organization a composite score stating that the score calculated in Newton is for a network, however the examiner respectfully disagrees as Newton [0018]-[0020], teaches who organization is associated with, type of organization as well as number of employees, an entity having employees and is a type of an organization is an organization.**

The applicant respectfully continues to disagree. Amended claim 1 requires the forming of a "composite rating". The composite rating is not just any composite rating, but rather a composite rating of "the organization". The cited paragraphs of Newton may have described maintaining in a database information about organization type, organization associations, and peer ISPs; but those cited paragraphs of Newton did not describe and would not have made obvious that a composite rating should be formed "of the organization that is indicative of a degree of risk to the organization or to a party through a business relationship with the organization."

Quite to the contrary, paragraph 0030 of Newton refers to establishing "respective reputations for networks" and allowing "a given network to determine whether to communicate with a particular network in dependence upon its reputation." In other words, Newton described the evaluation of networks, which was quite different from forming "a composite rating of the organization that is indicative of a degree of risk to the organization or to a party through a business relationship with the organization."

The applicant believes that the examiner is inappropriately (and without any support in Newton) equating networks to organizations. A network is not an organization although an organization may operate a network. Newton said nothing about forming a composite rating for an organization. His only concern was networks. ←Stephen, this argument, which I think is strong, probably disappears unless I add the "of the organization" clause to claim 1.]

> **Claims 1, 4, 5, 7-14, 16, 121, 122, 124, 126-132 and 134-140 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chris Newton (US Pre-Grant Publication No: 2004/0250122 Al) hereinafter referred to as Newton in view of in view of Shull et al. (US Pre-Grant Publication No: 2006/0212925 Al) hereinafter referred to as Shull.**

As per claim 1, Newton discloses a method comprising: collecting information about two or more companies or other organizations, that have computer systems, network resources, and employees, the organizations posing risks to themselves or to other parties through business relationships of the organizations with the other parties,

The applicant respectfully disagrees. Newton did not describe and would not have made obvious that information should be collected about organizations that pose "risks to themselves or to other parties through business relationships of the organizations with other parties." Newton's interest was in collecting information about networks. As he said in his paragraph 0041, "the master NID 12 includes information on networks through properties 22 of those networks and applies both a weighting system to those properties and time sensitivity...." Newton did not describe and would not have suggested that organizations that pose risks to themselves or to other parties through business relationships be the target of any collection of information. Again, the applicant respectfully believes that the examiner is inappropriately equating networks to organizations.

the information collected about the organizations being indicative of compromises or indicative of vulnerabilities of technology systems, data, or other information of the organizations, or resiliencies of the organizations to recover from security breaches the information about each of the organizations being collected from two or more sources, one or more of the sources not being controlled by the organization, the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization, Newton, [0012] teaches that every network in the world would have a rating in the database and [0030] teaches establishing a reputation for a network, and [0031] teaches having multiple agents gathering data and [0044]-[0048] teaches different agent types i.e. different network characterization as each agent type gathers different type of data in regards to the security and reputation of network, among these agents include data mining internet which is public information and data mining newsgroups and forums which are also public knowledge and externally observable information not controlled by an organization and figure 1, items 24 include information about the network which towards the bottom of item 24 states "company info resources" i.e. network is associated with a company and [0022] and [0072], teaches taking into account size of the network and number of employees.

at least one of the sources for each of the organizations comprising a public source or a commercial source, —Newton, [0044]-[0048] and [0029], teaches information gathered externally from multiple sources including proxy information and data mining internet which is public information.

processing the information from the two or more sources for each of the organizations to form (A) security vulnerability of the organization (b) compromise of a technology system of the organization, (c) a resilience of the organization to recover from a security breach, the processing including applying models that account for differences in the respective sources, —Newton, [0044]-[0048] and [0029], teaches information gathered externally from multiple sources including proxy information and data mining internet which is public information.

Claim 1 has been amended to recite that the metrics both (a) "a measure of the extent of or the frequency of or duration of compromise of the computer systems or data of the organization, or of a configuration or vulnerability of the organization," and (a) "measure of the resilience of the organization to recover from a security breach or vulnerability." The applicant respectfully disagrees that the cited portions of Newton described or would have made obvious anything with respect to measuring the resilience of the organization to recover from a security breach or vulnerability.

> **in connection with a assessing a business risk to the organization or to a party through a business relationship with or with at least one of the organizations, delivering a report of the composite ratings of the organizations through a reporting facility to enable a user of the reporting facility to monitor, assess, and mitigate the risks, based on the security vulnerabilities or resiliencies or both, in doing business with the organization and to compare the composite ratings of the organizations. —Newton, figure 3 item 14, teaches a database which stores information about the organizations i.e. portal.**

This paragraph of claim 1 has been amended to recite that the report is based on the security vulnerabilities "and" resiliencies. The cited portion of Newton did not describe and would not have made obvious anything about resiliencies.

In addition, this paragraph of claim 1 recites that the report is delivered in connection with "assessing a business risk to the organization or to a party through a business relationship with at least one of the organizations. As discussed earlier, Newton did not describe and would not have made obvious anything about business risks to organizations or to parties through business relationships with organizations. The implication that networks are equivalent to organizations is improper.

> **But does not teach the composite rating comprising a composite of two or more of (a) security vulnerability of the organization, (b) of compromise of a technology system, data, or information of the organization: (c) of a resilience of the organization to recover from a security breach, the processing including applying models that account for differences in the respective sources, the forming of the composite rating for each of the organizations including (a) aggregating metrics associated with the computer system of the organization, the metrics including measures of the frequency of or durations of compromises of the computer system of the organization, and (b) taking account of positive information about the organization,**
>
> **However, Shull [0058] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score which informs requester of the trust of the entity, this score is received by the requester where activities are accounted for both legitimate (i.e. positive) and illegitimate (i.e. negative) and [0069] and [0073], teaches giving an overall trust score between 1 and 5 i.e. a normalized composite score where 1 is a reputable business and 5 is likely engaged in illicit activity.**

The portions of the applicant's amended claim 1 that the examiner is addressing by the citation of these portions of Shull reads this way:

> "... the metrics including a measure of the extent of or the frequency of or duration of compromise of the computer systems or data of the organization, or of a configuration or vulnerability of the organization, and a measure of the resilience of the organization to recover from a security breach or vulnerability,"

Amended claim 1 now requires that the metrics include "a measure of the resilience of the organization to recover from a security breach or vulnerability." None of the cited portions of Shull described or would have made obvious anything about measuring the resilience of an organization to recover from a security breach or vulnerability.

> **It would have been obvious at the time of the invention for one of the ordinary skill in the art to modify the method of collecting security characteristics from multiple sources as taught by Newton by creating a score representative of the different collected data as taught by Shull because it would aid the requester in determining whether the entity is trusted or not.**

The applicant disagrees with the examiner's contention that it would have been obvious to modify Newton by what was described in Shull. But even if, for the sake of argument only, such a modification would have been obvious, it would not have produced the combination of features recited in the applicant's claim 1, because as explained in detail above, features of the claim are missing both from Shull and from Newton.

> **As per claim 136, Newton teaches a method comprising collecting, from at least two sources, information about two or more companies or other organizations, the collected information representing at least two data types, the collected information comprising outcomes of each of the organizations, at least some of the information for each of the organizations being collected automatically by computer from at least two sources, one or more of the sources not controlled by the organization, the information from at least the one or more sources that are not controlled by the organization being collected without permission of the-organization, at least one of the sources including a commercial data source, -Newton, [0012] teaches that every network in the world would have a rating in the database and [0030] teaches establishing a reputation for a network, and [0031] teaches having multiple agents gathering data and [0044]-[0048] teaches different agent types i.e. different network characterization as each agent type gathers different type of data in regards to the security and reputation of network, among these agents include data mining internet which is public information and data mining newsgroups and forums which are also public knowledge and externally observable information not controlled by an organization and figure 1, items 24 include information about the network which towards the bottom of item 24 states "company info resources" i.e. network is associated with a company, and [0022] and [0072], teaches taking into account size of the network and number of employees.**
>
> **and displaying the series of ratings through a portal and reporting the ratings of the organizations through a portal to cnable customers to monitor, assess, and mitigate risk in doing business with the organizations and to compare the composite ratings across the**

organizations. —Newton, figure 3 item 14, teaches a database which stores information about the organizations i.e. portal.

For reasons similar to those given above with respect to the applicant's amended claim 1, the applicant disagrees with the examiner's contentions with respect to Newton.

> **But Newton does not teach processing the information from both of the two sources for each of the organizations to form a composite rating of a security vulnerability of the organization to creation of a security breach or a compromise of a system of the organization or of a resilience of the organization to recover from a security breach or both, the processing including applying models that account for differences in the respective sources, normalizing the composite rating of each of the organizations based on a size characteristic of the organization to enable comparisons of composite ratings between the two or more organizations, forming a series of the security ratings of each of the organizations, determining a trend from the series of ratings, determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information.**
>
> **However, Shull [0058] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score which informs requester of the trust of the entity, this score is received by the requester where activities are accounted for both legitimate (i.e. positive) and illegitimate (i.e. negative) and [0069] and [0073], teaches giving an overall trust score between 1 and 5 i.e. a normalized composite score where 1 is a reputable business and 5 is likely engaged in illicit activity.**
>
> **It would have been obvious at the time of the invention for one of the ordinary skill in the art to modify the method of collecting security characteristics from multiple sources as taught by Newton by creating a score representative of the different collected data as taught by Shull because it would aid the requester in determining whether the entity is trusted or not.**

The applicant respectfully believes that the basis of the rejection based on the additional features allegedly found in Shull is an adequate to support a proper rejection.

The examiner recites the following features as missing from Newton: (a) forming a composite rating of a security vulnerability of the organization to creation of a security breach or a compromise of the system of the organization or of a resilience of the organization to recover from a security breach, (b) applying models that account for differences in the respective sources, (c) normalizing the composite rating of each of the organizations based on a size characteristic of the organization, (d) forming a series of security ratings of each of the organizations, (e) determining a trend from the series of ratings, (f) determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information.

Yet, in recounting the features of Shull that are allegedly relevant, the examiner did not identify any of the elements (a) through (f) mentioned in the prior paragraph. The applicant requests clarification.

As per claim 4, Newton in view of Shull discloses the method of Claim 1, wherein the collected information is represented by at least two data types. —Green, [0044]- [0048] teaches different agent types.

As per claim 5, Newton in view of Shull discloses the method of Claim 4, wherein the at least two data types include at least one of breach disclosures, block lists, configuration parameters, an identification of malware servers, an identification of a reputation, an identification of suspicious activity, an identification of spyware, white lists, an identification of compromised hosts, an identification of malicious activity, an identification of spam activity, an identification of vulnerable hosts, an identification of phishing activity, or an identification of e-mail viruses. —Newton, [0013]-[0029] teaches security measures etc.

As per claim 7, Newton in view of Shull discloses the method of Claim 1, wherein the collected information evidences internal security controls. —Newton, [0013]-[0029] teaches security measures etc.

As per claim 8, Newton in view of Shull discloses the method of Claim 1, wherein the collected information comprises outcomes of each of the organizations. —Newton, [0013]-[0029] teaches security measures and [0044]-[0048] teaches checking for information already available to the public about network.

As per claim 9, Newton in view of Shull discloses the method of Claim 1, wherein the collected information evidences operational execution of security measures of the organizations. —Newton, [0013]-[0029] teaches security measures.

As per claim 10, Newton in view of Shull discloses the method of Claim 1, wherein the collected information indicates whether a computer system of the organizations served malicious code to another system. —Newton, [0013], teaches hostility level and page 4, claim 6, teaches spam levels.

As per claim 11, Newton in view of Shull discloses the method of Claim 1, wherein the collected information indicates whether a computer system of the organizations communicated with a known attacker controlled network or sensor outside the control network of the organization. —Newton, [0013] teaches hostility level.

As per claim 12, Newton in view of Shull discloses the method of Claim 1, comprising: forming a series of the security ratings of the organizations. —Newton, [0042], teaches live remote updates i.e. continually computing rating and page 4, claim 6 teaches security information has multiple ratings and [0041], teaches the different information having different weight.

As per claim 13, Newton in view of Shull discloses the method of Claim 12, comprising determining a trend from the series of ratings. —Newton, [0042], teaches live remote updates i.e. continually computing rating.

As per claim 14, Newton in view of Shull discloses the method of Claim 12, comprising displaying the series of composite ratings. —Newton, [0033], teaches a master database for collecting and storing the network ratings and page 4, claim 6 teaches security information has multiple ratings and [0041], teaches the different information having different weight and Shull, [0058], [0076] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score with informs requester of the trust of the

entity, this score is received by the requester and a display device would display score as to help user determine whether to trust entity or not.

As per claim 16, Newton in view of Shull teaches the method of Claim 14, wherein displaying the series of composite ratings for each of the organizations comprises posting the series of composite ratings for each of the organizations to a web portal. -Newton, [0033], teaches a master database for collecting and storing the network ratings which includes information as listed in [0013]-[0029] which serve as warnings and Shull, [0058], [0076] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score with informs requester of the trust of the entity, this score is received by the requester and a display device would display score as to help user determine whether to trust entity or not.

As per claim 121, Newton in view of Shull teaches the method of Claim 1, wherein the collected information represents externally observable outcome information.

- Newton, [0054], teaches agents getting information from news groups or sending packets and checking their responses.

As per claim 122, Newton in view of Shull teaches the method of Claim 121, wherein the outcome information comprises outcome information associated with security vulnerability or resilience of each of the organizations. Shull, [0058] and Newton, page 4, claim 6, both teach that the information is associated with entity security and Newton even looks into active security systems as well.

As per claim 124, Newton in view of Shull teaches the method of Claim 1, comprising: determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information. - Newton, page 4, claim 6, teaches having spam levels etc. Which are a badness score.

As per claim 126, Newton in view of Shull teaches the method of Claim 1, wherein: the collected information comprises at least two security characterizations of a computer system of the entity. - Newton, page 4, claim 6, teaches checking open proxy servers and desktop security measures which are multiple characterizations of a system of the entity.

As per claim 127, Newton in view of Shull teaches the method of Claim 1, wherein the collected information comprises a characterization of behavior of an employee of at least one of the organizations. - Newton, page 4, claim 6, inappropriate content served, spam levels, language spoken, geographic placement, industry, which are characterizations of employees in the network and the employees behavior.

As per claim 128, Newton in view of Shull teaches the method of Claim 1, wherein the collected information comprises characterizations other than characterizations about a computer system of at least one of the organizations. - Newton, page 4, claim 6, teaches security characterization includes security personnel.

As per claim 129, Newton in view of Shull teaches the method of Claim 1, wherein the collected information comprises characterizations about policies of at least one of the organizations. —Newton, page 4, claim 6, teaches organization association, active security measures, desktop security measures, etc. which are policies see also [0059] and [0060].

As per claim 130, Newton in view of Shull teaches the method of Claim 1, wherein the collected information comprises characterizations about information technology assets that at least one of the organizations owns, controls, uses, or is affiliated with. —Newton, page 4, claim 6, teaches organization associations see also [0043] and [0053].

As per claim 131, Newton in view of Shull teaches the method of Claim 1 in which collected information represents: (a) physical states, (b) technical states, (c) organizational states, or

(d) cultural states of at least one of the organizations which can be exploited to create a security breach; or (e) the organization's ability to recover from a security breach; or any combination of two or more of these. —Newton, page 4, claim 6, teaches active security measures and desktop security measures among other information collected about the organization.

As per claim 132, Newton in view of Shull teaches the method of claim 1 in which processing the information to form a composite rating comprises correlating data across the sources of information.-Shull, [0058], teaches creating a score based on the different data received i.e. correlating the different data.

As per claim 134, Newton in view of Shull teaches the method of claim 1 in which processing the information to form a composite rating comprises statistically correlating the composite rating with actual outcomes. — Newton, [0041], teaches giving different information different weight where less weight given to information as it becomes less important over time which is a statistical correlation with the information collected.

As per claim 135, Newton in view of Shull teaches the method of claim 1 in which the vulnerability comprises physical, technical, organizational, or cultural states that can be exploited to create a security breach. —Newton, figure 1, item 24 and page 4, claim 6.

As per claim 137, Newton in view of Shull teaches the system of claim 1, determining a confidence range of the composite rating, the size of the range varying inversely with the level of confidence in the composite rating. - Shull, [0069] and [0073], teaches giving an overall trust score between 1 and 5 i.e. a normalized composite score where 1 is a reputable business and 5 is likely engaged in illicit activity.

As per claim 138, Newton in view of Shull teaches the system of claim 137, wherein the confidence range is based on redundancy of the security characterizations.

—Shull, [0081], teaches taking into account consistency which is redundancy.

As per claim 139, Newton in view of Shull teaches the system of claim 137, wherein the confidence range is based on a size of the third party computer system. — Newton, [0072], teaches taking into account size of the network.

As per claim 140, Newton in view of Shull teaches the method of claim 1 comprising ranking the organization and other organizations within sectors or peer groups or globally. —Shull, [0123]-[0124], teaches listing entities with similar scores together such as ones that scored a 3 or 4 so these would be ranked below ones which were listed as part of white list which ranked 1 or 2, see [0068], which teaches having white list, black list and grey lists.

The applicant acknowledges the examiner's indication of the patentability of these claims. Amendments have been made that recite rigid connectors and viscous liquids with a breadth that the applicant believes that the examiner will find patentable.

All of the dependent claims are patentable for at least the same reasons as those given for the independent claims on which they depend.

Canceled claims, if any, have been canceled without prejudice or disclaimer.

Any circumstance in which the applicant has (a) addressed certain comments of the examiner does not mean that the applicant concedes other comments of the examiner, (b) made

arguments for the patentability of some claims does not mean that there are not other good reasons for patentability of those claims and other claims, or (c) amended or canceled a claim does not mean that the applicant concedes any of the examiner's positions with respect to that claim or other claims.

Please apply any charges or credits to deposit account 06-1050, referencing attorney docket 38879-0006001.

Respectfully submitted,

Date:/12/23/15/_____

/David L. Feigenbaum/_____
David L. Feigenbaum
Reg. No. 30,378

Customer Number 26161
Fish & Richardson P.C.
Telephone: (617) 542-5070
Facsimile: (877) 769-7945

23472981.doc

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	38879-0006001
	Application Number	13/240,572
Title of Invention	Information Technology Security Assessment System	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.

Applicant Information:

Providing assignment information in this section does not substitute for compliance with any requirement of part 3 of Title 37 of CFR to have an assignment recorded by the Office.

Applicant 1

If the applicant is the inventor (or the remaining joint inventor or inventors under 37 CFR 1.45), this section should not be completed. The information to be provided in this section is the name and address of the legal representative who is the applicant under 37 CFR 1.43; or the name and address of the assignee, person to whom the inventor is under an obligation to assign the invention, or person who otherwise shows sufficient proprietary interest in the matter who is the applicant under 37 CFR 1.46. If the applicant is an applicant under 37 CFR 1.46 (assignee, person to whom the inventor is obligated to assign, or person who otherwise shows sufficient proprietary interest) together with one or more joint inventors, then the joint inventor or inventors who are also the applicant should be identified in this section.

☒ Assignee	☐ Legal Representative under 35 U.S.C. 117	☐ Joint Inventor
☐ Person to whom the inventor is obligated to assign.	☐ Person who shows sufficient proprietary interest	

If applicant is the legal representative, indicate the authority to file the patent application, the inventor is:

Name of the Deceased or Legally Incapacitated Inventor :

If the Applicant is an Organization check here. ☒

Organization Name BitSight Technologies, Inc.

Prefix	Given Name	Middle Name	Family Name	Suffix
	~~Stephen~~ ~~Nagarjuna~~ ~~Megumi~~		~~Boyer~~ ~~Venna~~ ~~Ando~~	

Mailing Address Information:

Address 1	738 Main Street , No. 388		
Address 2			
City	Waltham	State/Province	MA
Country	U.S.	Postal Code	02451
Phone Number		Fax Number	
Email Address			

Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/David L. Feigenbaum/			Date (**MM/DD/YYYY**)	11/17/2015
First Name	David	Last Name	Feigenbaum	Registration Number	30,378

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	38879-0006001
	Application Number	13/240,572
Title of Invention	Information Technology Security Assessment System	

23460854.doc

Electronic Acknowledgement Receipt

EFS ID:	24108139
Application Number:	13240572
International Application Number:	
Confirmation Number:	2423
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Customer Number:	26161
Filer:	David L Feigenbaum/jennifer franco
Filer Authorized By:	David L Feigenbaum
Attorney Docket Number:	38879-0006001
Receipt Date:	17-NOV-2015
Filing Date:	22-SEP-2011
Time Stamp:	15:06:01
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Application Data Sheet	SUPP-ADS.pdf	80314 0be1b048050bf3e4a6a4247f29ca22da68e4899d	no	2

Warnings:	
Information:	

This is not an USPTO supplied ADS fillable form	
Total Files Size (in bytes):	80314

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/240,572	09/22/2011	Stephen Wayne Boyer	38879-0006001	2423

26161 7590 10/26/2015

FISH & RICHARDSON P.C. (BO)
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
KANAAN, SIMON P	

ART UNIT	PAPER NUMBER
2492	

NOTIFICATION DATE	DELIVERY MODE
10/26/2015	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATDOCTC@fr.com

Applicant-Initiated Interview Summary	Application No.	Applicant(s)	
	13/240,572	BOYER ET AL.	
	Examiner	Art Unit	
	SIMON KANAAN	2432	

All participants (applicant, applicant's representative, PTO personnel):

(1) *SIMON KANAAN*. (3) *Samson Lemma*.

(2) *David Feigenbaum (Reg. No: 30,378)*. (4) *Stephen Boyer*.

Date of Interview: *24 September 2015*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1*.

Identification of prior art discussed: *Newton and Shull*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Applicant's representative and examiner discussed potential amendments to the claims to help overcome the art of record. No agreement was reached. Examiner suggested adding in detail on how the computed score is calculated. Parties also discussed differentiating organization and a network and more detail related to resilience of a company. Parties also discussed changing the claim language from "or" in many of the limitations as examiner does not need to find all the elements when an "or" is in the limitation .

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/SIMON KANAAN/ Examiner, Art Unit 2432	

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:

1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

Office Action Summary	Application No. 13/240,572	Applicant(s) BOYER ET AL.	
	Examiner SIMON KANAAN	Art Unit 2432	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *2 September 2015*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1,4,5,7-14,16,121,122,124,126-132 and 134-140* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1,4,5,7-14,16,121,122,124,126-132 and 134-140* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *22 September 2011* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some * c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Interim copies:

a)☐ All b)☐ Some c)☐ None of the: Interim copies of the priority documents have been received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

3) ☒ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions

2. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

Office Action Summary

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. Applicant's arguments/amendments filed 9/2/2015 in regards to 35 U.S.C. 101 and 35 U.S.C. 112 have been considered and are persuasive therefore the previously filed 35 U.S.C. 101 and 35 U.S.C. 112 rejections have been withdrawn.

5. Applicant's arguments/amendments filed 9/2/2015 have been considered but are not persuasive.

Applicant's Amendments and Examiner's Response

6. Applicant's arguments/amendments filed 9/2/2015 have been considered but are not persuasive. As for applicant's arguments, applicant argues that the cited prior art does not teach:

a. giving an organization a composite score stating that the score calculated in Newton is for a network, however the examiner respectfully disagrees as Newton [0018]-[0020], teaches who organization is associated with, type of organization as well as number of employees, an entity having employees and is a type of an organization is an organization.

b. a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information, however examiner respectfully disagrees as Newton, page 4, claim 6, teaches having spam levels etc. Which are a badness score as a spam level indicates if an item is spam i.e. bad.

Claim Rejections - 35 USC § 103

7. Claims 1, 4, 5, 7-14, 16, 121, 122, 124, 126-132 and 134-140 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chris Newton (US Pre-Grant Publication No: 2004/0250122 A1) hereinafter referred to as Newton in view of in view of Shull et al. (US Pre-Grant Publication No: 2006/0212925 A1) hereinafter referred to as Shull.

As per claim 1, Newton discloses a method comprising: collecting information about two or more companies or other organizations, that have computer systems, network resources, and employees, the organizations posing risks to themselves or to other parties through business relationships of the organizations with the other parties, the information collected about the organizations being indicative of compromises or indicative of vulnerabilities of technology systems, data, or other information of the

organizations, or resiliencies of the organizations to recover from security breaches the information about each of the organizations being collected from two or more sources, one or more of the sources not being controlled by the organization, the information format least the one or more sources that are not controlled by the organization being collected without permission of the organization, -Newton, [0012] teaches that every network in the world would have a rating in the database and [0030] teaches establishing a reputation for a network, and [0031] teaches having multiple agents gathering data and [0044]-[0048] teaches different agent types i.e. different network characterization as each agent type gathers different type of data in regards to the security and reputation of network, among these agents include data mining internet which is public information and data mining newsgroups and forums which are also public knowledge and externally observable information not controlled by an organization and figure 1, items 24 include information about the network which towards the bottom of item 24 states "company info resources" i.e. network is associated with a company and [0022] and [0072], teaches taking into account size of the network and number of employees.

at least one of the sources for each of the organizations comprising a public source or a commercial source, –Newton, [0044]-[0048] and [0029], teaches information gathered externally from multiple sources including proxy information and data mining internet which is public information.

processing the information from the two or more sources for each of the organizations to form (A) security vulnerability of the organization (b) compromise of a

technology system of the organization, (c) a resilience of the organization to recover from a security breach, the processing including applying models that account for differences in the respective sources, –Newton, [0044]-[0048] and [0029], teaches information gathered externally from multiple sources including proxy information and data mining internet which is public information.

in connection with a assessing a business risk to the organization or to a party through a business relationship with or with at least one of the organizations, delivering a report of the composite ratings of the organizations through a reporting facility to enable a user of the reporting facility to monitor, assess, and mitigate the risks, based on the security vulnerabilities or resiliencies or both, in doing business with the organization and to compare the composite ratings of the organizations. –Newton, figure 3 item 14, teaches a database which stores information about the organizations i.e. portal.

But does not teach the composite rating comprising a composite of two or more of (a) security vulnerability of the organization, (b) of compromise of a technology system, data, or information of the organization: (c) of a resilience of the organization to recover from a security breach, the processing including applying models that account for differences in the respective sources, the forming of the composite rating for each of the organizations including (a) aggregating metrics associated with the computer system of the organization, the metrics including measures of the frequency of or durations of compromises of the computer system o5 the organization, and (b) taking account of positive information about the

organization,

However, Shull [0058] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score which informs requester of the trust of the entity, this score is received by the requester where activities are accounted for both legitimate (i.e. positive) and illegitimate (i.e. negative) and [0069] and [0073], teaches giving an overall trust score between 1 and 5 i.e. a normalized composite score where 1 is a reputable business and 5 is likely engaged in illicit activity.

It would have been obvious at the time of the invention for one of the ordinary skill in the art to modify the method of collecting security characteristics from multiple sources as taught by Newton by creating a score representative of the different collected data as taught by Shull because it would aid the requester in determining whether the entity is trusted or not.

As per claim 4, Newton in view of Shull discloses the method of Claim 1, wherein the collected information is represented by at least two data types. –Green, [0044]-[0048] teaches different agent types.

As per claim 5, Newton in view of Shull discloses the method of Claim 4, wherein the at least two data types include at least one of breach disclosures, block lists, configuration parameters, an identification of malware servers, an identification of a reputation, an identification of suspicious activity, an identification of spyware, white lists, an identification of compromised hosts, an identification of malicious activity, an

identification of spam activity, an identification of vulnerable hosts, an identification of phishing activity, or an identification of e-mail viruses. –Newton, [0013]-[0029] teaches security measures etc.

As per claim 7, Newton in view of Shull discloses the method of Claim 1, wherein the collected information evidences internal security controls. –Newton, [0013]-[0029] teaches security measures etc.

As per claim 8, Newton in view of Shull discloses the method of Claim 1, wherein the collected information comprises outcomes of each of the organizations. –Newton, [0013]-[0029] teaches security measures and [0044]-[0048] teaches checking for information already available to the public about network.

As per claim 9, Newton in view of Shull discloses the method of Claim 1, wherein the collected information evidences operational execution of security measures of the organizations. –Newton, [0013]-[0029] teaches security measures.

As per claim 10, Newton in view of Shull discloses the method of Claim 1, wherein the collected information indicates whether a computer system of the organizations served malicious code to another system. –Newton, [0013], teaches hostility level and page 4, claim 6, teaches spam levels.

As per claim 11, Newton in view of Shull discloses the method of Claim 1, wherein the collected information indicates whether a computer system of the organizations communicated with a known attacker controlled network or sensor outside the control network of the organization. –Newton, [0013] teaches hostility level.

As per claim 12, Newton in view of Shull discloses the method of Claim 1, comprising: forming a series of the security ratings of the organizations. –Newton, [0042], teaches live remote updates i.e. continually computing rating and page 4, claim 6 teaches security information has multiple ratings and [0041], teaches the different information having different weight.

As per claim 13, Newton in view of Shull discloses the method of Claim 12, comprising determining a trend from the series of ratings. –Newton, [0042], teaches live remote updates i.e. continually computing rating.

As per claim 14, Newton in view of Shull discloses the method of Claim 12, comprising displaying the series of composite ratings. –Newton, [0033], teaches a master database for collecting and storing the network ratings and page 4, claim 6 teaches security information has multiple ratings and [0041], teaches the different information having different weight and Shull, [0058], [0076] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score with informs requester of the trust of the entity, this score is received by the requester and a display device would display score as to help user determine whether to trust entity or not.

As per claim 16, Newton in view of Shull teaches the method of Claim 14, wherein displaying the series of composite ratings for each of the organizations comprises posting the series of composite ratings for each of the organizations to a web portal. -Newton, [0033], teaches a master database for collecting and storing the network ratings which includes information as listed in [0013]-[0029] which serve as warnings and Shull, [0058], [0076] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score with informs requester of the trust of the entity, this score is received by the requester and a display device would display score as to help user determine whether to trust entity or not.

As per claim 121, Newton in view of Shull teaches the method of Claim 1, wherein the collected information represents externally observable outcome information. - Newton, [0054], teaches agents getting information from news groups or sending packets and checking their responses.

As per claim 122, Newton in view of Shull teaches the method of Claim 121, wherein the outcome information comprises outcome information associated with security vulnerability or resilience of each of the organizations. Shull, [0058] and Newton, page 4, claim 6, both teach that the information is associated with entity security and Newton even looks into active security systems as well.

As per claim 124, Newton in view of Shull teaches the method of Claim 1, comprising: determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information. - Newton, page 4, claim 6, teaches having spam levels etc. Which are a badness score.

As per claim 126, Newton in view of Shull teaches the method of Claim 1, wherein: the collected information comprises at least two security characterizations of a computer system of the entity. - Newton, page 4, claim 6, teaches checking open proxy servers and desktop security measures which are multiple characterizations of a system of the entity.

As per claim 127, Newton in view of Shull teaches the method of Claim 1, wherein the collected information comprises a characterization of behavior of an employee of at least one of the organizations. - Newton, page 4, claim 6, inappropriate content served, spam levels, language spoken, geographic placement, industry, which are characterizations of employees in the network and the employees' behavior.

As per claim 128, Newton in view of Shull teaches the method of Claim 1, wherein the collected information comprises characterizations other than characterizations about a computer system of at least one of the organizations. - Newton, page 4, claim 6, teaches security characterization includes security personnel.

As per claim 129, Newton in view of Shull teaches the method of Claim 1, wherein the collected information comprises characterizations about policies of at least one of the organizations. –Newton, page 4, claim 6, teaches organization association, active security measures, desktop security measures, etc. which are policies see also [0059] and [0060].

As per claim 130, Newton in view of Shull teaches the method of Claim 1, wherein the collected information comprises characterizations about information technology assets that at least one of the organizations owns, controls, uses, or is affiliated with. –Newton, page 4, claim 6, teaches organization associations see also [0043] and [0053].

As per claim 131, Newton in view of Shull teaches the method of Claim 1 in which collected information represents: (a) physical states, (b) technical states, (c) organizational states, or (d) cultural states of at least one of the organizations which can be exploited to create a security breach; or (e) the organization's ability to recover from a security breach; or any combination of two or more of these. –Newton, page 4, claim 6, teaches active security measures and desktop security measures among other information collected about the organization.

As per claim 132, Newton in view of Shull teaches the method of claim 1 in which processing the information to form a composite rating comprises correlating data across

the sources of information.-Shull, [0058], teaches creating a score based on the different data received i.e. correlating the different data.

As per claim 134, Newton in view of Shull teaches the method of claim 1 in which processing the information to form a composite rating comprises statistically correlating the composite rating with actual outcomes. – Newton, [0041], teaches giving different information different weight where less weight given to information as it becomes less important over time which is a statistical correlation with the information collected.

As per claim 135, Newton in view of Shull teaches the method of claim 1 in which the vulnerability comprises physical, technical, organizational, or cultural states that can be exploited to create a security breach. –Newton, figure 1, item 24 and page 4, claim 6.

As per claim 136, Newton teaches a method comprising collecting, from at least two sources, information about two or more companies or other organizations, the collected information representing at least two data types, the collected information comprising outcomes of each of the organizations, at least some of the information for each of the organizations being collected automatically by computer from at least two sources, one or more of the sources not controlled by the organization, the information from at least the one or more sources that are not controlled by the organization being collected without permission of the-organization, at least one of the sources including a commercial data source, -Newton, [0012] teaches that every network in the world would

have a rating in the database and [0030] teaches establishing a reputation for a network, and [0031] teaches having multiple agents gathering data and [0044]-[0048] teaches different agent types i.e. different network characterization as each agent type gathers different type of data in regards to the security and reputation of network, among these agents include data mining internet which is public information and data mining newsgroups and forums which are also public knowledge and externally observable information not controlled by an organization and figure 1, items 24 include information about the network which towards the bottom of item 24 states "company info resources" i.e. network is associated with a company, and [0022] and [0072], teaches taking into account size of the network and number of employees.

and displaying the series of ratings through a portal and reporting the ratings of the organizations through a portal to enable customers to monitor, assess, and mitigate risk in doing business with the organizations and to compare the composite ratings across the organizations. –Newton, figure 3 item 14, teaches a database which stores information about the organizations i.e. portal.

But Newton does not teach processing the information from both of the two sources for each of the organizations to form a composite rating of a security vulnerability of the organization to creation of a security breach or a compromise of a system of the organization or of a resilience of the organization to recover from a security breach or both, the processing including applying models that account for differences in the respective sources, normalizing the composite rating of each of the organizations based on a size characteristic of the organization to enable comparisons

of composite ratings between the two or more organizations, forming a series of the security ratings of each of the organizations, determining a trend from the series of ratings, determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information.

However, Shull [0058] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score which informs requester of the trust of the entity, this score is received by the requester where activities are accounted for both legitimate (i.e. positive) and illegitimate (i.e. negative) and [0069] and [0073], teaches giving an overall trust score between 1 and 5 i.e. a normalized composite score where 1 is a reputable business and 5 is likely engaged in illicit activity.

It would have been obvious at the time of the invention for one of the ordinary skill in the art to modify the method of collecting security characteristics from multiple sources as taught by Newton by creating a score representative of the different collected data as taught by Shull because it would aid the requester in determining whether the entity is trusted or not.

As per claim 137, Newton in view of Shull teaches the system of claim 1, determining a confidence range of the composite rating, the size of the range varying inversely with the level of confidence in the composite rating. - Shull, [0069] and [0073], teaches giving an overall trust score between 1 and 5 i.e. a normalized composite score where 1 is a reputable business and 5 is likely engaged in illicit activity.

As per claim 138, Newton in view of Shull teaches the system of claim 137, wherein the confidence range is based on redundancy of the security characterizations. –Shull, [0081], teaches taking into account consistency which is redundancy.

As per claim 139, Newton in view of Shull teaches the system of claim 137, wherein the confidence range is based on a size of the third party computer system. – Newton, [0072], teaches taking into account size of the network.

As per claim 140, Newton in view of Shull teaches the method of claim 1 comprising ranking the organization and other organizations within sectors or peer-groups or globally. –Shull, [0123]-[0124], teaches listing entities with similar scores together such as ones that scored a 3 or 4 so these would be ranked below ones which were listed as part of white list which ranked 1 or 2, see [0068], which teaches having white list, black list and grey lists.

Conclusion

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

9. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Simon Kanaan whose telephone number is (571)270-3906. The examiner can normally be reached on Mon-Thurs 7:30-5:00 EST.

If attempts to reach the above noted Examiner by telephone are unsuccessful, the Examiner's supervisor, Saleh Najjar, can be reached at the following telephone number: (571) 272-4006.

The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.

/S. K./
Examiner, Art Unit 2432

/SAMSON LEMMA/
Primary Examiner, Art Unit 2432

Applicant-Initiated Interview Summary	Application No.	Applicant(s)	
	13/240,572	BOYER ET AL.	
	Examiner	Art Unit	
	SIMON KANAAN	2432	

All participants (applicant, applicant's representative, PTO personnel):

(1) *SIMON KANAAN*. (3) *Samson Lemma*.

(2) *David Feigenbaum (Reg. No: 30,378)*. (4) *Stephen Boyer*.

Date of Interview: *24 September 2015*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1*.

Identification of prior art discussed: *Newton and Shull*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Applicant's representative and examiner discussed potential amendments to the claims to help overcome the art of record. No agreement was reached. Examiner suggested adding in detail on how the computed score is calculated. Parties also discussed differentiating organization and a network and more detail related to resilience of a company. Parties also discussed changing the claim language from "or" in many of the limitations as examiner does not need to find all the elements when an "or" is in the limitation .

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/SIMON KANAAN/ Examiner, Art Unit 2432	

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:

1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	**Art Unit**
	SIMON KANAAN	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/18/2013	11/07/2013	06/04/2014	02/22/2015	05/28/2015	09/25/2015			
	1	✓	✓	✓	✓	✓	✓			
	2	✓	✓	-	-	-	-			
	3	✓	✓	✓	✓	✓	-			
	4	✓	✓	✓	✓	✓	✓			
	5	✓	✓	✓	✓	✓	✓			
	6	✓	✓	-	-	-	-			
	7	✓	✓	✓	✓	✓	✓			
	8	✓	✓	✓	✓	✓	✓			
	9	✓	✓	✓	✓	✓	✓			
	10	✓	✓	✓	✓	✓	✓			
	11	✓	✓	✓	✓	✓	✓			
	12	✓	✓	✓	✓	✓	✓			
	13	✓	✓	✓	✓	✓	✓			
	14	✓	✓	✓	✓	✓	✓			
	15	✓	✓	-	-	-	-			
	16	✓	✓	✓	✓	✓	✓			
	17	✓	✓	-	-	-	-			
	18	✓	✓	-	-	-	-			
	19	✓	✓	-	-	-	-			
	20	✓	✓	-	-	-	-			
	21	-	-	-	-	-	-			
	22	-	-	-	-	-	-			
	23	-	-	-	-	-	-			
	24	-	-	-	-	-	-			
	25	-	-	-	-	-	-			
	26	-	-	-	-	-	-			
	27	-	-	-	-	-	-			
	28	-	-	-	-	-	-			
	29	-	-	-	-	-	-			
	30	-	-	-	-	-	-			
	31	-	-	-	-	-	-			
	32	-	-	-	-	-	-			
	33	-	-	-	-	-	-			
	34	-	-	-	-	-	-			
	35	-	-	-	-	-	-			
	36	-	-	-	-	-	-			

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	**Art Unit**
	SIMON KANAAN	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/18/2013	11/07/2013	06/04/2014	02/22/2015	05/28/2015	09/25/2015			
	37	-	-	-	-	-	-			
	38	-	-	-	-	-	-			
	39	-	-	-	-	-	-			
	40	-	-	-	-	-	-			
	41	-	-	-	-	-	-			
	42	-	-	-	-	-	-			
	43	-	-	-	-	-	-			
	44	-	-	-	-	-	-			
	45	-	-	-	-	-	-			
	46	-	-	-	-	-	-			
	47	-	-	-	-	-	-			
	48	-	-	-	-	-	-			
	49	-	-	-	-	-	-			
	50	-	-	-	-	-	-			
	51	-	-	-	-	-	-			
	52	-	-	-	-	-	-			
	53	-	-	-	-	-	-			
	54	-	-	-	-	-	-			
	55	-	-	-	-	-	-			
	56	-	-	-	-	-	-			
	57	-	-	-	-	-	-			
	58	-	-	-	-	-	-			
	59	-	-	-	-	-	-			
	60	-	-	-	-	-	-			
	61	-	-	-	-	-	-			
	62	-	-	-	-	-	-			
	63	-	-	-	-	-	-			
	64	-	-	-	-	-	-			
	65	-	-	-	-	-	-			
	66	-	-	-	-	-	-			
	67	-	-	-	-	-	-			
	68	-	-	-	-	-	-			
	69	-	-	-	-	-	-			
	70	-	-	-	-	-	-			
	71	-	-	-	-	-	-			
	72	-	-	-	-	-	-			

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	**Art Unit**
	SIMON KANAAN	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/18/2013	11/07/2013	06/04/2014	02/22/2015	05/28/2015	09/25/2015			
	73	-	-	-	-	-	-			
	74	-	-	-	-	-	-			
	75	-	-	-	-	-	-			
	76	-	-	-	-	-	-			
	77	-	-	-	-	-	-			
	78	-	-	-	-	-	-			
	79	-	-	-	-	-	-			
	80	-	-	-	-	-	-			
	81	-	-	-	-	-	-			
	82	-	-	-	-	-	-			
	83	-	-	-	-	-	-			
	84	-	-	-	-	-	-			
	85	-	-	-	-	-	-			
	86	-	-	-	-	-	-			
	87	-	-	-	-	-	-			
	88	-	-	-	-	-	-			
	89	-	-	-	-	-	-			
	90	-	-	-	-	-	-			
	91	-	-	-	-	-	-			
	92	-	-	-	-	-	-			
	93	-	-	-	-	-	-			
	94	-	-	-	-	-	-			
	95	-	-	-	-	-	-			
	96	-	-	-	-	-	-			
	97	-	-	-	-	-	-			
	98	-	-	-	-	-	-			
	99	-	-	-	-	-	-			
	100	-	-	-	-	-	-			
	101	-	-	-	-	-	-			
	102	-	-	-	-	-	-			
	103	-	-	-	-	-	-			
	104	-	-	-	-	-	-			
	105	-	-	-	-	-	-			
	106	-	-	-	-	-	-			
	107	-	-	-	-	-	-			
	108	-	-	-	-	-	-			

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	**Art Unit**
	SIMON KANAAN	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/18/2013	11/07/2013	06/04/2014	02/22/2015	05/28/2015	09/25/2015			
	109	-	-	-	-	-	-			
	110	-	-	-	-	-	-			
	111	-	-	-	-	-	-			
	112	-	-	-	-	-	-			
	113	-	-	-	-	-	-			
	114	-	-	-	-	-	-			
	115	-	-	-	-	-	-			
	116	-	-	-	-	-	-			
	117	-	-	-	-	-	-			
	118	-	-	-	-	-	-			
	119	-	-	-	-	-	-			
	120	-	-	-	-	-	-			
	121			✓	✓	✓	✓			
	122			✓	✓	✓	✓			
	123			✓	✓	✓	-			
	124			✓	✓	✓	✓			
	125			✓	-	-	-			
	126			✓	✓	✓	✓			
	127			✓	✓	✓	✓			
	128			✓	✓	✓	✓			
	129			✓	✓	✓	✓			
	130			✓	✓	✓	✓			
	131			✓	✓	✓	✓			
	132			✓	✓	✓	✓			
	133			✓	-	-	-			
	134			✓	✓	✓	✓			
	135			✓	✓	✓	✓			
	136				✓	✓	✓			
	137				✓	✓	✓			
	138				✓	✓	✓			
	139				✓	✓	✓			
	140				✓	✓	✓			

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	0	"13240572"	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L2	10	726/25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L3	0	apparatus and method for network vulnerability detection and compliance	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L4	0	network vulnerability detection and compliance assesment	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L5	0	network vulnerability detection compliance assesment	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L6	0	network with vulnerability with detection with compliance with assesment	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L7	7	network with vulnerability with detection with compliance with assessment	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L8	37	726/2,22,25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L9	31	726/2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L10	41	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L11	3	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L12	118	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L13	0	(external$5 or third party) with (security) with (commercial near data) with reputation	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L14	0	(external$5 or third party) with (commercial near data) with reputation	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L15	25	internet monitoring with report	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L16	10	internet monitoring with report and public	US-PGPUB;	ADJ	ON	2015/09/25 01:43

			USPAT			
L17	0	malwareurl	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L18	0	malwareurl$5	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L19	0	www$malwareurl$5	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L20	0	www$malwareurl$com	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L21	143	arbor networks	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L22	1	arbor networks and renesys	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L23	5473	reputation and domain	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L24	66	reputation and domain and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L25	124	reputation and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L26	58	L25 not L24	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L27	20	US-7194769-$.DID. OR US-7290275-$.DID. OR US-7971252-$.DID. OR US-20040010709-$.DID. OR US-20050138413-$.DID. OR US-20080047018-$.DID. OR US-20080209565-$.DID. OR US-20090265787-$.DID. OR US-20090293128-$.DID. OR US-2007304-$.DID. OR US-5200596-$.DID. OR US-2009104-$.DID. OR US-422009D-$.DID. OR US-1331018-$.DID.	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2015/09/25 01:43
L28	0	L25 and L27	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L29	0	(insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L27	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L30	0	(industry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L27	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L31	0	(industry reports or internet monitoring	US-	ADJ	ON	2015/09/25

		or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L27	PGPUB; USPAT			01:43
L32	0	L27 and user behavior	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L33	0	L27 and behavior	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L34	0	L27 and reputation	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L35	0	L27 and public with features	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2015/09/25 01:43
L36	0	L27 and externally	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2015/09/25 01:43
L37	7	L27 and external	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2015/09/25 01:43
L38	2	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L39	24	((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L40	226	((external$5 or third party) with audit$4)and reputation and security	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L41	420	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L42	400	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L43	258	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L44	0	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial data sources	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L45	4	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial data	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L46	4	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rating and commercial data	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43

L47	4	security and renesys	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L48	1	abor networks	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L50	44	(network near3 vulnerability) with public	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L51	21	(network near3 assessment) with public	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L52	37	(network near3 assessment) with external$3	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L53	1415	site secure	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L54	525	L53 and third party	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L55	202	L54 and assess$3	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L56	209	network reputation	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L57	195	network reputation and (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L58	15	network reputation with (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L59	10	network reputation with (rat$3 or assess$4) and public	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L60	3	network reputation with public	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L61	472	network (reputation or assess$4 or rat$3) with public	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L62	260	network (reputation or assess$4 or rat$3) with public and security	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L63	9	network (reputation or assess$4 or rat$3) with public with security	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L64	15	network (reputation or assess$4 or rat$3) with public with secur$5	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L65	6	L64 not L63	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L66	2	"20040250122"	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43

L67	2	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L68	0	"13240572"	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L70	4410	(organization or company or entity) same reputation	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L71	1061	(organization or company or entity) same reputation same (score or rating)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L72	19092	726/1,2,22,25.ccls.	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L73	120	L71 and L72	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L74	640	(organization or company) same reputation same (score or rating)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L75	55	L74 and L72	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L76	0	"13240572"	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L77	10	726/25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L78	0	apparatus and method for network vulnerability detection and compliance	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L79	0	network vulnerability detection and compliance assesment	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L80	0	network vulnerability detection compliance assesment	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L81	0	network with vulnerability with detection with compliance with assesment	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L82	7	network with vulnerability with detection with compliance with assessment	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L83	37	726/2,22,25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L84	31	726/2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L85	41	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L86	3	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43

L87	118	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L88	0	(external$5 or third party) with (security) with (commercial near data) with reputation	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L89	0	(external$5 or third party) with (commercial near data) with reputation	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L90	25	internet monitoring with report	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L91	10	internet monitoring with report and public	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L92	0	malwareurl	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L93	0	malwareurl$5	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L94	0	www$malwareurl$5	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L95	0	www$malwareurl$com	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L96	143	arbor networks	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L97	1	arbor networks and renesys	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L98	5473	reputation and domain	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L99	66	reputation and domain and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L100	124	reputation and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L101	58	L100 not L99	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L102	20	US-7194769-$.DID. OR US-7290275-$.DID. OR US-7971252-$.DID. OR US-20040010709-$.DID. OR US-20050138413-$.DID. OR US-20080047018-$.DID. OR US-20080209565-$.DID. OR US-20090265787-$.DID. OR US-20090293128-$.DID. OR US-2007304-$.DID. OR US-5200596-$.DID. OR US-	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2015/09/25 01:43

		2009104-$.DID. OR US-422009D-$.DID. OR US-1331018-$.DID.				
L103	0	L100 and L102	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L104	0	(insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L102	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L105	0	(industry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L102	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L106	0	(industry reports or internet monitoring or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L102	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L107	0	L102 and user behavior	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L108	0	L102 and behavior	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L109	0	L102 and reputation	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L110	0	L102 and public with features	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2015/09/25 01:43
L111	0	L102 and externally	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2015/09/25 01:43
L112	7	L102 and external	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2015/09/25 01:43
L113	31	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L114	2	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L115	24	((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L116	226	((external$5 or third party) with audit$4)and reputation and security	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L117	420	((external$5 or third party) with (audit$4 or observ$5)) and reputation and	US-PGPUB;	ADJ	ON	2015/09/25 01:43

		security	USPAT			
L118	400	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L119	258	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L120	0	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial data sources	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L121	4	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial data	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L122	4	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rating and commercial data	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L123	4	security and renesys	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L124	1	abor networks	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L125	44	(network near3 vulnerability) with public	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L126	21	(network near3 assessment) with public	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L127	37	(network near3 assessment) with external$3	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L128	1415	site secure	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L129	525	L128 and third party	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L130	202	L129 and assess$3	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L131	209	network reputation	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L132	195	network reputation and (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L133	15	network reputation with (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L134	10	network reputation with (rat$3 or assess$4) and public	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L135	3	network reputation with public	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L136	472	network (reputation or assess$4 or rat$3)	US-	ADJ	ON	2015/09/25

		with public	PGPUB; USPAT			01:43
L137	260	network (reputation or assess$4 or rat$3) with public and security	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L138	9	network (reputation or assess$4 or rat$3) with public with security	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L139	15	network (reputation or assess$4 or rat$3) with public with secur$5	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L140	6	L139 not L138	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L141	2	"20040250122"	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L142	0	"13240572"	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L143	4410	(organization or company or entity) same reputation	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L144	1061	(organization or company or entity) same reputation same (score or rating)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L145	19092	726/1,2,22,25.ccls.	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L146	120	L144 and L145	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L147	640	(organization or company) same reputation same (score or rating)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L148	55	L147 and L145	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L151	2	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L152	15	network (reputation or assess$4 or rat$3) with public with secur$5	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L153	31	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L154	23	L153 AND ((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L155	84	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43

		G06F21/577 OR G06F21/00).CPC.) and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)				
L156	36016	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L157	484	(network or organization or entity) reputation and (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L158	129	L157 and L156	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L159	0	"13240572"	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L160	0	"11237642"	US-PGPUB; USPAT; USOCR	ADJ	ON	2015/09/25 01:43
L163	0	"13240572"	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L164	10	726/25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L165	0	apparatus and method for network vulnerability detection and compliance	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L166	0	network vulnerability detection and compliance assesment	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L167	0	network vulnerability detection compliance assesment	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L168	0	network with vulnerability with detection with compliance with assesment	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L169	7	network with vulnerability with detection with compliance with assessment	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L170	37	726/2,22,25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L171	31	726/2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L172	41	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L173	3	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L174	118	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43

L175	10	726/25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L176	0	network with vulnerability with detection with compliance with assesment	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L177	20	US-7194769-$.DID. OR US-7290275-$.DID. OR US-7971252-$.DID. OR US-20040010709-$.DID. OR US-20050138413-$.DID. OR US-20080047018-$.DID. OR US-20080209565-$.DID. OR US-20090265787-$.DID. OR US-20090293128-$.DID. OR US-2007304-$.DID. OR US-5200596-$.DID. OR US-2009104-$.DID. OR US-422009D-$.DID. OR US-1331018-$.DID.	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2015/09/25 01:43
L178	0	(insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L177	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L179	260	network (reputation or assess$4 or rat$3) with public and security	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L180	84	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.) and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L181	118	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L183	84	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.) and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L184	118	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L185	0	L183 and L184	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L186	258	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L187	0	L183 and L185	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L188	0	L183 and L186	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L189	36016	((H04L63/20 OR H04L63/145 OR	US-	ADJ	ON	2015/09/25

		H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.)	PGPUB; USPAT			01:43
L190	8	L184 and L189	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43
L191	59	L186 and L189	US-PGPUB; USPAT	ADJ	ON	2015/09/25 01:43

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L49	0	"13240572"	US-PGPUB; USPAT; UPAD	ADJ	ON	2015/09/25 01:43
L69	0	"13240572"	US-PGPUB; USPAT; UPAD	ADJ	ON	2015/09/25 01:43
L149	0	"13240572"	US-PGPUB; USPAT; UPAD	ADJ	ON	2015/09/25 01:43
L150	0	"13240572"	US-PGPUB; USPAT; UPAD	ADJ	ON	2015/09/25 01:43
L161	1	"11237642"	US-PGPUB; USPAT; UPAD	ADJ	ON	2015/09/25 01:43
L162	1	"11368329"	US-PGPUB; USPAT; UPAD	ADJ	ON	2015/09/25 01:43
L182	0	"13240572"	US-PGPUB; USPAT; UPAD	ADJ	ON	2015/09/25 01:43

9/25/2015 1:49:39 AM
C:\Users\skanaan\Documents\EAST\Workspaces\13240572.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	Art Unit
	SIMON KANAAN	2432

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor and Assignee Search (PALM)	4/18/2013	SK
class/subclass search + text (EAST: 726/1,2,22,25+text)	11/13/2014	SK
CPC + text (EAST: H04L63/20,145,14,0236,1433,104 OR H04L67/306 OR H04L51/12 OR H04L61/1511 OR H04L9/321 OR G06F21/00,577 + text)	9/25/2015	SK

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/SIMON KANAAN/ Examiner.Art Unit 2432	

Substitute Disclosure Form	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No.	Application No.
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))		38879-0006001	13/240,572
		Applicant: Boyer et al.	
		Filing Date: September 22, 2011	Group Art Unit: 2432

U.S. Patent Documents							
Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate
	1.	2015/0074579	3-2015	Gladstone et al			

Foreign Patent Documents or Published Foreign Patent Applications								
Examiner Initial	Desig. ID	Document Number	Publication Date	Country or Patent Office	Class	Subclass	Translation Yes	Translation No

Other Documents (include Author, Title, Date, and Place of Publication)		
Examiner Initial	Desig. ID	Document
	2.	PAIR transaction history of US application no. 14/021,585 as of October 7, 2015 and application as filed.
	3.	PAIR transaction history of US application no. 61/386,156 as of October 7, 2015.

Examiner Signature	Date Considered

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Electronic Patent Application Fee Transmittal

Application Number:	13240572
Filing Date:	22-Sep-2011
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Filer:	David L Feigenbaum/jennifer franco
Attorney Docket Number:	38879-0006001

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Submission- Information Disclosure Stmt	2806	1	90	90
		Total in USD ($)		**90**

Electronic Acknowledgement Receipt

EFS ID:	23737338
Application Number:	13240572
International Application Number:	
Confirmation Number:	2423
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Customer Number:	26161
Filer:	David L Feigenbaum/jennifer franco
Filer Authorized By:	David L Feigenbaum
Attorney Docket Number:	38879-0006001
Receipt Date:	08-OCT-2015
Filing Date:	22-SEP-2011
Time Stamp:	19:02:55
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$90
RAM confirmation Number	5653
Deposit Account	061050
Authorized User	FISH & RICHARDSON P C

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		6001-IDS-1449.pdf	122676 3f93a8a838b14a22e43aa90ee3d48582136f630	yes	3
	Multipart Description/PDF files in .zip description				
	Document Description		**Start**	**End**	
	Transmittal Letter		1	2	
	Information Disclosure Statement (IDS) Form (SB08)		3	3	
Warnings:					
Information:					
2	Non Patent Literature	61386156-TH.pdf	88563 f6b5bee2f4ef6b14e885854d1e49d3efc06cb317	no	2
Warnings:					
Information:					
3	Non Patent Literature	14021585-TH-APP-.pdf	4935644 6e144a4e2fddfcc1c5c2189cec666e28aedaf250	no	70
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	30915 4a6aea8ce1ad727430f7b2296e78ef891f5c2b1e	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	5177798		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor	:	Stephen Boyer	Art Unit	:	2432
Serial No.	:	13/240,572	Examiner	:	Simon P. Kanaan
Filed	:	September 22, 2011	Conf. No.	:	2423
Title	:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM			

MAIL STOP AMENDMENT
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT

Please consider the references listed on the attached PTO-1449 form.

A copy of the United States patent document will be provided upon request. Copies of all non-U.S. patent documents and other documents are enclosed.

The United States patent applications and/or patents listed below contain material related to material in this application. Copies of the applications and/or patents, their current claims (in the case of patents), and their transaction histories from the patent office public PAIR website are enclosed (or were provided previously with information disclosure statements identified in the table).

The applicant invites the examiner to consider the claims and claim amendments of these other applications and/or patents, and the positions of the examiners and the applicant that appear in their prosecution histories. The applicant understands that the examiner has direct access to these papers at the patent office, but will be happy to provide copies to the examiner upon request.

US serial number and filing date/ status	Examiner and group art unit	Is patent or application attached and listed on form 1449 and/or what is the date of a prior information disclosure statement with which it was submitted	In the case of an application, are claims attached or what is the date of a prior information disclosure statement with which they were submitted	Is current PAIR transaction history attached and listed on form 1449
61/386,156 9/24/2010 Expired	N/A	No	No	Yes
61/492,287 6/1/2011 Issued	N/A	No	No	No - Unavailable in PAIR
14/021,585 9/9/2013 Pending	TBA GAU 2431	No – published application listed on 1449 form	Yes	Yes

This statement is being filed after a first action on the merits, but before receipt of a final action or a notice of allowance. A late submission fee in the amount of $90, specified by 37 CFR §1.17(p), is being paid with this statement.

Apply any necessary charges or credits to deposit account 06-1050, referencing the above attorney docket number.

Please contact the undersigned if there are any questions regarding this Statement.

Respectfully submitted,

Date:/10/8/15/_____

/David L. Feigenbaum/_____
David L. Feigenbaum
Reg. No. 30,378

Customer Number 26161
Fish & Richardson P.C.
Telephone: (617) 542-5070
Facsimile: (877) 769-7945

23445973.doc

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor	:	Stephen Boyer	Art Unit	:	2432
Serial No.	:	13/240,572	Examiner	:	Simon P. Kanaan
Filed	:	September 22, 2011	Conf. No.	:	2423
Title	:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM			

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY TO ACTION DATED JUNE 3, 2015

List of claims (replacing prior versions):

1. (currently amended) A method comprising:

collecting~~, from at least two sources,~~ information about two or more companies or other organizations that have computer systems, network resources, and employees, the organizations posing risks to themselves or to other parties through business relationships of the organizations with the other parties, the information collected about the organizations being indicative of ~~any one or more of (a) security vulnerabilities of the organizations, (b)~~ compromises ~~of~~ or indicative of vulnerabilities of technology systems, data, or other information of the organizations, or ~~(c)~~ indicative of resiliencies of the organizations to recover from security breaches,

at least some of the information about each of the organizations being collected automatically by computer using sensors on the Internet,

~~at least some of the information about each of the organizations being based on either or both of (a) communications from or to the organizations that are observed on the Internet and that do not explicitly identify and are indirectly indicative of the security vulnerabilities, compromises, or resiliencies, or (b) other observations that characterize the organizations,~~

the information about each of the organizations being collected from two or more sources, one or more of the sources not being controlled by the organization, the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization,

at least one of the sources for each of the organizations comprising a public source or a commercial source,

processing the information from ~~both of~~ the two or more sources for each of the organizations to form a composite rating that is indicative of a degree of risk to the organization or to a party through a business relationship with the organization, the composite rating comprising a calculated composite of metrics and data derived or collected from the sources, the processing comprising applying transformations to the data and metrics, and the processing comprising applying weights to the data and the metrics ~~two or more of (a) security vulnerability~~

~~of the organization, (b) compromise of a technology system, data, or information of the organization, (c) of a resilience of the organization to recover from a security breach~~,

~~the processing including applying models that account for differences in the respective sources,~~

~~the forming of the composite rating for each of the organizations including (a) aggregating metrics associated with a the computer system of the organization,~~ the metrics including ~~measures~~ a measure of the extent of or ~~of~~ the frequency of or ~~durations~~ duration of ~~compromises~~ compromise of the computer ~~system~~ systems or data, or of a configuration or vulnerability of the organization, or a measure of the resilience of the organization to recover from a security breach or vulnerability, ~~and (b) taking account of positive information about the organization,~~ and

in connection with ~~a~~ assessing a business risk to the organization or to a party through a business relationship with or with at least one of the organizations, delivering a report of the composite ratings of the organizations through a reporting facility to enable a user of the reporting facility to monitor, assess, and mitigate the risks, based on the security vulnerabilities or resiliencies or both, in doing business with the organization and to compare the composite ratings of the organizations.

2. (canceled)

3. (canceled)

4. (previously presented) The method of claim 1, wherein the collected information is represented by at least two data types.

5. (previously presented) The method of claim 4, wherein the at least two data types include at least one of breach disclosures, block lists, configuration parameters, an identification of malware servers, an identification of a reputation, an identification of suspicious activity, an identification of spyware, white lists, an identification of compromised hosts, an identification of malicious activity, an identification of spam activity, an identification of vulnerable hosts, an identification of phishing activity, or an identification of e-mail viruses.

6. (canceled)

7. (previously presented) The method of claim 1, wherein the collected information evidences internal security controls.

8. (previously presented) The method of claim 1, wherein the collected information comprises outcomes of each of the organizations.

9. (previously presented) The method of claim 1, wherein the collected information evidences operational execution of security measures of each of the organizations.

10. (previously presented) The method of claim 1, wherein the collected information indicates whether a computer system of each of the organizations served malicious code to another system.

11. (previously presented) The method of claim 1, wherein the collected information indicates whether a computer system of each of the organizations communicated with a known attacker controlled network or sensor outside the control or network of the organization.

12. (previously presented) The method of claim 1, comprising:
forming a series of the security ratings of each of the organizations.

13. (previously presented) The method of claim 12, comprising:
determining a trend from the series of ratings.

14. (previously presented) The method of claim 12, comprising:
displaying the series of composite ratings.

15. (canceled)

16. (previously presented) The method of claim 14, wherein displaying the series of composite ratings for each of the organizations comprises posting the series of composite ratings for the organization to a web portal.

17. (canceled)

18. (canceled)

19-120. (canceled)

121. (previously presented) The method of claim 1, wherein the collected information represents externally observable outcome information.

122. (previously presented) The method of claim 121, wherein the outcome information comprises outcome information associated with security vulnerability or resilience of each of the organizations.

123. (canceled)

124. (previously presented) The method of claim 1, comprising:

determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information.

125. (canceled)

126. (previously presented) The method of claim 1, wherein:

the collected information comprises at least two security characterizations of a computer system of each of the organizations.

127. (previously presented) The method of claim 1, wherein the collected information comprises a characterization of behavior of an employee of at least one of the organizations.

128. (previously presented) The method of claim 1, wherein the collected information comprises characterizations other than characterizations about a computer system of at least one of the organizations.

129. (previously presented) The method of claim 1, wherein the collected information comprises characterizations about policies of at least one of the organizations.

130. (previously presented) The method of claim 1, wherein the collected information comprises characterizations about information technology assets that at least one of the organizations owns, controls, uses, or is affiliated with.

131. (previously presented) The method of claim 1 in which collected information represents: (a) physical states, (b) technical states, (c) organizational states, or (d) cultural states of at least one of the organizations which can be exploited to create a security breach; or (e) the

organization's ability to recover from a security breach; or any combination of two or more of these.

132. (previously presented) The method of claim 1 in which processing the information to form a composite rating comprises correlating data across the sources of information.

133. (canceled)

134. (previously presented) The method of claim 1 in which processing the information to form a composite rating comprises statistically correlating the composite rating with actual outcomes.

135. (previously presented) The method of claim 1 in which the vulnerability comprises physical, technical, organizational, or cultural states that can be exploited to create a security breach.

136. (currently amended) A method comprising

collecting, from at least two sources, information about two or more companies or other organizations, the collected information representing at least two data types, the collected information comprising outcomes of each of the organizations,

at least some of the information for each of the organizations being collected automatically by computer from at least two sources, one or more of the sources not controlled by the organization,

the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization, at least one of the sources including a commercial data source,

processing the information from both of the two sources for each of the organizations to form a composite rating of a security vulnerability of the organization to creation of a security breach or a compromise of a system of the organization or of a resilience of the organization to ~~recovery~~ recover from a security breach or both, the processing including applying models that account for differences in the respective sources,

normalizing the composite rating of each of the organizations based on a size characteristic of the organization to enable comparisons of composite ratings between the two or more organizations,

forming a series of the security ratings of each of the organizations, determining a trend from the series of ratings, and displaying the series of composite ratings through a portal,

determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information, and

reporting the composite ratings of the organizations through a portal to enable customers to monitor, assess, and mitigate risk in doing business with the organizations and to compare the composite ratings across the organizations.

137. (previously presented) The system of claim 1, determining a confidence range of the composite rating, the size of the range varying inversely with the level of confidence in the composite rating.

138. (previously presented) The system of claim 137, wherein the confidence range is based on redundancy of the security characterizations.

139. (previously presented) The system of claim 137, wherein the confidence range is based on a size of the third party computer system.

140. (previously presented) The method of claim 1 comprising ranking the organization and other organizations within sectors or peer-groups or globally.

REMARKS

The comments of the applicant below are each preceded by related comments of the examiner (in small, bold type).

> **1. Claims 1 and 136, and 3-5, 7-14, 16, 121-122, 124, 126-135, and 137-140 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.**
>
> **2. The claim(s) does/do not fall within at least one of the four categories of patent eligible subject matter because the claimed invention is directed to a judicial exception (i.e., a law of nature, a natural phenomenon, or an abstract idea) without significantly more. Claim(s) 1 and 136 is/are directed towards the abstract idea gathering information regarding an entity and computing a rating score given the information gathered (See Oigitech, Organizing information through mathematical correlations).**

The applicant does not concede that the claims recite an abstract idea, nor that if they do the abstract idea is correctly characterized as "gathering information regarding an entity and computing a rating score given the information gathered."

> **The claims also recite the additional element including computer systems interacting with the internet to gather information about an organization and processing the information to form a rating. However, these additional elements are not sufficient to amount to significantly more than the judicial exception because the limitations are merely data gathering and instructions to implement the abstract idea on a computer which require no more than a generic computer to perform generic computer functions that are well-understood, routine and conventional activities previously known to the industry.**

The applicant respectfully disagrees with the examiner's premise and analysis. It is true that claim 1, for example, recites the collection of certain information "automatically by computer using sensors on the Internet," yet the examiner appears to have disregarded the substantial other features of the claim that amount to "significantly more" than the identified abstract idea.

These other features in claim 1 include, for example:

> "processing the information from both of the two or more sources for each of the organizations to form a [calculated] composite rating,"
>
> "the processing comprising applying weights to the data and the metrics,"
>
> "the metrics including a measure of the extent of or the frequency of or duration of compromise of the computer systems or data, or of a configuration or vulnerability the organization, or a measure of the resilience of the organization to recover from a security breach or vulnerability,"
>
> "delivering a report of the composite ratings of the organizations through a reporting facility to enable a user of the reporting facility to monitor, assess, and mitigate the risks, based on the security vulnerabilities or resiliencies or both, in

> doing business with the organization and to compare the composite ratings of the organizations."

These features alone and in combination amount to substantially more than the identified abstract idea.

As for claim 1, for claim 136 the examiner has apparently disregarded significant features that alone and in combination amount to substantially more than the alleged abstract idea, including, for example:

> "processing the information from both of the two sources for each of the organizations to form a composite rating of a security vulnerability of the organization to creation of a security breach or a compromise of a system of the organization or of a resilience of the organization to recovery recover from a security breach or both,
>
> "the processing including applying models that account for differences in the respective sources,"
>
> "normalizing the composite rating of each of the organizations based on a size characteristic of the organization to enable comparisons of composite ratings between the two or more organizations,"
>
> "forming a series of the security ratings of each of the organizations,"
>
> "determining a trend from the series of ratings,"
>
> "displaying the series of composite ratings through a portal,"
>
> "determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information, and"
>
> "reporting the composite ratings of the organizations through a portal to enable customers to monitor, assess, and mitigate risk in doing business with the organizations and to compare the composite ratings across the organizations."

> **Further, the claims do not recite an improvement to another technology or technical field, an improvement to the functioning of a computer itself, or meaningful limitations beyond generally linking the use of an abstract idea to a particular technological environment.**

The applicant respectfully disagrees. The features of the claims do recite an improvement to one or more technologies or technical fields, for example, the technology of deriving information about an organization from sources that include the Internet, without permission of the organization, and then using the information for determining how to interact with the organization. This is a challenging technology and a wide range of applications have been

proposed and used. Yet the applicant has invented a significant improvement that is not merely a linking of the abstract idea to that technology, as the recited features of the claims demonstrate.

Dependent claims 3-5,7-14, 16, 121-122, 124, 126-135, and 137-140 are also rejected for the same reason as cited above for not reciting any additional elements that amount to significantly more than the judicial exception.

9. Claims 1, 3-5, 7-14, 16, 121-122,124,126-140 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claim 1, the fifth limitation states "a party" renders the claim indefinite because it is unclear whether the "a party" is the party referred to in the first limitation or another party.

The applicant respectfully disagrees. The references in the first limitation are to "other parties", a phrase that differs from the words "a party" in the fifth limitation. The applicant believes that using these two phrases is appropriate claim wording and does not render the claim indefinite.

Regarding claim 1, the third limitation states "(a) communications from or to the organizations that are observed on the Internet and that do not explicitly identify and are indirectly indicative of the security vulnerabilities, compromises, or resiliencies" renders the claim indefinite as it is unclear what "that do not explicitly identify" is referring to and also it is unclear what the "are indirectly indicative" is referring to.

The limitation has been deleted.

Regarding claim 1, the fifth limitation states "both of the two or more" renders the claim indefinite as both refers to two while the two or more refers to two or more making the claim indefinite as it is unclear whether it is two or at least two.

Fixed.

Regarding claim 1, the second limitation states "at least some of the information about each of the organizations being collected automatically by computer," which renders the claim indefinite as it is unclear how the information is collected automatically whether the computer is gathering information without user input continuously or user inputs into the computer certain parameters and then the computer gathers information.

The limitation has been deleted.

Regarding claim 136, the second limitation states "at least some of the information about each of the organizations being collected automatically by computer," which renders the claim indefinite as it is unclear how the information is collected automatically whether the computer is gathering information without user input continuously or user inputs into the computer certain parameters and then the computer gathers information.

The limitation is meant to include both of those examples and others.

10. Claims 1,3-5,7-14,16, 121-124, 136-132 and 134-140 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chris Newton (US Pre-Grant Publication No: 2004/0250122 A 1)

hereinafter referred to as Newton in view of in view of Shull et al. (US Pre-Grant Publication No: 2006/0212925 A 1) hereinafter referred to as Shull.

As per claim 1, Newton discloses a method comprising: collecting, from at least two sources, information about two or more companies or other organizations, that have computer systems, network resources, and employees, the organizations posing risks to themselves or to other parties through business relationships of the organizations with the other parties, the information collected about the organizations being indicative of anyone or more of (a) security vulnerabilities of the organizations, (b) compromises of technology systems, data, or other information of the organizations, or (c) resiliencies of the organizations to recover from security breaches, at least some of the information about each of the organizations being collected automatically by computer, at least some of the information about each of the organizations being based on either or both of (a) communications from or to the organizations that are observed on the Internet and that do not explicitly identify and are indirectly indicative of the security vulnerabilities, compromises, or resiliencies, or (b) other observations that characterize the organizations, one or more of the sources not being controlled by the organization, the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization,

The applicant disputes that all of the above features of the applicant's claim 1 were described in or made obvious by Newton.

Newton, [0012] teaches that every network in the world would have a rating in the database

The applicant respectfully notes that Newton did not say that every network in the world would have a "rating" in the database. To the contrary, Newton merely said that every network in the world would have a "record" in the database, which is a very different notion. Furthermore, the applicant's claim 1 refers to forming a "composite rating that is indicative of a degree of risk to the organization or to a party through a business relationship with the organization." The cited part of Newton neither described nor would have made obvious a composite rating with respect to an organization as opposed to a network. This, too, is an important distinction.

and [0030] teaches establishing a reputation for a network,

Again, Newton's reference to a reputation for a network did not describe and would not have made obvious a composite rating related to an organization. Those are two quite different concepts.

and [0031] teaches having multiple agents gathering data and

[0044]-[0048] teaches different agent types i.e. different network characterization as each agent type gathers different type of data in regards to the security and reputation of network, among these agents include data mining internet which is public information and data mining newsgroups and forums which are also public knowledge and externally observable information not controlled by an organization and

> **figure 1, items 24 include information about the network which towards the bottom of item 24 states "company info resources" i.e. network is associated with a company and**
>
> **[0022] and [0072], teaches taking into account size of the network and number of employees.**
>
> **processing the information from both of the two or more sources for each of the organizations to form (A) security vulnerability of the organization (b) compromise of a technology system of the organization, (c) a resilience of the organization to recover from a security breach, the processing including applying models that account for differences in the respective sources,**

This element of claim 1 has been amended to recite

> … a composite rating that is indicative of a degree of risk to the organization or to a party through a business relationship with the organization, the composite rating comprising a calculated composite of metrics and data derived or collected from the sources, the processing comprising applying transformations to the data and metrics, and the processing comprising applying weight to the data and the metrics.

Paragraph 0022 of Newton, by contrast, was simply an item in a list of properties of networks. That paragraph said "Active security measures, firewalls, IDSs". Paragraph 0022 did not describe and would not have made obvious "a degree of risk to the organization or to a party through a business relationship with the organization," let alone the other quoted features of that clause of the applicant's claim 1.

> **Newton, [0044]-[0048] and [0029], teaches information gathered externally from multiple sources including proxy information. But does not teach the forming of the composite rating for each of the organizations including (a) aggregating metrics associated with the computer system of the organization, the metrics including measures of the frequency of or durations of compromises of the computer system of the organization, and taking account of positive information about the organization and in connection with a assessing a business risk to the organization or to a party through a business relationship with or with at least one of the organizations, delivering a report of the composite ratings of the organizations through a portal to enable a user of the reporting facility to monitor, assess, and mitigate the risks, based on the security vulnerability or resiliencies or both, in doing business with the organization and to compare the composite ratings of the organizations.**

The applicant does not dispute the examiner's position on this point.

> **However, Shull [0058] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score which informs requester of the trust of the entity, this score is received by the requester where activities are accounted for both legitimate (i.e. positive) and illegitimate (i.e. negative) and [0069] and [0073], teaches giving an overall trust score between 1 and 5 i.e. a normalized composite score where 1 is a reputable business and 5 is likely engaged in illicit activity. It would have been obvious at the time of the invention for one of the ordinary skill in the art to modify the method of collecting security characteristics from multiple sources as taught by Newton by creating a score representative of the different collected data as taught by Shull because it would aid the requester in determining whether the entity is trusted or not.**

The applicant has amended claim 1 to recite that the processing to form the calculated composite comprises applying transformations to the data and metrics and applying weight to the data and metrics. Paragraph 0058 of Shull did not, as far as the applicant can see, describe the processing done to reach score, except for the statement that the score was "based on its identifying information, relationship information, and history." Nor did figure 8. In paragraph 0069, Shull described that a portfolio score could "include factors such as a size of the corporation… and/or a number of IP addresses…" Or that a secure infrastructures score could include "factor counting a number of certificates associated with an online entity, number of unsecured servers associated with the entity, etc." Paragraph 0073 of Shull referred to a scoring system from 1 to 5.

Yet none of the cited portions of Shull described or would have made obvious that the score was derived by processing that included applying transformations to the data and metrics and applying weights to the data and the metrics.

Shull was silent about that.

Therefore, even if there would have been some reason to combine Newton with Shull (which the applicant does not concede), the result would not have been the effective and useful combination of features recited in the applicant's amended claim 1.

As per claim 3, Newton in view of Shull … .

As per claim 4, Newton in view of Shull … .

As per claim 5, Newton in view of Shull … .

As per claim 7, Newton in view of Shull … .

As per claim 8, Newton in view of Shull … .

As per claim 9, Newton in view of Shull … .

As per claim 10, Newton in view of Shull … .

As per claim 11, Newton in view of Shull … .

As per claim 12, Newton in view of Shull … .

As per claim 13, Newton in view of Shull … .

As per claim 14, Newton in view of Shull … .

As per claim 16, Newton in view of Shull … .

As per claim 121, Newton in view of Shull … .

As per claim 122, Newton in view of Shull … .

As per claim 123, Newton in view of Shull … .

As per claim 124, Newton in view of Shull … .

As per claim 126, Newton in view of Shull … .

As per claim 127, Newton in view of Shull … .

As per claim 128, Newton in view of Shull … .

As per claim 129, Newton in view of Shull … .

As per claim 130, Newton in view of Shull … .

As per claim 131, Newton in view of Shull … .

As per claim 132, Newton in view of Shull … .

As per claim 134, Newton in view of Shull … .

As per claim 135, Newton in view of Shull … .

As per claim 136, Newton teaches a method comprising collecting, from at least two sources, information about two or more companies or other organizations, the collected information representing at least two data types, the collected information comprising outcomes of each of the organizations, at least some of the information for each of the organizations being collected automatically by computer from at least two sources, one or more of the sources not controlled by the organization, the information from at least the one or more sources that are not controlled by the organization being collected without permission of the-organization, at least one of the sources including a commercial data source,

The applicant disputes that all of the above features of the applicant's claim 136 were described in or made obvious by Newton.

Newton, [0012] teaches that every network in the world would have a rating in the database and [0030] teaches establishing a reputation for a network, and [0031] teaches having multiple agents gathering data and [0044]-[0048] teaches different agent types i.e. different network characterization as each agent type gathers different type of data in regards to the security and reputation of network, among these agents include data mining internet which is public information and data mining newsgroups and forums which are also public knowledge and externally observable information not controlled by an organization and figure 1, items 24 include information about the network which towards the bottom of item 24 states "company info resources" i.e. network is associated with a company, and [0022] and [0072], teaches taking into account size of the network and number of employees.

Please refer to the applicant's comments with respect to the rejection of claim 1.

and displaying the series of ratings through a portal and reporting the ratings of the organizations through a portal to enable customers to monitor, assess, and mitigate risk in doing business with the organizations and to compare the composite ratings across the organizations. Newton, figure 3 item 14, teaches a database which stores information about the organizations i.e. portal.

The applicant respectfully disagrees. Newton described the use of the customer network intelligence database (C-NID) by the policy enforcer [0053] as follows:

> "the PE 20 allows an administrator to take conceptual ideas of who he wants his network to talk to … and turns them into the technical rules sets … via info from

> the C-NID .... The policy enforcer 20 then takes that concept, and with the help of the C-NID 14, turns it into a rule set of matching networks and feeds into the NID device agent on the mail server 46."

In other words, Newton's C-NID held information that could be used by the policy enforcer process but was not a portal through which a customer interacted let alone monitored, assessed, or mitigated risk in doing business with the organizations or to compare the composite ratings across the organizations.

> **But Newton does not teach processing the information from both of the two sources for each of the organizations to form a composite rating of a security vulnerability of the organization to creation of a security breach or a compromise of a system of the organization or of a resilience of the organization to recovery from a security breach or both, the processing including applying models that account for differences in the respective sources, normalizing the composite rating of each of the organizations based on a size characteristic of the organization to enable comparisons of composite ratings between the two or more organizations, forming a series of the security ratings of each of the organizations, determining a trend from the series of ratings, determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information.**

The applicant does not dispute the examiner's position.

> **However, Shull [0058] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score which informs requester of the trust of the entity, this score is received by the requester where activities are accounted for both legitimate (i.e. positive) and illegitimate (i.e. negative) and [0069] and [0073], teaches giving an overall trust score between 1 and 5 i.e. a normalized composite score where 1 is a reputable business and 5 is likely engaged in illicit activity. It would have been obvious at the time of the invention for one of the ordinary skill in the art to modify the method of collecting security characteristics from multiple sources as taught by Newton by creating a score representative of the different collected data as taught by Shull because it would aid the requester in determining whether the entity is trusted or not.**

Claim 136 recites that the processing includes applying models that account for differences in the respective sources. The recited portions of Shull did not describe and would not have made obvious applying models that account for differences in the respective sources, nor does the examiner contend that they do.

The score determined by Shull as described in paragraph 0058 appears to have been a score indicative of "the relative reliability of various online entities in adhering to determined characteristics." In addition, with respect to Shull's score range 1 through 5, paragraph 0058 said "a score of 1 may indicate the online entity has been verified and/or certified as reliable … A score of 2 may indicate that the entity is relatively likely to be reputable … While escort 3 may indicate that the identification and/or reputation of an entity is doubtful…" Therefore, the scoring

range was representative of relative reliability or reputation and not of the elements recited in the applicant's claim 136. Claim 136 recites that the composite rating is a rating of "a security vulnerability of the organization to creation of a security breach or a compromise of the system of the organization or of a resilience of the organization to recover from a security breach or both." Shull did not describe and would not have made obvious such a rating.

Claim 136 recites "determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information." The examiner cited Shull's paragraphs 0069 and 0073 as having described this feature because a low score in Shull indicated negative activities. But Shull did not describe and would not have made obvious that a badness score should correspond to "an intensity or duration of malicious activity determined from the collected information."

Claim 136 recites "normalizing the composite rating of each of the organizations based on a size characteristic of the organization to enable comparisons of composite ratings between the two or more organizations. The cited portions of Shull did not describe and would not of made obvious that the scoring range of 1 through 5 was derived by "normalizing based on a size characteristic of the organization."

Because of the absence of particular claimed features in both Shull and Newton, even if there had been some reason to combine the two references (which the applicant does not concede), the result could not have been the combination of the applicant's amended claim 136.

As per claim 137, Newton in view of Shull … .

As per claim 138, Newton in view of Shull … .

As per claim 139, Newton in view of Shull … .

As per claim 140, Newton in view of Shull … .

All of the dependent claims are patentable for at least similar reasons as those for the claims on which they depend are patentable.

Canceled claims, if any, have been canceled without prejudice or disclaimer.

Any circumstance in which the applicant has (a) addressed certain comments of the examiner does not mean that the applicant concedes other comments of the examiner, (b) made

arguments for the patentability of some claims does not mean that there are not other good reasons for patentability of those claims and other claims, or (c) amended or canceled a claim does not mean that the applicant concedes any of the examiner's positions with respect to that claim or other claims.

Please apply any charges or credits to deposit account 06-1050, referencing attorney docket 38879-0006001.

Respectfully submitted,

Date: September 2, 2015

/Paul Pysher/

Paul A. Pysher
Reg. No. 40,780

Customer Number 26161
Fish & Richardson P.C.
Telephone: (617) 542-5070
Facsimile: (877) 769-7945

23410480.doc

Electronic Acknowledgement Receipt

EFS ID:	23378956
Application Number:	13240572
International Application Number:	
Confirmation Number:	2423
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Customer Number:	26161
Filer:	Paul A Pysher/jennifer franco
Filer Authorized By:	Paul A Pysher
Attorney Docket Number:	38879-0006001
Receipt Date:	02-SEP-2015
Filing Date:	22-SEP-2011
Time Stamp:	11:09:04
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		response.pdf	125794 0c0c6d81dfdd4dc51a53872b7afc3b2b548aefa5	yes	17

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	7
	Applicant Arguments/Remarks Made in an Amendment	8	17
Warnings:			
Information:			
	Total Files Size (in bytes):	125794	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/240,572	Filing Date 09/22/2011	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT **09/02/2015**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 29	Minus	** 31	= 0	X $40 =	0
Independent (37 CFR 1.16(h))	* 2	Minus	***2	= 0	X $210 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/CHERYL CLARK/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/240,572	09/22/2011	Stephen Wayne Boyer	38879-0006001	2423

26161 7590 06/03/2015

FISH & RICHARDSON P.C. (BO)
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
KANAAN, SIMON P	

ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
06/03/2015	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATDOCTC@fr.com

Office Action Summary	Application No. 13/240,572	Applicant(s) BOYER ET AL.	
	Examiner SIMON KANAAN	Art Unit 2432	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 May 2015*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1,3-5,7-14,16,121-124,126-132 and 134-140* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1,3-5,7-14,16,121-124,126-132 and 134-140* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *22 September 2011* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some * c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Interim copies:

a)☐ All b)☐ Some c)☐ None of the: Interim copies of the priority documents have been received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions

2. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 22 MAY 2015 has been entered.

Office Action Summary

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. Applicant’s arguments/amendments filed 5/22/2015 have been considered but are not persuasive. Please refer to the grounds of rejection presented below.

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. Claims 1 and 136, and 3-5, 7-14, 16, 121-122, 124, 126-135, and 137-140 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

7. The claim(s) does/do not fall within at least one of the four categories of patent eligible subject matter because the claimed invention is directed to a judicial exception (i.e., a law of nature, a natural phenomenon, or an abstract idea) without significantly more. Claim(s) 1 and 136 is/are directed towards the abstract idea gathering information regarding an entity and computing a rating score given the information gathered (See *Digitech, Organizing information through mathematical correlations*). The claims also recite the additional element including computer systems interacting with the internet to gather information about an organization and processing the information to form a rating. However, these additional elements are not sufficient to amount to significantly more than the judicial exception because the limitations are merely data gathering and instructions to implement the abstract idea on a computer which require no more than a generic computer to perform generic computer functions that are well-understood, routine and conventional activities previously known to the industry. Further, the claims do not recite an improvement to another technology or technical field, an improvement to the functioning of a computer itself, or meaningful limitations

beyond generally linking the use of an abstract idea to a particular technological environment.

Dependent claims 3-5, 7-14, 16, 121-122, 124, 126-135, and 137-140 are also rejected for the same reason as cited above for not reciting any additional elements that amount to significantly more than the judicial exception.

Claim Rejections - 35 USC § 112

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 1, 3-5, 7-14, 16, 121-122, 124, 126-140 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claim 1, the fifth limitation states "a party" renders the claim indefinite because it is unclear whether the “a party” is the party referred to in the first limitation or another party.

Regarding claim 1, the third limitation states “(a) communications from or to the organizations that are observed on the Internet and that do not explicitly identify and are indirectly indicative of the security vulnerabilities, compromises, or resiliencies” renders the claim indefinite as it is unclear what “that do not explicitly identify” is referring to and also it is unclear what the “are indirectly indicative" is referring to.

Regarding claim 1, the fifth limitation states “both of the two or more” renders the claim indefinite as both refers to two while the two or more refers to two or more making the claim indefinite as it is unclear whether it is two or at least two.

Regarding claim 1, the last limitation states "a party" renders the claim indefinite because it is unclear whether the “a party” is the party referred to in the first limitation or another party.

Regarding claim 1, the second limitation states “at least some of the information about each of the organizations being collected automatically by computer,” which renders the claim indefinite as it is unclear how the information is collected automatically whether the computer is gathering information without user input continuously or user inputs into the computer certain parameters and then the computer gathers information.

Regarding claim 136, the second limitation states “at least some of the information about each of the organizations being collected automatically by computer,” which renders the claim indefinite as it is unclear how the information is collected automatically whether the computer is gathering information without user input continuously or user inputs into the computer certain parameters and then the computer gathers information.

Claims 3-5, 7-14, 16, 121-122, 124, 126-135 and 137-140 are dependent on claims 1 and 136 but do not clarify the deficiencies of independent claims 1 and 136 and are rejected for the same rational as claims 1 and 136.

Claim Rejections - 35 USC § 103

10. Claims 1,3-5,7-14,16, 121-124, 136-132 and 134-140 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chris Newton (US Pre-Grant Publication No: 2004/0250122 A1) hereinafter referred to as Newton in view of in view of Shull et al. (US Pre-Grant Publication No: 2006/0212925 A1) hereinafter referred to as Shull.

As per claim 1, Newton discloses a method comprising: collecting, from at least two sources, information about two or more companies or other organizations, that have computer systems, network resources, and employees, the organizations posing risks to themselves or to other parties through business relationships of the organizations with the other parties, the information collected about the organizations being indicative of any one or more of (a) security vulnerabilities of the organizations, (b) compromises of technology systems, data, or other information of the organizations, or (c) resiliencies of the organizations to recover from security breaches, at least some of the information about each of the organizations being collected automatically by computer, at least some of the information about each of the organizations being based on either or both of (a) communications from or to the organizations that are observed on the Internet and that do not explicitly identify and are indirectly indicative of the security vulnerabilities, compromises, or resiliencies, or (b) other observations that characterize the organizations, one or more of the sources not being controlled by the organization, the information format least the one or more sources that are not controlled by the

organization being collected without permission of the organization, -Newton, [0012] teaches that every network in the world would have a rating in the database and [0030] teaches establishing a reputation for a network, and [0031] teaches having multiple agents gathering data and [0044]-[0048] teaches different agent types i.e. different network characterization as each agent type gathers different type of data in regards to the security and reputation of network, among these agents include data mining internet which is public information and data mining newsgroups and forums which are also public knowledge and externally observable information not controlled by an organization and figure 1, items 24 include information about the network which towards the bottom of item 24 states "company info resources" i.e. network is associated with a company and [0022] and [0072], teaches taking into account size of the network and number of employees.

processing the information from both of the two or more sources for each of the organizations to form (A) security vulnerability of the organization (b) compromise of a technology system of the organization, (c) a resilience of the organization to recover from a security breach, the processing including applying models that account for differences in the respective sources, –Newton, [0044]-[0048] and [0029], teaches information gathered externally from multiple sources including proxy information.

But does not teach the forming of the composite rating for each of the organizations including (a) aggregating metrics associated with the computer system of the organization, the metrics including measures of the frequency of or durations of compromises of the computer system of the organization, and taking account of positive

information about the organization and in connection with a assessing a business risk to the organization or to a party through a business relationship with or with at least one of the organizations, delivering a report of the composite ratings of the organizations through a portal to enable a user of the reporting facility to monitor, assess, and mitigate the risks, based on the security vulnerability or resiliencies or both, in doing business with the organization and to compare the composite ratings of the organizations.

However, Shull [0058] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score which informs requester of the trust of the entity, this score is received by the requester where activities are accounted for both legitimate (i.e. positive) and illegitimate (i.e. negative) and [0069] and [0073], teaches giving an overall trust score between 1 and 5 i.e. a normalized composite score where 1 is a reputable business and 5 is likely engaged in illicit activity.

It would have been obvious at the time of the invention for one of the ordinary skill in the art to modify the method of collecting security characteristics from multiple sources as taught by Newton by creating a score representative of the different collected data as taught by Shull because it would aid the requester in determining whether the entity is trusted or not.

As per claim 3, Newton in view of Shull teaches the method of Claim 1, wherein at least one source includes a commercial data source. –Newton, [0044]-[0048] teaches using different search engines such as Google and [0016] teaches hosted services.

As per claim 4, Newton in view of Shull discloses the method of Claim 1, wherein the collected information is represented by at least two data types. –Green, [0044]-[0048] teaches different agent types.

As per claim 5, Newton in view of Shull discloses the method of Claim 4, wherein the at least two data types include at least one of breach disclosures, block lists, configuration parameters, an identification of malware servers, an identification of a reputation, an identification of suspicious activity, an identification of spyware, white lists, an identification of compromised hosts, an identification of malicious activity, an identification of spam activity, an identification of vulnerable hosts, an identification of phishing activity, or an identification of e-mail viruses. –Newton, [0013]-[0029] teaches security measures etc.

As per claim 7, Newton in view of Shull discloses the method of Claim 1, wherein the collected information evidences internal security controls. –Newton, [0013]-[0029] teaches security measures etc.

As per claim 8, Newton in view of Shull discloses the method of Claim 1, wherein the collected information comprises outcomes of each of the organizations. –Newton, [0013]-[0029] teaches security measures and [0044]-[0048] teaches checking for information already available to the public about network.

As per claim 9, Newton in view of Shull discloses the method of Claim 1, wherein the collected information evidences operational execution of security measures of the organizations. –Newton, [0013]-[0029] teaches security measures.

As per claim 10, Newton in view of Shull discloses the method of Claim 1, wherein the collected information indicates whether a computer system of the organizations served malicious code to another system. –Newton, [0013], teaches hostility level and page 4, claim 6, teaches spam levels.

As per claim 11, Newton in view of Shull discloses the method of Claim 1, wherein the collected information indicates whether a computer system of the organizations communicated with a known attacker controlled network or sensor outside the control network of the organization. –Newton, [0013] teaches hostility level.

As per claim 12, Newton in view of Shull discloses the method of Claim 1, comprising: forming a series of the security ratings of the organizations. –Newton, [0042], teaches live remote updates i.e. continually computing rating and page 4, claim 6 teaches security information has multiple ratings and [0041], teaches the different information having different weight.

As per claim 13, Newton in view of Shull discloses the method of Claim 12, comprising determining a trend from the series of ratings. –Newton, [0042], teaches live remote updates i.e. continually computing rating.

As per claim 14, Newton in view of Shull discloses the method of Claim 12, comprising displaying the series of composite ratings. –Newton, [0033], teaches a master database for collecting and storing the network ratings and page 4, claim 6 teaches security information has multiple ratings and [0041], teaches the different information having different weight and Shull, [0058], [0076] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score with informs requester of the trust of the entity, this score is received by the requester and a display device would display score as to help user determine whether to trust entity or not.

As per claim 16, Newton in view of Shull teaches the method of Claim 14, wherein displaying the series of composite ratings for each of the organizations comprises posting the series of composite ratings for each of the organizations to a web portal. -Newton, [0033], teaches a master database for collecting and storing the network ratings which includes information as listed in [0013]-[0029] which serve as warnings and Shull, [0058], [0076] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score with informs requester of the trust of the entity, this score is received by the requester and a display device would display score as to help user determine whether to trust entity or not.

As per claim 121, Newton in view of Shull teaches the method of Claim 1, wherein the collected information represents externally observable outcome information.

- Newton, [0054], teaches agents getting information from news groups or sending packets and checking their responses.

As per claim 122, Newton in view of Shull teaches the method of Claim 121, wherein the outcome information comprises outcome information associated with security vulnerability or resilience of each of the organizations. Shull, [0058] and Newton, page 4, claim 6, both teach that the information is associated with entity security and Newton even looks into active security systems as well.

As per claim 123, Newton in view of Shull teaches the method of Claim 1, wherein the customers have a security risk associated with the vulnerability or resilience of at least one of the organizations. - Shull, [0058], teaches a composite score which would be indicative of risk.

As per claim 124, Newton in view of Shull teaches the method of Claim 1, comprising: determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information. - Newton, page 4, claim 6, teaches having spam levels etc. Which are a badness score.

As per claim 126, Newton in view of Shull teaches the method of Claim 1, wherein: the collected information comprises at least two security characterizations of a computer system of the entity. - Newton, page 4, claim 6, teaches checking open proxy

servers and desktop security measures which are multiple characterizations of a system of the entity.

As per claim 127, Newton in view of Shull teaches the method of Claim 1, wherein the collected information comprises a characterization of behavior of an employee of at least one of the organizations. - Newton, page 4, claim 6, inappropriate content served, spam levels, language spoken, geographic placement, industry, which are characterizations of employees in the network and the employees' behavior.

As per claim 128, Newton in view of Shull teaches the method of Claim 1, wherein the collected information comprises characterizations other than characterizations about a computer system of at least one of the organizations. - Newton, page 4, claim 6, teaches security characterization includes security personnel.

As per claim 129, Newton in view of Shull teaches the method of Claim 1, wherein the collected information comprises characterizations about policies of at least one of the organizations. –Newton, page 4, claim 6, teaches organization association, active security measures, desktop security measures, etc. which are policies see also [0059] and [0060].

As per claim 130, Newton in view of Shull teaches the method of Claim 1, wherein the collected information comprises characterizations about information

technology assets that at least one of the organizations owns, controls, uses, or is affiliated with. –Newton, page 4, claim 6, teaches organization associations see also [0043] and [0053].

As per claim 131, Newton in view of Shull teaches the method of Claim 1 in which collected information represents: (a) physical states, (b) technical states, (c) organizational states, or (d) cultural states of at least one of the organizations which can be exploited to create a security breach; or (e) the organization's ability to recover from a security breach; or any combination of two or more of these. –Newton, page 4, claim 6, teaches active security measures and desktop security measures among other information collected about the organization.

As per claim 132, Newton in view of Shull teaches the method of claim 1 in which processing the information to form a composite rating comprises correlating data across the sources of information.-Shull, [0058], teaches creating a score based on the different data received i.e. correlating the different data.

As per claim 134, Newton in view of Shull teaches the method of claim 1 in which processing the information to form a composite rating comprises statistically correlating the composite rating with actual outcomes. – Newton, [0041], teaches giving different information different weight where less weight given to information as it becomes less important over time which is a statistical correlation with the information collected.

As per claim 135, Newton in view of Shull teaches the method of claim 1 in which the vulnerability comprises physical, technical, organizational, or cultural states that can be exploited to create a security breach. –Newton, figure 1, item 24 and page 4, claim 6.

As per claim 136, Newton teaches a method comprising collecting, from at least two sources, information about two or more companies or other organizations, the collected information representing at least two data types, the collected information comprising outcomes of each of the organizations, at least some of the information for each of the organizations being collected automatically by computer from at least two sources, one or more of the sources not controlled by the organization, the information from at least the one or more sources that are not controlled by the organization being collected without permission of the-organization, at least one of the sources including a commercial data source, -Newton, [0012] teaches that every network in the world would have a rating in the database and [0030] teaches establishing a reputation for a network, and [0031] teaches having multiple agents gathering data and [0044]-[0048] teaches different agent types i.e. different network characterization as each agent type gathers different type of data in regards to the security and reputation of network, among these agents include data mining internet which is public information and data mining newsgroups and forums which are also public knowledge and externally observable information not controlled by an organization and figure 1, items 24 include information about the network which towards the bottom of item 24 states "company info

resources" i.e. network is associated with a company, and [0022] and [0072], teaches taking into account size of the network and number of employees.

and displaying the series of ratings through a portal and reporting the ratings of the organizations through a portal to enable customers to monitor, assess, and mitigate risk in doing business with the organizations and to compare the composite ratings across the organizations. –Newton, figure 3 item 14, teaches a database which stores information about the organizations i.e. portal.

But Newton does not teach processing the information from both of the two sources for each of the organizations to form a composite rating of a security vulnerability of the organization to creation of a security breach or a compromise of a system of the organization or of a resilience of the organization to recovery from a security breach or both, the processing including applying models that account for differences in the respective sources, normalizing the composite rating of each of the organizations based on a size characteristic of the organization to enable comparisons of composite ratings between the two or more organizations, forming a series of the security ratings of each of the organizations, determining a trend from the series of ratings, determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information.

However, Shull [0058] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score which informs requester of the trust of the entity, this score is received by the requester where activities are accounted for both legitimate (i.e. positive) and illegitimate (i.e. negative) and [0069]

and [0073], teaches giving an overall trust score between 1 and 5 i.e. a normalized composite score where 1 is a reputable business and 5 is likely engaged in illicit activity.

It would have been obvious at the time of the invention for one of the ordinary skill in the art to modify the method of collecting security characteristics from multiple sources as taught by Newton by creating a score representative of the different collected data as taught by Shull because it would aid the requester in determining whether the entity is trusted or not.

As per claim 137, Newton in view of Shull teaches the system of claim 1, determining a confidence range of the composite rating, the size of the range varying inversely with the level of confidence in the composite rating. - Shull, [0069] and [0073], teaches giving an overall trust score between 1 and 5 i.e. a normalized composite score where 1 is a reputable business and 5 is likely engaged in illicit activity.

As per claim 138, Newton in view of Shull teaches the system of claim 137, wherein the confidence range is based on redundancy of the security characterizations. –Shull, [0081], teaches taking into account consistency which is redundancy.

As per claim 139, Newton in view of Shull teaches the system of claim 137, wherein the confidence range is based on a size of the third party computer system. – Newton, [0072], teaches taking into account size of the network.

As per claim 140, Newton in view of Shull teaches the method of claim 1 comprising ranking the organization and other organizations within sectors or peer-groups or globally. –Shull, [0123]-[0124], teaches listing entities with similar scores together such as ones that scored a 3 or 4 so these would be ranked below ones which were listed as part of white list which ranked 1 or 2, see [0068], which teaches having white list, black list and grey lists.

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Simon Kanaan whose telephone number is (571)270-3906. The examiner can normally be reached on Mon-Thurs 7:30-5:00 EST.

If attempts to reach the above noted Examiner by telephone are unsuccessful, the Examiner's supervisor, Gilberto Barron, can be reached at the following telephone number: (571) 272-3799.

The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.

/S. K./
Examiner, Art Unit 2432

/GILBERTO BARRON JR/
Supervisory Patent Examiner, Art Unit 2432

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	72	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.) and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2015/05/28 23:54
L2	117	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2015/05/28 23:54
L3	0	L1 and L2	US-PGPUB; USPAT	ADJ	ON	2015/05/28 23:54
L4	241	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial	US-PGPUB; USPAT	ADJ	ON	2015/05/28 23:54
L5	0	l1 and l3	US-PGPUB; USPAT	ADJ	ON	2015/05/28 23:55
L6	0	l1 and l4	US-PGPUB; USPAT	ADJ	ON	2015/05/28 23:55
L7	33676	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.)	US-PGPUB; USPAT	ADJ	ON	2015/05/28 23:55
L8	8	l2 and l7	US-PGPUB; USPAT	ADJ	ON	2015/05/28 23:55
L9	53	l4 and l7	US-PGPUB; USPAT	ADJ	ON	2015/05/28 23:55

EAST Search History (Interference)

< This search history is empty>

5/28/2015 11:57:08 PM
C:\Users\skanaan\Documents\EAST\Workspaces\13240572.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	Art Unit
	SIMON KANAAN	2432

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor and Assignee Search (PALM)	4/18/2013	SK
class/subclass search + text (EAST: 726/1,2,22,25+text)	11/13/2014	SK
CPC + text (EAST: H04L63/20,145,14,0236,1433,104 OR H04L67/306 OR H04L51/12 OR H04L61/1511 OR H04L9/321 OR G06F21/00,577 + text)	5/28/2015	SK

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/SIMON KANAAN/ Examiner.Art Unit 2432	

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	Art Unit
	SIMON KANAAN	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/18/2013	11/07/2013	06/04/2014	02/22/2015	05/28/2015				
	1	✓	✓	✓	✓	✓				
	2	✓	✓	-	-	-				
	3	✓	✓	✓	✓	✓				
	4	✓	✓	✓	✓	✓				
	5	✓	✓	✓	✓	✓				
	6	✓	✓	-	-	-				
	7	✓	✓	✓	✓	✓				
	8	✓	✓	✓	✓	✓				
	9	✓	✓	✓	✓	✓				
	10	✓	✓	✓	✓	✓				
	11	✓	✓	✓	✓	✓				
	12	✓	✓	✓	✓	✓				
	13	✓	✓	✓	✓	✓				
	14	✓	✓	✓	✓	✓				
	15	✓	✓	-	-	-				
	16	✓	✓	✓	✓	✓				
	17	✓	✓	-	-	-				
	18	✓	✓	-	-	-				
	19	✓	✓	-	-	-				
	20	✓	✓	-	-	-				
	21	-	-	-	-	-				
	22	-	-	-	-	-				
	23	-	-	-	-	-				
	24	-	-	-	-	-				
	25	-	-	-	-	-				
	26	-	-	-	-	-				
	27	-	-	-	-	-				
	28	-	-	-	-	-				
	29	-	-	-	-	-				
	30	-	-	-	-	-				
	31	-	-	-	-	-				
	32	-	-	-	-	-				
	33	-	-	-	-	-				
	34	-	-	-	-	-				
	35	-	-	-	-	-				
	36	-	-	-	-	-				

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	**Art Unit**
	SIMON KANAAN	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/18/2013	11/07/2013	06/04/2014	02/22/2015	05/28/2015				
	37	-	-	-	-	-				
	38	-	-	-	-	-				
	39	-	-	-	-	-				
	40	-	-	-	-	-				
	41	-	-	-	-	-				
	42	-	-	-	-	-				
	43	-	-	-	-	-				
	44	-	-	-	-	-				
	45	-	-	-	-	-				
	46	-	-	-	-	-				
	47	-	-	-	-	-				
	48	-	-	-	-	-				
	49	-	-	-	-	-				
	50	-	-	-	-	-				
	51	-	-	-	-	-				
	52	-	-	-	-	-				
	53	-	-	-	-	-				
	54	-	-	-	-	-				
	55	-	-	-	-	-				
	56	-	-	-	-	-				
	57	-	-	-	-	-				
	58	-	-	-	-	-				
	59	-	-	-	-	-				
	60	-	-	-	-	-				
	61	-	-	-	-	-				
	62	-	-	-	-	-				
	63	-	-	-	-	-				
	64	-	-	-	-	-				
	65	-	-	-	-	-				
	66	-	-	-	-	-				
	67	-	-	-	-	-				
	68	-	-	-	-	-				
	69	-	-	-	-	-				
	70	-	-	-	-	-				
	71	-	-	-	-	-				
	72	-	-	-	-	-				

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	**Art Unit**
	SIMON KANAAN	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/18/2013	11/07/2013	06/04/2014	02/22/2015	05/28/2015				
	73	-	-	-	-	-				
	74	-	-	-	-	-				
	75	-	-	-	-	-				
	76	-	-	-	-	-				
	77	-	-	-	-	-				
	78	-	-	-	-	-				
	79	-	-	-	-	-				
	80	-	-	-	-	-				
	81	-	-	-	-	-				
	82	-	-	-	-	-				
	83	-	-	-	-	-				
	84	-	-	-	-	-				
	85	-	-	-	-	-				
	86	-	-	-	-	-				
	87	-	-	-	-	-				
	88	-	-	-	-	-				
	89	-	-	-	-	-				
	90	-	-	-	-	-				
	91	-	-	-	-	-				
	92	-	-	-	-	-				
	93	-	-	-	-	-				
	94	-	-	-	-	-				
	95	-	-	-	-	-				
	96	-	-	-	-	-				
	97	-	-	-	-	-				
	98	-	-	-	-	-				
	99	-	-	-	-	-				
	100	-	-	-	-	-				
	101	-	-	-	-	-				
	102	-	-	-	-	-				
	103	-	-	-	-	-				
	104	-	-	-	-	-				
	105	-	-	-	-	-				
	106	-	-	-	-	-				
	107	-	-	-	-	-				
	108	-	-	-	-	-				

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	**Art Unit**
	SIMON KANAAN	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/18/2013	11/07/2013	06/04/2014	02/22/2015	05/28/2015				
	109	-	-	-	-	-				
	110	-	-	-	-	-				
	111	-	-	-	-	-				
	112	-	-	-	-	-				
	113	-	-	-	-	-				
	114	-	-	-	-	-				
	115	-	-	-	-	-				
	116	-	-	-	-	-				
	117	-	-	-	-	-				
	118	-	-	-	-	-				
	119	-	-	-	-	-				
	120	-	-	-	-	-				
	121			✓	✓	✓				
	122			✓	✓	✓				
	123			✓	✓	✓				
	124			✓	✓	✓				
	125			✓	-	-				
	126			✓	✓	✓				
	127			✓	✓	✓				
	128			✓	✓	✓				
	129			✓	✓	✓				
	130			✓	✓	✓				
	131			✓	✓	✓				
	132			✓	✓	✓				
	133			✓	-	-				
	134			✓	✓	✓				
	135			✓	✓	✓				
	136				✓	✓				
	137				✓	✓				
	138				✓	✓				
	139				✓	✓				
	140				✓	✓				

PTO/SB/30 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995. no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Request for Continued Examination (RCE) Transmittal

Address to:
Mail Stop RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Application Number	13/240,572
Filing Date	September 22, 2011
First Named Inventor	Stephen Boyer
Art Unit	2432
Examiner Name	Simon P. Kanaan
Attorney Docket Number	38879-0006001

This is a Request for Continued Examination (RCE) under 37 CFR 1 .114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. See Instruction Sheet for RCEs (not to be submitted to the USPTO) on page 2.

1. Submission required under 37 CFR 1.114 Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

   a. ☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

      i. ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

      ii. ☐ Other _____

   b. ☒ Enclosed

      i. ☒ Amendment/Reply

      ii. ☐ Affidavit(s)/ Declaration(s)

      iii. ☐ Information Disclosure Statement (IDS)

      iv. ☐ Other _____

2. Miscellaneous

   Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a

   a. ☐ period of _____ months. (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

   b. ☐ Other _____

3. Fees The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.
   The Director is hereby authorized to charge the following fees any underpayment of fees or credit any overpayments to

   a. ☒ Deposit Account No. 06-1050 .

      i. ☒ RCE fee required under 37 CFR 1.17(e)

      ii ☐ Extension of time fee (37 CFR 1.136 and 1.17)

      iii ☒ Other any deficiencies

   b. ☐ Check in the amount of $ _____ enclosed

   c. ☐ Payment by credit card (Form PTO-2038 enclosed)

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Signature	/David L. Feigenbaum/	Date	May 22, 2015
Name (Print/Type)	David L. Feigenbaum	Registration No.	30,378

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop RCE, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450 or facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.

Signature			
Name (Print/Type)		Date	

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

American LegalNet, Inc.
www.FormsWorkFlow.com

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor	:	Stephen Boyer	Art Unit	:	2432
Serial No.	:	13/240,572	Examiner	:	Simon P. Kanaan
Filed	:	September 22, 2011	Conf. No.	:	2423
Title	:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM			

MAIL STOP AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY TO ACTION DATED FEBRUARY 27, 2015

Amendments to the claims (this listing replaces all prior versions):

Claims (replacing prior versions):

1. (currently amended) A method comprising:

collecting, from at least two sources, information about two or more companies or other organizations that have computer systems, network resources, and employees, the organizations posing risks to themselves or to other parties through business relationships of the organizations with the other parties, the information collected about the organizations being indicative of any one or more of (a) security vulnerabilities of the organizations, (b) compromises of technology systems, data, or other information of the organizations, or (c) resiliencies of the organizations to recover from security breaches,

at least some of the information ~~for~~ about each of the organizations being collected automatically by computer ~~from at least two sources~~,

at least some of the information about each of the organizations being based on either or both of (a) communications from or to the organizations that are observed on the Internet and that do not explicitly identify and are indirectly indicative of the security vulnerabilities, compromises, or resiliencies, or (b) other observations that characterize the organizations,

one or more of the sources not being controlled by the organization, the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization,

processing the information from both of the two or more sources for each of the organizations to form a composite rating that is indicative of a degree of risk to the organization or to a party through a business relationship with the organization, the composite rating comprising a composite of two or more of (a) ~~of~~ security vulnerability of the organization, (b) ~~or of~~ compromise of a technology system, data, or information of the organization, ~~or~~ (~~b~~c) of a resilience of the organization to recover from a security breach~~, or (c) both~~,

the processing including applying models that account for differences in the respective sources,

the forming of the composite rating for each of the organizations including (a) aggregating metrics associated with ~~a~~ the computer system of the organization, the metrics including measures of the frequency of or durations of compromises of the computer system of the organization, and (b) taking account of positive information about the organization,

~~normalizing the composite rating of each of the organizations based on an amount of networking assets, a number of employees, or another size characteristic of the organization to enable comparisons of composite ratings between the two or more organizations~~, and

in connection with a assessing a business risk to the organization or to a party through a business relationship with or with at least one of the organizations, delivering a report of ~~reporting~~ the composite ratings of the organizations through a reporting facility to enable a ~~customers~~ user of the reporting facility to monitor, assess, and mitigate the risks, based on the security vulnerabilities or resiliencies or both, ~~risk~~ in doing business with the ~~organizations~~ organization and to compare the composite ratings ~~across~~ of the organizations.

2. (canceled)

3. (previously presented) The method of claim 1, wherein at least one of the sources includes a commercial data source.

4. (previously presented) The method of claim 1, wherein the collected information is represented by at least two data types.

5. (previously presented) The method of claim 4, wherein the at least two data types include at least one of breach disclosures, block lists, configuration parameters, an identification of malware servers, an identification of a reputation, an identification of suspicious activity, an identification of spyware, white lists, an identification of compromised hosts, an identification of malicious activity, an identification of spam activity, an identification of vulnerable hosts, an identification of phishing activity, or an identification of e-mail viruses.

6. (canceled)

7. (previously presented) The method of claim 1, wherein the collected information evidences internal security controls.

8. (previously presented) The method of claim 1, wherein the collected information comprises outcomes of each of the organizations.

9. (previously presented) The method of claim 1, wherein the collected information evidences operational execution of security measures of each of the organizations.

10. (previously presented) The method of claim 1, wherein the collected information indicates whether a computer system of each of the organizations served malicious code to another system.

11. (currently amended) The method of claim 1, wherein the collected information indicates whether a computer system of each of the organizations communicated with a known attacker controlled network or sensor outside the control or network of the organization.

12. (previously presented) The method of claim 1, comprising:
forming a series of the security ratings of each of the organizations.

13. (previously presented) The method of claim 12, comprising:
determining a trend from the series of ratings.

14. (previously presented) The method of claim 12, comprising:
displaying the series of composite ratings.

15. (canceled)

16. (previously presented) The method of claim 14, wherein displaying the series of composite ratings for each of the organizations comprises posting the series of composite ratings for the organization to a web portal.

17. (canceled)

18. (canceled)

19-120. (canceled)

121. (previously presented) The method of claim 1, wherein the collected information represents externally observable outcome information.

122. (previously presented) The method of claim 121, wherein the outcome information comprises outcome information associated with security vulnerability or resilience of each of the organizations.

123. (canceled)

124. (previously presented) The method of claim 1, comprising:

determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information.

125. (canceled)

126. (previously presented) The method of claim 1, wherein:

the collected information comprises at least two security characterizations of a computer system of each of the organizations.

127. (previously presented) The method of claim 1, wherein the collected information comprises a characterization of behavior of an employee of at least one of the organizations.

128. (previously presented) The method of claim 1, wherein the collected information comprises characterizations other than characterizations about a computer system of at least one of the organizations.

129. (previously presented) The method of claim 1, wherein the collected information comprises characterizations about policies of at least one of the organizations.

130. (previously presented) The method of claim 1, wherein the collected information comprises characterizations about information technology assets that at least one of the organizations owns, controls, uses, or is affiliated with.

131. (previously presented) The method of claim 1 in which collected information represents: (a) physical states, (b) technical states, (c) organizational states, or (d) cultural states of at least one of the organizations which can be exploited to create a security breach; or (e) the

organization's ability to recover from a security breach; or any combination of two or more of these.

132. (previously presented) The method of claim 1 in which processing the information to form a composite rating comprises correlating data across the sources of information.

133. (canceled)

134. (previously presented) The method of claim 1 in which processing the information to form a composite rating comprises statistically correlating the composite rating with actual outcomes.

135. (previously presented) The method of claim 1 in which the vulnerability comprises physical, technical, organizational, or cultural states that can be exploited to create a security breach.

136. (previously presented) A method comprising

collecting, from at least two sources, information about two or more companies or other organizations, the collected information representing at least two data types, the collected information comprising outcomes of each of the organizations,

at least some of the information for each of the organizations being collected automatically by computer from at least two sources, one or more of the sources not controlled by the organization,

the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization, at least one of the sources including a commercial data source,

processing the information from both of the two sources for each of the organizations to form a composite rating of a security vulnerability of the organization to creation of a security breach or a compromise of a system of the organization or of a resilience of the organization to recovery from a security breach or both, the processing including applying models that account for differences in the respective sources,

normalizing the composite rating of each of the organizations based on a size characteristic of the organization to enable comparisons of composite ratings between the two or more organizations,

forming a series of the security ratings of each of the organizations, determining a trend from the series of ratings, and displaying the series of composite ratings through a portal,

determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information, and

reporting the composite ratings of the organizations through a portal to enable customers to monitor, assess, and mitigate risk in doing business with the organizations and to compare the composite ratings across the organizations.

137. (previously presented) The system of claim 1, determining a confidence range of the composite rating, the size of the range varying inversely with the level of confidence in the composite rating.

138. (previously presented) The system of claim 137, wherein the confidence range is based on redundancy of the security characterizations.

139. (previously presented) The system of claim 137, wherein the confidence range is based on a size of the third party computer system.

140. (previously presented) The method of claim 1 comprising ranking the organization and other organizations within sectors or peer-groups or globally.

REMARKS

The applicant has amended the claims for consideration in an RCE that is also being filed.

Any circumstance in which the applicant has (a) addressed certain comments of the examiner does not mean that the applicant concedes other comments of the examiner, (b) made arguments for the patentability of some claims does not mean that there are not other good reasons for patentability of those claims and other claims, or (c) amended or canceled a claim does not mean that the applicant concedes any of the examiner's positions with respect to that claim or other claims.

Please apply any charges or credits to deposit account 06-1050, referencing attorney docket 38879-0006001.

Respectfully submitted,

Date:/5/22/15/_____

/David L. Feigenbaum/_____
David L. Feigenbaum
Reg. No. 30,378

Customer Number 26161
Fish & Richardson P.C.
Telephone: (617) 542-5070
Facsimile: (877) 769-7945

23363488.doc

Electronic Patent Application Fee Transmittal

Application Number:	13240572
Filing Date:	22-Sep-2011
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Filer:	David L Feigenbaum/jennifer franco
Attorney Docket Number:	38879-0006001

Filed as Small Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
RCE- 2nd and Subsequent Request	2820	1	850	850
		Total in USD ($)		**850**

Electronic Acknowledgement Receipt

EFS ID:	22422027
Application Number:	13240572
International Application Number:	
Confirmation Number:	2423
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Customer Number:	26161
Filer:	David L Feigenbaum/jennifer franco
Filer Authorized By:	David L Feigenbaum
Attorney Docket Number:	38879-0006001
Receipt Date:	22-MAY-2015
Filing Date:	22-SEP-2011
Time Stamp:	09:48:00
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$850
RAM confirmation Number	7517
Deposit Account	061050
Authorized User	FISH & RICHARDSON P C

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	RCE.pdf	143896 36e0de1066da9da0946ccd832eaf0b5c56b3e773	no	1
Warnings:					
This is not a USPTO supplied RCE SB30 form.					
Information:					
2		amendment.pdf	77534 0199b173a9a68de2949a6fa4057f96ff16c49b7b	yes	8

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment Submitted/Entered with Filing of CPA/RCE	1	1
	Claims	2	7
	Applicant Arguments/Remarks Made in an Amendment	8	8

Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	31030 dd328436cbe46849406a39abcf13e74bf0dca468	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	252460	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/240,572	Filing Date 09/22/2011	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT **05/22/2015**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 30	Minus	** 31	= 0	X $40 =	0
Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $210 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/VIKKI GRAY/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/240,572	09/22/2011	Stephen Wayne Boyer	38879-0006001	2423

26161 7590 02/27/2015
FISH & RICHARDSON P.C. (BO)
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
KANAAN, SIMON P	

ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
02/27/2015	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATDOCTC@fr.com

Office Action Summary	Application No. 13/240,572	Applicant(s) BOYER ET AL.	
	Examiner SIMON KANAAN	Art Unit 2432	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *3 November 2014*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1,3-5,7-14,16,121-124,126-132 and 134-140* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1,3-5,7-14,16,121-124,126-132 and 134-140* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *22 September 2011* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some * c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Interim copies:

a)☐ All b)☐ Some c)☐ None of the: Interim copies of the priority documents have been received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions

2. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

Office Action Summary

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. Applicant's arguments/amendments filed 11/03/2015 have been considered but are not persuasive.

Applicant's Arguments and Examiner's Response

5. Applicant's arguments/amendments filed 11/03/2015 have been considered but are not persuasive. As for applicant's arguments, applicant argues that the cited prior art does not teach "normalizing the composite rating of each of the organization based on an amount of networking assets, a number of employees, or another size characteristics of the organization to enable comparisons of composite ratings between the two or

more organizations, and reporting the composite ratings of the organizations through a portal to enable customers to monitor, assess, and mitigate risk in doing business with the organization and to compare the composite ratings across the organizations.", however the examiner respectfully disagrees as Shull [0058] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score which informs requester of the trust of the entity, this score is received by the requester where activities are accounted for both legitimate (i.e. positive) and illegitimate (i.e. negative) and [0069] and [0073], teaches giving an overall trust score between 1 and 5 i.e. a normalized composite score where 1 is a reputable business and 5 is likely engaged in illicit activity and Newton [0022] and [0072], teaches taking into account size of the network and number of employees.

Claim Rejections - 35 USC § 103

6. Claims 1,3-5,7-14,16, 121-124, 136-132 and 134-140 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chris Newton (US Pre-Grant Publication No: 2004/0250122 A1) hereinafter referred to as Newton in view of in view of Shull et al. (US Pre-Grant Publication No: 2006/0212925 A1) hereinafter referred to as Shull.

As per claim 1, Newton discloses a method comprising: collecting, from at least two sources, information about two or more companies or other organizations, at least some of the information for each of the organizations being collected automatically by computer from at least two sources, one or more of the sources not controlled by the

organization, the information format least the one or more sources that are not controlled by the organization being collected without permission of the organization, - Newton, [0012] teaches that every network in the world would have a rating in the database and [0030] teaches establishing a reputation for a network, and [0031] teaches having multiple agents gathering data and [0044]-[0048] teaches different agent types i.e. different network characterization as each agent type gathers different type of data in regards to the security and reputation of network, among these agents include data mining internet which is public information and data mining newsgroups and forums which are also public knowledge and externally observable information not controlled by an organization and figure 1, items 24 include information about the network which towards the bottom of item 24 states "company info resources" i.e. network is associated with a company and [0022] and [0072], teaches taking into account size of the network and number of employees.

processing the information from both of the two or more sources for each of the organizations to form security vulnerability of the organization or of compromise of a system of the organization or of a resilience of the organization to recover from a security breach or both, the processing including applying models that account for differences in the respective sources, –Newton, [0044]-[0048] and [0029], teaches information gathered externally from multiple sources including proxy information.

But does not teach the forming of the composite rating for each of the organizations including aggregating metrics associated with a computer system of the organization, the metrics including measures of the frequency of or durations of

compromises of the computer system, and taking account of positive information about the organization, normalizing the composite rating of each of the organization based on an amount of networking assets, a number of employees, or another size characteristics of the organization to enable comparisons of composite ratings between the two or more organizations, and reporting the composite ratings of the organizations through a portal to enable customers to monitor, assess, and mitigate risk in doing business with the organization and to compare the composite ratings across the organizations.

However, Shull [0058] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score which informs requester of the trust of the entity, this score is received by the requester where activities are accounted for both legitimate (i.e. positive) and illegitimate (i.e. negative) and [0069] and [0073], teaches giving an overall trust score between 1 and 5 i.e. a normalized composite score where 1 is a reputable business and 5 is likely engaged in illicit activity.

It would have been obvious at the time of the invention for one of the ordinary skill in the art to modify the method of collecting security characteristics from multiple sources as taught by Newton by creating a score representative of the different collected data as taught by Shull because it would aid the requester in determining whether the entity is trusted or not.

As per claim 3, Newton in view of Shull teaches the method of Claim 1, wherein at least one source includes a commercial data source. –Newton, [0044]-[0048] teaches using different search engines such as Google and [0016] teaches hosted services.

As per claim 4, Newton in view of Shull discloses the method of Claim 1, wherein the collected information is represented by at least two data types. –Green, [0044]-[0048] teaches different agent types.

As per claim 5, Newton in view of Shull discloses the method of Claim 4, wherein the at least two data types include at least one of breach disclosures, block lists, configuration parameters, an identification of malware servers, an identification of a reputation, an identification of suspicious activity, an identification of spyware, white lists, an identification of compromised hosts, an identification of malicious activity, an identification of spam activity, an identification of vulnerable hosts, an identification of phishing activity, or an identification of e-mail viruses. –Newton, [0013]-[0029] teaches security measures etc.

As per claim 7, Newton in view of Shull discloses the method of Claim 1, wherein the collected information evidences internal security controls. –Newton, [0013]-[0029] teaches security measures etc.

As per claim 8, Newton in view of Shull discloses the method of Claim 1, wherein the collected information comprises outcomes of each of the organizations. –Newton, [0013]-[0029] teaches security measures and [0044]-[0048] teaches checking for information already available to the public about network.

As per claim 9, Newton in view of Shull discloses the method of Claim 1, wherein the collected information evidences operational execution of security measures of the organizations. –Newton, [0013]-[0029] teaches security measures.

As per claim 10, Newton in view of Shull discloses the method of Claim 1, wherein the collected information indicates whether a computer system of the organizations served malicious code to another system. –Newton, [0013], teaches hostility level and page 4, claim 6, teaches spam levels.

As per claim 11, Newton in view of Shull discloses the method of Claim 1, wherein the collected information indicates whether a computer system of the organizations communicated with a known attacker controlled network. –Newton, [0013] teaches hostility level.

As per claim 12, Newton in view of Shull discloses the method of Claim 1, comprising: forming a series of the security ratings of the organizations. –Newton, [0042], teaches live remote updates i.e. continually computing rating and page 4, claim 6 teaches security information has multiple ratings and [0041], teaches the different information having different weight.

As per claim 13, Newton in view of Shull discloses the method of Claim 12, comprising determining a trend from the series of ratings. –Newton, [0042], teaches live remote updates i.e. continually computing rating.

As per claim 14, Newton in view of Shull discloses the method of Claim 12, comprising displaying the series of composite ratings. –Newton, [0033], teaches a master database for collecting and storing the network ratings and page 4, claim 6 teaches security information has multiple ratings and [0041], teaches the different information having different weight and Shull, [0058], [0076] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score with informs requester of the trust of the entity, this score is received by the requester and a display device would display score as to help user determine whether to trust entity or not.

As per claim 16, Newton in view of Shull teaches the method of Claim 14, wherein displaying the series of composite ratings for each of the organizations comprises posting the series of composite ratings for each of the organizations to a web portal. -Newton, [0033], teaches a master database for collecting and storing the network ratings which includes information as listed in [0013]-[0029] which serve as warnings and Shull, [0058], [0076] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score with informs requester

of the trust of the entity, this score is received by the requester and a display device would display score as to help user determine whether to trust entity or not.

As per claim 121, Newton in view of Shull teaches the method of Claim 1, wherein the collected information represents externally observable outcome information. - Newton, [0054], teaches agents getting information from news groups or sending packets and checking their responses.

As per claim 122, Newton in view of Shull teaches the method of Claim 121, wherein the outcome information comprises outcome information associated with security vulnerability or resilience of each of the organizations. Shull, [0058] and Newton, page 4, claim 6, both teach that the information is associated with entity security and Newton even looks into active security systems as well.

As per claim 123, Newton in view of Shull teaches the method of Claim 1, wherein the customers have a security risk associated with the vulnerability or resilience of at least one of the organizations. - Shull, [0058], teaches a composite score which would be indicative of risk.

As per claim 124, Newton in view of Shull teaches the method of Claim 1, comprising: determining a badness score that corresponds to an intensity or duration of

malicious activity determined from the collected information. - Newton, page 4, claim 6, teaches having spam levels etc. Which are a badness score.

As per claim 126, Newton in view of Shull teaches the method of Claim 1, wherein: the collected information comprises at least two security characterizations of a computer system of the entity. - Newton, page 4, claim 6, teaches checking open proxy servers and desktop security measures which are multiple characterizations of a system of the entity.

As per claim 127, Newton in view of Shull teaches the method of Claim 1, wherein the collected information comprises a characterization of behavior of an employee of at least one of the organizations. - Newton, page 4, claim 6, inappropriate content served, spam levels, language spoken, geographic placement, industry, which are characterizations of employees in the network and the employees' behavior.

As per claim 128, Newton in view of Shull teaches the method of Claim 1, wherein the collected information comprises characterizations other than characterizations about a computer system of at least one of the organizations. - Newton, page 4, claim 6, teaches security characterization includes security personnel.

As per claim 129, Newton in view of Shull teaches the method of Claim 1, wherein the collected information comprises characterizations about policies of at least

one of the organizations. –Newton, page 4, claim 6, teaches organization association, active security measures, desktop security measures, etc. which are policies see also [0059] and [0060].

As per claim 130, Newton in view of Shull teaches the method of Claim 1, wherein the collected information comprises characterizations about information technology assets that at least one of the organizations owns, controls, uses, or is affiliated with. –Newton, page 4, claim 6, teaches organization associations see also [0043] and [0053].

As per claim 131, Newton in view of Shull teaches the method of Claim 1 in which collected information represents: (a) physical states, (b) technical states, (c) organizational states, or (d) cultural states of at least one of the organizations which can be exploited to create a security breach; or (e) the organization's ability to recover from a security breach; or any combination of two or more of these. –Newton, page 4, claim 6, teaches active security measures and desktop security measures among other information collected about the organization.

As per claim 132, Newton in view of Shull teaches the method of claim 1 in which processing the information to form a composite rating comprises correlating data across the sources of information.-Shull, [0058], teaches creating a score based on the different data received i.e. correlating the different data.

As per claim 134, Newton in view of Shull teaches the method of claim 1 in which processing the information to form a composite rating comprises statistically correlating the composite rating with actual outcomes. – Newton, [0041], teaches giving different information different weight where less weight given to information as it becomes less important over time which is a statistical correlation with the information collected.

As per claim 135, Newton in view of Shull teaches the method of claim 1 in which the vulnerability comprises physical, technical, organizational, or cultural states that can be exploited to create a security breach. –Newton, figure 1, item 24 and page 4, claim 6.

As per claim 136, Newton teaches a method comprising collecting, from at least two sources, information about two or more companies or other organizations, the collected information representing at least two data types, the collected information comprising outcomes of each of the organizations, at least some of the information for each of the organizations being collected automatically by computer from at least two sources, one or more of the sources not controlled by the organization, the information from at least the one or more sources that are not controlled by the organization being collected without permission of the-organization, at least one of the sources including a commercial data source, -Newton, [0012] teaches that every network in the world would have a rating in the database and [0030] teaches establishing a reputation for a network, and [0031] teaches having multiple agents gathering data and [0044]-[0048]

teaches different agent types i.e. different network characterization as each agent type gathers different type of data in regards to the security and reputation of network, among these agents include data mining internet which is public information and data mining newsgroups and forums which are also public knowledge and externally observable information not controlled by an organization and figure 1, items 24 include information about the network which towards the bottom of item 24 states "company info resources" i.e. network is associated with a company, and [0022] and [0072], teaches taking into account size of the network and number of employees.

and displaying the series of ratings through a portal and reporting the ratings of the organizations through a portal to enable customers to monitor, assess, and mitigate risk in doing business with the organizations and to compare the composite ratings across the organizations. –Newton, figure 3 item 14, teaches a database which stores information about the organizations i.e. portal.

But Newton does not teach processing the information from both of the two sources for each of the organizations to form a composite rating of a security vulnerability of the organization to creation of a security breach or a compromise of a system of the organization or of a resilience of the organization to recovery from a security breach or both, the processing including applying models that account for differences in the respective sources, normalizing the composite rating of each of the organizations based on a size characteristic of the organization to enable comparisons of composite ratings between the two or more organizations, forming a series of the security ratings of each of the organizations, determining a trend from the series of

ratings, determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information.

However, Shull [0058] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score which informs requester of the trust of the entity, this score is received by the requester where activities are accounted for both legitimate (i.e. positive) and illegitimate (i.e. negative) and [0069] and [0073], teaches giving an overall trust score between 1 and 5 i.e. a normalized composite score where 1 is a reputable business and 5 is likely engaged in illicit activity.

It would have been obvious at the time of the invention for one of the ordinary skill in the art to modify the method of collecting security characteristics from multiple sources as taught by Newton by creating a score representative of the different collected data as taught by Shull because it would aid the requester in determining whether the entity is trusted or not.

As per claim 137, Newton in view of Shull teaches the system of claim 1, determining a confidence range of the composite rating, the size of the range varying inversely with the level of confidence in the composite rating. - Shull, [0069] and [0073], teaches giving an overall trust score between 1 and 5 i.e. a normalized composite score where 1 is a reputable business and 5 is likely engaged in illicit activity.

As per claim 138, Newton in view of Shull teaches the system of claim 137, wherein the confidence range is based on redundancy of the security characterizations. –Shull, [0081], teaches taking into account consistency which is redundancy.

As per claim 139, Newton in view of Shull teaches the system of claim 137, wherein the confidence range is based on a size of the third party computer system. – Newton, [0072], teaches taking into account size of the network.

As per claim 140, Newton in view of Shull teaches the method of claim 1 comprising ranking the organization and other organizations within sectors or peer-groups or globally. –Shull, [0123]-[0124], teaches listing entities with similar scores together such as ones that scored a 3 or 4 so these would be ranked below ones which were listed as part of white list which ranked 1 or 2, see [0068], which teaches having white list, black list and grey lists.

Conclusion

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

8. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Simon Kanaan whose telephone number is (571)270-3906. The examiner can normally be reached on Mon-Thurs 7:30-5:00 EST.

If attempts to reach the above noted Examiner by telephone are unsuccessful, the Examiner's supervisor, Gilberto Barron, can be reached at the following telephone number: (571) 272-3799.

The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.

/S. K./
Examiner, Art Unit 2432

/GILBERTO BARRON JR/
Supervisory Patent Examiner, Art Unit 2432

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	**Art Unit**
	SIMON KANAAN	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/18/2013	11/07/2013	06/04/2014	02/22/2015					
	1	✓	✓	✓	✓					
	2	✓	✓	-	-					
	3	✓	✓	✓	✓					
	4	✓	✓	✓	✓					
	5	✓	✓	✓	✓					
	6	✓	✓	-	-					
	7	✓	✓	✓	✓					
	8	✓	✓	✓	✓					
	9	✓	✓	✓	✓					
	10	✓	✓	✓	✓					
	11	✓	✓	✓	✓					
	12	✓	✓	✓	✓					
	13	✓	✓	✓	✓					
	14	✓	✓	✓	✓					
	15	✓	✓	-	-					
	16	✓	✓	✓	✓					
	17	✓	✓	-	-					
	18	✓	✓	-	-					
	19	✓	✓	-	-					
	20	✓	✓	-	-					
	21	-	-	-	-					
	22	-	-	-	-					
	23	-	-	-	-					
	24	-	-	-	-					
	25	-	-	-	-					
	26	-	-	-	-					
	27	-	-	-	-					
	28	-	-	-	-					
	29	-	-	-	-					
	30	-	-	-	-					
	31	-	-	-	-					
	32	-	-	-	-					
	33	-	-	-	-					
	34	-	-	-	-					
	35	-	-	-	-					
	36	-	-	-	-					

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	**Art Unit**
	SIMON KANAAN	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/18/2013	11/07/2013	06/04/2014	02/22/2015					
	37	-	-	-	-					
	38	-	-	-	-					
	39	-	-	-	-					
	40	-	-	-	-					
	41	-	-	-	-					
	42	-	-	-	-					
	43	-	-	-	-					
	44	-	-	-	-					
	45	-	-	-	-					
	46	-	-	-	-					
	47	-	-	-	-					
	48	-	-	-	-					
	49	-	-	-	-					
	50	-	-	-	-					
	51	-	-	-	-					
	52	-	-	-	-					
	53	-	-	-	-					
	54	-	-	-	-					
	55	-	-	-	-					
	56	-	-	-	-					
	57	-	-	-	-					
	58	-	-	-	-					
	59	-	-	-	-					
	60	-	-	-	-					
	61	-	-	-	-					
	62	-	-	-	-					
	63	-	-	-	-					
	64	-	-	-	-					
	65	-	-	-	-					
	66	-	-	-	-					
	67	-	-	-	-					
	68	-	-	-	-					
	69	-	-	-	-					
	70	-	-	-	-					
	71	-	-	-	-					
	72	-	-	-	-					

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	**Art Unit**
	SIMON KANAAN	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/18/2013	11/07/2013	06/04/2014	02/22/2015					
	73	-	-	-	-					
	74	-	-	-	-					
	75	-	-	-	-					
	76	-	-	-	-					
	77	-	-	-	-					
	78	-	-	-	-					
	79	-	-	-	-					
	80	-	-	-	-					
	81	-	-	-	-					
	82	-	-	-	-					
	83	-	-	-	-					
	84	-	-	-	-					
	85	-	-	-	-					
	86	-	-	-	-					
	87	-	-	-	-					
	88	-	-	-	-					
	89	-	-	-	-					
	90	-	-	-	-					
	91	-	-	-	-					
	92	-	-	-	-					
	93	-	-	-	-					
	94	-	-	-	-					
	95	-	-	-	-					
	96	-	-	-	-					
	97	-	-	-	-					
	98	-	-	-	-					
	99	-	-	-	-					
	100	-	-	-	-					
	101	-	-	-	-					
	102	-	-	-	-					
	103	-	-	-	-					
	104	-	-	-	-					
	105	-	-	-	-					
	106	-	-	-	-					
	107	-	-	-	-					
	108	-	-	-	-					

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	**Art Unit**
	SIMON KANAAN	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/18/2013	11/07/2013	06/04/2014	02/22/2015					
	109	-	-	-	-					
	110	-	-	-	-					
	111	-	-	-	-					
	112	-	-	-	-					
	113	-	-	-	-					
	114	-	-	-	-					
	115	-	-	-	-					
	116	-	-	-	-					
	117	-	-	-	-					
	118	-	-	-	-					
	119	-	-	-	-					
	120	-	-	-	-					
	121			✓	✓					
	122			✓	✓					
	123			✓	✓					
	124			✓	✓					
	125			✓	-					
	126			✓	✓					
	127			✓	✓					
	128			✓	✓					
	129			✓	✓					
	130			✓	✓					
	131			✓	✓					
	132			✓	✓					
	133			✓	-					
	134			✓	✓					
	135			✓	✓					
	136				✓					
	137				✓					
	138				✓					
	139				✓					
	140				✓					

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L5	8	726/25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2015/02/22 23:19
L6	0	network with vulnerability with detection with compliance with assesment	US-PGPUB; USPAT	ADJ	ON	2015/02/22 23:19
L7	21	US-7194769-$.DID. OR US-7290275-$.DID. OR US-7971252-$.DID. OR US-20040010709-$.DID. OR US-20050138413-$.DID. OR US-20080047018-$.DID. OR US-20080209565-$.DID. OR US-20090265787-$.DID. OR US-20090293128-$.DID. OR US-2007304-$.DID. OR US-5200596-$.DID. OR US-2009104-$.DID. OR US-422009D-$.DID. OR US-1331018-$.DID.	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2015/02/22 23:20
L8	0	(insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and L7	US-PGPUB; USPAT	ADJ	ON	2015/02/22 23:20
L9	237	network (reputation or assess$4 or rat$3) with public and security	US-PGPUB; USPAT	ADJ	ON	2015/02/22 23:20
L10	67	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.) and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2015/02/22 23:20
L11	115	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2015/02/22 23:20

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	0	"13240572"	US-PGPUB; USPAT; UPAD	ADJ	ON	2015/02/22 22:25

2/ 22/ 2015 11:23:28 PM
C:\ Users\ skanaan\ Documents\ EAST\ Workspaces\ 13240572.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	Art Unit
	SIMON KANAAN	2432

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor and Assignee Search (PALM)	4/18/2013	SK
class/subclass search + text (EAST: 726/1,2,22,25+text)	11/13/2014	SK
CPC + text (EAST: H04L63/20,145,14,0236,1433,104 OR H04L67/306 OR H04L51/12 OR H04L61/1511 OR H04L9/321 OR G06F21/00,577 + text)	2/22/2015	SK

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/SIMON KANAAN/ Examiner.Art Unit 2432	

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor	:	Stephen Boyer	Art Unit	:	2432
Serial No.	:	13/240,572	Examiner	:	Simon P. Kanaan
Filed	:	September 22, 2011	Conf. No.	:	2423
Title	:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM			

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

SUPPLEMENTAL REPLY TO ACTION DATED JUNE 16, 2014

List of claims (replacing prior versions):

1. (currently amended) A method comprising:

collecting, from at least two sources, information about two or more companies or other organizations,

at least some of the information for each of the organizations being collected automatically by computer from at least two sources, one or more of the sources not controlled by the organization,

the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization,

processing the information from both of the two or more sources for each of the organizations to form a composite rating (a) of security vulnerability of the organization ~~to creation of a security breach~~ or ~~to~~ of compromise of a system of the organization or (b) of a resilience of the organization to ~~recovery~~ recover from a security breach, or (c) both,

the processing including applying models that account for differences in the respective sources,

the forming of the composite rating for each of the organizations including (a) aggregating metrics associated with a computer system of the organization, the metrics including measures of the frequency of or durations of compromises of the computer system, and (b) taking account of positive information about the organization,

normalizing the composite rating of each of the organizations based on an amount of networking assets, a number of employees, or another ~~a~~ size characteristic of the organization to enable comparisons of composite ratings between the two or more organizations, and

reporting the composite ratings of the organizations through a portal to enable customers to monitor, assess, and mitigate risk in doing business with the organizations and to compare the composite ratings across the organizations. [[.]]

2. (canceled)

3. (previously presented) The method of claim 1, wherein at least one of the sources includes a commercial data source.

4. (previously presented) The method of claim 1, wherein the collected information is represented by at least two data types.

5. (previously presented) The method of claim 4, wherein the at least two data types include at least one of breach disclosures, block lists, configuration parameters, an identification of malware servers, an identification of a reputation, an identification of suspicious activity, an identification of spyware, white lists, an identification of compromised hosts, an identification of malicious activity, an identification of spam activity, an identification of vulnerable hosts, an identification of phishing activity, or an identification of e-mail viruses.

6. (canceled)

7. (previously presented) The method of claim 1, wherein the collected information evidences internal security controls.

8. (previously presented) The method of claim 1, wherein the collected information comprises outcomes of each of the organizations.

9. (previously presented) The method of claim 1, wherein the collected information evidences operational execution of security measures of each of the organizations.

10. (previously presented) The method of claim 1, wherein the collected information indicates whether a computer system of each of the organizations served malicious code to another system.

11. (previously presented) The method of claim 1, wherein the collected information indicates whether a computer system of each of the organizations communicated with a known attacker controlled network.

12. (previously presented) The method of claim 1, comprising:
forming a series of the security ratings of each of the organizations.

13. (previously presented) The method of claim 12, comprising:
determining a trend from the series of ratings.

14. (previously presented) The method of claim 12, comprising:

displaying the series of composite ratings.

15. (canceled)

16. (previously presented) The method of claim 14, wherein displaying the series of composite ratings for each of the organizations comprises posting the series of composite ratings for the organization to a web portal.

17. (canceled)

18. (canceled)

19-120. (canceled)

121. (previously presented) The method of claim 1, wherein the collected information represents externally observable outcome information.

122. (previously presented) The method of claim 121, wherein the outcome information comprises outcome information associated with security vulnerability or resilience of each of the organizations.

123. (previously presented) The method of claim 1, wherein the customers have a security risk associated with the vulnerability or resilience of at least one of the organizations.

124. (previously presented) The method of claim 1, comprising:

determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information.

125. (canceled)

126. (previously presented) The method of claim 1, wherein:

the collected information comprises at least two security characterizations of a computer system of each of the organizations.

127. (previously presented) The method of claim 1, wherein the collected information comprises a characterization of behavior of an employee of at least one of the organizations.

128. (previously presented) The method of claim 1, wherein the collected information comprises characterizations other than characterizations about a computer system of at least one of the organizations.

129. (previously presented) The method of claim 1, wherein the collected information comprises characterizations about policies of at least one of the organizations.

130. (previously presented) The method of claim 1, wherein the collected information comprises characterizations about information technology assets that at least one of the organizations owns, controls, uses, or is affiliated with.

131. (previously presented) The method of claim 1 in which collected information represents: (a) physical states, (b) technical states, (c) organizational states, or (d) cultural states of at least one of the organizations which can be exploited to create a security breach; or (e) the organization's ability to recover from a security breach; or any combination of two or more of these.

132. (previously presented) The method of claim 1 in which processing the information to form a composite rating comprises correlating data across the sources of information.

133. (canceled)

134. (previously presented) The method of claim 1 in which processing the information to form a composite rating comprises statistically correlating the composite rating with actual outcomes.

135. (previously presented) The method of claim 1 in which the vulnerability comprises physical, technical, organizational, or cultural states that can be exploited to create a security breach.

136. (previously presented) A method comprising

collecting, from at least two sources, information about two or more companies or other organizations, the collected information representing at least two data types, the collected information comprising outcomes of each of the organizations,

at least some of the information for each of the organizations being collected automatically by computer from at least two sources, one or more of the sources not controlled by the organization,

the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization, at least one of the sources including a commercial data source,

processing the information from both of the two sources for each of the organizations to form a composite rating of a security vulnerability of the organization to creation of a security breach or a compromise of a system of the organization or of a resilience of the organization to recovery from a security breach or both, the processing including applying models that account for differences in the respective sources,

normalizing the composite rating of each of the organizations based on a size characteristic of the organization to enable comparisons of composite ratings between the two or more organizations,

forming a series of the security ratings of each of the organizations, determining a trend from the series of ratings, and displaying the series of composite ratings through a portal,

determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information, and

reporting the composite ratings of the organizations through a portal to enable customers to monitor, assess, and mitigate risk in doing business with the organizations and to compare the composite ratings across the organizations.

137. (previously presented) The system of claim 1, determining a confidence range of the composite rating, the size of the range varying inversely with the level of confidence in the composite rating.

138. (previously presented) The system of claim 137, wherein the confidence range is based on redundancy of the security characterizations.

139. (previously presented) The system of claim 137, wherein the confidence range is based on a size of the third party computer system.

140. (new) The method of claim 1 comprising ranking the organization and other organizations within sectors or peer-groups or globally.

REMARKS

The applicant thanks the examiner for the telephone interview with the undersigned on October 24, 2014, in which we generally discussed claim 1 as submitted in the original reply to the action of June 16, 2014. The examiner's suggested that additional detail be recited in claim 1 with respect to the processing and normalizing activities. We thank the examiner for also agreeing to accept this supplemental amendment of claim 1 based on the conversation, for consideration in an action that the examiner will be working on shortly. We have also added a new claim 140 related to the ranking of the organization and other organizations.

Canceled claims, if any, have been canceled without prejudice or disclaimer.

Any circumstance in which the applicant has (a) addressed certain comments of the examiner does not mean that the applicant concedes other comments of the examiner, (b) made arguments for the patentability of some claims does not mean that there are not other good reasons for patentability of those claims and other claims, or (c) amended or canceled a claim does not mean that the applicant concedes any of the examiner's positions with respect to that claim or other claims.

Please apply any charges or credits to deposit account 06-1050, referencing attorney docket 38879-0006001.

Respectfully submitted,

Date:/10/3/14/_____

/David L. Feigenbaum/_____
David L. Feigenbaum
Reg. No. 30,378

Customer Number 26161
Fish & Richardson P.C.
Telephone: (617) 542-5070
Facsimile: (877) 769-7945

23248511.doc

Electronic Acknowledgement Receipt

EFS ID:	20596058
Application Number:	13240572
International Application Number:	
Confirmation Number:	2423
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Customer Number:	26161
Filer:	David L Feigenbaum/jennifer franco
Filer Authorized By:	David L Feigenbaum
Attorney Docket Number:	38879-0006001
Receipt Date:	03-NOV-2014
Filing Date:	22-SEP-2011
Time Stamp:	22:01:01
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		supp-amdt.pdf	77885 95fdedf99051ab38488fbed376b2dc18454 1b1b6	yes	8

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Supplemental Response or Supplemental Amendment	1	1
	Claims	2	7
	Applicant summary of interview with examiner	8	8
Warnings:			
Information:			
	Total Files Size (in bytes):	77885	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 11/06/2014

BMURPHY SALE #00000002 Mailroom Dt: 11/03/2014 061050 13240572
01 FC : 2202 40.00 DA

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/240,572	Filing Date 09/22/2011	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT **11/03/2014**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 31	Minus	** 30	= 1	X $40 =	40
Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $210 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	**40**

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/BRENDA MURPHY/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/240,572	09/22/2011	Stephen Wayne Boyer	38879-0006001	2423

26161 7590 10/29/2014

FISH & RICHARDSON P.C. (BO)
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
KANAAN, SIMON P	
ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
10/29/2014	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATDOCTC@fr.com

Applicant-Initiated Interview Summary	Application No.	Applicant(s)	
	13/240,572	BOYER ET AL.	
	Examiner	Art Unit	
	SIMON KANAAN	2432	

All participants (applicant, applicant's representative, PTO personnel):

(1) *SIMON KANAAN*. (3)_____.

(2) *David Feigenbaum Reg. 30,378*. (4)_____.

Date of Interview: *24 October 2014*.

Type: ☒ Telephonic ☐ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☐ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☐102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1 and 136*.

Identification of prior art discussed: *Newton in view of Shull*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Applicant and examiner discussed the proposed amendments filed 9/16/2014, examiner agreed that the proposed amendments would overcome the cited prior art as he does not believe the cited prior art teaches calculating resilience of organization however since the calculation of resilience is not clear and in the interest of compact prosecution examiner suggested adding more detail regarding the calculation of the resilience of the organization; applicant's representative appreciated examiner's comments and will be submitting a supplemental amendment by 10/31/2014 .

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/SIMON KANAAN/ Examiner, Art Unit 2432	/GILBERTO BARRON JR/ Supervisory Patent Examiner, Art Unit 2432

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor	:	Stephen Boyer	Art Unit	:	2432
Serial No.	:	13/240,572	Examiner	:	Simon P. Kanaan
Filed	:	September 22, 2011	Conf. No.	:	2423
Title	:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM			

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY TO ACTION DATED JUNE 16, 2014

List of claims (replacing prior versions):

1. (currently amended) A method comprising:

collecting, from at least two sources, information about ~~an organizational entity~~ two or more companies or other organizations,

at least some of the information for each of the organizations being collected automatically by computer from at least two sources, one or more of the sources not controlled by the ~~organizational entity~~ organization,

the information from at least the one or more sources that are not controlled by the ~~organizational entity~~ organization being collected without permission of the ~~organizational entity~~ organization,

processing the information from both of the two sources for each of the organizations to form a composite rating of a security vulnerability of the organization to creation of a security breach or to compromise of a system of the organization or of a resilience of the organization to recovery from a security breach or both ~~of the organizational entity~~, the processing including applying models that account for differences in the respective sources,

normalizing the composite rating of each of the organizations based on a size characteristic of the organization to enable comparisons of composite ratings between the two or more organizations, and

reporting the composite ratings of the organizations through a portal to enable customers to monitor, assess, and mitigate risk in doing business with the organizations and to compare the composite ratings across the organizations.

~~providing the composite rating to a party for use in one or more of: monitoring, assessing, or mitigating the security vulnerability or resilience or both of the organizational entity~~.

2. (canceled)

3. (previously presented) The method of claim 1, wherein at least one of the sources includes a commercial data source.

4. (previously presented) The method of claim 1, wherein the collected information is represented by at least two data types.

5. (previously presented) The method of claim 4, wherein the at least two data types include at least one of breach disclosures, block lists, configuration parameters, an identification of malware servers, an identification of a reputation, an identification of suspicious activity, an identification of spyware, white lists, an identification of compromised hosts, an identification of malicious activity, an identification of spam activity, an identification of vulnerable hosts, an identification of phishing activity, or an identification of e-mail viruses.

6. (canceled)

7. (previously presented) The method of claim 1, wherein the collected information evidences internal security controls.

8. (currently amended) The method of claim 1, wherein the collected information comprises outcomes of each of the ~~organizational entity~~ organizations.

9. (currently amended) The method of claim 1, wherein the collected information evidences operational execution of security measures of each of the ~~organizational entity~~ organizations.

10. (currently amended) The method of claim 1, wherein the collected information indicates whether a computer system of each of the ~~organizational entity~~ organizations served malicious code to another system.

11. (currently amended) The method of claim 1, wherein the collected information indicates whether a computer system of each of the ~~organizational entity~~ organizations communicated with a known attacker controlled network.

12. (currently amended) The method of claim 1, comprising:

forming a series of the security ratings of each of the ~~organizational entity~~ organizations.

13. (previously presented) The method of claim 12, comprising:

determining a trend from the series of ratings.

14. (previously presented) The method of claim 12, comprising:

displaying the series of composite ratings.

15. (canceled)

16. (currently amended) The method of claim 14, wherein displaying the series of composite ratings for each of the ~~entity~~ organizations comprises posting the series of composite ratings for the ~~entity~~ organization to a web portal.

17. (canceled)

18. (canceled)

19-120. (canceled)

121. (previously presented) The method of claim 1, wherein the collected information represents externally observable outcome information.

122. (currently amended) The method of claim 121, wherein the outcome information comprises outcome information associated with security vulnerability or resilience of each of the ~~entity~~ organizations.

123. (currently amended) The method of claim 1, wherein the ~~party~~ customers ~~to whom the composite rating is provided has~~ have a security risk associated with the vulnerability or resilience of at least one of the ~~organizational entity~~ organizations.

124. (previously presented) The method of claim 1, comprising:

determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information.

125. (canceled)

126. (currently amended) The method of claim 1, wherein:

the collected information comprises at least two security characterizations of a computer system of each of the ~~entity~~ organizations.

127. (currently amended) The method of claim 1, wherein the collected information comprises a characterization of behavior of an employee of at least one of the ~~organizational entity~~ organizations.

128. (currently amended) The method of claim 1, wherein the collected information comprises characterizations other than characterizations about a computer system of at least one of the ~~entity~~ organizations.

129. (currently amended) The method of claim 1, wherein the collected information comprises characterizations about policies of at least one of the ~~entity~~ organizations.

130. (currently amended) The method of claim 1, wherein the collected information comprises characterizations about information technology assets that at least one of the ~~entity~~ organizations owns, controls, uses, or is affiliated with.

131. (currently amended) The method of claim 1 in which collected information represents: (a) physical states, (b) technical states, (c) organizational states, or (d) cultural states of at least one of the ~~entity~~ organizations which can be exploited to create a security breach; or (e) the ~~entity's~~ organization's ability to recover from a security breach; or any combination of two or more of these.

132. (previously presented) The method of claim 1 in which processing the information to form a composite rating comprises correlating data across the sources of information.

133. (canceled)

134. (previously presented) The method of claim 1 in which processing the information to form a composite rating comprises statistically correlating the composite rating with actual outcomes.

135. (previously presented) The method of claim 1 in which the vulnerability comprises physical, technical, organizational, or cultural states that can be exploited to create a security breach.

136. (new) A method comprising

collecting, from at least two sources, information about two or more companies or other organizations, the collected information representing at least two data types, the collected information comprising outcomes of each of the organizations,

at least some of the information for each of the organizations being collected automatically by computer from at least two sources, one or more of the sources not controlled by the organization,

the information from at least the one or more sources that are not controlled by the organization being collected without permission of the organization, at least one of the sources including a commercial data source,

processing the information from both of the two sources for each of the organizations to form a composite rating of a security vulnerability of the organization to creation of a security breach or a compromise of a system of the organization or of a resilience of the organization to recovery from a security breach or both, the processing including applying models that account for differences in the respective sources,

normalizing the composite rating of each of the organizations based on a size characteristic of the organization to enable comparisons of composite ratings between the two or more organizations,

forming a series of the security ratings of each of the organizations, determining a trend from the series of ratings, and displaying the series of composite ratings through a portal,

determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information, and

reporting the composite ratings of the organizations through a portal to enable customers to monitor, assess, and mitigate risk in doing business with the organizations and to compare the composite ratings across the organizations.

137. (new) The system of claim 1, determining a confidence range of the composite rating, the size of the range varying inversely with the level of confidence in the composite rating.

138. (new) The system of claim 137, wherein the confidence range is based on redundancy of the security characterizations.

139. (new) The system of claim 137, wherein the confidence range is based on a size of the third party computer system.

REMARKS

The comments of the applicant below are each preceded by related comments of the examiner (in small, bold type).

> **6. Applicant's arguments/amendments filed 05/07/2014 have been considered but are moot based on new grounds of rejection necessitated by applicant's amendments. As for applicants argument that the cited prior art Newton fails to teach an "organizational entity" the examiner respectfully disagrees. Applicant's remarks do not point out where support is found for applicant's preferred definition of "organizational entity" and page 7, last paragraph teaches entity information being information about IT assets as taught by Newton; also Newton, figure 1, items 24 include information about the network which towards the bottom of item 24 states "company info resources" i.e. network is associated with a company.**

The applicant respectfully disagrees.

Claim 1 has been amended to replace the phrase "organizational entity" with the term "organization" and, as an example specified in the claim, "a company." For support in the specification, the applicant points the examiner to the following passages, for example: the third paragraph on page 1; the first full paragraph on page 4; the fourth paragraph on page 9; the second and third full paragraphs on page 10; the paragraph that begins at the bottom of page 11; the paragraph that appears after the heading, and the last full paragraph, on page 13.

> **7. Claims 1, 3-5,7-14,16 and 121-135 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chris Newton (US Pre-Grant Publication No: 2004/0250122 A1) hereinafter referred to as Newton in view of in view of Shull et al. (US Pre-Grant Publication No: 2006/0212925 A1) hereinafter referred to as Shull.**
>
> **As per claim 1, Newton discloses a method comprising: collecting, from at least two source, information about an organizational entity, at least some of the information being collected automatically by computer from at least two sources, one or more of the sources not controlled by the organizational entity, -Newton, [0012] teaches that every network in the world would have a rating in the database and [0030] teaches establishing a reputation for a network, and [0031] teaches having multiple agents gathering data and [0044]-[0048] teaches different agent types i.e. different network characterization as each agent type gathers different type of data in regards to the security and reputation of network, among these agents include data mining internet which is public information and data mining newsgroups and forums which are also public knowledge and externally observable information not controlled by an organization and figure 1, items 24 include information about the network which towards the bottom of item 24 states "company info resources" i.e. network is associated with a company.**
>
> **processing the information from both of the two sources to form of a security vulnerability of resilience or both of the organizational entity, and -Newton, [0044]- [0048] and [0029], teaches information gathered externally from multiple sources including proxy information.**

But does not teach forming a composite score and providing the composite rating to a party for use in one or more of: monitoring, assessing, or mitigating the security vulnerability or resilience or both of the organizational entity.

However, Shull teaches forming a composite score and providing the composite rating to a party for use in one or more of: monitoring, assessing, or mitigating the security vulnerability or resilience or both of the organizational entity. -Shull, [0058] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score with informs requester of the trust of the entity, this score is received by the requester.

It would have been obvious at the time of the invention for one of the ordinary skill in the art to modify the method of collecting security characteristics from multiple sources as taught by Newton by creating a score representative of the different collected data as taught by Shull because it would aid the requester in determining whether the entity is trusted or not.

The applicant has amended claim 1 and respectfully disagrees with the examiner's position.

In amended claim 1, information is collected and processed about two or more companies or other organizations. The composite rating is formed for each of the organizations. The composite rating is of "a security vulnerability of the organization to creation of a security breach or to compromise of a system of the organization" or "resilience of the organization to recovery from a security breach" or both. The processing includes "applying models that account for differences in the respective sources." The composite rating of each of the organizations is normalized based on a size characteristic of the organization to enable comparisons of composite ratings between the two or more organizations." The composite ratings of the organizations are reported through a portal to enable customers to monitor, assess, and mitigate "risk in doing business with the organizations and to compare the composite ratings across the organizations." Among other things, the combination of features recited in claim 1 enables customers to understand and compare the security vulnerabilities and resilience of different organizations in order to make decisions about, for example, whether to do business with an organization or whether to switch vendors.

As the examiner recognizes, the cited passages of Newton did not describe and would not have made obvious forming a composite rating as recited in amended claim 1. Nor does the applicant believe that other features of amended claim 1 were described in or would have been made obvious by those passages.

The examiner cited Shull with respect to the forming of a score that is a composite score. Without conceding that point, the applicant notes for the examiner that Shull does not seem to have described or made obvious other important features now recited in amended claim 1, for example: 1. "applying models that account for differences in the respective sources" of information. 2. "normalizing the composite rating of each of the organizations based on a size characteristic of the organization to enable comparisons of composite ratings between the two or more organizations." 3. "reporting the composite ratings of the organizations through a portal to enable customers to monitor, assess, and mitigate risk in doing business with the organizations and to compare the composite ratings across the organizations."

Therefore, the combination of features recited in claim 1 was not described or made obvious by either of the Newton or Shull references or a combination of them.

As per claim 3, . . .

As per claim 4, . . .

As per claim 5, . . .

As per claim 7, . . .

As per claim 8, . . .

As per claim 9, . . .

As per claim 10 . . .

As per claim 11, . . .

As per claim 12, . . .

As per claim 13, . . .

As per claim 14, . . .

As per claim 16, . . .

As per claim 121, . . .

As per claim 122, . . .

As per claim 123, . . .

As per claim 124, . . .

As per claim 125, . . .

As per claim 126, . . .

As per claim 127, . . .

As per claim 128, . . .

As per claim 129, . . .

As per claim 130, . . .

As per claim 131, . . .

As per claim 132, . . .

As per claim 133, . . .

As per claim 134, . . .

As per claim 135, . . .

All of the dependent claims are patentable for at least similar reasons as those stated for the claims on which they depend are patentable.

Canceled claims, if any, have been canceled without prejudice or disclaimer.

Any circumstance in which the applicant has (a) addressed certain comments of the examiner does not mean that the applicant concedes other comments of the examiner, (b) made arguments for the patentability of some claims does not mean that there are not other good reasons for patentability of those claims and other claims, or (c) amended or canceled a claim does not mean that the applicant concedes any of the examiner's positions with respect to that claim or other claims.

Please apply Enter $ amount for excess claim fees and Enter $ amount for the Petition for Extension of Time fee and any other charges or credits to deposit account 06-1050, referencing attorney docket 38879-0006001.

Respectfully submitted,

Date:/9/16/14/_____

/David L. Feigenbaum/_____
David L. Feigenbaum
Reg. No. 30,378

Customer Number 26161
Fish & Richardson P.C.
Telephone: (617) 542-5070
Facsimile: (877) 769-7945

23248511.doc

Electronic Acknowledgement Receipt

EFS ID:	20155140
Application Number:	13240572
International Application Number:	
Confirmation Number:	2423
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Customer Number:	26161
Filer:	David L Feigenbaum/jennifer franco
Filer Authorized By:	David L Feigenbaum
Attorney Docket Number:	38879-0006001
Receipt Date:	16-SEP-2014
Filing Date:	22-SEP-2011
Time Stamp:	16:42:00
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		response.pdf	101348 7019fa03d43b9671eb3c9385071ad679b3dc3cf2	yes	11

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Claims	2	7
	Abstract	8	11
Warnings:			
Information:			
	Total Files Size (in bytes):	101348	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/240,572	Filing Date 09/22/2011	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT **09/16/2014**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 30	Minus	** 28	= 2	X $40 =	80
Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $210 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	**80**

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/VINCENT BUTLER/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 09/18/2014

VBUTLER SALE #00000002 Mailroom Dt: 09/16/2014 061050 13240572
01 FC : 2202 80.00 DA

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/240,572	09/22/2011	Stephen Wayne Boyer	38879-0006001	2423

26161 7590 06/16/2014

FISH & RICHARDSON P.C. (BO)
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
KANAAN, SIMON P	
ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
06/16/2014	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATDOCTC@fr.com

Office Action Summary	Application No. 13/240,572	Applicant(s) BOYER ET AL.	
	Examiner SIMON KANAAN	Art Unit 2432	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *7 May 2014*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1,3-5,7-14,16 and 121-135* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1,3-5,7-14,16 and 121-135* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *22 September 2011* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some * c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Interim copies:

a)☐ All b)☐ Some c)☐ None of the: Interim copies of the priority documents have been received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *5/7/2014*.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

Notice of Pre-AIA or AIA Status

1. The present application is being examined under the pre-AIA first to invent provisions

2. In the event the determination of the status of the application as subject to AIA 35 U.S.C. 102 and 103 (or as subject to pre-AIA 35 U.S.C. 102 and 103) is incorrect, any correction of the statutory basis for the rejection will not be considered a new ground of rejection if the prior art relied upon, and the rationale supporting the rejection, would be the same under either status.

Continued Examination Under 37 CFR 1.114

3. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114.

4. Applicant's submission filed on 05/13/2014 has been entered.

Office Action Summary

5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Applicant's Arguments and Examiner's Response

6. Applicant's arguments/amendments filed 05/07/2014 have been considered but are moot based on new grounds of rejection necessitated by applicant's amendments. As for applicants argument that the cited prior art Newton fails to teach an "organizational entity" the examiner respectfully disagrees. Applicant's remarks do not point out where support is found for applicant's preferred definition of "organizational entity" and page 7, last paragraph teaches entity information being information about IT assets as taught by Newton; also Newton, figure 1, items 24 include information about the network which towards the bottom of item 24 states "company info resources" i.e. network is associated with a company.

Claim Rejections - 35 USC § 103

7. Claims 1,3-5,7-14,16 and 121-135 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chris Newton (US Pre-Grant Publication No: 2004/0250122 A1) hereinafter referred to as Newton in view of in view of Shull et al. (US Pre-Grant Publication No: 2006/0212925 A1) hereinafter referred to as Shull.

As per claim 1, Newton discloses a method comprising: collecting, from at least two source, information about an organizational entity, at least some of the information being collected automatically by computer from at least two sources, one or more of the sources not controlled by the organizational entity, -Newton, [0012] teaches that every

network in the world would have a rating in the database and [0030] teaches establishing a reputation for a network, and [0031] teaches having multiple agents gathering data and [0044]-[0048] teaches different agent types i.e. different network characterization as each agent type gathers different type of data in regards to the security and reputation of network, among these agents include data mining internet which is public information and data mining newsgroups and forums which are also public knowledge and externally observable information not controlled by an organization and figure 1, items 24 include information about the network which towards the bottom of item 24 states "company info resources" i.e. network is associated with a company.

processing the information from both of the two sources to form of a security vulnerability of resilience or both of the organizational entity, and –Newton, [0044]-[0048] and [0029], teaches information gathered externally from multiple sources including proxy information.

But does not teach forming a composite score and providing the composite rating to a party for use in one or more of: monitoring, assessing, or mitigating the security vulnerability or resilience or both of the organizational entity.

However, Shull teaches forming a composite score and providing the composite rating to a party for use in one or more of: monitoring, assessing, or mitigating the security vulnerability or resilience or both of the organizational entity. –Shull, [0058] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is

similar to a credit score with informs requester of the trust of the entity, this score is received by the requester.

It would have been obvious at the time of the invention for one of the ordinary skill in the art to modify the method of collecting security characteristics from multiple sources as taught by Newton by creating a score representative of the different collected data as taught by Shull because it would aid the requester in determining whether the entity is trusted or not.

As per claim 3, Newton in view of Shull teaches the method of Claim 1 as noted above, wherein at least one source includes a commercial data source. –Newton, [0044]-[0048] teaches using different search engines such as Google and [0016] teaches hosted services.

As per claim 4, Newton in view of Shull discloses the method of Claim 1, wherein the collected information is represented by at least two data types. –Green, [0044]-[0048] teaches different agent types.

As per claim 5, Newton in view of Shull discloses the method of Claim 4, wherein the at least two data types include at least one of breach disclosures, block lists, configuration parameters, an identification of malware servers, an identification of a reputation, an identification of suspicious activity, an identification of spyware, white lists, an identification of compromised hosts, an identification of malicious activity, an

identification of spare activity, an identification of vulnerable hosts, an identification of phishing activity, or an identification of e-mail viruses. –Newton, [0013]-[0029] teaches security measures etc.

As per claim 7, Newton in view of Shull discloses the method of Claim 1, wherein the collected information evidences internal security controls. –Newton, [0013]-[0029] teaches security measures etc.

As per claim 8, Newton in view of Shull discloses the method of Claim 1, wherein the collected information evidences outcomes of the organizational entity. –Newton, [0013]-[0029] teaches security measures and [0044]-[0048] teaches checking for information already available to the public about network.

As per claim 9, Newton in view of Shull discloses the method of Claim 1, wherein the collected information evidences operational execution of security measures of the organizational entity. –Newton, [0013]-[0029] teaches security measures.

As per claim 10, Newton in view of Shull discloses the method of Claim 1, wherein the collected information indicates whether a computer system of the organizational entity served malicious code to another system. –Newton, [0013], teaches hostility level and page 4, claim 6, teaches spam levels.

As per claim 11, Newton in view of Shull discloses the method of Claim 1, wherein the collected information indicates whether a computer system of the organizational entity communicated with a known attacker controlled network. –Newton, [0013] teaches hostility level.

As per claim 12, Newton in view of Shull discloses the method of Claim 1, comprising: forming a series of the security ratings of the organizational entity. –Newton, [0042], teaches live remote updates i.e. continually computing rating and page 4, claim 6 teaches security information has multiple ratings and [0041], teaches the different information having different weight.

As per claim 13, Newton in view of Shull discloses the method of Claim 12, comprising determining a trend from the series of ratings. –Newton, [0042], teaches live remote updates i.e. continually computing rating.

As per claim 14, Newton in view of Shull discloses the method of Claim 12, comprising displaying the series of composite ratings. –Newton, [0033], teaches a master database for collecting and storing the network ratings and page 4, claim 6 teaches security information has multiple ratings and [0041], teaches the different information having different weight and Shull, [0058], [0076] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score with informs requester of the trust of the entity, this score is received by the

requester and a display device would display score as to help user determine whether to trust entity or not.

As per claim 16, Newton in view of Shull teaches the method of Claim 14, wherein displaying the series of composite ratings for the entity comprises posting the series of composite ratings for the entity to a web portal. -Newton, [0033], teaches a master database for collecting and storing the network ratings which includes information as listed in [0013]-[0029] which serve as warnings and Shull, [0058], [0076] and figure 8, item 812, teaches creating a score for an entity from multiple sources which is similar to a credit score with informs requester of the trust of the entity, this score is received by the requester and a display device would display score as to help user determine whether to trust entity or not.

As per claim 121, Newton in view of Shull teaches the method of Claim 1, wherein the collected information represents externally observable outcome information. - Newton, [0054], teaches agents getting information from news groups or sending packets and checking their responses.

As per claim 122, Newton in view of Shull teaches the method of Claim 121, wherein the outcome information comprises outcome information associated with security vulnerability or resilience of the entity. Shull, [0058] and Newton, page 4, claim

6, both teach that the information is associated with entity security and Newton even looks into active security systems as well.

As per claim 123, Newton in view of Shull teaches the method of Claim 1, wherein the party to whom the composite rating is provided has a security risk associated with the vulnerability or resilience of the organizational entity. - Shull, [0058], teaches a composite score which would be indicative of risk.

As per claim 124, Newton in view of Shull teaches the method of Claim 1, comprising: determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information. - Newton, page 4, claim 6, teaches having spam levels etc. Which are a badness score.

As per claim 125, Newton in view of Shull teaches the method of Claim 1, comprising: determining a level of confidence of the composite rating of the entity. – Shull, [0058] and Newton, [0041], teaches weight on the different factors indicative of how confident/important the information is.

As per claim 126, Newton in view of Shull teaches the method of Claim 1, wherein: the collected information comprises at least two security characterizations of a computer system of the entity. - Newton, page 4, claim 6, teaches checking open proxy

servers and desktop security measures which are multiple characterizations of a system of the entity.

As per claim 127, Newton in view of Shull teaches the method of Claim 1, wherein the collected information comprises a characterization of behavior of an employee of the organizational entity. - Newton, page 4, claim 6, inappropriate content served, spam levels, language spoken, geographic placement, industry, which are characterizations of employees in the network and the employees' behavior.

As per claim 128, Newton in view of Shull teaches the method of Claim 1, wherein the collected information comprises characterizations other than characterizations about a computer system of the entity. -Newton, page 4, claim 6, teaches security characterization includes security personnel.

As per claim 129, Newton in view of Shull teaches the method of Claim 1, wherein the collected information comprises characterizations about policies of the entity. –Newton, page 4, claim 6, teaches organization association, active security measures, desktop security measures, etc. which are policies see also [0059] and [0060].

As per claim 130, Newton in view of Shull teaches the method of Claim 1, wherein the collected information comprises characterizations about information

technology assets that the entity owns, controls, uses, or is affiliated with. –Newton, page 4, claim 6, teaches organization associations see also [0043] and [0053].

As per claim 131, Newton in view of Shull teaches the method of Claim 1 in which collected information represents: (a) physical states, (b) technical states, (c) organizational states, or (d) cultural states of the entity which can be exploited to create a security breach; or (e) the entity's ability to recover from a security breach; or any combination of two or more of these. –Newton, page 4, claim 6, teaches active security measures and desktop security measures among other information collected about the organization.

As per claim 132, Newton in view of Shull teaches the method of claim 1 in which processing the information to form a composite rating comprises correlating data across the sources of information.-Shull, [0058], teaches creating a score based on the different data received i.e. correlating the different data.

As per claim 133, Newton in view of Shull teaches the method of claim 1 in which processing the information to form a composite rating comprises normalizing information from at least one of the sources. – Newton, [0041], teaches giving different information different weight.

As per claim 134, Newton in view of Shull teaches the method of claim 1 in which processing the information to form a composite rating comprises statistically correlating the composite rating with actual outcomes. – Newton, [0041], teaches giving different information different weight where less weight given to information as it becomes less important over time which is a statistical correlation with the information collected.

As per claim 135, Newton in view of Shull teaches the method of claim 1 in which the vulnerability comprises physical, technical, organizational, or cultural states that can be exploited to create a security breach. –Newton, figure 1, item 24 and page 4, claim 6.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Simon Kanaan whose telephone number is (571)270-3906. The examiner can normally be reached on Mon-Thurs 7:30-5:00 EST.

If attempts to reach the above noted Examiner by telephone are unsuccessful, the Examiner's supervisor, Gilberto Barron, can be reached at the following telephone number: (571) 272-3799.

The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.

/S. K./
Examiner, Art Unit 2432

/GILBERTO BARRON JR/
Supervisory Patent Examiner, Art Unit 2432

Notice of References Cited	Application/Control No. 13/240,572	Applicant(s)/Patent Under Reexamination BOYER ET AL.	
	Examiner SIMON KANAAN	Art Unit 2432	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2006/0212925	09-2006	Shull et al.	726/001
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Substitute Disclosure Form / U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No.	Application No.
Information Disclosure Statement by Applicant (Use several sheets if necessary) (37 CFR §1.98(b))	38879-0006001	13/240,572
	Applicant: Boyer et al.	
	Filing Date: September 22, 2011	Group Art Unit: 2432

U.S. Patent Documents							
Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate

Foreign Patent Documents or Published Foreign Patent Applications								
Examiner Initial	Desig. ID	Document Number	Publication Date	Country or Patent Office	Class	Subclass	Translation Yes	Translation No

Other Documents (include Author, Title, Date, and Place of Publication)		
Examiner Initial	Desig. ID	Document
	1	Edmonds, Robert, "ISC Passive DNS Architecture", Internet Systems Consortium, Inc., March 2012 (18 pages).

Examiner Signature	/Simon Kanaan/	Date Considered	06/04/2014

EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2014/06/06 11:12
L2	15	network (reputation or assess$4 or rat$3) with public with secur$5	US-PGPUB; USPAT	ADJ	ON	2014/06/06 11:13
L4	24	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation	US-PGPUB; USPAT	ADJ	ON	2014/06/06 11:13
L5	19	4 AND ((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.)	US-PGPUB; USPAT	ADJ	ON	2014/06/06 11:16
L6	58	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.) and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2014/06/06 11:17
L7	27724	((H04L63/20 OR H04L63/145 OR H04L67/306 OR H04L63/14 OR H04L51/12 OR H04L61/1511 OR H04L63/0236 OR H04L63/104 OR H04L63/1433 OR H04L9/321 OR G06F21/577 OR G06F21/00).CPC.)	US-PGPUB; USPAT	ADJ	ON	2014/06/06 11:17
L8	390	(network or organization or entity) reputation and (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2014/06/06 11:18
L9	87	L8 and L7	US-PGPUB; USPAT	ADJ	ON	2014/06/06 11:18
S1	0	"13240572"	US-PGPUB; USPAT	ADJ	ON	2012/11/14 18:15
S2	2	726/25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2012/11/14 18:18
S3	0	apparatus and method for network vulnerability detection and compliance	US-PGPUB; USPAT	ADJ	ON	2012/11/15 11:41
S4	0	network vulnerability detection and compliance assesment	US-PGPUB; USPAT	ADJ	ON	2012/11/15 11:42
S5	0	network vulnerability detection	US-	ADJ	ON	2012/11/15

		compliance assesment	PGPUB; USPAT			11:42
S6	0	network with vulnerability with detection with compliance with assesment	US-PGPUB; USPAT	ADJ	ON	2012/11/15 11:42
S7	7	network with vulnerability with detection with compliance with assessment	US-PGPUB; USPAT	ADJ	ON	2012/11/15 11:42
S8	19	726/2,22,25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2012/11/15 13:03
S9	24	726/2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:22
S10	30	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:23
S11	2	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:23
S12	95	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:25
S13	0	(external$5 or third party) with (security) with (commercial near data) with reputation	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:25
S14	0	(external$5 or third party) with (commercial near data) with reputation	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:25
S15	20	internet monitoring with report	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:27
S16	9	internet monitoring with report and public	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:27
S17	0	malwareurl	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:28
S18	0	malwareurl$5	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:28
S19	0	www$malwareurl$5	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:28
S20	0	www$malwareurl$com	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:28
S21	69	arbor networks	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:46
S22	1	arbor networks and renesys	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:46
S23	3268	reputation and domain	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:48
S24	32	reputation and domain and (insustry	US-	ADJ	ON	2012/11/15

		reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	PGPUB; USPAT			18:49
S25	49	reputation and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:56
S26	17	S25 not S24	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:56
S27	20	US-7194769-$.DID. OR US-7290275-$.DID. OR US-7971252-$.DID. OR US-20040010709-$.DID. OR US-20050138413-$.DID. OR US-20080047018-$.DID. OR US-20080209565-$.DID. OR US-20090265787-$.DID. OR US-20090293128-$.DID. OR US-2007304-$.DID. OR US-5200596-$.DID. OR US-2009104-$.DID. OR US-422009D-$.DID. OR US-1331018-$.DID.	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2012/11/15 18:59
S28	0	S25 and S27	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:02
S29	0	(insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and S27	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:02
S30	0	(industry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and S27	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:02
S31	0	(industry reports or internet monitoring or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and S27	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:03
S32	0	S27 and user behavior	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:03
S33	0	S27 and behavior	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:03
S34	0	S27 and reputation	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:03
S35	0	S27 and public with features	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2012/11/15 19:06
S36	0	S27 and externally	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2012/11/15 19:06

S37	7	S27 and external	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2012/11/15 19:06
S39	1	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:11
S40	13	((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:16
S41	132	((external$5 or third party) with audit$4)and reputation and security	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:21
S42	237	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:21
S43	230	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:21
S44	164	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:22
S45	0	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial data sources	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:22
S46	3	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial data	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:22
S47	3	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rating and commercial data	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:22
S48	3	security and renesys	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:24
S49	1	abor networks	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:27
S51	27	(network near3 vulnerability) with public	US-PGPUB; USPAT	ADJ	ON	2013/11/06 19:02
S52	17	(network near3 assessment) with public	US-PGPUB; USPAT	ADJ	ON	2013/11/06 20:17
S53	29	(network near3 assessment) with external$3	US-PGPUB; USPAT	ADJ	ON	2013/11/06 20:18
S54	1167	site secure	US-PGPUB; USPAT	ADJ	ON	2013/11/06 21:02
S55	438	S54 and third party	US-PGPUB; USPAT	ADJ	ON	2013/11/06 21:02
S56	166	S55 and assess$3	US-PGPUB; USPAT	ADJ	ON	2013/11/06 21:02

S57	146	network reputation	US-PGPUB; USPAT	ADJ	ON	2013/11/07 09:56
S58	138	network reputation and (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2013/11/07 09:56
S59	12	network reputation with (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2013/11/07 09:57
S61	8	network reputation with (rat$3 or assess$4) and public	US-PGPUB; USPAT	ADJ	ON	2013/11/07 14:21
S62	2	network reputation with public	US-PGPUB; USPAT	ADJ	ON	2013/11/07 14:25
S63	365	network (reputation or assess$4 or rat$3) with public	US-PGPUB; USPAT	ADJ	ON	2013/11/07 14:28
S64	176	network (reputation or assess$4 or rat$3) with public and security	US-PGPUB; USPAT	ADJ	ON	2013/11/07 14:30
S65	9	network (reputation or assess$4 or rat$3) with public with security	US-PGPUB; USPAT	ADJ	ON	2013/11/07 14:31
S66	14	network (reputation or assess$4 or rat$3) with public with secur$5	US-PGPUB; USPAT	ADJ	ON	2013/11/07 14:37
S67	5	S66 not S65	US-PGPUB; USPAT	ADJ	ON	2013/11/07 14:38
S68	2	"20040250122"	US-PGPUB; USPAT	ADJ	ON	2013/11/07 15:10
S69	1	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2013/11/07 23:33
S70	0	"13240572"	US-PGPUB; USPAT	ADJ	ON	2014/06/03 09:14
S72	3577	(organization or company or entity) same reputation	US-PGPUB; USPAT	ADJ	ON	2014/06/04 08:33
S73	823	(organization or company or entity) same reputation same (score or rating)	US-PGPUB; USPAT	ADJ	ON	2014/06/04 08:33
S74	15274	726/1,2,22,25.ccls.	US-PGPUB; USPAT	ADJ	ON	2014/06/04 08:34
S75	86	S73 and S74	US-PGPUB; USPAT	ADJ	ON	2014/06/04 08:34
S76	509	(organization or company) same reputation same (score or rating)	US-PGPUB; USPAT	ADJ	ON	2014/06/04 08:41
S77	36	S76 and S74	US-PGPUB; USPAT	ADJ	ON	2014/06/04 08:41

S78	0	"13240572"	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S79	7	726/25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S80	0	apparatus and method for network vulnerability detection and compliance	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S81	0	network vulnerability detection and compliance assesment	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S82	0	network vulnerability detection compliance assesment	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S83	0	network with vulnerability with detection with compliance with assesment	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S84	7	network with vulnerability with detection with compliance with assessment	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S85	28	726/2,22,25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S86	28	726/2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S87	37	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S88	3	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S89	108	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S90	0	(external$5 or third party) with (security) with (commercial near data) with reputation	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S91	0	(external$5 or third party) with (commercial near data) with reputation	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S92	23	internet monitoring with report	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S93	9	internet monitoring with report and public	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S94	0	malwareurl	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S95	0	malwareurl$5	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S96	0	www$malwareurl$5	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15

S97	0	www$malwareurl$com	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S98	107	arbor networks	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S99	1	arbor networks and renesys	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S100	4364	reputation and domain	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S101	46	reputation and domain and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S102	78	reputation and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S103	32	S102 not S101	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S104	21	US-7194769-$.DID. OR US-7290275-$.DID. OR US-7971252-$.DID. OR US-20040010709-$.DID. OR US-20050138413-$.DID. OR US-20080047018-$.DID. OR US-20080209565-$.DID. OR US-20090265787-$.DID. OR US-20090293128-$.DID. OR US-2007304-$.DID. OR US-5200596-$.DID. OR US-2009104-$.DID. OR US-422009D-$.DID. OR US-1331018-$.DID.	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2014/06/04 15:15
S105	0	S102 and S104	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S106	0	(insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and S104	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S107	0	(industry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and S104	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S108	0	(industry reports or internet monitoring or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and S104	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S109	0	S104 and user behavior	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S110	0	S104 and behavior	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S111	0	S104 and reputation	US-PGPUB;	ADJ	ON	2014/06/04 15:15

			USPAT			
S112	0	S104 and public with features	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2014/06/04 15:15
S113	0	S104 and externally	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2014/06/04 15:15
S114	7	S104 and external	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2014/06/04 15:15
S115	24	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S116	1	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S117	15	((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S118	179	((external$5 or third party) with audit$4)and reputation and security	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S119	322	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S120	308	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S121	204	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S122	0	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial data sources	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S123	4	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial data	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S124	4	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rating and commercial data	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S125	4	security and renesys	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S126	1	abor networks	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S127	29	(network near3 vulnerability) with public	US-PGPUB;	ADJ	ON	2014/06/04 15:15

			USPAT			
S128	19	(network near3 assessment) with public	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S129	32	(network near3 assessment) with external$3	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S130	1264	site secure	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S131	478	S130 and third party	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S132	185	S131 and assess$3	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S133	166	network reputation	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S134	156	network reputation and (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S135	14	network reputation with (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S136	9	network reputation with (rat$3 or assess$4) and public	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S137	2	network reputation with public	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S138	395	network (reputation or assess$4 or rat$3) with public	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S139	200	network (reputation or assess$4 or rat$3) with public and security	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S140	9	network (reputation or assess$4 or rat$3) with public with security	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S141	15	network (reputation or assess$4 or rat$3) with public with secur$5	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S142	6	S141 not S140	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:15
S143	2	"20040250122"	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:16
S145	0	"13240572"	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:16
S146	3577	(organization or company or entity) same reputation	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:16
S147	823	(organization or company or entity) same reputation same (score or rating)	US-PGPUB;	ADJ	ON	2014/06/04 15:16

			USPAT			
S148	15274	726/1,2,22,25.ccls.	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:16
S149	86	S147 and S148	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:16
S150	509	(organization or company) same reputation same (score or rating)	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:16
S151	36	S150 and S148	US-PGPUB; USPAT	ADJ	ON	2014/06/04 15:16

6/6/2014 11:21:42 AM
C:\Users\skanaan\Documents\EAST\Workspaces\13240572.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	**Art Unit**
	SIMON KANAAN	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/18/2013	11/07/2013	06/04/2014						
	1	✓	✓	✓						
	2	✓	✓	-						
	3	✓	✓	✓						
	4	✓	✓	✓						
	5	✓	✓	✓						
	6	✓	✓	-						
	7	✓	✓	✓						
	8	✓	✓	✓						
	9	✓	✓	✓						
	10	✓	✓	✓						
	11	✓	✓	✓						
	12	✓	✓	✓						
	13	✓	✓	✓						
	14	✓	✓	✓						
	15	✓	✓	-						
	16	✓	✓	✓						
	17	✓	✓	-						
	18	✓	✓	-						
	19	✓	✓	-						
	20	✓	✓	-						
	21	-	-	-						
	22	-	-	-						
	23	-	-	-						
	24	-	-	-						
	25	-	-	-						
	26	-	-	-						
	27	-	-	-						
	28	-	-	-						
	29	-	-	-						
	30	-	-	-						
	31	-	-	-						
	32	-	-	-						
	33	-	-	-						
	34	-	-	-						
	35	-	-	-						
	36	-	-	-						

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	**Art Unit**
	SIMON KANAAN	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/18/2013	11/07/2013	06/04/2014						
	37	-	-	-						
	38	-	-	-						
	39	-	-	-						
	40	-	-	-						
	41	-	-	-						
	42	-	-	-						
	43	-	-	-						
	44	-	-	-						
	45	-	-	-						
	46	-	-	-						
	47	-	-	-						
	48	-	-	-						
	49	-	-	-						
	50	-	-	-						
	51	-	-	-						
	52	-	-	-						
	53	-	-	-						
	54	-	-	-						
	55	-	-	-						
	56	-	-	-						
	57	-	-	-						
	58	-	-	-						
	59	-	-	-						
	60	-	-	-						
	61	-	-	-						
	62	-	-	-						
	63	-	-	-						
	64	-	-	-						
	65	-	-	-						
	66	-	-	-						
	67	-	-	-						
	68	-	-	-						
	69	-	-	-						
	70	-	-	-						
	71	-	-	-						
	72	-	-	-						

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	**Art Unit**
	SIMON KANAAN	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/18/2013	11/07/2013	06/04/2014						
	73	-	-	-						
	74	-	-	-						
	75	-	-	-						
	76	-	-	-						
	77	-	-	-						
	78	-	-	-						
	79	-	-	-						
	80	-	-	-						
	81	-	-	-						
	82	-	-	-						
	83	-	-	-						
	84	-	-	-						
	85	-	-	-						
	86	-	-	-						
	87	-	-	-						
	88	-	-	-						
	89	-	-	-						
	90	-	-	-						
	91	-	-	-						
	92	-	-	-						
	93	-	-	-						
	94	-	-	-						
	95	-	-	-						
	96	-	-	-						
	97	-	-	-						
	98	-	-	-						
	99	-	-	-						
	100	-	-	-						
	101	-	-	-						
	102	-	-	-						
	103	-	-	-						
	104	-	-	-						
	105	-	-	-						
	106	-	-	-						
	107	-	-	-						
	108	-	-	-						

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	Art Unit
	SIMON KANAAN	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/18/2013	11/07/2013	06/04/2014						
	109	-	-	-						
	110	-	-	-						
	111	-	-	-						
	112	-	-	-						
	113	-	-	-						
	114	-	-	-						
	115	-	-	-						
	116	-	-	-						
	117	-	-	-						
	118	-	-	-						
	119	-	-	-						
	120	-	-	-						
	121			✓						
	122			✓						
	123			✓						
	124			✓						
	125			✓						
	126			✓						
	127			✓						
	128			✓						
	129			✓						
	130			✓						
	131			✓						
	132			✓						
	133			✓						
	134			✓						
	135			✓						

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	Art Unit
	SIMON KANAAN	2432

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor and Assignee Search (PALM)	4/18/2013	SK
class/subclass search + text (EAST: 726/1,2,22,25+text)	6/4/2014	SK
CPC + text (EAST: H04L63/20,145,14,0236,1433,104 OR H04L67/306 OR H04L51/12 OR H04L61/1511 OR H04L9/321 OR G06F21/00,577 + text)	6/4/2014	SK

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/SIMON KANAAN/ Examiner.Art Unit 2432	

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

MAILED
JUN 05 2014
OFFICE OF PETITIONS

FISH & RICHARDSON P.C. (BO)
P.O. BOX 1022
MINNEAPOLIS MN 55440-1022

Doc Code: TRACK1.GRANT

Decision Granting Request for Prioritized Examination (Track I or After RCE)	Application No.: 13/240,572

1. THE REQUEST FILED May 7, 2014 IS **GRANTED.**

The above-identified application has met the requirements for prioritized examination

A. ☐ for an original nonprovisional application (Track I).
B. ☒ for an application undergoing continued examination (RCE).

2. **The above-identified application will undergo prioritized examination.** The application will be accorded special status throughout its entire course of prosecution until one of the following occurs:

A. filing a **petition for extension of time** to extend the time period for filing a reply;
B. filing an **amendment to amend the application to contain more than four independent claims, more than thirty total claims**, or a multiple dependent claim;
C. filing a **request for continued examination**;
D. filing a notice of appeal;
E. filing a request for suspension of action;
F. mailing of a notice of allowance;
G. mailing of a final Office action;
H. completion of examination as defined in 37 CFR 41.102; or
I. abandonment of the application.

Telephone inquiries with regard to this decision should be directed to Brian W. Brown at 571-272-5338.

/Brian W. Brown/
[*Signature*]

Petitions Examiner, Office of Petitions
(Title)

PTO/SB/30 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995. no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Request for Continued Examination (RCE) Transmittal

Address to:
Mail Stop RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Application Number	13/240,572
Filing Date	September 22, 2011
First Named Inventor	Stephen Boyer
Art Unit	2432
Examiner Name	Simon P. Kanaan
Attorney Docket Number	38879-0006001

This is a Request for Continued Examination (RCE) under 37 CFR 1 .114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. See Instruction Sheet for RCEs (not to be submitted to the USPTO) on page 2.

1. Submission required under 37 CFR 1.114 Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

   a. ☐ Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

      i. ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

      ii. ☐ Other _____

   b. ☒ Enclosed

      i. ☒ Amendment/Reply

      ii. ☐ Affidavit(s)/ Declaration(s)

      iii. ☒ Information Disclosure Statement (IDS)

      iv. ☒ Other Interview Summary

2. Miscellaneous

   Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a

   a. ☐ period of _____ months. (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

   b. ☐ Other _____

3. Fees The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.
   The Director is hereby authorized to charge the following fees any underpayment of fees or credit any overpayments to

   a. ☒ Deposit Account No. 06-1050 .

      i. ☒ RCE fee required under 37 CFR 1.17(e)

      ii ☒ Extension of time fee (37 CFR 1.136 and 1.17)

      iii ☒ Other any deficiencies

   b. ☐ Check in the amount of $ _____ enclosed

   c. ☐ Payment by credit card (Form PTO-2038 enclosed)

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Signature	/David L. Feigenbaum/	Date	5/7/14
Name (Print/Type)	David L. Feigenbaum	Registration No.	30,378

CERTIFICATE OF MAILING OR TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop RCE, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450 or facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.

Signature			
Name (Print/Type)		Date	

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Mail Stop RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

American LegalNet, Inc.
www.FormsWorkFlow.com

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor	:	Stephen Boyer	Art Unit	:	2432
Serial No.	:	13/240,572	Examiner	:	Simon P. Kanaan
Filed	:	September 22, 2011	Conf. No.	:	2423
Title	:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM			

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PETITION FOR THREE-MONTH EXTENSION OF TIME UNDER 37 C.F.R. §1.136

Please extend the period for response to the action dated November 21, 2013, for three months to and including May 21, 2014.

The fees of $700 are being paid with this petition. In addition, please apply any other necessary charges or credits to deposit account 06-1050, referencing the above attorney docket number.

Respectfully submitted,

Date:/5/7/14/_____

/David L. Feigenbaum/_____
David L. Feigenbaum
Reg. No. 30,378

Customer Number 26161
Fish & Richardson P.C.
Telephone: (617) 542-5070
Facsimile: (877) 769-7945

23217871.doc

Electronic Patent Application Fee Transmittal

Application Number:	13240572
Filing Date:	22-Sep-2011
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Filer:	David L Feigenbaum/jennifer franco
Attorney Docket Number:	38879-0006001

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 3 months with $0 paid	2253	1	700	700

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
Request for Continued Examination	2801	1	600	600
		Total in USD ($)		**1300**

Electronic Acknowledgement Receipt

EFS ID:	18967413
Application Number:	13240572
International Application Number:	
Confirmation Number:	2423
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Customer Number:	26161
Filer:	David L Feigenbaum/jennifer franco
Filer Authorized By:	David L Feigenbaum
Attorney Docket Number:	38879-0006001
Receipt Date:	07-MAY-2014
Filing Date:	22-SEP-2011
Time Stamp:	16:43:21
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$1300
RAM confirmation Number	3146
Deposit Account	061050
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

Black Kite Ex. 1003, Page 787 of 1060

1		response.pdf	118903 1d845880a0d71b00bfaab5f20885f0b9a2193a68	yes	10

Multipart Description/PDF files in .zip description		
Document Description	**Start**	**End**
Amendment Submitted/Entered with Filing of CPA/RCE	1	1
Claims	2	5
Applicant summary of interview with examiner	6	6
Applicant Arguments/Remarks Made in an Amendment	7	10

Warnings:					
Information:					
2	Transmittal Letter	IDS.pdf	59446 3d13a32a2457c53d271c9c67d6fc5ba99bf31541	no	1
Warnings:					
Information:					
3	Information Disclosure Statement (IDS) Form (SB08)	1449.pdf	84971 363623adfe43ae3ee072833d7164a7e479d4253b	no	1
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
4	Non Patent Literature	Edmonds.pdf	733697 779c3c98b8d31b691aef58a0c1c498c902d21bf3	no	18
Warnings:					
Information:					
5	Request for Continued Examination (RCE)	rce.pdf	142275 773ba711df1d27342aaa15e6fe6e703a4b758ed8	no	1
Warnings:					
This is not a USPTO supplied RCE SB30 form.					
Information:					
6	Extension of Time	ext.pdf	45940 c042d29904c510ee1f1aa9356025769b50f2be29	no	1
Warnings:					
Information:					

7	Fee Worksheet (SB06)	fee-info.pdf	32570 c50e6de198eebdf768254bcf399852b24e66abab	no	2

Warnings:	
Information:	
Total Files Size (in bytes):	1217802

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant :	Boyer et al.	Art Unit :	2432
Serial No. :	13/240,572	Examiner :	Simon P. Kanaan
Filed :	September 22, 2011	Conf. No. :	2423
Title :	Information Technology Security Assessment System		

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY TO ACTION OF NOVEMBER 21, 2013

List of claims (replacing prior versions):

1. (Currently Amended) A method ~~of evaluating information security of a third party computer system, the method~~ comprising:

collecting, from at least two sources, information about an organizational entity, ~~a plurality of security characterizations~~ at least some of the information being collected automatically by computer from at least two sources, one or more of the sources not controlled by the organizational entity,

the information from at least the one or more sources that are not controlled by the organizational entity being collected without permission of the organizational entity, ~~from a plurality of providers independent of the third party computer system, wherein the security characterizations are publicly available and based on externally observable security outcome information~~;

~~determining at least two of the security characterizations that are proxies for the vulnerability of the third party system; and~~

processing the information from both of the two sources to form ~~generating~~ a composite ~~security~~ rating of a security vulnerability or resilience or both of the organizational entity, and

~~the third party computer system using the proxy security characterizations~~

providing the composite rating to a party for use in one or more of: monitoring, assessing, or mitigating the security vulnerability or resilience or both of the organizational entity.

2. (Canceled)

3. (Currently Amended) [[A]] The method of Claim 1 [[2]], wherein ~~the independent entities~~ at least one of the sources includes a ~~include~~ commercial data ~~sources~~ source.

4. (Currently Amended) [[A]] The method of Claim 1 [[2]], wherein the ~~security characterizations~~ collected information is represented by ~~include~~ at least two data types.

5. (Currently Amended) [[A]] The method of Claim 4, wherein the at least two data types include at least one of breach disclosures, block lists, configuration parameters, an identification

of malware servers, an identification of a reputation, an identification of suspicious activity, an identification of spyware, white lists, an identification of compromised hosts, an identification of malicious activity, an identification of spam activity, an identification of vulnerable hosts, an identification of phishing activity, or an identification of e-mail viruses.

6. (Canceled)

7. (Currently Amended) [[A]] The method of Claim 1, wherein the ~~security characterizations~~ collected information evidences ~~evidence~~ internal security controls.

8. (Currently Amended) [[A]] The method of Claim 1, wherein the ~~security characterizations are~~ collected information comprises outcomes of the organizational entity.

9. (Currently Amended) [[A]] The method of Claim 1, wherein the ~~security characterizations evidence~~ collected information evidences operational execution of security measures of the organizational entity ~~third party computer system~~.

10. (Currently Amended) [[A]] The method of Claim 1, wherein the ~~security characterizations~~ collected information indicates whether a computer system of the organizational entity served ~~include serving of~~ malicious code to another system.

11. (Currently Amended) [[A]] The method of Claim 1, wherein the ~~security characterizations~~ collected information indicates whether a computer system of the organizational entity communicated ~~include communications~~ with a known attacker controlled ~~networks~~ network.

12. (Currently Amended) [[A]] The method of Claim 1, ~~wherein collecting the data and generating the ratings are repeated to~~ comprising:

forming ~~generate~~ a series of the security ratings of the organizational entity.

13. (Currently Amended) [[A]] The method of Claim 12 [[11]], ~~further~~ comprising:

determining a trend from the series of ratings.

14. (Currently Amended) [[A]] The method of Claim 12, ~~further~~ comprising:

~~reporting~~ displaying the series of composite ratings.

15. (Canceled)

16. (Currently Amended) [[A]] The method of Claim 14, wherein ~~reporting includes~~ displaying the series of composite ratings for the entity comprises posting the series of composite ratings for the entity ~~and warning~~ to a web portal.

17. (Canceled)

18. (Canceled)

19-120. (Canceled)

121. (New) The method of Claim 1, wherein the collected information represents externally observable outcome information.

122. (New) The method of Claim 121, wherein the outcome information comprises outcome information associated with security vulnerability or resilience of the entity.

123. (New) The method of Claim 1, wherein the party to whom the composite rating is provided has a security risk associated with the vulnerability or resilience of the organizational entity.

124. (New) The method of Claim 1, comprising:

determining a badness score that corresponds to an intensity or duration of malicious activity determined from the collected information.

125. (New) The method of Claim 1, comprising:

determining a level of confidence of the composite rating of the entity.

126. (New) The method of Claim 1, wherein:

the collected information comprises at least two security characterizations of a computer system of the entity.

127. (New) The method of Claim 1, wherein the collected information comprises a characterization of behavior of an employee of the organizational entity.

128. (New) The method of Claim 1, wherein the collected information comprises characterizations other than characterizations about a computer system of the entity.

129. (New) The method of Claim 1, wherein the collected information comprises characterizations about policies of the entity.

130. (New) The method of Claim 1, wherein the collected information comprises characterizations about information technology assets that the entity owns, controls, uses, or is affiliated with.

131. (New) The method of Claim 1 in which collected information represents: (a) physical states, (b) technical states, (c) organizational states, or (d) cultural states of the entity which can be exploited to create a security breach; or (e) the entity's ability to recover from a security breach; or any combination of two or more of these.

132. (New) The method of claim 1 in which processing the information to form a composite rating comprises correlating data across the sources of information.

133. (New) The method of claim 1 in which processing the information to form a composite rating comprises normalizing information from at least one of the sources.

134. (New) The method of claim 1 in which processing the information to form a composite rating comprises statistically correlating the composite rating with actual outcomes.

135. (New) The method of claim 1 in which the vulnerability comprises physical, technical, organizational, or cultural states that can be exploited to create a security breach.

REMARKS

The applicant thanks Examiner Kanaan and Supervisory Patent Examiner Barron for the in person interview conducted on March 13, 2014, with the applicant's representative, Joel D. Couenhoven, and inventor Stephen Boyer. The interview included a discussion of the prior art with respect to the claims and potential amendments to the claims regarding the differences between the term "entity" recited in the claims and the network disclosed in Newton. No agreement was reached.

The comments of the applicant below are each preceded by related comments of the examiner (in small, bold type). Support for the amendments can be found in the application as filed, for example, at pages 1-2, and 7-20.

9. Claims 1 through 20 are rejected under 35 U.S.C. 1 02(b) as being anticipated by Chris Newton (US Pre-Grant Publication No: 2004/0250122 A 1) hereinafter referred to as Newton. Application/Control Number: 13/240,572

As per claim 1, Newton discloses a method of evaluating information security of a third party computer system, the method comprising: collecting at a plurality of security characterizations from a plurality of providers independent of the third party computer system, wherein the security characterizations are publicly available and based on externally observable security outcome information.; -Newton, [0012] teaches that every network in the world would have a rating in the database and [0030] teaches establishing a reputation for a network, and [0031] teaches having multiple agents gathering data and [0044]-[0048] teaches different agent types i.e. different network characterization as each agent type gathers different type of data in regards to the security and reputation of network, among these agents include data mining internet which is public information and data mining newsgroups and forums which are also public knowledge and externally observable information; determining at least two of the security characterizations that are proxies for the vulnerability of the third party system; and -Newton, [0044]-[0048] and [0029], teaches information gathered externally from multiple sources including proxy information. generating a composite security rating of the third party computer system using the proxy security characterizations; -Newton, [0030] teaches computing the network reputation where a reputation is a score.

Without conceding the examiner's position, the applicant has amended claim 1.

In amended claim 1, information from both of two sources is processed to form a "composite rating of the security vulnerability or resilience" of an "organizational entity". The phrase "organizational entity" is meant to connote that the entity is an organization of some form. An IP network (hardware and software) *itself and taken alone* is not meant to be considered an "organizational entity". Also, in amended claim 1, the resulting composite rating is

provided to a party for use in one or more of "monitoring, assessing, or mitigating the security vulnerability or resilience or both of the organizational entity." In some examples, the party could use the composite rating in deciding whether to invest in the organizational entity, do business with the organizational entity, or report the organizational entity to another party, among others.

Newton, by contrast, did not describe and would not have made obvious forming a composite rating of an organizational entity, let alone providing it to a party for use in such activities.

The applicant does not dispute that Newton described maintaining databases about properties of networks. Although the properties included, for example, "organization type" and "organization associations", those were considered by Newton to be properties of the network. As Newton said (column 2, beginning at line 54) "every network in the world would have a record in the database with a large number of properties." Then Newton noted that his invention established "respective reputations for networks and allow a given network to determine whether to communicate with a particular network in dependence upon its reputation." (Column 3, beginning at line 10). Newton repeatedly referred to providing intelligence about other networks rather than about other organizational entities.

Thus, Newton did not describe and would not have made obvious using the information in his database to form a composite rating of the security vulnerability or resilience of the organizational entity. To the contrary, the reputations referred to by Newton were reputations of networks (not of organizational entities) and were reputations that were to have been inferred from the properties of the network in the database by an administrator of a network. Newton did not describe and would not have made obvious forming and providing composite ratings of organizational entities to parties. To the contrary, Newton apparently only contemplated making the database properties available for example to administrator who could do what he wished with the information. Newton did not form a composite rating let alone providing it to someone.

As Newton explained it, the database was used by an administrator "to take conceptual ideas of who he wants his network to talk to, not talk to, or how he wants to configure services, and turns them into technical rule sets that the devices require." (column 4, beginning at line 4) The devices would then use the technical rule sets to manage specific communications with the

IP network involved. In other words, to the extent that a reputation was derived from the database in Newton, the reputation was derived by the administrator in an ad hoc way and then used to instruct the hardware and software devices that communicated with the IP network involved. Even if Newton's so-called "reputation" were somehow to be construed as a "security rating", it was not a security rating that was formed by processing of the collected information, as in the applicant's claim 1, but was one inferred by a human being who might review the properties contained in the database and then set ad hoc principles for interaction with the network.

Therefore, Newton did not describe and would not have made obvious processing the information from both of the two sources to form a composite rating of the security vulnerability or resilience or both of an organizational entity, let alone (in the words of the applicant's amended claim 1) "providing such a composite rating for use in monitoring, assessing, or mitigating the security vulnerability or resilience or both of the organizational entity."

As per claim 2, Newton discloses a method of Claim 1, wherein each of the security characterizations is from an associated one of a plurality of independent entities. -Newton, [0030] teaches having multiple agents gathering data and [0044]-Application/Control Number: 13/240,572 [0048] teaches different agent types i.e. different network characterization as each agent type gathers different type of data in regards to the security and reputation of network, among these agents include data mining internet which is public information and data mining newsgroups and forums which are also public knowledge and externally observable information.

As per claim 3, Newton teaches a method of Claim 2 as noted above, wherein the independent entities include commercial data sources. -Newton, [0044]-[0048] teaches using different search engines such as Google and [0016] teaches hosted services.

As per claim 4, Newton discloses a method of Claim 2, wherein the security characterizations include at least two data types. -Green, [0044]-[0048] teaches different agent types.

**As per claim 5, Newton discloses a method of Claim 4, wherein the data types include at least one of breach disclosures, block lists, configuration parameters, malware servers, reputation, suspicious activity, spyware, white lists, compromised hosts, malicious activity, spare activity, vulnerable hosts, phishing, or e-mail viruses. - Newton, [0013]-[0029] teaches security measures etc. Application/Control Number: 13/240,572 As per claim 6, Newton discloses a method of Claim 1, wherein the security characterizations are derived without permission of the third party computer system. - Newton, [0044]-[0048], teaches using the internet to compute the network reputation i.e.
without authorization.**

As per claim 7, Newton discloses a method of Claim 1, wherein the security characterizations evidence internal security controls. -Newton, [0013]-[0029] teaches security measures etc.

As per claim 8, Newton discloses a method of Claim 1, wherein the security characterizations are outcomes. -Newton, [0013]-[0029] teaches security measures and [0044]-[0048] teaches checking for information already available to the public about network.

As per claim 9, Newton discloses a method of Claim 1, wherein the security characterizations evidence operational execution of security measures of the third party computer system. -Newton, [0013]-[0029] teaches security measures.

As per claim 10, Newton discloses a method of Claim 1, wherein the security characterizations include serving of malicious code. -Newton, [0013], teaches hostility level. Application/Control Number: 13/240,572

As per claim 11, Newton discloses a method of Claim 1, wherein the security characterizations include communications with known attacker controlled networks. -Newton, [0013] teaches hostility level.

As per claim 12, Newton discloses a method of Claim 1, wherein collecting the data and generating the ratings are repeated to generate a series of ratings. -Newton, [0042], teaches live remote updates i.e. continually computing rating.

As per claim 13, Newton discloses a method of Claim 11, further comprising determining a trend from the series of ratings. -Newton, [0042], teaches live remote updates i.e. continually computing rating.

As per claim 14, Newton discloses a method of Claim 12, further comprising reporting the ratings. -Newton, [0033], teaches a master database for collecting and storing the network ratings.

As per claim 15, Newton discloses a method of Claim 13, wherein reporting includes reporting a warning based on a change in the ratings. -Newton, [0033], teaches a master database for collecting and storing the network ratings which includes information as listed in [0013]-[0029] which serve as warnings. Application/Control Number: 13/240,572

As per claim 16, Newton teaches a method of Claim 14, wherein reporting includes posting the ratings and warning to a web portal. -Newton, [0033], teaches a master database for collecting and storing the network ratings which includes information as listed in [0013]-[0029] which serve as warnings.

As per claim 17, Green discloses a method of Claim 1, wherein collecting the security characterizations includes using tools such as WGET, RSYNC or proprietary and manual methods. -Newton, [0022] teaches security measures and firewalls and [0020] teaches peer ISPs.

As per claim 18, Newton discloses a method of Claim 1, further comprising mapping the third party computer system to an IP space and using the IP space for collecting the security characterizations. -Newton, [0020], teaches including peer ISPs.

As per claim 19, Newton discloses a method of Claim 18, wherein mapping includes querying a regional internet registry. -Newton, [0044]-[0048], teaches using the internet to compute the network reputation i.e. without authorization.

As per claim 20, Newton discloses a method of Claim 19, wherein querying includes submitting an entity name. -Newton, [0019] teaches who organization is owned by.

All of the dependent claims are patentable for at least similar reasons as those for the claims on which they depend are patentable.

Canceled claims, if any, have been canceled without prejudice or disclaimer.

Any circumstance in which the applicant has (a) addressed certain comments of the examiner does not mean that the applicant concedes other comments of the examiner, (b) made arguments for the patentability of some claims does not mean that there are not other good reasons for patentability of those claims and other claims, or (c) amended or canceled a claim does not mean that the applicant concedes any of the examiner's positions with respect to that claim or other claims.

The fees for excess claims and extension of time are being paid with this reply on the Electronic Filing System. Apply those fees and any other necessary charges or credits to Deposit Account 06 1050, referencing the above attorney docket number.

Respectfully submitted,

Date:/5/7/14/_____

/David L. Feigenbaum/_____
David L. Feigenbaum
Reg. No. 30,378

Customer Number 26161
Fish & Richardson P.C.
Telephone: (202) 626-6397
Facsimile: (877) 769-7945

1203391o.docx

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Boyer et al.	Art Unit	: 2432
Serial No.	: 13/240,572	Examiner	: Simon P. Kanaan
Filed	: September 22, 2011	Conf. No.	: 2423
Title	: INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM		

MAIL STOP RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT

Please consider the reference listed on the enclosed PTO-SB-08 or Disclosure Form.

Respectfully submitted,

Date:/5/7/14/_____

/David L. Feigenbaum/_____
David L. Feigenbaum
Reg. No. 30,378

Customer Number 26161
Fish & Richardson P.C.
Telephone: (202) 626-6397
Facsimile: (877) 769-7945

23166580.doc

Substitute Disclosure Form	U.S. Department of Commerce Patent and Trademark Office	Attorney Docket No. 38879-0006001	Application No. 13/240,572
Information Disclosure Statement by Applicant (Use several sheets if necessary)		Applicant Boyer et al.	
(37 CFR §1.98(b))		Filing Date September 22, 2011	Group Art Unit 2432

U.S. Patent Documents

Examiner Initial	Desig. ID	Document Number	Publication Date	Patentee	Class	Subclass	Filing Date If Appropriate

Foreign Patent Documents or Published Foreign Patent Applications

Examiner Initial	Desig. ID	Document Number	Publication Date	Country or Patent Office	Class	Subclass	Translation Yes	Translation No

Other Documents (include Author, Title, Date, and Place of Publication)

Examiner Initial	Desig. ID	Document
	1	Edmonds, Robert, "ISC Passive DNS Architecture", Internet Systems Consortium, Inc., March 2012 (18 pages).

Examiner Signature	Date Considered
EXAMINER: Initials citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.	

CERTIFICATION AND REQUEST FOR PRIORITIZED EXAMINATION UNDER 37 CFR 1.102(e) (Page 1 of 1)

First Named Inventor:	Stephen Boyer	Nonprovisional Application Number (if known):	13/240,572
Title of Invention:	Information Technology Security Assessment System		

APPLICANT HEREBY CERTIFIES THE FOLLOWING AND REQUESTS PRIORITIZED EXAMINATION FOR THE ABOVE-IDENTIFIED APPLICATION.

1. The processing fee set forth in 37 CFR 1.17(i), the prioritized examination fee set forth in 37 CFR 1.17(c), and if not already paid, the publication fee set forth in 37 CFR 1.18(d) have been filed with the request. The basic filing fee, search fee, examination fee, and any required excess claims and application size fees are filed with the request or have been already been paid.

2. The application contains or is amended to contain no more than four independent claims and no more than thirty total claims, and no multiple dependent claims.

3. The applicable box is checked below:

I. ☐ Original Application (Track One) - Prioritized Examination under § 1.102(e)(1)

i. (a) The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a). This certification and request is being filed with the utility application via EFS-Web.

---OR---

(b) The application is an original nonprovisional plant application filed under 35 U.S.C. 111(a). This certification and request is being filed with the plant application in paper.

ii. An executed oath or declaration under 37 CFR 1.63 is filed with the application.

II. ☒ Request for Continued Examination - Prioritized Examination under § 1.102(e)(2)

i. A request for continued examination has been filed with, or prior to, this form,
ii. If the application is a utility application, this certification and request is being filed via EFS-Web.
iii. The application is an original nonprovisional utility application filed under 35 U.S.C. 111(a), or is a national stage entry under 35 U.S.C. 371.
iv. This certification and request is being filed prior to the mailing of a first Office action responsive to the request for continued examination.
v. No prior request for continued examination has been granted prioritized examination status under 37 CFR 1.102(e)(2).

Signature /David L. Feigenbaum/	Date May 7, 2014
Name David L. Feigenbaum (Print/Typed)	Practitioner Registration Number 30,378

Note: *Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required in accordance with 37 CFR 1.33 and 11.18. Please see 37 CFR 1.4(d) for the form of the signature. If necessary, submit multiple forms for more than one signature, see below*.*

☒ *Total of 1 forms are submitted.

23218939.doc

American LegalNet, Inc. www.FormsWorkflow.com

Electronic Patent Application Fee Transmittal

Application Number:	13240572
Filing Date:	22-Sep-2011
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Filer:	David L Feigenbaum/jennifer franco
Attorney Docket Number:	38879-0006001

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Request for Prioritized Examination	2817	1	2000	2000
Pages:				
Claims:				
Miscellaneous-Filing:				
PROCESSING FEE, EXCEPT PROV. APPLS.	2830	1	70	70
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**2070**

Electronic Acknowledgement Receipt

EFS ID:	18973081
Application Number:	13240572
International Application Number:	
Confirmation Number:	2423
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Customer Number:	26161
Filer:	David L Feigenbaum/jennifer franco
Filer Authorized By:	David L Feigenbaum
Attorney Docket Number:	38879-0006001
Receipt Date:	07-MAY-2014
Filing Date:	22-SEP-2011
Time Stamp:	19:42:46
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$2070
RAM confirmation Number	5363
Deposit Account	061050
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

1	TrackOne Request	track-1-request.pdf	137564 c23c6b9689d78a55a2c64f3f9f720f42c3d154ed	no	1
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	32772 81991c0821ac34169bbfe709723dbfb593b26b4c	no	2
Warnings:					
Information:					
			Total Files Size (in bytes):	170336	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/240,572	Filing Date 09/22/2011	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT **05/07/2014**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 28	Minus	** 20	= 8	X $40 =	320
Independent (37 CFR 1.16(h))	* 1	Minus	***3	= 0	X $210 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	**320**

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/PEARLIE A. FENNELL/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 05/12/2014

PFENNELL SALE #00000001 Mailroom Dt: 05/07/2014 061050 13240572
01 FC : 2202 320.00 DA

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/240,572	09/22/2011	Stephen Wayne Boyer	38879-0006001	2423

26161 7590 03/27/2014
FISH & RICHARDSON P.C. (BO)
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
KANAAN, SIMON P	
ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
03/27/2014	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATDOCTC@fr.com

Applicant-Initiated Interview Summary	Application No.	Applicant(s)	
	13/240,572	BOYER ET AL.	
	Examiner	Art Unit	
	SIMON KANAAN	2432	

All participants (applicant, applicant's representative, PTO personnel):

(1) *SIMON KANAAN*.

(2) *Gilberto Barron*.

(3) *Joel Couenhoven (Reg. no: 68,848)*.

(4) *Stephen Bpyer*.

Date of Interview: *13 March 2014*.

Type: ☐ Telephonic ☒ Video Conference
☐ Personal [copy given to: ☐ applicant ☐ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☒102 ☐103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1 and 12-25*.

Identification of prior art discussed: *Newton*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Applicant's representative as well as one of the inventors and examiner discussed the proposed claim amendments. No agreement was reached however both parties discussed clarifying organization vs. network to help distinguish application over art of record. Examiner would consider such an amendment when submitted to see whether he agrees whether the network as taught by the reference still reads on the organization as taught by the instant application .

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☒ Attachment

/SIMON KANAAN/ Examiner, Art Unit 2432	/GILBERTO BARRON JR/ Supervisory Patent Examiner, Art Unit 2432

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/240,572	09/22/2011	Stephen Wayne Boyer	38879-0006001

CONFIRMATION NO. 2423

POA ACCEPTANCE LETTER

26161
FISH & RICHARDSON P.C. (BO)
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

OC000000065532254

Date Mailed: 12/17/2013

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 12/11/2013.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/sleutchit/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

PTO/SB/81 (01-09)
Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY OR REVOCATION OF POWER OF ATTORNEY WITH A NEW POWER OF ATTORNEY AND CHANGE OF CORRESPONDENCE ADDRESS

Application Number	13/240,572
Filing Date	September 22, 2011
First Named Inventor	Stephen Boyer
Title	Information Technology Security Assessment System
Art Unit	2432
Examiner Name	Simon P. Kanaan
Attorney Docket Number	38879-0006001

I hereby revoke all previous powers of attorney given in the above-identified application.

☐ A Power of Attorney is submitted herewith.

OR

☒ I hereby appoint Practitioner(s) associated with the following Customer Number as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith: 26161

OR

☐ I hereby appoint Practitioner(s) named below as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith:

Practitioner(s) Name	Registration Number

Please recognize or change the correspondence address for the above-identified application to:

☒ The address associated with the above-mentioned Customer Number.

OR

☐ The address associated with Customer Number: 26161

OR

☐ Firm or Individual Name	Fish & Richardson P.C.				
Address	P.O. Box 1022				
City	Minneapolis	State	MN	Zip	55440-1022
Country	United States				
Telephone	617-542-5070	Email	apsi@fr.com		

I am the:

☐ Applicant/Inventor.

OR

☒ Assignee of record of the entire interest. See 37 CFR 3.71.

Statement under 37 CFR 3.73(b) (Form PTO/SB/96) submitted herewith or filed on _____

SIGNATURE of Applicant or Assignee of Record

Signature	N. V.	Date	12/10/2013
Name	Nagarjuna Venna	Telephone	617-910-0684
Title and Company	COO and Bitsight Technologies, Inc.		

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☒ *Total of 2 forms are submitted.

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

American LegalNet, Inc.
www.FormsWorkflow.com

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: Boyer et al.

Application No./Patent No.: 13/240,572 Filed/Issue Date: 9/22/2011

Entitled: Information Technology Security Assessment System

BitSight Technologies, Inc.
(Name of Assignee)

a corporation
(Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that it is:

1. ☒ the assignee of the entire right, title, and interest; or
2. ☐ an assignee of less than the entire right, title and interest.
   The extent (by, percentage) of its ownership interest is _____%
3. ☐ the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made)

in the patent application/patent identified above by virtue of either:

A. ☒ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 027658, Frame 0906.

OR

B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as shown below:

1. From: _____ To _____
   The document was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.
2. From: _____ To _____
   The document was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.
3. From: _____ To _____
   The document was recorded in the United States Patent and Trademark Office at Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet.

☒ As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.
[NOTE: A separate copy (*i.e.*, a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, if the assignment is to be recorded in the records of the USPTO. See MPEP 302.8]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

Nagarjuna V.
Signature

12/10/2013
Date

Nagarjuna Venna
Printed or Typed Name

617-910-0684
Telephone Number

Founder & COO
Title

Electronic Acknowledgement Receipt

EFS ID:	17630581
Application Number:	13240572
International Application Number:	
Confirmation Number:	2423
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Customer Number:	96039
Filer:	David L Feigenbaum/jennifer franco
Filer Authorized By:	David L Feigenbaum
Attorney Docket Number:	10131-002US1
Receipt Date:	11-DEC-2013
Filing Date:	22-SEP-2011
Time Stamp:	16:03:18
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	POA-statement.pdf	162152 61400c4bbf0d068fa6aa294170e74b23da61fa59	no	2

Warnings:	
Information:	

Total Files Size (in bytes):	162152

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/240,572	09/22/2011	Stephen Wayne Boyer	10131-002US1	2423

96039 7590 11/21/2013

Meunier Carlin & Curfman LLC
817 W. Peachtree Street, Suite 500
Atlanta, GA 30308

EXAMINER	
KANAAN, SIMON P	
ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
11/21/2013	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@mcciplaw.com

Office Action Summary	Application No. 13/240,572	Applicant(s) BOYER ET AL.	
	Examiner SIMON KANAAN	Art Unit 2432	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *7 August 2013*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-20* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-20* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *22 September 2011* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some * c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Interim copies:

a)☐ All b)☐ Some c)☐ None of the: Interim copies of the priority documents have been received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

DETAILED ACTION

1. The present application is being examined under the pre-AIA first to invent provisions.

2. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

3. This office action is in response to applicant's amendment filed on 8/7/2013 for Application No. 13/240572.

4. Claims 1 through 20 are pending in this application.

5. Claims 1, 7-11 and 17 are amended by applicant's amendment filed 8/7/2013.

6. Applicant's arguments/ amendments with respect to the claim objection are persuasive therefor the previously filed claim objection have been withdrawn.

7. Applicant's arguments/ amendments with respect to the 35 U.S.C. 112 rejection are persuasive therefor the previously filed 35 U.S.C. 112 rejection has been withdrawn.

8. Applicant's arguments/ amendments with respect to pending claims 1 through 20 filed 8/7/2013, have been fully considered but are moot in view of new grounds of rejection necessitated by the amendments.

Claim Rejections - 35 USC § 102

9. Claims 1 through 20 are rejected under 35 U.S.C. 102(b) as being anticipated by Chris Newton (US Pre-Grant Publication No: 2004/0250122 A1) hereinafter referred to as Newton.

As per claim 1, Newton discloses a method of evaluating information security of a third party computer system, the method comprising: collecting at a plurality of security characterizations from a plurality of providers independent of the third party computer system, wherein the security characterizations are publicly available and based on externally observable security outcome information.; -Newton, [0012] teaches that every network in the world would have a rating in the database and [0030] teaches establishing a reputation for a network, and [0031] teaches having multiple agents gathering data and [0044]-[0048] teaches different agent types i.e. different network characterization as each agent type gathers different type of data in regards to the security and reputation of network, among these agents include data mining internet which is public information and data mining newsgroups and forums which are also public knowledge and externally observable information.

determining at least two of the security characterizations that are proxies for the vulnerability of the third party system; and –Newton, [0044]-[0048] and [0029], teaches information gathered externally from multiple sources including proxy information.

generating a composite security rating of the third party computer system using the proxy security characterizations; -Newton, [0030] teaches computing the network reputation where a reputation is a score.

As per claim 2, Newton discloses a method of Claim 1, wherein each of the security characterizations is from an associated one of a plurality of independent entities. –Newton, [0030] teaches having multiple agents gathering data and [0044]-

[0048] teaches different agent types i.e. different network characterization as each agent type gathers different type of data in regards to the security and reputation of network, among these agents include data mining internet which is public information and data mining newsgroups and forums which are also public knowledge and externally observable information.

As per claim 3, Newton teaches a method of Claim 2 as noted above, wherein the independent entities include commercial data sources. –Newton, [0044]-[0048] teaches using different search engines such as Google and [0016] teaches hosted services.

As per claim 4, Newton discloses a method of Claim 2, wherein the security characterizations include at least two data types. –Green, [0044]-[0048] teaches different agent types.

As per claim 5, Newton discloses a method of Claim 4, wherein the data types include at least one of breach disclosures, block lists, configuration parameters, malware servers, reputation, suspicious activity, spyware, white lists, compromised hosts, malicious activity, spare activity, vulnerable hosts, phishing, or e-mail viruses. –Newton, [0013]-[0029] teaches security measures etc.

As per claim 6, Newton discloses a method of Claim 1, wherein the security characterizations are derived without permission of the third party computer system. – Newton, [0044]-[0048], teaches using the internet to compute the network reputation i.e. without authorization.

As per claim 7, Newton discloses a method of Claim 1, wherein the security characterizations evidence internal security controls. –Newton, [0013]-[0029] teaches security measures etc.

As per claim 8, Newton discloses a method of Claim 1, wherein the security characterizations are outcomes. –Newton, [0013]-[0029] teaches security measures and [0044]-[0048] teaches checking for information already available to the public about network.

As per claim 9, Newton discloses a method of Claim 1, wherein the security characterizations evidence operational execution of security measures of the third party computer system. –Newton, [0013]-[0029] teaches security measures.

As per claim 10, Newton discloses a method of Claim 1, wherein the security characterizations include serving of malicious code. –Newton, [0013], teaches hostility level.

As per claim 11, Newton discloses a method of Claim 1, wherein the security characterizations include communications with known attacker controlled networks. – Newton, [0013] teaches hostility level.

As per claim 12, Newton discloses a method of Claim 1, wherein collecting the data and generating the ratings are repeated to generate a series of ratings. –Newton, [0042], teaches live remote updates i.e. continually computing rating.

As per claim 13, Newton discloses a method of Claim 11, further comprising determining a trend from the series of ratings. –Newton, [0042], teaches live remote updates i.e. continually computing rating.

As per claim 14, Newton discloses a method of Claim 12, further comprising reporting the ratings. –Newton, [0033], teaches a master database for collecting and storing the network ratings.

As per claim 15, Newton discloses a method of Claim 13, wherein reporting includes reporting a warning based on a change in the ratings. -Newton, [0033], teaches a master database for collecting and storing the network ratings which includes information as listed in [0013]-[0029] which serve as warnings.

As per claim 16, Newton teaches a method of Claim 14, wherein reporting includes posting the ratings and warning to a web portal. -Newton, [0033], teaches a master database for collecting and storing the network ratings which includes information as listed in [0013]-[0029] which serve as warnings.

As per claim 17, Green discloses a method of Claim 1, wherein collecting the security characterizations includes using tools such as WGET, RSYNC or proprietary and manual methods. –Newton, [0022] teaches security measures and firewalls and [0020] teaches peer ISPs.

As per claim 18, Newton discloses a method of Claim 1, further comprising mapping the third party computer system to an IP space and using the IP space for collecting the security characterizations. –Newton, [0020], teaches including peer ISPs.

As per claim 18, Newton discloses a method of Claim 18, wherein mapping includes querying a regional internet registry. –Newton, [0044]-[0048], teaches using the internet to compute the network reputation i.e. without authorization.

As per claim 20, Newton discloses a method of Claim 19, wherein querying includes submitting an entity name. –Newton, [0019] teaches who organization is owned by.

Conclusion

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

11. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Simon Kanaan whose telephone number is (571) 270-3906. The examiner can normally be reached on Monday to Friday 8:30 AM to 5:00 PM.

If attempts to reach the above noted Examiner by telephone are unsuccessful, the Examiner's supervisor, Gilberto Barron, can be reached at the following telephone number: (571) 272-3799.

The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.

/S. K./
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432

Notice of References Cited	Application/Control No. 13/240,572	Applicant(s)/Patent Under Reexamination BOYER ET AL.	
	Examiner SIMON KANAAN	Art Unit 2432	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2004/0250122	12-2004	Newton, Chris	713/201
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	**Art Unit**
	SIMON KANAAN	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/18/2013	11/07/2013							
	1	✓	✓							
	2	✓	✓							
	3	✓	✓							
	4	✓	✓							
	5	✓	✓							
	6	✓	✓							
	7	✓	✓							
	8	✓	✓							
	9	✓	✓							
	10	✓	✓							
	11	✓	✓							
	12	✓	✓							
	13	✓	✓							
	14	✓	✓							
	15	✓	✓							
	16	✓	✓							
	17	✓	✓							
	18	✓	✓							
	19	✓	✓							
	20	✓	✓							

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2013/11/07 23:33
S1	0	"13240572"	US-PGPUB; USPAT	ADJ	ON	2012/11/14 18:15
S2	2	726/25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2012/11/14 18:18
S3	0	apparatus and method for network vulnerability detection and compliance	US-PGPUB; USPAT	ADJ	ON	2012/11/15 11:41
S4	0	network vulnerability detection and compliance assesment	US-PGPUB; USPAT	ADJ	ON	2012/11/15 11:42
S5	0	network vulnerability detection compliance assesment	US-PGPUB; USPAT	ADJ	ON	2012/11/15 11:42
S6	0	network with vulnerability with detection with compliance with assesment	US-PGPUB; USPAT	ADJ	ON	2012/11/15 11:42
S7	7	network with vulnerability with detection with compliance with assessment	US-PGPUB; USPAT	ADJ	ON	2012/11/15 11:42
S8	19	726/2,22,25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2012/11/15 13:03
S9	24	726/2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:22
S10	30	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:23
S11	2	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:23
S12	95	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:25
S13	0	(external$5 or third party) with (security) with (commercial near data) with reputation	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:25
S14	0	(external$5 or third party) with (commercial near data) with reputation	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:25
S15	20	internet monitoring with report	US-PGPUB;	ADJ	ON	2012/11/15 18:27

			USPAT			
S16	9	internet monitoring with report and public	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:27
S17	0	malwareurl	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:28
S18	0	malwareurl$5	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:28
S19	0	www$malwareurl$5	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:28
S20	0	www$malwareurl$com	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:28
S21	69	arbor networks	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:46
S22	1	arbor networks and renesys	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:46
S23	3268	reputation and domain	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:48
S24	32	reputation and domain and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:49
S25	49	reputation and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:56
S26	17	S25 not S24	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:56
S27	20	US-7194769-$.DID. OR US-7290275-$.DID. OR US-7971252-$.DID. OR US-20040010709-$.DID. OR US-20050138413-$.DID. OR US-20080047018-$.DID. OR US-20080209565-$.DID. OR US-20090265787-$.DID. OR US-20090293128-$.DID. OR US-2007304-$.DID. OR US-5200596-$.DID. OR US-2009104-$.DID. OR US-422009D-$.DID. OR US-1331018-$.DID.	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2012/11/15 18:59
S28	0	S25 and S27	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:02
S29	0	(insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and S27	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:02
S30	0	(industry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and S27	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:02

S31	0	(industry reports or internet monitoring or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and S27	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:03
S32	0	S27 and user behavior	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:03
S33	0	S27 and behavior	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:03
S34	0	S27 and reputation	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:03
S35	0	S27 and public with features	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2012/11/15 19:06
S36	0	S27 and externally	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2012/11/15 19:06
S37	7	S27 and external	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2012/11/15 19:06
S38	19	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:10
S39	1	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:11
S40	13	((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:16
S41	132	((external$5 or third party) with audit$4)and reputation and security	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:21
S42	237	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:21
S43	230	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:21
S44	164	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:22
S45	0	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial data sources	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:22
S46	3	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial data	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:22

S47	3	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rating and commercial data	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:22
S48	3	security and renesys	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:24
S49	1	abor networks	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:27
S51	27	(network near3 vulnerability) with public	US-PGPUB; USPAT	ADJ	ON	2013/11/06 19:02
S52	17	(network near3 assessment) with public	US-PGPUB; USPAT	ADJ	ON	2013/11/06 20:17
S53	29	(network near3 assessment) with external$3	US-PGPUB; USPAT	ADJ	ON	2013/11/06 20:18
S54	1167	site secure	US-PGPUB; USPAT	ADJ	ON	2013/11/06 21:02
S55	438	S54 and third party	US-PGPUB; USPAT	ADJ	ON	2013/11/06 21:02
S56	166	S55 and assess$3	US-PGPUB; USPAT	ADJ	ON	2013/11/06 21:02
S57	146	network reputation	US-PGPUB; USPAT	ADJ	ON	2013/11/07 09:56
S58	138	network reputation and (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2013/11/07 09:56
S59	12	network reputation with (rat$3 or assess$4)	US-PGPUB; USPAT	ADJ	ON	2013/11/07 09:57
S61	8	network reputation with (rat$3 or assess$4) and public	US-PGPUB; USPAT	ADJ	ON	2013/11/07 14:21
S62	2	network reputation with public	US-PGPUB; USPAT	ADJ	ON	2013/11/07 14:25
S63	365	network (reputation or assess$4 or rat$3) with public	US-PGPUB; USPAT	ADJ	ON	2013/11/07 14:28
S64	176	network (reputation or assess$4 or rat$3) with public and security	US-PGPUB; USPAT	ADJ	ON	2013/11/07 14:30
S65	9	network (reputation or assess$4 or rat$3) with public with security	US-PGPUB; USPAT	ADJ	ON	2013/11/07 14:31
S66	14	network (reputation or assess$4 or rat$3) with public with secur$5	US-PGPUB; USPAT	ADJ	ON	2013/11/07 14:37
S67	5	S66 not S65	US-PGPUB; USPAT	ADJ	ON	2013/11/07 14:38

S68	2	"20040250122"	US-PGPUB; USPAT	ADJ	ON	2013/11/07 15:10

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S50	0	"13240572"	US-PGPUB; USPAT; UPAD	ADJ	ON	2013/04/18 09:53

11/7/2013 11:34:44 PM
C:\Users\skanaan\Documents\EAST\Workspaces\13240572.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	Art Unit
	SIMON KANAAN	2432

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor and Assignee Search (PALM)	4/18/2013	SK
class/subclass search + text (EAST: 726/1,2,22,25+text)	11/7/2013	SK

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/SIMON KANAAN/ Examiner.Art Unit 2432	

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Boyer, *et al.*	Art Unit	: 2876
Serial No.	: 13/240,572	Examiner	: Kanaan, Simon
Filed	: September 22, 2011	Conf. No.	: 2423
Title	: INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM		

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT AND RESPONSE TO OFFICE ACTION

In response to the Office Action mailed on May 7, 2013, please amend the application as indicated on the following pages. Amendments to the claims begin on page 2, and remarks begin on page 4.

Amendments to the Claims:

Applicant requests cancellation of Claims 21-120. This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) A method of evaluating information security of a third party computer system, the method comprising:

collecting ~~at least two~~a plurality of security characterizations from a plurality of providers independent of the third party computer system, wherein the security characterizations are publicly available and based on externally observable security outcome information;

determining at least two of the security characterizations that are proxies for the vulnerability of the third party system; and

generating a composite security rating of the third party computer system using the ~~at least two~~ proxy security characterizations~~;~~

~~wherein the two security characterizations are derived from externally observable characteristics of the third party computer system~~.

2. (Currently Amended) A method of Claim 1, wherein each of the security characterizations is from an associated one of ~~a~~ the plurality of independent entities.

3. (Original) A method of Claim 2, wherein the independent entities include commercial data sources.

4. (Original) A method of Claim 2, wherein the security characterizations include at least two data types.

5. (Original) A method of Claim 4, wherein the data types include at least one of breach disclosures, block lists, configuration parameters, malware servers, reputation, suspicious activity, spyware, white lists, compromised hosts, malicious activity, spam activity, vulnerable hosts, phishing, or e-mail viruses.

6. (Original) A method of Claim 1, wherein the security characterizations are derived without permission of the third party computer system.

7. (Currently Amended) A method of Claim 1, wherein the ~~externally observable characteristics~~security characterizations evidence internal security controls.

8. (Currently Amended) A method of Claim 1, wherein the security characterizations ~~externally observable characteristics~~ are outcomes.

9. (Currently Amended) A method of Claim 1, wherein the security characterizations ~~externally observable characteristics~~ evidence operational execution of security measures of the third party computer system.

10. (Currently Amended) A method of Claim 1, wherein the security characterizations ~~externally observable characteristics~~ include serving of malicious code.

11. (Currently Amended) A method of Claim 1, wherein the security characterizations ~~externally observable characteristics~~ include communications with known attacker controlled networks.

12. (Original) A method of Claim 1, wherein collecting the data and generating the ratings~~s~~ are repeated to generate a series of ratings.

13. (Original) A method of Claim 11, further comprising determining a trend from the series of ratings.

14. (Original) A method of Claim 12, further comprising reporting the ratings.

15. (Original) A method of Claim 13, wherein reporting includes reporting a warning based on a change in the ratings.

16. (Original) A method of Claim 14, wherein reporting includes posting the ratings and warning to a web portal.

17. (Currently Amended) A method of Claim 1, wherein collecting the security characterizations includes using tools ~~such as~~including at least one of WGET, RSYNC ~~or~~, proprietary ~~and~~ or manual methods.~~.~~

18. (Original) A method of Claim 1, further comprising mapping the third party computer system to an IP space and using the IP space for collecting the security characterizations.

19. (Original) A method of Claim 18, wherein mapping includes querying a regional internet registry.

20. (Original) A method of Claim 19, wherein querying includes submitting an entity name.

21.-120. (Cancelled)

REMARKS

The amendments above and the remarks below are in response to an Office Action mailed on May 7th, 2013. Claims 1-20 are currently pending. In the Office Action, claim 17 was rejected under 35 U.S.C. 112 and objected to. Claims 1-2, 4-15 and 17-20 were rejected under 35 U.S.C. 102(b) over U.S. Pat. App. Pub. No. 2004/0193918 to Green et al. ("Green"). Claims 3 and 16 were rejected under 35 U.S.C. 103(a) over Green in combination with U.S. Pat. App. Pub. No. 2005/0108415 to Turk et al. ("Turk").

Claim 17 has been amended to remove the additional period and the "such as" language. Applicant has therefore overcome the rejection under 35 U.S.C. 112 and the objection.

Applicant thanks Examiner Kanaan for the interview on March 26, 2013. During the interview the attendees discussed the difference between Turk, Green and the presently claimed invention.

Turk and Green are concerned with direct evaluation of the security of a computer system.

Green for example, queries the third party system directly, as described in paragraph [0011].

> One way that data may be input into a network assessor may be through the use of a customized questionnaire. Such a questionnaire may be provided on a traditional paper medium, or may be provided in an electronic format, for example, through an HTML interface. Once the data has been gathered, or even simultaneously as the data is gathered, the data input into the network assessor may be provided to a network scanner module. The network scanner module may accomplish a variety of tasks. For example, the network scanner module may first attempt to resolve any IP addresses if, for example, the user inputs a domain name as opposed to an IP address. The network scanner module may subsequently begin a number of other enumerative tasks which may include attempting to determine missing information, such as the identities of related systems, such as mail servers and domain name servers.

The questionnaire requires the involvement and permission of the third party computer system.

Turk discloses the redirection of malicious, unrouted electronic traffic to be trapped by a "honey pot" while routing appropriate traffic to a subscriber. See paragraphs [0006] and [0012]

of Turk. Turk is merely a network router for the subscriber that redirects malicious traffic to the honey pot and then reports the activity to a subscriber.

The method recited in claim 1, on the other hand, obtains security characterizations from a plurality of providers. The security characterizations are publicly available and based on externally observable security outcome information. (Publicly available means, for example, the security characterizations may be purchased or otherwise obtained from the providers without the permission – or "independent" – of the third party computer system.)

The presently claimed method also determines at least two of the security characterizations that are proxies for the vulnerability of the third party system. The presently claimed method further generates a composite security rating using the proxy security characterizations.

During the interview, the inventors likened Green to a service that directly tests the locks on a home (i.e., using the questionnaire) to determine if it is secure. Meanwhile, the claimed invention looks for publicly available information on thefts (e.g., such as police reports of stolen items) and finds the stolen items that belonged to the home. This information is then used, as a proxy, to determine the security of the home.

Neither Green, nor Green, therefore, alone or in combination, teaches or suggests the claimed invention. The rejections under 35 U.S.C. 102 and 103 have therefore been overcome. The present application is in a condition for allowance.

The required fees are being paid concurrently herewith on the Electronic Filing System (EFS) by way of Electronic Funds Transfer; however, please apply any other charges or credits to deposit account 50-5226.

Respectfully submitted,

Date: August 7, 2013

/Gregory J. Carlin/
Gregory J. Carlin
Reg. No. 45,607

Customer Number 96039
Telephone: (404) 645-7700
Facsimile: (404) 645-7707

Electronic Acknowledgement Receipt

EFS ID:	16520803
Application Number:	13240572
International Application Number:	
Confirmation Number:	2423
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Customer Number:	96039
Filer:	Gregory J. Carlin/Christina Hankins
Filer Authorized By:	Gregory J. Carlin
Attorney Docket Number:	10131-002US1
Receipt Date:	07-AUG-2013
Filing Date:	22-SEP-2011
Time Stamp:	13:19:27
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	10131_002US1_OA_Response.pdf	80412 f0dac2f8c3c4cb2db4b901c6aca453f7f990cff5	no	5

Warnings:	
Information:	

Total Files Size (in bytes):	80412

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (09-11)
Approved for use through 1/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/240,572	Filing Date 09/22/2011	☐ To be Mailed

ENTITY: ☐ LARGE ☒ SMALL ☐ MICRO

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT **08/07/2013**

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 20	Minus	** 20	= 0	X $40 =	0
Independent (37 CFR 1.16(h))	* 1	Minus	***3	= 0	X $210 =	0
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	0

AMENDMENT

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))						
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))						
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
/Theresa Dawkins/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Office Action Summary	Application No. 13/240,572	Applicant(s) BOYER ET AL.	
	Examiner SIMON KANAAN	Art Unit 2432	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 September 2011*.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-20* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-20* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *22 September 2011* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some * c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Interim copies:

a)☐ All b)☐ Some c)☐ None of the: Interim copies of the priority documents have been received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.

3) ☒ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

4) ☐ Other: _____.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/240,572	09/22/2011	Stephen Wayne Boyer	10131-002US1	2423

96039 7590 05/07/2013

Meunier Carlin & Curfman LLC
817 W. Peachtree Street, Suite 500
Atlanta, GA 30308

EXAMINER	
KANAAN, SIMON P	
ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
05/07/2013	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Applicant-Initiated Interview Summary	Application No.	Applicant(s)	
	13/240,572	BOYER ET AL.	
	Examiner	Art Unit	
	SIMON KANAAN	2432	

All participants (applicant, applicant's representative, PTO personnel):

(1) *SIMON KANAAN*.

(2) *Gilberto Barron*.

(3) *Stephen Boyer & Nagarjuna Venna*.

(4) *Gregory Carlin Reg. No. 45607*.

Date of Interview: *26 March 2013*.

Type: ☐ Telephonic ☐ Video Conference
☒ Personal [copy given to: ☒ applicant ☒ applicant's representative]

Exhibit shown or demonstration conducted: ☐ Yes ☒ No.
If Yes, brief description: _____.

Issues Discussed ☐101 ☐112 ☒102 ☒103 ☐Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: *1*.

Identification of prior art discussed: *Green and Turk*.

Substance of Interview
(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Applicant and examiner discussed the references, the invention and the proposed amendment. No agreement was reached and the proposed amendment would not be entered. A formal FIRST ACTION office action will be sent out to the applicant's representative. A response to the first office action with clarification on what is externally observable was discussed as a way to move forward with prosecution.

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

☐ Attachment

/SIMON KANAAN/ Examiner, Art Unit 2432	/Gilberto Barron Jr./ Supervisory Patent Examiner, Art Unit 2432

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

DETAILED ACTION

Claim Objections

1. Claim 17 is objected to because it ends with two periods.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 17 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claim 17, the phrase "such as" renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-2, 4-15 and 17-20 are rejected under 35 U.S.C. 102(b) as being anticipated by Green et al. (US Pre-Grant Publication No: 2004/0193918 A1) hereinafter referred to as Green.

As per claim 1, Green discloses a method of evaluating information security of a third party computer system, the method comprising: collecting at least two security characterizations of the third party computer system; -Green, [0013] and [0034], teaches having multiple security tools to check vulnerability, also see [0048] and [0055] teaches connecting to a system externally through internet.

generating a composite security rating using the at least two security characterizations; -Green, [0040], teaches sending the results from one entity to another the entities include multiple tools [0038], and [0065] teaches 3rd party known tools such as Dig and nslookup.

wherein the two security characterizations are derived from externally observable characteristics of the third party computer system. –Green, [0065] teaches 3rd party known tools such as Dig and nslookup.

As per claim 2, Green discloses a method of Claim 1, wherein each of the security characterizations is from an associated one of a plurality of independent entities. –Green, [0065] teaches 3rd party known tools such as Dig and nslookup.

As per claim 4, Green discloses a method of Claim 2, wherein the security characterizations include at least two data types. –Green, [0065] teaches 3rd party known tools such as Dig and nslookup which are two data types.

As per claim 5, Green discloses a method of Claim 4, wherein the data types include at least one of breach disclosures, block lists, configuration parameters, malware servers, reputation, suspicious activity, spyware, white lists, compromised hosts, malicious activity, spare activity, vulnerable hosts, phishing, or e-mail viruses. –Green, [0044] teaches vulnerability scans.

As per claim 6, Green discloses a method of Claim 1, wherein the security characterizations are derived without permission of the third party computer system. –Green, [0065] teaches 3rd party known tools such as Dig and nslookup which are externally observant.

As per claim 7, Green discloses a method of Claim 1, wherein the externally observable characteristics evidence internal security controls. –Green, [0065] teaches 3rd party known tools such as Dig and nslookup which are externally observant and retrieve information about the internal security of system.

As per claim 8, Green discloses a method of Claim 1, wherein the externally observable characteristics are outcomes. –Green, [0065] teaches 3rd

party known tools such as Dig and nslookup which are externally observant which obtain outcomes of system.

As per claim 9, Green discloses a method of Claim 1, wherein the externally observable characteristics evidence operational execution of security measures of the third party computer system. –Green, [0065] and [0077] teaches 3rd party known tools such as Dig and nslookup which are externally observant which obtain outcomes of system which would include determining if firewall and other security characterizations are available which include third party security.

As per claim 10, Green discloses a method of Claim 1, wherein the externally observable characteristics include serving of malicious code. –Green, [0066], determines if there is malicious code.

As per claim 11, Green discloses a method of Claim 1, wherein the externally observable characteristics include communications with known attacker controlled networks. –Green, [0077] teaches exposed services and other tools used to discover associations of client system.

As per claim 12, Green discloses a method of Claim 1, wherein collecting the data and generating the ratings are repeated to generate a series of ratings. - Green, [0040], teaches having multiple modules sending characterizations to a single module to obtain a security characterization of system.

As per claim 13, Green discloses a method of Claim 11, further comprising determining a trend from the series of ratings. -Green, [0040], teaches having multiple modules sending characterizations to a single module to obtain a security characterization of system.

As per claim 14, Green discloses a method of Claim 12, further comprising reporting the ratings. -Green, [0040], teaches having multiple modules sending characterizations to a single module to obtain a security characterization of system.

As per claim 15, Green discloses a method of Claim 13, wherein reporting includes reporting a warning based on a change in the ratings. -Green, [0017], teaches creating a warning.

As per claim 17, Green discloses a method of Claim 1, wherein collecting the security characterizations includes using tools such as WGET, RSYNC or proprietary and manual methods. –Green, [0090], teaches tools such as WGET.

As per claim 18, Green discloses a method of Claim 1, further comprising mapping the third party computer system to an IP space and using the IP space for collecting the security characterizations. –Green, [0014], teaches IP network characterization.

As per claim 18, Green discloses a method of Claim 18, wherein mapping includes querying a regional internet registry. –Green, [0060], teaches using different registry including DNS WhoIs etc. which would include regional characterizations and [0076] teaches clientinfo and associations such as MAC address and domain names.

As per claim 20, Green discloses a method of Claim 19, wherein querying includes submitting an entity name. –Green, [0060], teaches using different registry including DNS WhoIs etc. which would include lookup by name.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 3 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Green in view of Turk et al. (US Pre-Grant Publication No: 2005/0108415 A1) hereinafter referred to as Turk.

Green teaches a method of Claim 2 as noted above, but does not teach wherein the independent entities include commercial data sources.

However, Turk teaches wherein the independent entities include commercial data sources. - Turk figure 2 and [0006] and [0007], teaches Arbor Networks used to identify policy violations, network attacks.... and reporting results.

It would have been obvious at the time of the invention for one of the ordinary skill in the art to modify the security assessment method of Green which uses multiple sources to determine a security rating with including the security rating of Turk because it Turks method identify and remove worms, DES attacks, unauthorized network routing etc. -See Turk Abstract.

As per claim 16, Green teaches a method of Claim 14,

But does not teach wherein reporting includes posting the ratings and warning to a web portal.

However, Turk teaches wherein reporting includes posting the ratings and warning to a web portal. - Turk figure 2 and [0006] and [0007], teaches Arbor Networks used to identify policy violations, network attacks.... and reporting results.

It would have been obvious at the time of the invention for one of the ordinary skill in the art to modify the security assessment method of Green which uses multiple sources to determine a security rating with including the security rating of Turk because it Turks method identify and remove worms, DES attacks, unauthorized network routing etc. -See Turk Abstract.

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Simon Kanaan whose telephone number is (571) 270-3906. The examiner can normally be reached on Monday to Friday 8:30 AM to 5:00 PM.

If attempts to reach the above noted Examiner by telephone are unsuccessful, the Examiner's supervisor, Gilberto Barron, can be reached at the following telephone number: (571) 272-3799.

The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/S. K./
Examiner, Art Unit 2432

/Gilberto Barron Jr./
Supervisory Patent Examiner, Art Unit 2432

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	0	"13240572"	US-PGPUB; USPAT	ADJ	ON	2012/11/14 18:15
S2	2	726/25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2012/11/14 18:18
S3	0	apparatus and method for network vulnerability detection and compliance	US-PGPUB; USPAT	ADJ	ON	2012/11/15 11:41
S4	0	network vulnerability detection and compliance assesment	US-PGPUB; USPAT	ADJ	ON	2012/11/15 11:42
S5	0	network vulnerability detection compliance assesment	US-PGPUB; USPAT	ADJ	ON	2012/11/15 11:42
S6	0	network with vulnerability with detection with compliance with assesment	US-PGPUB; USPAT	ADJ	ON	2012/11/15 11:42
S7	7	network with vulnerability with detection with compliance with assessment	US-PGPUB; USPAT	ADJ	ON	2012/11/15 11:42
S8	19	726/2,22,25.ccls. and (external$5 or third party) and (security) and (WGET or RSYNC or CURL)	US-PGPUB; USPAT	ADJ	ON	2012/11/15 13:03
S9	24	726/2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:22
S10	30	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data)	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:23
S11	2	726/1,2,22,25.ccls. and (external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:23
S12	95	(external$5 or third party) and (security) and (commercial near data) and reputation	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:25
S13	0	(external$5 or third party) with (security) with (commercial near data) with reputation	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:25
S14	0	(external$5 or third party) with (commercial near data) with reputation	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:25
S15	20	internet monitoring with report	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:27
S16	9	internet monitoring with report and public	US-PGPUB;	ADJ	ON	2012/11/15 18:27

			USPAT			
S17	0	malwareurl	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:28
S18	0	malwareurl$5	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:28
S19	0	www$malwareurl$5	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:28
S20	0	www$malwareurl$com	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:28
S21	69	arbor networks	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:46
S22	1	arbor networks and renesys	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:46
S23	3268	reputation and domain	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:48
S24	32	reputation and domain and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:49
S25	49	reputation and (insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior)	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:56
S26	17	S25 not S24	US-PGPUB; USPAT	ADJ	ON	2012/11/15 18:56
S27	20	US-7194769-$.DID. OR US-7290275-$.DID. OR US-7971252-$.DID. OR US-20040010709-$.DID. OR US-20050138413-$.DID. OR US-20080047018-$.DID. OR US-20080209565-$.DID. OR US-20090265787-$.DID. OR US-20090293128-$.DID. OR US-2007304-$.DID. OR US-5200596-$.DID. OR US-2009104-$.DID. OR US-422009D-$.DID. OR US-1331018-$.DID.	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2012/11/15 18:59
S28	0	S25 and S27	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:02
S29	0	(insustry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and S27	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:02
S30	0	(industry reports or internet monitoring web site or news article or court record) and (renesys or propriety data or arbor networks or user behavior) and S27	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:02
S31	0	(industry reports or internet monitoring or news article or court record) and (renesys or propriety data or arbor networks or user	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:03

		behavior) and S27				
S32	0	S27 and user behavior	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:03
S33	0	S27 and behavior	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:03
S34	0	S27 and reputation	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:03
S35	0	S27 and public with features	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2012/11/15 19:06
S36	0	S27 and externally	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2012/11/15 19:06
S37	7	S27 and external	US-PGPUB; USPAT; USOCR; EPO; DERWENT	ADJ	ON	2012/11/15 19:06
S38	19	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:10
S39	1	726/1,2,22,25.ccls. and ((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:11
S40	13	((external$5 or third party) with audit$4)and reputation and (proprietary information)	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:16
S41	132	((external$5 or third party) with audit$4)and reputation and security	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:21
S42	237	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:21
S43	230	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:21
S44	164	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:22
S45	0	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial data sources	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:22
S46	3	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rat$3 and commercial data	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:22
S47	3	((external$5 or third party) with (audit$4 or observ$5)) and reputation and security and rating and commercial data	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:22

S48	3	security and renesys	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:24
S49	1	abor networks	US-PGPUB; USPAT	ADJ	ON	2012/11/15 19:27

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S50	0	"13240572"	US-PGPUB; USPAT; UPAD	ADJ	ON	2013/04/18 09:53

4/ 18/ 2013 10:56:57 AM
C:\ Users\ skanaan\ Documents\ EAST\ Workspaces\ 13240572.wsp

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	**Art Unit**
	SIMON KANAAN	2432

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	04/18/2013								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								
	11	✓								
	12	✓								
	13	✓								
	14	✓								
	15	✓								
	16	✓								
	17	✓								
	18	✓								
	19	✓								
	20	✓								

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 2423

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/240,572	09/22/2011	726	2432	10131-002US1

APPLICANTS

Stephen Wayne Boyer, Waltham, MA;
Nagarjuna Venna, Waltham, MA;
Megumi Ando, Cambridge, MA;

**** CONTINUING DATA ***************************

This appln claims benefit of 61/492,287 06/01/2011
and claims benefit of 61/386,156 09/24/2010

**** FOREIGN APPLICATIONS ***************************

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED **** ** SMALL ENTITY **
10/03/2011

Foreign Priority claimed ☐ Yes ☑ No 35 USC 119(a-d) conditions met ☐ Yes ☑ No Verified and Acknowledged /SIMON P KANAAN/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		MA	4	20	1

ADDRESS

Meunier Carlin & Curfman LLC
817 W. Peachtree Street, Suite 500
Atlanta, GA 30308
UNITED STATES

TITLE

INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM

FILING FEE RECEIVED		
527	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13240572	BOYER ET AL.
	Examiner	Art Unit
	SIMON KANAAN	2432

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES		
Search Notes	Date	Examiner
Inventor and Assignee Search (PALM)	4/18/2013	SK
class/subclass search + text (EAST: 726/1,2,22,25+text)	4/18/2013	SK

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

/SIMON KANAAN/ Examiner.Art Unit 2432	

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	:	Boyer et al.	Art Unit	:	2876
Serial No.	:	13/240,572	Examiner	:	Simon Kanaan
Filed	:	September 22, 2011	Conf. No.	:	2423
Title	:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM			

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PROPOSED AMENDMENT

1. (Amended) A method of evaluating information security of a third party computer system using a rating organization system, the method comprising:

collecting, with the rating organization system, at least two security characterizations of the third party computer system;

generating, with the rating organization system, a composite security rating using the at least two security characterizations;

wherein the two security characterizations are derived from externally observable characteristics of the third party computer system; and

wherein the security characterizations are obtained from a sensor system separate from, and intervening between, the rating organization system and the third party computer system.

REMARKS

The above proposed amendments to claim 1 are for discussion during the interview requested in the accompanying Applicant Initiated Interview Request Form. These filings are in response to the First Action Interview Pilot Program Pre-Interview Communication mailed on November 26, 2012 in the above-listed patent application.

No additional fees are believed to be due; however, the Commissioner is hereby authorized to charge any additional fees that may be required, or credit any overpayment, to Deposit Account No. 50-5226.

Respectfully submitted

MEUNIER CARLIN & CURFMAN, LLC

Date: December 26, 2012

/Gregory J. Carlin/
Gregory J. Carlin
Reg. No. 45,607

Customer No. 96039
docketing@mcciplaw.com
404.645.7700 Phone
404.645.7707 Fax

Doc Code: M865 or FAI.REQ.INTV

PTOL-413A (10-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Applicant Initiated Interview Request Form

Application No.: 13/240,572 First Named Applicant: Stephen Boyer
Examiner: Simon Kanaan Art Unit: 2432 Status of Application: Pending

Tentative Participants:
(1) Gregory Carlin (2) Stephen Boyer
(3) Nagarjuna Venna (4) _____

Proposed Date of Interview: After January 24, 2013 **Proposed Time:** Afternoon **(AM/PM)**

Type of Interview Requested:
(1) [ ] Telephonic (2) [X] Personal (3) [ ] Video Conference

Exhibit To Be Shown or Demonstrated: [ ] YES [X] NO
If yes, provide brief description: _____

Issues To Be Discussed

Issues (Rej., Obj., etc)	Claims/ Fig. #s	Prior Art	Discussed	Agreed	Not Agreed
(1) Rej.	1-20	US2004/0193918	[ ]	[ ]	[ ]
(2) Rej.	1-20	US2005/0108415	[ ]	[ ]	[ ]
(3)			[ ]	[ ]	[ ]
(4)			[ ]	[ ]	[ ]

[ ] Continuation Sheet Attached
[X] Proposed Amendment or Arguments Attached
Brief Description of Arguments to be Presented:
The prior art does not teach or suggest generating a composite security score using at least two security characterizations obtained from an intervening sensor system.

An interview was conducted on the above-identified application on _____.
NOTE: This form should be completed by applicant and submitted to the examiner in advance of the interview (see MPEP § 713.01).
This application will not be delayed from issue because of applicant's failure to submit a written record of this interview. Therefore, applicant is advised to file a statement of the substance of this interview (37 CFR 1.133(b)) as soon as possible.

/Gregory J. Carlin/
Applicant/Applicant's Representative Signature

Examiner/SPE Signature

Gregory J. Carlin
Typed/Printed Name of Applicant or Representative

45,607
Registration Number, if applicable

This collection of information is required by 37 CFR 1.133. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 21 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	14558300
Application Number:	13240572
International Application Number:	
Confirmation Number:	2423
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Customer Number:	96039
Filer:	Gregory J. Carlin/Cheryl McKinzie
Filer Authorized By:	Gregory J. Carlin
Attorney Docket Number:	10131-002US1
Receipt Date:	26-DEC-2012
Filing Date:	22-SEP-2011
Time Stamp:	14:55:50
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Reply under 1.111 to Pre-Interview Communication	10131_002US1_Amendment.pdf	80273 14e7b727b46ac4974026804c00ba933a9e7760b8	no	2

Warnings:	
Information:	

2	First Action Interview - Schedule Interview request	10131_002US1_First_Action_413A.pdf	130324 19db1d037c6f8bee25ad88f09200bc17c6a68770	no	2

Warnings:	
Information:	
Total Files Size (in bytes):	210597

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

First Action Interview Pilot Program Pre-Interview Communication	Application No. 13/240,572	Applicant(s) BOYER ET AL.	
	Examiner SIMON KANAAN	Art Unit 2432	Page 1 of 2

-The MAILING OR NOTIFICATION DATE of this communication appears on the cover sheet with the correspondence address -

THE SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE **ONE MONTH OR THIRTY (30) DAYS,** WHICHEVER IS LONGER, FROM THE MAILING OR NOTIFICATION DATE OF THIS COMMUNICATION.

This time period for reply is extendable under 37 CFR 1.136(a) for only ONE additional MONTH.
This communication constitutes notice under 37 CFR 1.136(a)(1)(i).

Applicant must, within the time period for reply, file: (1) A letter requesting not to have a first action interview; (2) A reply under 37 CFR 1.111 waiving the first action interview and First Action Interview Office Action; or (3) An Applicant Initiated Interview Request Form (PTOL-413A) electronically via EFS-Web, accompanied by a proposed amendment or arguments, and schedule the interview within 2 months from the filing of the request. A failure to respond to this communication will be treated as a request not to have an interview. If applicant waives the First Action Interview Office Action, the instant Pre-Interview Communication is deemed the first Office Action on the Merits. The next subsequent Office action may be made final if appropriate. See MPEP 706.07(a).

Disposition of Claims

3)☒ Claim(s) *1-20* is/are pending in the application.
3a) Of the above claim(s) _____ is/are withdrawn from consideration.
4)☐ Claim(s) _____ is/are allowed.
5)☒ Claim(s) *1-20* is/are rejected.
6)☐ Claim(s) _____ is/are objected to.
7)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

8)☐ The specification is objected to by the Examiner.
9)☒ The drawing(s) filed on *15 December, 2011* is/are: a)☒ accepted or b)☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

10)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a)☐ All b)☐ Some * c)☐ None of:
1.☐ Certified copies of the priority documents have been received.
2.☐ Certified copies of the priority documents have been received in Application No. _____.
3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

*See the attached detailed Office action for a list of the certified copies not received.

Contact Information

Examiner's Telephone Number: (571) 270-3906
Examiner's Typical Work Schedule: Mon-Thurs 7:30-5:00 EST
Supervisor's Name: Gilberto Barron
Supervisor's Telephone Number: (571) 272-3799

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
4) ☐ Other: _____.

First Action Interview Pilot Program Pre-Interview Communication	Application No. 13240572	Applicant(s) BOYER ET AL.	
	Examiner SIMON KANAAN	Art Unit 2432	Page 2 of 2

Notification of Rejection(s) and/or Objection(s)

#	Claim(s)	Reference(s) (if applicable)	Rejection Statutory Basis	Brief Explanation of Rejection
1	17		112 2nd	"such as" renders the claim vague
2	17		Objection	claim ends with two periods, i.e. typo.
3	1-2, 4-15, and 17-20	A	102(b)	Green [0086]-[0090] and [0098], teaches using multiple external sources to check security characteristic of third party system.
4	3, 16	A,B	103(a)	Turk figure 2 and [0006] and [0007], teaches Arbor Networks used to identidy policy violations, network attacks.... and reporting results.

Expanded Discussion/Commentary		
1		it would have been obvious at the time of the invention for one of the ordinary skill in the art to modify the security assesment method of Green which uses multiple sources to determine a security rating with including the security rating of Turk because it Turks method identify and remove worms, DES attacks, usauthorized netowrk routing etc. -See Turk Abstract.

DATE: 19 November, 2012	/SIMON KANAAN/ Examiner, Art Unit 2432	/Gilberto Barron Jr./ Supervisory Patent Examiner, Art Unit 2432

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/240,572	09/22/2011	Stephen Wayne Boyer	10131-002US1	2423

96039 7590 11/26/2012

Meunier Carlin & Curfman LLC
817 W. Peachtree Street, Suite 500
Atlanta, GA 30308

EXAMINER	
KANAAN, SIMON P	
ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
11/26/2012	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@mcciplaw.com

Notice of References Cited	Application/Control No. 13/240,572	Applicant(s)/Patent Under Reexamination BOYER ET AL.	
	Examiner SIMON KANAAN	Art Unit 2432	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2004/0193918	09-2004	Green et al.	713/201
*	B	US-2005/0108415	05-2005	Turk et al.	709/232
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Doc code: IDS
Doc description: Information Disclosure Statement (IDS) Filed
PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13240572
Filing Date	2011-09-22
First Named Inventor	Boyer et al.
Art Unit	2876
Examiner Name	Not Yet Assigned
Attorney Docket Number	10131-002US1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7194769	B2	2007-03-20	Lippmann et al.	
	2	7290275	B2	2007-10-30	Baudoin et al.	
	3	7971252	B2	2011-06-28	Lippmann et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20040010709	A1	2004-01-15	Baudoin et al.	
	2	20050138413	A1	2005-06-23	Lippmann et al.	
	3	20080047018	A1	2008-02-21	Baudoin et al.	

ALL REFERENCES CONSIDERED EXCEPT WHERE INDICATED OTHERWISE. /S.K./

Receipt date: 01/24/2012	Application Number	13240572	13240572 - GAU: 2432
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99**)	Filing Date	2011-09-22	
	First Named Inventor	Boyer et al.	
	Art Unit	2876	
	Examiner Name	Not Yet Assigned	
	Attorney Docket Number	10131-002US1	

	4	20080209565	A2	2008-08-28	Baudoin et al.	
	5	20090265787	A9	2009-10-22	Baudoin et al.	
	6	20090293128	A1	2009-11-26	Lippmann et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	SBIR Phase I: Enterprise Cyber Security Scoring, CyberAnalytix, LLC, http://www.nsf.gov/awardsearch/showAward.do?AwardNumber=1013603, April 28, 2010.	☐
	2	"Twenty Critical Controls for Effective Cyber Defense: Consensus Audit," Version 2.3, November 13, 2009, retrieved on April 9, 2010 from http://www.sans.org/critical-security-controls/print.php.	☐
	3	"An Executive View of IT Governance," IT Governance Institute, 2009, 32 pages.	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE INDICATED OTHERWISE BY APPLICANT. /S.K./

Receipt date: 01/24/2012	Application Number	13240572	13240572 - GAU: 2432
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2011-09-22	
	First Named Inventor	Boyer et al.	
	Art Unit	2876	
	Examiner Name	Not Yet Assigned	
	Attorney Docket Number	10131-002US1	

	4	Lippmann, R.P., et al., "An Annotated Review of Papers on Attack Graphs," Project Report IA-1, Lincoln Laboratory, Massachusetts Institute of Technology, March 31, 2005, 39 pages.	☐
	5	Artz, Michael Lyle, "NetSPA: A Network Security Planning Architecture," Massachusetts Institute of Technology, May 24, 2002, 97 pages.	☐
	6	Nye, John, "Avoiding Audit Overlap," Moody's Risk Services, Presentation, Source Boston, March 14, 2008, 19 pages.	☐
	7	"Agreed Upon Procedures," Version 4.0, BITS, The Financial Institution Shared Assessments Program, Assessment Guide, September 2008, 56 pages.	☐
	8	"Master Security Criteria," Version 3.0, BITS Financial Services Security Laboratory, October, 2001, 47 pages.	☐
	9	The Financial Institution Shared Assessments Program, Industry Positioning and Mapping Document, BITS, October 2007, 44 pages.	☐
	10	Browne, Niall, et al., "Shared Assessments Program AUP and SAS70 Frequently Asked Questions," BITS, 4 pages.	☐
	11	"Shared Assessments: Getting Started," BITS, 2008, 4 pages.	☐
	12	Boyer, Stephen, et al., "Playing with Blocks: SCAP-Enable Higher-Level Analyses, MIT Lincoln Laboratory, 5th Annual IT Security Automation Conference, October 26-29, 2009, 35 pages.	☐
	13	Buckshaw, Donald L., "Use of Decision Support Techniques for Information System Risk Management," submitted for publication in Wiley's Encyclopedia of Quantitative Risk Assessment in January 2007, 11 pages.	☐
	14	Buehler, Kevin S., et al., "Running with risk," The McKinsey Quarterly, No. 4, 2003, pp. 40-49.	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE INDICATED OTHERWISE. /S.K./

Black Lotus Ex. 1002, Page 873 of 1060

Receipt date: 01/24/2012	Application Number	13240572 13240572 - GAU: 2432
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2011-09-22
	First Named Inventor	Boyer et al.
	Art Unit	2876
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	10131-002US1

	15	Chu, Matthew, et al., "Visualizing Attack Graphs, Reachability, and Trust Relationships with NAVIGATOR," MIT Lincoln Library, VizSEC '10, Ontario, Canada, September 14, 2010, 12 pages.	☐
	16	The CIS Security Metrics v1.0.0, The Center for Internet Security, May 11, 2009, 90 pages.	☐
	17	Method Documentation, CNSS Risk Assessment Tool Version 1.1, March 31, 2009, 24 pages.	☐
	18	Crowther, Kenneth G., et al., "Principles for Better Information Security through More Accurate, Transparent Risk Scoring," Journal of Homeland Security and Emergency Management, Vol. 7, Issue 1, Article 37, 2010, 20 pages.	☐
	19	"Assuring a Trusted and Resilient Information and Communications Infrastructure," Cyberspace Policy Review, May, 2009, 76 pages.	☐
	20	Davis, Lois M., et al., "The National Computer Security Survey (NCSS) Final Methodology," Technical report prepared for the Bureau of Justice Statistics, Safety and Justice Program, RAND Infrastructure, Safety and Environment (ISE), 2008, 91 pages.	☐
	21	Dillon-Merrill, Ph.D., Robin L., et al., "Logic Trees: Fault, Success, Attack, Event, Probability, and Decision Trees," Wiley Handbook of Science and Technology for Homeland Security, 13 pages.	☐
	22	Dun & Bradstreet, The DUNSRight Quality Process: Power Behind Quality Information, 24 pages.	☐
	23	The Dun & Bradstreet Corp. Stock Report, Standard & Poor's, June 6, 2009, 8 pages.	☐
	24	Equifax Inc. Stock Report, Standard & Poor's, June 6, 2009, 8 pages.	☐
	25	The Fair Credit Reporting Act (FCRA) of the Federal Trade Commission (FTC), July 30, 2004, 86 pages.	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE INDICATED OTHERWISE. /S.K./

Receipt date: 01/24/2012	Application Number	13240572	13240572 - GAU: 2432
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2011-09-22	
	First Named Inventor	Boyer et al.	
	Art Unit	2876	
	Examiner Name	Not Yet Assigned	
	Attorney Docket Number	10131-002US1	

	26	Report to the Congress on Credit Scoring and Its Effects on the Availability and Affordability of Credit, Board of Governors of the Federal Reserve System, August 2007, 304 pages.	☐
	27	Stone-Gross, Brett, et al., "FIRE: FInding Rogue nEtworks," 10 pages.	☐
	28	Ingols, Kyle, et al., "Modeling Modern Network Attacks and Countermeasures Using Attack Graphs," MIT Lincoln Laboratory, 16 pages.	☐
	29	Ingols, Kyle, et al., "Practical Attack Graph Generation for Network Defense," MIT Lincoln Library, IEEE Computer Society, Proceedings of the 22nd Annual Computer Security Applications Conference (ACSAC'06), 2006, 10 pages.	☐
	30	Ingols, Kyle, et al., "Practical Experiences Using SCAP to Aggregate CND Data," MIT Lincoln Library, Presentation to NIST SCAP Conference, September 24, 2008, 59 pages.	☐
	31	Johnson, Eric, et al., "Information Risk and the Evolution of the Security Rating Industry," March 24, 2009, 27 pages.	☐
	32	Lippmann, R.P., et al., "Evaluating and Strengthening Enterprise Network Security Using Attack Graphs," Project Report IA-2, MIT Lincoln Laboratory, October 5, 2005, 96 pages.	☐
	33	"Assessing Risk in Turbulent Times," A Workshop for Information Security Executives, Glassmeyter/McNamee Center for Digital Strategies, Tuck School of Business at Dartmouth, Institute for Information Infrastructure Protection, 2009, 17 pages.	☐
	34	Lippmann, Richard, et al., "Validating and Restoring Defense in Depth Using Attack Graphs," MIT Lincoln Laboratory, 10 pages.	☐
	35	"Plugging the Right Holes," Lab Notes, MIT Lincoln Library, Posted July 2008, retrieved September 14, 2010 from http://www.11.mit.edu/publications/labnotes/pluggingtherightthol..., 2 pages.	☐
	36	Rare Events, October 2009, JASON, The MITRE Corporation, October 2009, 104 pages.	☐

ALL REFERENCES CONSIDERED EXCEPT WHERE INDICATED THROUGH. /S.K./

Receipt date: 01/24/2012	Application Number	13240572	13240572 - GAU: 2432
INFORMATION DISCLOSURE STATEMENT BY APPLICANT (**Not for submission under 37 CFR 1.99)**	Filing Date	2011-09-22	
	First Named Inventor	Boyer et al.	
	Art Unit	2876	
	Examiner Name	Not Yet Assigned	
	Attorney Docket Number	10131-002US1	

	37	Lippmann, Rich, et al., "NetSPA: a Network Security Planning Architecture, MIT Lincoln Laboratory, 11 pages.	☐
	38	Proposal and Award Policies and Procedures Guide, Part I - Proposal Preparation & Submission Guidelines GPG, The National Science Foundation, February 2009, 68 pages.	☐
	39	Paxson, Vern, "How The Pursuit of Truth Led Me To Selling Viagra," EECS Department, University of California, International Computer Science Institute, Lawrence Berkeley National Laboratory, August 13, 2009, 68 pages.	☐
	40	"Report on Controls Placed in Operation and Test of Operating Effectiveness," EasCorp, January 1 through December 31, 2008, prepared by Crowe Horwath, 58 pages.	☐
	41	Taleb, Nassim N., et al., "The Six Mistakes Executives Make in Risk Management," Harvard Business Review, October 2009, 5 pages.	☐
	42	2009 Data Breach Investigations Report, study conducted by Verizon Business RISK Team, 52 pages.	☐
	43	Williams, Leevar, et al., "GARNET: A Graphical Attack Graph and Reachability Network Evaluation Tool," MIT Lincoln Library, VizSEC 2009, pp. 44-59.	☐
	44	Williams, Leevar, et al., "An Interactive Attack Graph Cascade and Reachability Display," MIT Lincoln Laboratory, 17 pages.	☐

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature	/Simon Kanaan/	Date Considered	11/08/2012

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE INDICATED OTHERWISE. /S.K./

PTO/SB/08a (01-10)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Application Number	13240572
Filing Date	2011-09-22
First Named Inventor	Boyer et al.
Art Unit	2876
Examiner Name	Not Yet Assigned
Attorney Docket Number	10131-002US1

U.S.PATENTS Remove

Examiner Initial*	Cite No	Patent Number	Kind Code[1]	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	7194769	B2	2007-03-20	Lippmann et al.	
	2	7290275	B2	2007-10-30	Baudoin et al.	
	3	7971252	B2	2011-06-28	Lippmann et al.	

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS Remove

Examiner Initial*	Cite No	Publication Number	Kind Code[1]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20040010709	A1	2004-01-15	Baudoin et al.	
	2	20050138413	A1	2005-06-23	Lippmann et al.	
	3	20080047018	A1	2008-02-21	Baudoin et al.	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13240572
	Filing Date	2011-09-22
	First Named Inventor	Boyer et al.
	Art Unit	2876
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	10131-002US1

	4	20080209565	A2	2008-08-28	Baudoin et al.	
	5	20090265787	A9	2009-10-22	Baudoin et al.	
	6	20090293128	A1	2009-11-26	Lippmann et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS Remove

Examiner Initial*	Cite No	Foreign Document Number[3]	Country Code[2] i	Kind Code[4]	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T[5]
	1							☐

If you wish to add additional Foreign Patent Document citation information please click the Add button Add

NON-PATENT LITERATURE DOCUMENTS Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T[5]
	1	SBIR Phase I: Enterprise Cyber Security Scoring, CyberAnalytix, LLC, http://www.nsf.gov/awardsearch/showAward.do?AwardNumber=1013603, April 28, 2010.	☐
	2	"Twenty Critical Controls for Effective Cyber Defense: Consensus Audit," Version 2.3, November 13, 2009, retrieved on April 9, 2010 from http://www.sans.org/critical-security-controls/print.php.	☐
	3	"An Executive View of IT Governance," IT Governance Institute, 2009, 32 pages.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13240572
	Filing Date	2011-09-22
	First Named Inventor	Boyer et al.
	Art Unit	2876
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	10131-002US1

	4	Lippmann, R.P., et al., "An Annotated Review of Papers on Attack Graphs," Project Report IA-1, Lincoln Laboratory, Massachusetts Institute of Technology, March 31, 2005, 39 pages.	☐
	5	Artz, Michael Lyle, "NetSPA: A Network Security Planning Architecture," Massachusetts Institute of Technology, May 24, 2002, 97 pages.	☐
	6	Nye, John, "Avoiding Audit Overlap," Moody's Risk Services, Presentation, Source Boston, March 14, 2008, 19 pages.	☐
	7	"Agreed Upon Procedures," Version 4.0, BITS, The Financial Institution Shared Assessments Program, Assessment Guide, September 2008, 56 pages.	☐
	8	"Master Security Criteria," Version 3.0, BITS Financial Services Security Laboratory, October, 2001, 47 pages.	☐
	9	The Financial Institution Shared Assessments Program, Industry Positioning and Mapping Document, BITS, October 2007, 44 pages.	☐
	10	Browne, Niall, et al., "Shared Assessments Program AUP and SAS70 Frequently Asked Questions," BITS, 4 pages.	☐
	11	"Shared Assessments: Getting Started," BITS, 2008, 4 pages.	☐
	12	Boyer, Stephen, et al., "Playing with Blocks: SCAP-Enable Higher-Level Analyses, MIT Lincoln Laboratory, 5th Annual IT Security Automation Conference, October 26-29, 2009, 35 pages.	☐
	13	Buckshaw, Donald L., "Use of Decision Support Techniques for Information System Risk Management," submitted for publication in Wiley's Encyclopedia of Quantitative Risk Assessment in January 2007, 11 pages.	☐
	14	Buehler, Kevin S., et al., "Running with risk," The McKinsey Quarterly, No. 4, 2003, pp. 40-49.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13240572
	Filing Date	2011-09-22
	First Named Inventor	Boyer et al.
	Art Unit	2876
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	10131-002US1

	15	Chu, Matthew, et al., "Visualizing Attack Graphs, Reachability, and Trust Relationships with NAVIGATOR," MIT Lincoln Library, VizSEC '10, Ontario, Canada, September 14, 2010, 12 pages.	☐
	16	The CIS Security Metrics v1.0.0, The Center for Internet Security, May 11, 2009, 90 pages.	☐
	17	Method Documentation, CNSS Risk Assessment Tool Version 1.1, March 31, 2009, 24 pages.	☐
	18	Crowther, Kenneth G., et al., "Principles for Better Information Security through More Accurate, Transparent Risk Scoring," Journal of Homeland Security and Emergency Management, Vol. 7, Issue 1, Article 37, 2010, 20 pages.	☐
	19	"Assuring a Trusted and Resilient Information and Communications Infrastructure," Cyberspace Policy Review, May, 2009, 76 pages.	☐
	20	Davis, Lois M., et al., "The National Computer Security Survey (NCSS) Final Methodology," Technical report prepared for the Bureau of Justice Statistics, Safety and Justice Program, RAND Infrastructure, Safety and Environment (ISE), 2008, 91 pages.	☐
	21	Dillon-Merrill, Ph.D., Robin L., et al., "Logic Trees: Fault, Success, Attack, Event, Probability, and Decision Trees," Wiley Handbook of Science and Technology for Homeland Security, 13 pages.	☐
	22	Dun & Bradstreet, The DUNSRight Quality Process: Power Behind Quality Information, 24 pages.	☐
	23	The Dun & Bradstreet Corp. Stock Report, Standard & Poor's, June 6, 2009, 8 pages.	☐
	24	Equifax Inc. Stock Report, Standard & Poor's, June 6, 2009, 8 pages.	☐
	25	The Fair Credit Reporting Act (FCRA) of the Federal Trade Commission (FTC), July 30, 2004, 86 pages.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13240572
	Filing Date	2011-09-22
	First Named Inventor	Boyer et al.
	Art Unit	2876
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	10131-002US1

	26	Report to the Congress on Credit Scoring and Its Effects on the Availability and Affordability of Credit, Board of Governors of the Federal Reserve System, August 2007, 304 pages.	☐
	27	Stone-Gross, Brett, et al., "FIRE: FInding Rogue nEtworks," 10 pages.	☐
	28	Ingols, Kyle, et al., "Modeling Modern Network Attacks and Countermeasures Using Attack Graphs," MIT Lincoln Laboratory, 16 pages.	☐
	29	Ingols, Kyle, et al., "Practical Attack Graph Generation for Network Defense," MIT Lincoln Library, IEEE Computer Society, Proceedings of the 22nd Annual Computer Security Applications Conference (ACSAC'06), 2006, 10 pages.	☐
	30	Ingols, Kyle, et al., "Practical Experiences Using SCAP to Aggregate CND Data," MIT Lincoln Library, Presentation to NIST SCAP Conference, September 24, 2008, 59 pages.	☐
	31	Johnson, Eric, et al., "Information Risk and the Evolution of the Security Rating Industry," March 24, 2009, 27 pages.	☐
	32	Lippmann, R.P., et al., "Evaluating and Strengthening Enterprise Network Security Using Attack Graphs," Project Report IA-2, MIT Lincoln Laboratory, October 5, 2005, 96 pages.	☐
	33	"Assessing Risk in Turbulent Times," A Workshop for Information Security Executives, Glassmeyter/McNamee Center for Digital Strategies, Tuck School of Business at Dartmouth, Institute for Information Infrastructure Protection, 2009, 17 pages.	☐
	34	Lippmann, Richard, et al., "Validating and Restoring Defense in Depth Using Attack Graphs," MIT Lincoln Laboratory, 10 pages.	☐
	35	"Plugging the Right Holes," Lab Notes, MIT Lincoln Library, Posted July 2008, retrieved September 14, 2010 from http://www.11.mit.edu/publications/labnotes/pluggingtherightthol..., 2 pages.	☐
	36	Rare Events, October 2009, JASON, The MITRE Corporation, October 2009, 104 pages.	☐

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13240572
	Filing Date	2011-09-22
	First Named Inventor	Boyer et al.
	Art Unit	2876
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	10131-002US1

	37	Lippmann, Rich, et al., "NetSPA: a Network Security Planning Architecture, MIT Lincoln Laboratory, 11 pages.	☐
	38	Proposal and Award Policies and Procedures Guide, Part I - Proposal Preparation & Submission Guidelines GPG, The National Science Foundation, February 2009, 68 pages.	☐
	39	Paxson, Vern, "How The Pursuit of Truth Led Me To Selling Viagra," EECS Department, University of California, International Computer Science Institute, Lawrence Berkeley National Laboratory, August 13, 2009, 68 pages.	☐
	40	"Report on Controls Placed in Operation and Test of Operating Effectiveness," EasCorp, January 1 through December 31, 2008, prepared by Crowe Horwath, 58 pages.	☐
	41	Taleb, Nassim N., et al., "The Six Mistakes Executives Make in Risk Management," Harvard Business Review, October 2009, 5 pages.	☐
	42	2009 Data Breach Investigations Report, study conducted by Verizon Business RISK Team, 52 pages.	☐
	43	Williams, Leevar, et al., "GARNET: A Graphical Attack Graph and Reachability Network Evaluation Tool," MIT Lincoln Library, VizSEC 2009, pp. 44-59.	☐
	44	Williams, Leevar, et al., "An Interactive Attack Graph Cascade and Reachability Display," MIT Lincoln Laboratory, 17 pages.	☐

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. [2] Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). [3] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [4] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [5] Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)		
	Application Number	13240572
	Filing Date	2011-09-22
	First Named Inventor	Boyer et al.
	Art Unit	2876
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	10131-002US1

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

☐ That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

☐ That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

☐ See attached certification statement.

☐ Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

☒ None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Gregory J. Carlin/	Date (YYYY-MM-DD)	2012-01-24
Name/Print	Gregory J. Carlin	Registration Number	45,607

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these record s.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	11899948
Application Number:	13240572
International Application Number:	
Confirmation Number:	2423
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Customer Number:	96039
Filer:	Gregory J. Carlin/Karen Carroll
Filer Authorized By:	Gregory J. Carlin
Attorney Docket Number:	10131-002US1
Receipt Date:	24-JAN-2012
Filing Date:	22-SEP-2011
Time Stamp:	12:36:05
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Non Patent Literature	20_CriticalSecurityControls.pdf	362077 76fb91dc6d8b144a69c2d1e6519df9a06cd3029c	no	52

Warnings:	
Information:	

2	Non Patent Literature	AnExecutiveViewofITGovernance.pdf	9943860 916217c5132c9f5f4ac16a862d53927d65e604cd	no	32
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
3	Non Patent Literature	Artz_NetSPA.pdf	6159472 09281f933d3e2d5ce726a4194f8309a3e149a184	no	97
Warnings:					
Information:					
4	Non Patent Literature	Assessing_Risk_Turbulent_Times.pdf	322424 54ba52e690d642d357b40cdb5ab3e87d1028dec4	no	17
Warnings:					
Information:					
5	Non Patent Literature	BITS_AssessmentGuide_version4.pdf	214608 174a48b5918c852f84de15da9e28f10397d6ad22	no	56
Warnings:					
Information:					
6	Non Patent Literature	BITS_MasterSecurityCriteria.pdf	389070 baf7824e7de5bd4f43d02c7238adc84ff0edca54	no	47
Warnings:					
Information:					
7	Non Patent Literature	BITS_SharedAssessmentProgram_FAQ.pdf	155397 85dd3bc853362cf9962abbaf9f68b164a5125fdb	no	4
Warnings:					
Information:					
8	Non Patent Literature	BITS_SharedAssessmentProgram_IndustryPositioning.pdf	363843 85aef2c017aa3c7188c32b70531cd8e306caf416	no	44
Warnings:					
Information:					
9	Non Patent Literature	BITS_SharedAssessments_GettingStarted.pdf	197178 b9e3a97294daf94e3fc23f4ae54e15f953eda7f6	no	4
Warnings:					
Information:					
10	Non Patent Literature	Boyer_PlayingWithBlocks.pdf	6888215 e738fc44e0711479ada04fcc6be8075c6eab	no	35

Warnings:					
Information:					
11	Non Patent Literature	Buckshaw_UseOfDecisionSupportTechniques.pdf	132199 770a9835a1683046de964e5009d98ced47bdea17	no	11
Warnings:					
Information:					
12	Non Patent Literature	Buehler_etal_RunningWithRisk.pdf	2358814 eff4956e6a4913ac75ce08d36ad417d7699bdb85	no	10
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
13	Non Patent Literature	Chu_VisualizingAttackGraphs.pdf	578868 2e9f7feccd898ae2de24188a498ac9a122903bf2	no	12
Warnings:					
Information:					
14	Non Patent Literature	CIS_Security_Metrics.pdf	773627 79ed8d3066a5b5374c484661038f3438776318ce	no	90
Warnings:					
Information:					
15	Non Patent Literature	CNSS_RiskAssessmentTool_MethodDocumentation.pdf	1181460 764db169d0fc51a9d7439d12d1aabe1d04a8a32c	no	24
Warnings:					
Information:					
16	Non Patent Literature	Crowther_PrinciplesForBetterInformation.pdf	252571 711ad2469d9a30c5e930356aec87c80d46bc726f	no	20
Warnings:					
Information:					
17	Non Patent Literature	Cyberspace_Policy_Review.pdf	941457 1243f299a847aa53bde5cec961e5f414af6bcb6f	no	76
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
18	Non Patent Literature	Dillon-Merrill_LogicTrees.pdf	184514 cdbc0f580d511303d4ab69200fff2fdfa52b5439	no	13
Warnings:					

Information:					
19	Non Patent Literature	Dun_Bradstreet_DUNSRightQualityProcess.pdf	790281 9841dff95367f3bbb448efd6213d66f7f5078341	no	24
Warnings:					
Information:					
20	Non Patent Literature	Dun_Bradstreet_SandP_Report.pdf	157131 9c122ff1ab77ab21dc86ba0ebfe2af2cc03b637f	no	8
Warnings:					
Information:					
21	Non Patent Literature	Equifax_SandP_Report.pdf	154942 9cb6bb5be1cfa8b1eb055743c79f2d60313add55	no	8
Warnings:					
Information:					
22	Non Patent Literature	Fair_Credit_Reporting_Act.pdf	383842 b01e6ce615f9e440fdad47cb4fe68a7e30cf99bd	no	86
Warnings:					
Information:					
23	Non Patent Literature	Federal_Creditscore_Report.pdf	4922991 6d6291dd4236fa6ed9ee74d2dd615ca1581bcd34	no	304
Warnings:					
Information:					
24	Non Patent Literature	Ingols_ModelingModern.pdf	1238142 fb796ba39ba6094d7993e04ef36de5f6dfeadef7	no	16
Warnings:					
Information:					
25	Non Patent Literature	Ingols_PracticalAttackGraph.pdf	608086 a7e0dcf1d4070f4f65b283048d4c07c535d981fa	no	10
Warnings:					
Information:					
26	Non Patent Literature	Ingols_PracticalExperiences.pdf	6448860 d763384b3f1c8438ccee89d142d2b095a7854010	no	59
Warnings:					
Information:					
27	Non Patent Literature	Johnson_InformationRisk.pdf	334252 4d8207fde27920ed0aa1aea4a90a051142e3c03e	no	27
Warnings:					

Information:					
28	Non Patent Literature	Lippman_EvaluatingAndStrengthening.pdf	1555741 52f643413c4cf8dde56485b278aef2dfa3550028	no	96
Warnings:					
Information:					
29	Non Patent Literature	Lippmann_AnnotatedReview.pdf	334515 20b15ac2d72c53194255577a3d5b2126713fb8e9	no	39
Warnings:					
Information:					
30	Non Patent Literature	Lippmann_ValidatingAndRestoring.pdf	452868 ef1342031adf99bdc134f57e6e0d060d31394233	no	10
Warnings:					
Information:					
31	Non Patent Literature	MITLL_Journal_PluggingTheRightHoles.pdf	166952 21766b7018ef215f2aed51a5352b0f6bc4d6eb91	no	2
Warnings:					
Information:					
32	Non Patent Literature	MitreCorp_RareEvents.pdf	1990408 6c633d185254a2c4e5b297fef06d6abb497dd7ad	no	104
Warnings:					
Information:					
33	Non Patent Literature	Davis_NCSS.pdf	7621874 0d2dea1c4ee1e7206574027cbcccf94e5d6d06c4	no	91
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
34	Non Patent Literature	NetSPA_InformationBundle.pdf	622782 0f4af04ecc579a585867f7b8cb4ec11a60870ab9	no	11
Warnings:					
Information:					
35	Non Patent Literature	NSF_SBIR_PhaseI_EnterpriseCyberSecurityScoring.PDF	381501 b3f4a972e6f4320b80a49e5a52102d4cc08c8b0b	no	2
Warnings:					
Information:					

36	Non Patent Literature	Paxson_HowThePursuitOfTruth.pdf	14098763 6d54636e3a445a7c18cc96e28a60791388089325	no	68
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
37	Non Patent Literature	SAS_70_Report.pdf	9871686 2975d07e33de4803c5f121cbc011feb03d7e5c9c	no	58
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
38	Non Patent Literature	Stone-Gross_FIRE_FindingRogueNetworks.pdf	225952 f049d122d7731128a4c2380bb139f2dec6940b05	no	10
Warnings:					
Information:					
39	Non Patent Literature	Taleb_RiskManagementMistakes.pdf	998701 3189e80c0b50e70b06b96a51a2910a195c1f1d55	no	5
Warnings:					
Information:					
40	Non Patent Literature	Verizon_2009_DataBreachInvestigationsReport.pdf	275841 3d7512be2d4b207ddde19220f6858d68d1b530cc	no	52
Warnings:					
Information:					
41	Non Patent Literature	Williams_GraphicalAttack.pdf	503049 211cc7efc15816550988 45d072fbdf5deee84c6f	no	16
Warnings:					
Information:					
42	Non Patent Literature	Williams_InteractiveAttack.pdf	387581 c27af6adc65bc32ee3e9124dbfe67685b6bb84dc	no	17
Warnings:					
Information:					
43	Transmittal Letter	10131-002US1_IDS_Tns_Ltr.pdf	45302 671714714f25543a3dc6fc73c0ebc4f8e1b2a467	no	1
Warnings:					
Information:					

44	Information Disclosure Statement (IDS) Form (SB08)	10131-002US1_IDS_PTO_SB_08a.pdf	615629 a226e183f63754c2ec905218d65f07a352fa1cd5	no	8
Warnings:					
Information:					
45	Non Patent Literature	NSF_ProposalAwardPolicies.pdf	9877490 49bfb53c14d373969e4b6bd558f4a4bf89ed262b	no	68
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
46	Non Patent Literature	Nye_AvoidingAuditOverlap.pdf	6869989 02bbc4070967120ee5f61352cf1cb8c3743e6f96	no	19
Warnings:					
The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing					
Information:					
		Total Files Size (in bytes):	103334805		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Boyer et al.	Art Unit	: 2876
Serial No.	: 13/240,572	Examiner	: Not Yet Assigned
Filed	: September 22, 2011		
Title	: INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM		

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT

Applicants request consideration of the references listed on the attached PTO/SB/08a form(s). Under 37 C.F.R. § 1.98 (a)(2)(ii), only copies of foreign patent documents and/or non-patent literature are enclosed. Copies of any listed U.S. patents or U.S. patent application publications can be provided upon request.

This document is being filed before issuance of a first Office Action on the merits. Accordingly, no fee is required.

Date: January 24, 2012

/Gregory J. Carlin/
Gregory J. Carlin
Reg. No. 45,607

McKeon, Meunier, Carlin & Curfman, LLC
817 W. Peachtree St., NW
Suite 900
Atlanta, GA 30308
phone: (404) 645-7713
fax: (404) 645-7707

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 13/240,572

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	95		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	310		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	125		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	20 minus 20 =	*	x 30 =	0.00	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	1 minus 3 =	*	x 125 =	0.00			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	530		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/240,572	09/22/2011	2876	527	10131-002US1	20	1

CONFIRMATION NO. 2423

UPDATED FILING RECEIPT

96039
McKeon Meunier Carlin & Curfman LLC
817 W. Peachtree Street, Suite 900
Atlanta, GA 30308

OC00000051581714

Date Mailed: 12/23/2011

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Stephen Wayne Boyer, Waltham, MA;
Nagarjuna Venna, Waltham, MA;
Megumi Ando, Cambridge, MA;

Assignment For Published Patent Application

BITSIGHT TECHNOLOGIES, INC., Waltham, MA

Power of Attorney: None

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/492,287 06/01/2011
and claims benefit of 61/386,156 09/24/2010

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)

If Required, Foreign Filing License Granted: 10/03/2011

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/240,572**

Projected Publication Date: Request for Non-Publication Acknowledged

Non-Publication Request: Yes

Early Publication Request: No
**** SMALL ENTITY ****

Title

INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM

Preliminary Class

235

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as

set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

SelectUSA

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage, facilitate, and accelerate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Boyer, *et al.*	Art Unit	: 2876
Serial No.	: 13/240,572	Examiner	: To Be Assigned
Filed	: September 22, 2011	Conf. No.	: 2423
Title	: INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM		

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PRELIMINARY AMENDMENT

Prior to examination, please amend the application as indicated on the following pages.

Amendments to the claims begin on page 2, and remarks begin on page 14.

Amendments to the Claims:

Applicant requests cancellation of Claims 21-120. This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Original) A method of evaluating information security of a third party computer system, the method comprising:

collecting at least two security characterizations of the third party computer system;

generating a composite security rating using the at least two security characterizations;

wherein the two security characterizations are derived from externally observable characteristics of the third party computer system.

2. (Original) A method of Claim 1, wherein each of the security characterizations is from an associated one of a plurality of independent entities.

3. (Original) A method of Claim 2, wherein the independent entities include commercial data sources.

4. (Original) A method of Claim 2, wherein the security characterizations include at least two data types.

5. (Original) A method of Claim 4, wherein the data types include at least one of breach disclosures, block lists, configuration parameters, malware servers, reputation, suspicious activity, spyware, white lists, compromised hosts, malicious activity, spam activity, vulnerable hosts, phishing, or e-mail viruses.

6. (Original) A method of Claim 1, wherein the security characterizations are derived without permission of the third party computer system.

7. (Original) A method of Claim 1, wherein the externally observable characteristics evidence internal security controls.

8. (Original) A method of Claim 1, wherein the externally observable characteristics are outcomes.

9. (Original) A method of Claim 1, wherein the externally observable characteristics evidence operational execution of security measures of the third party computer system.

10. (Original) A method of Claim 1, wherein the externally observable characteristics include serving of malicious code.

11. (Original) A method of Claim 1, wherein the externally observable characteristics include communications with known attacker controlled networks.

12. (Original) A method of Claim 1, wherein collecting the data and generating the ratings are repeated to generate a series of ratings.

13. (Original) A method of Claim 11, further comprising determining a trend from the series of ratings.

14. (Original) A method of Claim 12, further comprising reporting the ratings.

15. (Original) A method of Claim 13, wherein reporting includes reporting a warning based on a change in the ratings.

16. (Original) A method of Claim 14, wherein reporting includes posting the ratings and warning to a web portal.

17. (Original) A method of Claim 1, wherein collecting the security characterizations includes using tools such as WGET, RSYNC or proprietary and manual methods..

18. (Original) A method of Claim 1, further comprising mapping the third party computer system to an IP space and using the IP space for collecting the security characterizations.

19. (Original) A method of Claim 18, wherein mapping includes querying a regional internet registry.

20. (Original) A method of Claim 19, wherein querying includes submitting an entity name.

21. (Canceled) A method of Claim 20, wherein submitting the entity name includes submitting spelling variations of the entity name.

22. (Canceled) A method of Claim 18, wherein mapping includes using a domain name associated with the third party computer system.

23. (Canceled) A method of Claim 22, wherein mapping includes using a dig tool on the domain name to determine a published IP address.

24. (Canceled) A method of Claim 23, wherein mapping includes probing addresses around the published IP address.

25. (Canceled) A method of Claim 24, wherein probing includes probing addresses in powers of 2 around the published IP address.

26. (Canceled) A method of Claim 22, wherein mapping includes adapting the domain name with server naming conventions.

27. (Canceled) A method of Claim 26, wherein mapping includes using nslookup to verify an IP address associated with the domain name.

28. (Canceled) A method of Claim 1, wherein generating the composite security rating includes assessing a vulnerability and resilience of the third party computer systems.

29. (Canceled) A method of Claim 28, wherein vulnerability includes a number of IP addresses with malicious behavior.

30. (Canceled) A method of Claim 28, wherein resilience is inversely proportional to a duration of malicious behavior.

31. (Canceled) A method of Claim 18, wherein the IP space includes a plurality of IP addresses.

32. (Canceled) A method of Claim 31, further comprising determining at least one badness score for each of the IP addresses.

33. (Canceled) A method of Claim 32, wherein the badness score corresponds to an intensity and duration of malicious activity determined from one of the security characterizations.

34. (Canceled) A method of Claim 33, wherein generating the composite security rating includes aggregating a plurality of badness scores.

35. (Canceled) A method of Claim 34, wherein generating the composite security rating includes aggregating the IP addresses associated with the third party computer system.

36. (Canceled) A method of Claim 31, wherein determining the badness score includes adjusting for false positives in the security characterizations.

37. (Canceled) A method of Claim 36, wherein adjusting for false positives includes determining occurrence of an event which includes persistent, reported activity on one of the IP addresses for a predetermined period of time.

38. (Canceled) A method of Claim 37, wherein adjusting for false positives includes determining an intensity of the IP address for the predetermined period of time.

39. (Canceled) A method of Claim 38, wherein the predetermined period of time is at least one day.

40. (Canceled) A method of Claim 38, wherein the predetermined period of time accounts for inactive periods.

41. (Canceled) A method of Claim 40, wherein the maximum inactive period is 3 days.

42. (Canceled) A method of Claim 38, wherein determining an intensity includes increasing intensity in proportion to a number of reporting targets from the security characterizations.

43. (Canceled) A method of Claim 33, wherein determining the badness score includes weighting recent events heavier than older events.

44. (Canceled) A method of Claim 32, wherein determining the badness score includes assigning a raw score for each of the IP addresses appearing on a block list of one of the security characterizations.

45. (Canceled) A method of Claim 44, wherein the block list does not delist the IP address until requested.

46. (Canceled) A method of Claim 45, further comprising attenuating the raw score after delisting of the IP address.

47. (Canceled) A method of Claim 46, wherein attenuating is at an exponential decay.

48. (Canceled) A method of Claim 32, wherein determining the badness score includes generating a raw score in proportion to a CIDR block size.

49. (Canceled) A method of Claim 35, wherein generating the composite security rating includes normalizing the aggregate of the plurality of badness scores.

50. (Canceled) A method of Claim 49, wherein normalizing includes normalizing based on at least one of network size or number of employees.

51. (Canceled) A method of Claim 32, wherein the security characterizations include non-negative information.

52. (Canceled) A method of Claim 1, further comprising correlating the composite security score with statistical outcomes and adjusting the step of generating based on the statistical outcomes.

53. (Canceled) A method of Claim 1, further comprising determining a confidence range of the composite security score.

54. (Canceled) A method of Claim 53, wherein the confidence range is based on redundancy of the security characterizations.

55. (Canceled) A method of Claim 54, wherein the confidence range is based on a size of the third party computer system.

56. (Canceled) A method of Claim 1, further comprising predicting future information security performance of the third party computer system using the security characterizations.

57. (Canceled) A method of Claim 1, further comprising determining an accuracy of each of the security characterizations.

58. (Canceled) A method of Claim 57, wherein determining the accuracy includes determining a level of coverage of the third party computer system by the security characterizations.

59. (Canceled) A system for evaluating information security of third party computer systems, the system comprising:

a data collection module configured to receive at least two security characterizations, each of the security characterizations describing a security outcome associated with one of the third party computer systems; and

a scoring module connected in communication with the data collection module and configured to use the security characterizations to generate a composite security score for the associated third party computer system;

wherein the security outcome is derived from external investigation of the associated third party computer system.

60. (Canceled) A system of Claim 59, wherein each of the security characterizations

is from an associated one of a plurality of independent entities.

61. (Canceled) A system of Claim 60, wherein the independent entities include commercial data sources.

62. (Canceled) A system of Claim 60, wherein the security characterizations include at least two data types.

63. (Canceled) A system of Claim 62, wherein the data types include at least one of breach disclosures, block lists, configuration, malware servers, reputation, suspicious activity, spyware, white lists, compromised hosts, malicious activity, spam activity, vulnerable hosts, phishing, or e-mail viruses.

64. (Canceled) A system of Claim 59, wherein the security characterizations are derived without permission of the third party computer system.

65. (Canceled) A system of Claim 59, wherein the externally observable characteristics evidence internal security controls.

66. (Canceled) A system of Claim 59, wherein the externally observable characteristics are outcomes.

67. (Canceled) A system of Claim 59, wherein the externally observable characteristics evidence operational execution of security measures of the third party computer system.

68. (Canceled) A system of Claim 59, wherein the externally observable characteristics include serving of malicious code.

69. (Canceled) A system of Claim 59, wherein the externally observable characteristics include communications with known attacker controlled networks.

70. (Canceled) A system of Claim 59, wherein the scoring module is configured to generate a series of ratings.

71. (Canceled) A system of Claim 70, further comprising a trend module configured to determine a trend from the series of ratings.

72. (Canceled) A system of Claim 71, further comprising a reporting module configured to report the ratings.

73. (Canceled) A system of Claim 72, wherein the reporting module is configured to report a warning based on a change in the ratings.

74. (Canceled) A system of Claim 74, wherein the reporting module is configured to post the ratings and warning to a web portal.

75. (Canceled) A system of Claim 59, wherein the data collection module is configured to collect the security characterizations includes using tools such as WGET, RSYNC or proprietary and manual methods.

76. (Canceled) A system of Claim 59, further comprising a mapping module configured to map the third party computer system to an IP space and use the IP space for collecting the security characterizations.

77. (Canceled) A system of Claim 76, wherein the mapping module is further configured to submit a query a regional internet registry.

78. (Canceled) A system of Claim 77, wherein the query includes an entity name.

79. (Canceled) A system of Claim 78, wherein the query includes spelling variations of the entity name.

80. (Canceled) A system of Claim 76, wherein the mapping module is configured to obtain a domain name associated with the third party computer system.

81. (Canceled) A system of Claim 80, wherein the mapping module is configured to use a dig tool on the domain name.

82. (Canceled) A system of Claim 81, wherein the mapping module is configured to

probe addresses around the published IP address.

83. (Canceled) A system of Claim 82, wherein the mapping module is configured to probe addresses in powers of 2 around the published IP address.

84. (Canceled) A system of Claim 80, wherein the mapping module is configured to adapt the domain name with server naming conventions.

85. (Canceled) A system of Claim 84, wherein the mapping module is configured to use nslookup to verify an IP address associated with the domain name.

86. (Canceled) A system of Claim 59, the scoring module is configured to assess a vulnerability and resilience of the third party computer systems.

87. (Canceled) A system of Claim 86, wherein the vulnerability includes a number of IP addresses with malicious behavior.

88. (Canceled) A system of Claim 86, wherein the resilience is inversely proportional to a duration of the malicious behavior.

89. (Canceled) A system of Claim 76, wherein the IP space includes a plurality of IP addresses.

90. (Canceled) A system of Claim 89, further comprising a badness module configured to determine a badness score for each of the IP addresses.

91. (Canceled) A system of Claim 90, wherein the badness score corresponds to an intensity and duration of malicious activity determined from one of the security characterizations.

92. (Canceled) A system of Claim 91, wherein the scoring module is configured to aggregate a plurality of the badness scores.

93. (Canceled) A system of Claim 92, wherein the scoring module is further configured to aggregate the IP addresses associated with the third party computer system.

94. (Canceled) A system of Claim 90, wherein the badness module is further configured to adjust for false positives in the security characterizations.

95. (Canceled) A system of Claim 94, wherein the badness module is further configured to determine an occurrence of an event which includes persistent, reported activity on one of the IP addresses for a predetermined period of time.

96. (Canceled) A system of Claim 95, wherein the badness module is configured to determine an intensity of the IP address for the predetermined period of time.

97. (Canceled) A system of Claim 96, wherein the predetermined period of time is a day.

98. (Canceled) A system of Claim 96, wherein the predetermined period of time accounts for inactive periods.

99. (Canceled) A system of Claim 98, wherein the maximum inactive period is a configurable number.

100. (Canceled) A system of Claim 96, wherein the intensity is in proportion to a number of reporting targets from the security characterizations.

101. (Canceled) A system of Claim 91, wherein the badness module is configured to weight recent events heavier than older events.

102. (Canceled) A system of Claim 90, wherein the badness module is configured to assign a flat score for each of the IP addresses appearing on a block list of one of the security characterizations.

103. (Canceled) A system of Claim 102, wherein the block list does not delist the IP address until requested.

104. (Canceled) A system of Claim 103, wherein the badness module is configured to attenuate the flat score after delisting of the IP address.

105. (Canceled) A system of Claim 104, wherein the badness module is configured to attenuate the flat score at an exponential decay.

106. (Canceled) A system of Claim 90, wherein the badness module is configured to determine the badness score by generating a flat score in proportion to a CIDR block size.

107. (Canceled) A system of Claim 93, wherein the scoring module is configured to normalize the aggregate of the plurality of badness scores.

108. (Canceled) A system of Claim 107, wherein the scoring module is configured to normalize based on at least one of network size or number of employees.

109. (Canceled) A system of Claim 90, wherein the security characterizations include non-negative information.

110. (Canceled) A system of Claim 59, further comprising an accuracy module configured to correlate the composite security score with statistical outcomes and adjust the scoring module to account for the correlation.

111. (Canceled) A system of Claim 59, further comprising a confidence module configured to determine a confidence range of the composite security score.

112. (Canceled) A system of Claim 111, wherein the confidence range is based on redundancy of the security characterizations.

113. (Canceled) A system of Claim 112, wherein the confidence range is based on a size of the third party computer system.

114. (Canceled) A system of Claim 59, further comprising a predictive module configured to predict future information security performance of the third party computer system using the security characterizations.

115. (Canceled) A system of Claim 59, further comprising an accuracy module configured to determine an accuracy of each of the security characterizations.

116. (Canceled) A system of Claim 115, wherein the accuracy module is configured to determine a level of coverage of the third party security system using the security characterizations.

117. (Canceled) A method of evaluating information security of a third party computer system, the method comprising:

collecting at least one security characterization of the third party computer system;

generating a composite security score using the at least one security characterization;

wherein the at least one security characterization is derived from externally observable characteristics of the third party computer system; and

wherein the composite security score has a relatively high likelihood of corresponding to an internal audit score.

118. (Canceled) A method of Claim 117, further comprising one or more of a plurality of the methods of Claims 2-58.

119. (Canceled) A system for evaluating information security of third party computer systems, the system comprising:

a data collection module configured to receive at least one security characterization, the security characterization describing a security outcome associated with one of the third party computer systems; and

a scoring module connected in communication with the data collection module and configured to use the security characterization to generate a composite security score for the associated third party computer system;

wherein the security outcome of the security characterization is derived from external investigation of the associated third party computer system;

wherein the composite score has a relatively high likelihood of corresponding to an internal audit score.

120. (Canceled) A system of Claim 119, further comprising one or more of a plurality of the systems of Claims 59-116.

REMARKS

Claims 1 - 20 are pending. Claims 21 - 120 are canceled in order to comply with the requirements of a Request for First Action Interview filed September 22, 2011. Only 20 total claims and 1 independent claim are pending.

The required fees are being paid concurrently herewith on the Electronic Filing System (EFS) by way of Electronic Funds Transfer; however, please apply any other charges or credits to deposit account 50-5226.

Respectfully submitted,

Date: December 15, 2011

/Gregory J. Carlin/
Gregory J. Carlin
Reg. No. 45,607

Customer Number 96039
Telephone: (404) 645-7700
Facsimile: (404) 645-7707

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Boyer, *et al.*	Art Unit	: 2876
Serial No.	: 13/240,572	Examiner	: Not yet assigned
Filed	: September 22, 2011	Conf. No.	: 2423
Title	: INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM		

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

RESPONSE TO NOTICE TO FILE MISSING PARTS OF APPLICATION

The remarks below are in response to a Notice of Missing Parts mailed on October 6, 2011. In the Notice of Missing Parts, the following items were requested:

- Oath or declaration;
- Marked up copy of Specification;
- Clean Copy of Specification;
- Replacement drawings due to the filed figures being blurry; and
- Payment of fees for claims over 20 and independent claims more than 3.

Applicant as a small entity submits a Declaration herewith in compliance with 37 CFR §1.63 and payment of a surcharge of $65 for late filing of the basic fee and/or declaration. Also being submitted herewith is a Petition for Extension of Time with a one-month fee of $75.

A substitute specification is being filed herewith. The substitute specification contains no new matter.

Replacement drawings are also being submitted herewith. The replacement drawings contain no new matter.

Applicant's attorney inadvertently (as shown by the Transmittal) did not upload a preliminary amendment with the filing of the original application. The Preliminary Amendment

is being filed along with this Response in order to comply with the requirements of a previously-filed Request for First Action Interview. In the preliminary amendment, Claims 21 – 120 have been cancelled. As a result, the additional fees for claims over 20 and independent claims over 3 are no longer required.

It is understood that this perfects the application. It is our understanding that no additional fees are required beyond those enumerated above. The required fees are being paid concurrently herewith on the Electronic Filing System (EFS) by way of Electronic Funds Transfer authorization. Please apply any other charges or credits to Deposit Account No. 50-5226.

Respectfully submitted

McKEON MEUNIER CARLIN & CURFMAN, LLC

Date: December 15, 2011

/Gregory J. Carlin/

Gregory J. Carlin
Reg. No. 45,607

Customer No. 96039
docketing@m2iplaw.com
404.645.7700 Phone
404.645.7707 Fax

INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM

ACKNOWLEDGEMENT

This invention was made with government support under 1127185 awarded by the National Science Foundation. The government has certain rights to this invention.

CROSS-REFERENCE TO RELATED APPLICATIONS

The present application claims priority to U.S. Prov. Pat. App. No. 61/386,156 entitled "Enterprise Information Security Score" and filed on Sept. 24, 2010; and 61/492,287 entitled "Information Technology Security Assessment System" and filed on June 1, 2011 which are hereby incorporated herein in their entirety by reference.

BACKGROUND

The present invention relates to systems for determining the security of information systems and, in particular, for evaluating the security of third-party computer systems.

When a company wants to reduce its cyber security risk of doing business with another company's computer systems, it either performs, or hires an outside firm to perform, a cyber security assessment of the other company to determine if it is following good security practices. The theory is that these good practices make it difficult for attackers to compromise the networks of the other company. If the auditing company is satisfied with the assessment, it may choose to continue doing business with the other company. Or, it may ask the other company to make some improvements to its security systems or terminate the business relationship.

Generally, these audits are slow, expensive and impractical given the high volume of service provider security systems that need to be characterized by the company. And, the inventors have noted that audits are not entirely predictive of the performance of the security systems.

SUMMARY

A method and system is disclosed for creating a composite security rating from security characterization data of a third party computer system. The security

characterization data is derived from externally observable characteristics of the third party computer system. Advantageously, the composite security rating has a relatively high likelihood of corresponding to an internal audit score despite use of externally observable security characteristics. Also, the method and system may include use of multiple security characterizations all solely derived from externally observable characteristics of the third party computer system.

A method of evaluating information security of a third party computer system is disclosed. The method includes collecting at least two security characterizations of the third party computer system. A composite security rating is generated using the at least two security characterizations. Advantageously, the two security characterizations are derived from externally observable characteristics of the third party system.

Each of the security characterizations may be from an associated one of a plurality of independent entities. For example, the independent entities may include commercial data sources. Also, the security characterizations may be derived without permission of the third party system.

The security characterizations may include multiple data types, such as breach disclosures, block lists, configuration parameters, malware servers, reputation metrics, suspicious activity, spyware, white lists, compromised hosts, malicious activity, spam activity, vulnerable hosts, phishing, user-behavior or e-mail viruses. The externally observable characteristics may also include serving of malicious code or communications with known attacker controlled networks.

The externally observable characteristics may be evidence of internal security controls or outcomes or operational execution of security measures of the third party computer system.

The collecting and generating steps may be repeated to generate a series of scores and the series examined to determine a trend. Also, the scores may be reported to a consumer. For instance, reporting may include reporting a warning based on a change in the scores. Or, reporting may include posting the score and warning to a web portal.

Collecting the security characterizations may include using various tools such as WGET, RSYNC, CURL or interfaces that may be characterization specific.

The method may also include mapping the third party computer system to an IP space and using the IP space for collecting the security characterizations. Mapping, for

example, may include querying a Regional Internet Registry (RIR), such as by submitting an entity name to the RIR. Querying an entity name may include querying for variations of the entity name.

Mapping may also include using a domain name associated with the third party computer system. For example, tools such as nslookup or dig may be used on the domain name to determine a published IP address. Mapping may also include probing addresses around the published IP address. For example, IP addresses could be probed in powers of two around the published IP address. Mapping could also include adapting the domain name to server naming conventions and using tools like nslookup to verify an IP address associated with the domain name.

Generating the composite security rating may include assessing vulnerability and resilience of the third party computer systems. Vulnerability, for example, may include a number of IP addresses with malicious behavior. Resilience may be inversely proportional to a duration of malicious behavior.

The IP space may include a plurality of IP addresses. And, the composite security rating may correspond to an intensity and duration of malicious activity determined from one of the security characterizations. Generation of the composite security rating may include aggregation of a plurality of individual security metrics and/or the IP addresses associated with the third party computer system.

Determination of the individual security metric may include adjusting for false positives in the security characterizations. Correlating data across multiple related security characterizations may help improve the quality of any single security characterization. Further, adjusting for false positives may include determining an occurrence of an event, which includes persistent, reported activity on one of the IP addresses for a predetermined period of time. It may also include determining an intensity of the IP address for the predetermined period of time, such as a day.

Determining the intensity may include increasing intensity in proportion to a number of reporting targets from the security characterizations.

Determining an individual security metric may include assigning a raw score for each of the IP addresses appearing on a block list as one of the security characterizations. After an IP address is delisted, the raw score may be exponentially attenuated.

The individual security metric may also incorporate a raw score in proportion to a

CIDR block size.

Individual security metrics or the composite ratings may be normalized based on, for example, network size or a number of employees.

Security characterizations may also include positive information about an organization that's aggregated into the composite rating.

The method could also include statistically correlating the composite security rating with actual outcomes and adjusting the generating step based on the statistical correlations.

Further, the method may include determining a confidence range of the composite security rating. For example, the confidence range may be based on a redundancy of the security characterizations or a size of the third party computer system.

The method may also include determining an accuracy of each of the security characterizations, such as by determining a level of coverage of the third party computer system by the security characterizations.

Also disclosed herein are a system and computer program product for data collection and scoring, including systems and software for performing the methods described above.

Another method may include generating a composite security rating using at least one security characterization that's derived from externally observable characteristics of the third party computer system wherein the composite security rating has a relatively high likelihood of corresponding to an internal audit score.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

Figure 1 is a schematic of a system for evaluating information security;
Figure 2 is a schematic of a system for gathering security data from external sensors;
Figure 3 is a schematic of a composite security rating calculation; and
Figure 4 is a schematic of a distributed system for evaluating information security.

DETAILED DESCRIPTION

Generally, the present invention includes a method, system and computer program product for creating composite security ratings from security characterization data of a third party computer system. The security characterization data is derived from externally observable characteristics of the third party computer system. Advantageously, the composite security rating has a relatively high likelihood of corresponding to an internal

audit score despite use of externally observable security characteristics. Also, the method and system may include use of multiple security characterizations all solely derived from externally observable characteristics of the third party computer system.

The terminology used herein is for the purpose of describing particular embodiments only and is not intended to be limiting of the invention. As used herein, the singular forms "a", "an" and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the terms "comprises" and/or "comprising," when used in this specification, specify the presence of stated features, integers, steps, operations, elements, and/or components, but do not preclude the presence or addition of one or more other features, integers, steps, operations, elements, components, and/or groups thereof.

The corresponding structures, materials, acts, and equivalents of all means or step plus function elements in the claims below are intended to include any structure, material, or act for performing the function in combination with other claimed elements as specifically claimed. The description of the present invention has been presented for purposes of illustration and description, but is not intended to be exhaustive or limited to the invention in the form disclosed. Many modifications and variations will be apparent to those of ordinary skill in the art without departing from the scope and spirit of the invention. The embodiment was chosen and described in order to best explain the principles of the invention and the practical application, and to enable others of ordinary skill in the art to understand the invention for various embodiments with various modifications as are suited to the particular use contemplated.

Any combination of one or more computer readable medium(s) may be utilized. The computer readable medium may be a computer readable signal medium or a computer readable storage medium. A computer readable storage medium may be, for example, but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, or device, or any suitable combination of the foregoing. More specific examples (a non-exhaustive list) of the computer readable storage medium would include the following: an electrical connection having one or more wires, a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), an optical fiber, a portable compact disc read-only memory (CD-ROM), an optical storage device, a magnetic

storage device, or any suitable combination of the foregoing. In the context of this document, a computer readable storage medium may be any tangible medium that can contain, or store a program for use by or in connection with an instruction execution system, apparatus, or device.

A computer readable signal medium may include a propagated data signal with computer readable program code embodied therein, for example, in baseband or as part of a carrier wave. Such a propagated signal may take any of a variety of forms, including, but not limited to, electro-magnetic, optical, or any suitable combination thereof. A computer readable signal medium may be any computer readable medium that is not a computer readable storage medium and that can communicate, propagate, or transport a program for use by or in connection with an instruction execution system, apparatus, or device.

Program code embodied on a computer readable medium may be transmitted using any appropriate medium, including but not limited to wireless, wireline, optical fiber cable, RF, etc., or any suitable combination of the foregoing.

Computer program code for carrying out operations for aspects of the present invention may be written in any combination of one or more programming languages, including an object oriented programming language such as Java, Smalltalk, C++ or the like and conventional procedural programming languages, such as the "C" programming language or similar programming languages. The program code may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider).

Aspects of the present invention are described below with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems) and computer program products according to embodiments of the invention. It will be understood that each block of the flowchart illustrations and/or block diagrams, and combinations of blocks in the flowchart illustrations and/or block diagrams, can be implemented by computer program instructions. These computer program instructions may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data

processing apparatus to produce a machine, such that the instructions, which execute via the processor of the computer or other programmable data processing apparatus, create means for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

These computer program instructions may also be stored in a computer readable medium that can direct a computer, other programmable data processing apparatus, or other devices to function in a particular manner, such that the instructions stored in the computer readable medium produce an article of manufacture including instructions which implement the function/act specified in the flowchart and/or block diagram block or blocks.

The computer program instructions may also be loaded onto a computer, other programmable data processing apparatus, or other devices to cause a series of operational steps to be performed on the computer, other programmable apparatus or other devices to produce a computer implemented process such that the instructions which execute on the computer or other programmable apparatus provide processes for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

Referring again to Fig. 1, a system 10 for evaluating information security of a third party computer system includes the following systems: a global data source 12, an entity ownership collector 14, a data collection processor 16, a data collection management 18, a data archive 20, an entity database 22, a manual entity input 24, an entity data join process 26, an entity mapped meta-reports repository 28, a ratings processing 30, a normalization, consolidation and global relative rank 32, a report generation 34, a report archive 36 and a report delivery 38 systems. Different delivery modules 40 are configured to use different methods to deliver the reports to customers 42.

The global data source system 12 obtains data sources that characterize any observation about an entity (e.g., a third party computer system) and these sources can be highly varied and disparate. Each data source has a particular vantage point of the security related characteristics of entities.

The entity ownership collection system 14 gathers information about an entity. This includes information about which IT assets an entity owns, controls, uses, or is affiliated with. Examples of asset ownership include control and operation of an Internet Protocol (IP) network address range or computer services such as web servers residing within that address block. Information about entities also includes relationships such as subsidiaries,

affiliates, etc., that describe entity association.

The data collection processing system 16 includes custom modules configured to collect and process unique data sources.

The data collection management system 18 is configured to schedule and coordinate the constant collection of the different data sources.

The data archive 20 is configured to store all of the terabytes of data constantly collected by the data collection management system 18.

The entity database 22 holds all of the information about an entity such as its name, address, web site address, industry sector, IP address ranges owned, etc. This data base includes the "Entity Map" which maps data back to an entity. For example, if observations are made about a particular IP address, the IP address can be looked up in the entity map to determine which entity controls or owns that address. This database is populated by automatic or manual data collection methods, or combinations thereof.

The manual entity input system is configured to place non-automatic data on an entity into the entity database 22.

The entity data join process or system 26 is configured to match the collected data to the entity. In most instances, this is a computationally expensive operation because it requires going though all of the data collected and performing the map operation. Any evidence of security outcomes or configurations in the larger data collection pool is then assigned to an entity based on the entity map.

The entity mapped meta-reports repository 28 contains data summaries of observations made with respect to a particular entity for each data set after the map/join process is complete.

The ratings processing system 30 may include custom models for applying data source specific ratings to determine an entity rating. Each data source generally requires a custom model due to the unique nature of that data source. Each model accounts for the custom attributes and idiosyncrasies of the different data sources that have been mapped to the entity being rated. Custom data source models can account for any data source feature including temporal and cross-data source behaviors.

The ratings normalization, cross-validation, and relative ranking system 32 is configured to normalize ratings so appropriate entity-to-entity comparisons can be made and the ratings are normalized and ranked within sectors or peer-groups and globally.

An entity and rating analytics repository or archive 36 is configured to hold all of the ratings data and resulting analytics produced by the ratings process.

A report generation system 34 takes the ratings and analytics and generates report objects. These objects are not rendered into any particular presentation format at this stage but are in a generic intermediary format that can be then transformed into a specific deliverable format.

A report delivery system 38 is configured to translate generic reports into a specific report format. Examples of these formats include HTML, PDF, text, and XML. Delivery modules 40 are different methods for delivering the reports include by web portal, API or data feed.

Advantages include ratings based on the quality of outcomes of the information security practices of the third party computer systems and enablement of comparisons of ratings across organizations. The system 10 can be entirely, or to a large extent, automated and need not have the permission of the entity being rated. The reports will allow risk management professionals to monitor, assess and mitigate partner risk by up-to-date ratings due to its persistent monitoring of the third party computer systems. Also, the portal may provide for location of new partners, such as suppliers, with lower risk profiles and improved security postures.

Unlike internal audit systems, the system 10 is not relying upon a correlation between practices and outcomes. Instead, evidence of actual security outcomes is collected through the data source partners.

Also advantageously, trial data on 50 entities revealed that rankings produced using the system 10 matched internal evaluations. In some cases the system 10 revealed problems with the entities not revealed by internal evaluations.

Data Sources

External ratings from data sources available outside an entity provide an information security based view into internal workings of the organization. For example, infection by malicious software can be determined using non-invasive website scanning technology. Communication between the entity computer system and known attacker controlled networks may reveal when the computer system has been compromised. Also, if an entity computer system is serving malicious code to visitors the system was compromised at some

point. The entity may not have the capability to detect such compromises or cannot quickly react operationally to resolve the issue. External observations also can measure operational execution, which may not occur despite good internal policies.

A diverse set of network sensors and services around the Internet collect and observe information about the third party entity computer systems. The system 10 then gathers, processes, and stores the data collected about entities from the sensors and service providers using custom developed data source specific collection processors. The collection manager 18 automates the scheduling and execution of the different collectors.

The global data source system 12 includes hundreds of potential data sources, including, for example during experimental testing, 97 data sources owned by 37 organizations. At least 82 data sources are on active collection, being stored on the data archive 20. Trial ratings were performed on at least 11 data sources from 7 organizations. Rankings were produced on nearly 600 different entities.

A data source is a single type of data from a single organization. For example, if two organizations provide a list of hosts that participate in phishing attacks, they are counted as two data sources. The 15 types of data in Table 3 all provide different information security related views of an organization. New types of data and new sources of existing data types are constantly added to the data sources used to characterize the performance of the entity. Breach disclosures for example indicate that an organization has experienced a particular kind of data or integrity breach. Configuration data on the other hand provides any number of configuration related information and could for example state the type of encryption used on the organization's website.

Table 1 Data Sources Summary

Total Data Sources	97
Total Sourcing Organizations	37
Total Sources on Active Collection	82
Total Different Source Types	15

Table 3 Data Source Types

Breach Disclosures	Spam Activity

Block Lists	Vulnerable Hosts
Configuration Parameters	Spyware
Compromised Hosts	Whitelists
Malicious Activity	Email viruses
Malware Servers	Multi-type
Reputation	Phishing
Suspicious Activity	User Behavior

Of the 97 data sources identified, 82 are on "Active Collection" meaning there is a method for obtaining the data source and that its collection is automated. The high degree of automation helps to satisfy the methodology objective for adoption of techniques that are principally automated.

Table 2 lists the 6 collections methods employed for data acquisition with the "Unknown" category meaning that the sources are identified but the method and ability to collect that data source has yet be determined. The method Instances are the number of data sources that are collected using that particular method. For example, 32 of the sources are collected using the network file transfer and synchronization tool rsync (http://samba.anu.edu.au/rsync/).

Table 2 Data Collection Methods

Methods	Instances	Methods	Instances
WGET	35	WHOIS	1
RSYNC	32	HTTP GET	1
API	13	UNKNOWN	9
MANUAL	6		

A collection processing infrastructure 50, configured to build and validate composite security ratings, is shown in Fig. 2. A plurality of different clouds represents different network segments. Rated Entity clouds 52 are organizations for which the system 10 generates a rating. Those entities include an entity perimeter or boundary, indicated by the firewall that connects to the Internet. Services clouds 54 provide data or reports on observed activity from a rated entity 52. An example of a report from a Service 54 could be a list of hosts that have been participating in malicious activity. Services use Sensor networks 56 to

observe the behavior of entities. For example, a sensor could observe SPAM messages sent from a rated entity network 52 to the Internet 58.

Entity Mapping

There is no single central repository that holds information about the IP address allocation. Determining the correct and complete IP address space owned by a given entity improves the reliability and robustness of a rating.

In general, Regional Internet Registries (RIRs) manage the allocation and registration of Internet number resources (IP Addresses, Autonomous System Numbers, etc.) within a particular region of the world. There are five RIRs - ARIN for North America, AfriNIC for Africa, APNIC for Asia Pacific, RIPE for Europe, Middle East, Central Asia, and LACNIC for Latin America.

The RIRs allocate the address space to service providers, corporations, universities, etc. The RIRs provide various interfaces that enable queries of the RIR to determine who owns a given IP address. It is also possible to query the database by an entity name and get a list of IP addresses allocated to that entity. Despite lack of standardization of entity names in the RIR databases, well chosen queries can result in a very high coverage of addresses owned by an entity.

Another problem is that RIRs often allocate large chunks of addresses to Internet Service Providers (ISPs) who go on to allocate smaller address spaces to their customers. ISPs are under no obligation to report this data back to anyone. Most small companies contract with their local ISP for Internet access and don't obtain addresses from RIRs.

These problems are addressed by the entity ownership collection system 14 being configured to execute various heuristic processes including the following non-limiting list of examples:

1. Using the 'dig' (http://linux.die.net/man/1/dig) tool to determine any IP information published by an entity. The dig tool takes the domain name of the entity as an argument. For example, execution of 'dig a.com ANY' returns all IP information published by the entity a.com.

2. Use the IP addresses and domain names published to find ranges of IP addresses actually used. ISPs almost always allocate addresses in size of powers of 2 (2, 4, 8 etc.). Knowing one IP address allows probing around that space. The 'whois'

(http://linux.die.net/man/1/whois) tool can be used to determine ownership of neighborhood addresses.

3. Even if the entity does not publish any IP information that can be retrieved through dig, most entities have servers whose names may be guessed. Mail servers for the domain a.com often have the name mail.a.com, SMTP servers tend to be smtp.a.com, FTP servers tend to be ftp.a.com etc. Using a tool like nslookup, the entity ownership collection system 14 can verify if any of these common names are in use by the entity.

4. If an IP address is found, the system 14 is configured to probe around the address (such as in step 2) to determine any addresses in the neighborhood owned by that entity.

5. Searching around the website of the company often gives a hint of other servers hosted by the company (ex: reports.a.com) which can be used as a starting point for search.

Rating Methodology

Organizational security risk may be measured along two vectors: vulnerability and resilience. An entity's vulnerability is defined as its "physical, technical, organizational, and cultural states," which can be exploited to create a security breach. An entity's resilience is defined to be its ability to recover from a security breach.

The system 10 uses the concepts of vulnerability and resilience by examining externally observable proxies for them. An example proxy for entity vulnerability is the number of entity-owned IP addresses, which are reported to be malicious. The higher the number of reports the more likely the entity was vulnerable and had been compromised. Resilience is inversely proportional to the duration of detected malicious activity. The shorter the duration of the malicious activity, the higher level of resilience the entity demonstrates as it can quickly identify and remove malicious infections.

To compute the ratings for an entity, the system 10 aggregates all of the data collected pertaining to the IT assets owned by that organization, such as the IP addresses controlled by the entity and the associated activity of those IP addresses. The types of activities depend on the types of data. The data sources may include false positives and the system 10 is configured to account for those uncertainties.

To determine quality metrics for IP address based assets, every IP address is uniquely mapped to an entity. Processing the data from a data source yields a list of IPs for each organization that has demonstrated suspicious or malicious behavior. The processing

steps are as follows:

1. For each IP address, determine a security quality metric called "badness".
2. Badness is a number between 0 and 1 that corresponds to the extent and duration of malicious activity that was reported.
3. For each data source in which the IP address is reported, determine a data source specific badness score for that IP.
4. Consolidate the badness score for a given IP across all data sources by cross validating data to determine the aggregate Badness for that IP.
5. Aggregate the badness scores of IPs from an entity to determine the entity's IP asset based security quality metric.

The ratings processing system 30 is configured to account for differences in data sources and types. Given each data source's potentially unique view of an entity, there is not a universal technique that treated them all the same way. Data source specific modeling techniques, for example, were developed for 11 of the 97 data sources in experimental trials in order to demonstrate feasibility and validate the approach. The data sources incorporated accounted for five different data source types: Block Lists, Suspicious Activity, Malicious Servers, Compromised Hosts, and Spamming.

The following two sections give detailed examples of modeling techniques developed for calculating IP address badness for two different data sources that are representative of the data collected.

One of the data sources is a daily updated list of IP addresses that were reported by volunteer hosts from across the Internet. IP Addresses are reported in this data source if they have communicated with hosts that do not expect any inbound communication from them. It lists many more IP addresses on a given day compared with the other data sources and therefore, provides a significant amount of information contained only in this data source. However, this data source has a high incidence of false positives, where a false positive is an unwarranted report due to an incorrectly configured reporting host (i.e., the target) or a listing of an incorrect IP address due to backscatter.

False positives are accounted for by identifying events – where an event is defined as persistent, reported activity on a single IP address within a time period. For each event, heuristics are applied to determine the average intensity for the event. The intensity of an IP address on a given day is a measure of the confidence that malicious activity originated

from the IP address on that day.

For the case where an event spans multiple days, the IP address is generally reported on each day in the event. However, if an IP address is listed on one day but not the next, this omission does not necessarily signify that the host has stopped its malicious behavior; rather, it could be that the host was offline for the day. For example, many corporate hosts are offline for weekends and holidays. Thus, an event is allowed to have short inactive periods, or days without any reports on the IP address. To generate the IP address quality metric, a maximum inactive period of three days is used.

The intensity of an IP address for a given day is calculated dynamically and increases both with the number of reporting targets as well as the duration of the event. Reports with a larger number of targets have larger intensities. This is because false positives due to mis-configured hosts are less likely to have occurred when multiple targets report the same IP address on the same day. Likewise, reports that belong to a persistent event have larger intensities, since persistent reports also signal the legitimacy of the malicious activity on the IP address.

The intensity, I(s) is calculated as follows:

$$I(s) = \begin{cases} 0.1, & \text{if } s < 2 \\ 0.01e^{\frac{\ln(99)(s-1)}{4}}, & \text{if } 2 \le s < 5 \\ 0.8 - 0.7e^{-\frac{\ln(80)(s-5)}{4}}, & \text{if } s \le 5 \end{cases}$$

where s is the number of hosts reporting the IP address. Thus, the average intensity, I_{avg}, of an event is the average of the intensities calculated per active day (a day with reports) and is determined as follows:

$$I_{avg} = \frac{I(s)}{T} + \frac{A \cdot I_{prev}}{T},$$

where T is the list time, A is T minus the number of days since the last update, and I_{prev} is the average intensity at the last update. The Badness, B_{IP}, of an IP address is derived from the intensity and duration of the events for the IP, such that recent events are weighted heavier than historical events and is calculated as follows:

$$B_{IP} = min(1, \frac{I_{avg}(1-e^{-0.02})}{1-e^{-0.12}} \sum_{t_l}^{t_n} e^{-0.02}),$$

where t_l and t_n denote time lapsed from the end and beginning of an event, respectively; and

the average intensity is readjusted if the persistence surpasses a threshold.

The second data source example is a host block list that lists IP addresses that have been compromised. Based on an analysis of the data sources collection methods, the block list is considered very reliable in the sense that a listing implies that malicious activity originated from the listed address. This block list removes IP addresses from the list if no malicious activity is detected for a small window of time. Because of the high confidence in the data source's accuracy, any IP address on the block list is assigned a raw Badness of 0.8.

Once an IP address is delisted and is no longer on the block list, its Badness decays exponentially with respect to the time since it was last listed. Thus, the Badness is:

$$B_{ip} = 0.8e^{-\frac{\ln(2)T}{182.625}},$$

where T is the time in days since the last listing. This decay rate corresponds to a half-life of six months.

Various other data sources are handled similarly but the raw score is based on the confidence in the data source's collection methods. Other data sources track CIDR blocks as opposed to individual IP addresses, and so the Badness assigned to a listing on these lists are weighted by the CIDR block size as follows:

$$B_{ip} = 0.8We^{-\frac{\ln(2)T}{182.625}},$$

where W is the natural log of the block size.

The total IP space badness of an entity is an aggregation of the badness of the entity's individual IP addresses and/or CIDR blocks. In the simplest model where all data sources are IP address based, the entity badness is the total badness of the IP addresses owned by the entity. To normalize ratings across entities of different sizes, the entity's network size defined as the number of active IP addresses owned by the entity is used:

$$B_{entity} = \frac{\sum_{IP \in entity} B_{ip}}{\ln(N)},$$

where N denotes the network size. Normalizing avoids penalizing of smaller entities allowing fair comparisons between entities of differing sizes.

Enhancements to the Ratings Methodology

The system 10 may also include expanded the methodology to support additional

and different types of data sources. It could identify data sources that indicate different levels of IT sophistication - such information is a measure of the level of IT practice maturity.

Entity normalization methods can also account for differences in entity size beyond network size. For example, the use of other normalization methods such as number of employees may help produce more robust normalizations under certain circumstances.

Also, statistical properties of the model's internal parameters may be analyzed and adjust based on the findings. For example, certain inputs or features may be disproportionately skewing the ratings and such inputs or features may be modulated through weighting factors.

The composite security rating described above measured, amongst other things, how much, to what extent, and how recently malicious activity was detected on an entity's cumulative IP space. The score could also be adapted to show a level of confidence. For example, a failure to detect malicious activity on an entity's IP space does not necessarily imply non-malicious behavior. Rather, the data sources may lack coverage on the entity's IP space. By outputting a range as opposed to a number, the system 10 is able to convey its confidence in a rating where a larger range necessarily implies a lower confidence, and a smaller range necessarily implies a higher confidence.

Such a range could be computed from a mean score and a confidence range, which could be determined from a developed discrete choice model. Features such as the Badness scores from each data source could help determine the mean score. Features such as redundancy between data sources and network size could also help determine the confidence range.

Entity mapping may also be improved through other data sources and functions. Data sharing relationships with Internet Service Providers might provide additional data on security outcomes and practices at entity computer systems. Also, consumers of the scoring reports may already have partner-mapping data through the nature of their relationship with the entity or may be able to request the information.

Entity mapping may also be facilitated by persistent updates of the heuristics, such as updating prefixes from BGP announcements and data from Regional Internet Registries.

Data storage used by the system 10 may be improved to minimize the disk space required while supporting rapid inclusion of new entity ratings. For example, high-speed

data access layers may be created for daily ratings computation.

Speed and scale can be accomplished through distributed or parallel processing on different systems. A distributed data source query interface may be implemented so that massive and expensive centralized data storage is not required.

The system 10 may also be configured to develop and evaluate predictive capabilities of information security ratings and incorporate them into the rating methodology.

The ability to demonstrate predictability has a dependency on data reliability. For example, improving coverage of malicious events improves data reliability. Statistical evaluations may be used to disambiguate strong entity performance (e.g., no malicious activity) from low coverage (e.g., lack of information on the malicious activity). These evaluations can then be used in the rating methodology.

Statistical evaluations of data coverage may include a data accuracy assessment wherein levels of coverage assurance associated with a particular adopted data source are determined. Also, observations across data sources may be compared to determine data sources of high probability or low probability of coverage for a given entity.

Predictive modeling may include determination of entity historical trends to display and predict future performance. Regression and machine learning based models may be developed to predict information security performance. Models may be evaluated and further developed for predictive capability through a series of prediction experiments.

Also, the data source features may be analyzed for correlations of high and low performance. For example, entities with behavior "X" tend to perform well and entities that demonstrate property "Y" tend to behave poorly.

Use of External and Internal Security Data

The system 10 may also include internally derived security assessments. For example, such a score computation is shown in Fig. 3. The final score S_{Total} has two components, the Internal score and the External score.

The Internal score, S_{int}, is derived from data collected and observed from inside the enterprise. Data sources that provide inputs to the internal scoring function could include, but are not limited to, the following:

- Vulnerability scans
- Firewall Rules
- Incident Reports
- Configurations
- Software inventory
- Policies
- Controls
- User Behavior

The features from each of the data sources are extracted to create a feature vector. This feature vector is $X_{\text{int}} = \{InternalFeatures\}$ in the "Internal Source Score," as shown in Fig. 3. Features include, but are not limited to, derived metrics from the data sources (e.g., the number of remotely exploitable vulnerabilities from outside the entity, the number of incidents, or the number of vulnerable versions of software).

Each feature x_i in X_{INT} has a corresponding transformation function $f_{i(x_i)}(x_i)$ that performs a normalization transformation such that the resultants can be summed.

Each feature x_i in X_{INT} also has corresponding weight ω_i such that different weights can be placed on the resultant feature transformation where the sum of the weights equal is unity $\sum_{i=1}^{n} \omega_i = 1$. The sum of the transformed and weighted feature vector is computed by summing each resultant for each of the features $\sum_{i=1, x \in X_{\text{int}}}^{n} \omega_i f_{i(x_i)}(x_i)$.

The final score S_{int} is the summation normalized by a set of normalization factors given as $f_{i(x_\alpha)}(x_\alpha) + f_{i(x_\beta)}(x_\beta)$ where each normalization factor $x_\alpha, x_\beta, \ldots$ also has a factor normalization transformation function.

The computation of the Internal Score is given as: $$S_{\text{int}} = \frac{\sum_{i=1, x \in X_{\text{int}}}^{n} \omega_i f_{i(x_i)}(x_i)}{f_{i(x_\alpha)}(x_\alpha) + f_{i(x_\beta)}(x_\beta)}$$

The External Score is the combination of the Public Sources Score (S_{pub}) and the Commercial Sources (S_{com}). S_{pub} and S_{com} are derived using the same heuristic combinatorial functions as the Internal Score. However, the input data sources, weights, transformation functions and normalization factors are different.

S_{pub} and S_{com} have their own feature vectors $X_{pub} = \{PublicFeatures\}$ and $X_{com} = \{CommercialFeatures\}$ based on the data input sources used.

Data sources in X_{pub} that provide inputs to the S_{pub} score could include but are not limited to the following:

- Industry reports
- Internet monitoring web sites that publish reports (ex: *www.malwareurl.com*)
- News articles
- Court records

Data sources in X_{com} that provide inputs to the S_{com} score could include but are not limited to the following:

- Company proprietary data collected during operations
- Renesys
- Arbor Networks
- Business intelligence bought from corporations and services
- User Behavior

With the Internal and External Scores computed, the final total score is computed and the weighted sum of the three: $S_{Total} = \omega_{int} S_{int} + \omega_{pub} S_{pub} + \omega_{com} S_{com}$

It is possible that the algorithm does not have the same inputs for all entities. More information may be available for some entities compared to other entities. Given this, each data source is assigned a normalized confidence level based on how much they contribute to the computation of the enterprise score. Depending on the actual data that went into rating the company, the confidence level is assigned as a sum of the confidence levels associated with the data sources. The confidence level can be used to assign a range of scores for an enterprise. For instance, if an enterprise is rated as 750 with a confidence level of 0.8, the

entity's actual score is reported as (750 – (1 – 0.8) * 100, 750) = (730 – 750). An entity's score is deemed to be unavailable if the confidence level is below a minimum threshold of 0.5.

It should be noted that the S_{int} may be zero due to a lack of available information or permission, wherein S_{total} becomes characteristic only of externally observable characteristics. Also, characteristics for the calculation can be used in conjunction, or vice versa, with functions and aspects of the remaining systems described hereinabove and below.

Distributed System

Referring now to Fig. 4, a schematic diagram of a central server 500, or similar network entity, configured to implement a system for creating a composite security score is provided. As used herein, the designation "central" merely serves to describe the common functionality the server provides for multiple clients or other computing devices and does not require or infer any centralized positioning of the server relative to other computing devices. As may be understood from Fig. 4, the central server 500 may include a processor 510 that communicates with other elements within the central server 500 via a system interface or bus 545. Also included in the central server 500 may be a display device/input device 520 for receiving and displaying data. This display device/input device 520 may be, for example, a keyboard or pointing device that is used in combination with a monitor. The central server 500 may further include memory 505, which may include both read only memory (ROM) 535 and random access memory (RAM) 530. The server's ROM 535 may be used to store a basic input/output system 540 (BIOS), containing the basic routines that help to transfer information across the one or more networks.

In addition, the central server 500 may include at least one storage device 515, such as a hard disk drive, a floppy disk drive, a CD Rom drive, or optical disk drive, for storing information on various computer-readable media, such as a hard disk, a removable magnetic disk, or a CD-ROM disk. As will be appreciated by one of ordinary skill in the art, each of these storage devices 515 may be connected to the system bus 545 by an appropriate interface. The storage devices 515 and their associated computer-readable media may provide nonvolatile storage for a central server. It is important to note that the computer-readable media described above could be replaced by any other type of computer-readable

media known in the art. Such media include, for example, magnetic cassettes, flash memory cards and digital video disks.

A number of program modules may be stored by the various storage devices and within RAM 530. Such program modules may include an operating system 550 and a plurality of one or more (N) modules 560. The modules 560 may control certain aspects of the operation of the central server 500, with the assistance of the processor 510 and the operating system 550. For example, the modules may perform the functions described above and illustrated by the figures and other materials disclosed herein, such as collecting security characterizations 570, generating a composite rating 580, determining a trend 590, reporting the ratings 600, IP mapping 610, determining a badness quality metric 620, attenuating a raw score 630, correlating with statistical outcomes 640, determining a confidence range 650, predicting future performance 660 and determining an accuracy 670.

The flowchart and block diagrams in the figures illustrate the architecture, functionality, and operation of possible implementations of systems, methods and computer program products according to various embodiments of the present invention. In this regard, each block in the flowchart or block diagrams may represent a module, segment, or portion of code, which comprises one or more executable instructions for implementing the specified logical function(s). It should also be noted that, in some alternative implementations, the functions noted in the block may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams and/or flowchart illustration, and combinations of blocks in the block diagrams and/or flowchart illustration, can be implemented by special purpose hardware-based systems that perform the specified functions or acts, or combinations of special purpose hardware and computer instructions.

The corresponding structures, materials, acts, and equivalents of all means or step plus function elements in the claims below are intended to include any structure, material, or act for performing the function in combination with other claimed elements as specifically claimed. The description of the present invention has been presented for purposes of illustration and description, but is not intended to be exhaustive or limited to the invention in the form disclosed. Many modifications and variations will be apparent to

those of ordinary skill in the art without departing from the scope and spirit of the invention. The embodiment was chosen and described in order to best explain the principles of the invention and the practical application, and to enable others of ordinary skill in the art to understand the invention for various embodiments with various modifications as are suited to the particular use contemplated.

CLAIMS

1. A method of evaluating information security of a third party computer system, the method comprising:

collecting at least two security characterizations of the third party computer system;

generating a composite security rating using the at least two security characterizations;

wherein the two security characterizations are derived from externally observable characteristics of the third party computer system.

2. A method of Claim 1, wherein each of the security characterizations is from an associated one of a plurality of independent entities.

3. A method of Claim 2, wherein the independent entities include commercial data sources.

4. A method of Claim 2, wherein the security characterizations include at least two data types.

5. A method of Claim 4, wherein the data types include at least one of breach disclosures, block lists, configuration parameters, malware servers, reputation, suspicious activity, spyware, white lists, compromised hosts, malicious activity, spam activity, vulnerable hosts, phishing, or e-mail viruses.

6. A method of Claim 1, wherein the security characterizations are derived without permission of the third party computer system.

7. A method of Claim 1, wherein the externally observable characteristics evidence internal security controls.

8. A method of Claim 1, wherein the externally observable characteristics are outcomes.

9. A method of Claim 1, wherein the externally observable characteristics evidence operational execution of security measures of the third party computer system.

10. A method of Claim 1, wherein the externally observable characteristics include serving of malicious code.

11. A method of Claim 1, wherein the externally observable characteristics include communications with known attacker controlled networks.

12. A method of Claim 1, wherein collecting the data and generating the ratings are repeated to generate a series of ratings.

Formatted: Line spacing: 1.5 lines

13. A method of Claim 11, further comprising determining a trend from the series of ratings.

14. A method of Claim 12, further comprising reporting the ratings.

15. A method of Claim 13, wherein reporting includes reporting a warning based on a change in the ratings.

16. A method of Claim 14, wherein reporting includes posting the ratings and warning to a web portal.

17. A method of Claim 1, wherein collecting the security characterizations includes using tools such as WGET, RSYNC or proprietary and manual methods..

18. A method of Claim 1, further comprising mapping the third party computer system to an IP space and using the IP space for collecting the security characterizations.

19. A method of Claim 18, wherein mapping includes querying a regional internet registry.

20. A method of Claim 19, wherein querying includes submitting an entity name.

21. A method of Claim 20, wherein submitting the entity name includes submitting spelling variations of the entity name.

22. A method of Claim 18, wherein mapping includes using a domain name associated with the third party computer system.

23. A method of Claim 22, wherein mapping includes using a dig tool on the domain name to determine a published IP address.

24. A method of Claim 23, wherein mapping includes probing addresses around the published IP address.

25. A method of Claim 24, wherein probing includes probing addresses in powers of 2 around the published IP address.

26. A method of Claim 22, wherein mapping includes adapting the domain name with server naming conventions.

27. A method of Claim 26, wherein mapping includes using nslookup to verify an IP address associated with the domain name.

28. A method of Claim 1, wherein generating the composite security rating includes assessing a vulnerability and resilience of the third party computer systems.

29. A method of Claim 28, wherein vulnerability includes a number of IP addresses with malicious behavior.

30. A method of Claim 28, wherein resilience is inversely proportional to a duration of malicious behavior.

31. A method of Claim 18, wherein the IP space includes a plurality of IP addresses.

32. A method of Claim 31, further comprising determining at least one badness score for each of the IP addresses.

33. A method of Claim 32, wherein the badness score corresponds to an intensity and duration of malicious activity determined from one of the security characterizations.

34. A method of Claim 33, wherein generating the composite security rating includes aggregating a plurality of badness scores.

35. A method of Claim 34, wherein generating the composite security rating includes aggregating the IP addresses associated with the third party computer system.

36. A method of Claim 31, wherein determining the badness score includes adjusting for false positives in the security characterizations.

37. A method of Claim 36, wherein adjusting for false positives includes determining occurrence of an event which includes persistent, reported activity on one of the IP addresses for a predetermined period of time.

38. A method of Claim 37, wherein adjusting for false positives includes determining an intensity of the IP address for the predetermined period of time.

39. A method of Claim 38, wherein the predetermined period of time is at least one day.

40. A method of Claim 38, wherein the predetermined period of time accounts for inactive periods.

41. A method of Claim 40, wherein the maximum inactive period is 3 days.

42. A method of Claim 38, wherein determining an intensity includes increasing intensity in proportion to a number of reporting targets from the security characterizations.

43. A method of Claim 33, wherein determining the badness score includes weighting recent events heavier than older events.

44. A method of Claim 32, wherein determining the badness score includes assigning a raw score for each of the IP addresses appearing on a block list of one of the security characterizations.

45. A method of Claim 44, wherein the block list does not delist the IP address until requested.

46. A method of Claim 45, further comprising attenuating the raw score after delisting of the IP address.

47. A method of Claim 46, wherein attenuating is at an exponential decay.

48. A method of Claim 32, wherein determining the badness score includes generating a raw score in proportion to a CIDR block size.

49. A method of Claim 35, wherein generating the composite security rating includes normalizing the aggregate of the plurality of badness scores.

50. A method of Claim 49, wherein normalizing includes normalizing based on at least one of network size or number of employees.

51. A method of Claim 32, wherein the security characterizations include non-negative information.

52. A method of Claim 1, further comprising correlating the composite security score with statistical outcomes and adjusting the step of generating based on the statistical outcomes.

53. A method of Claim 1, further comprising determining a confidence range of the composite security score.

54. A method of Claim 53, wherein the confidence range is based on redundancy of the security characterizations.

55. A method of Claim 54, wherein the confidence range is based on a size of the third party computer system.

56. A method of Claim 1, further comprising predicting future information security performance of the third party computer system using the security characterizations.

57. A method of Claim 1, further comprising determining an accuracy of each of the security characterizations.

58. A method of Claim 57, wherein determining the accuracy includes determining a level of coverage of the third party computer system by the security characterizations.

59. A system for evaluating information security of third party computer systems, the system comprising:

a data collection module configured to receive at least two security characterizations, each of the security characterizations describing a security outcome associated with one of the third party computer systems; and

a scoring module connected in communication with the data collection module and configured to use the security characterizations to generate a composite security score for the associated third party computer system;

wherein the security outcome is derived from external investigation of the associated third party computer system.

60. A system of Claim 59, wherein each of the security characterizations is from an associated one of a plurality of independent entities.

Formatted: Indent: Left: 0"

61. A system of Claim 60, wherein the independent entities include commercial data sources.

62. A system of Claim 60, wherein the security characterizations include at least two data types.

63. A system of Claim 62, wherein the data types include at least one of breach disclosures, block lists, configuration, malware servers, reputation, suspicious activity, spyware, white lists, compromised hosts, malicious activity, spam activity, vulnerable hosts, phishing, or e-mail viruses.

Formatted: Indent: Left: 0", Line spacing: 1.5 lines

64. A system of Claim 59, wherein the security characterizations are derived without permission of the third party computer system.

65. A system of Claim 59, wherein the externally observable characteristics evidence internal security controls.

66. A system of Claim 59, wherein the externally observable characteristics are outcomes.

67. A system of Claim 59, wherein the externally observable characteristics

evidence operational execution of security measures of the third party computer system.

68. A system of Claim 59, wherein the externally observable characteristics include serving of malicious code.

69. A system of Claim 59, wherein the externally observable characteristics include communications with known attacker controlled networks.

70. A system of Claim 59, wherein the scoring module is configured to generate a series of ratings.

71. A system of Claim 70, further comprising a trend module configured to determine a trend from the series of ratings.

72. A system of Claim 71, further comprising a reporting module configured to report the ratings.

73. A system of Claim 72, wherein the reporting module is configured to report a warning based on a change in the ratings.

74. A system of Claim 74, wherein the reporting module is configured to post the ratings and warning to a web portal.

75. A system of Claim 59, wherein the data collection module is configured to collect the security characterizations includes using tools such as WGET, RSYNC or proprietary and manual methods.

76. A system of Claim 59, further comprising a mapping module configured to map the third party computer system to an IP space and use the IP space for collecting the security characterizations.

77. A system of Claim 76, wherein the mapping module is further configured to submit a query a regional internet registry.

78. A system of Claim 77, wherein the query includes an entity name.

79. A system of Claim 78, wherein the query includes spelling variations of the entity name.

80. A system of Claim 76, wherein the mapping module is configured to obtain a domain name associated with the third party computer system.

81. A system of Claim 80, wherein the mapping module is configured to use a dig tool on the domain name.

82. A system of Claim 81, wherein the mapping module is configured to probe addresses around the published IP address.

83. A system of Claim 82, wherein the mapping module is configured to probe addresses in powers of 2 around the published IP address.

84. A system of Claim 80, wherein the mapping module is configured to adapt the domain name with server naming conventions.

85. A system of Claim 84, wherein the mapping module is configured to use nslookup to verify an IP address associated with the domain name.

86. A system of Claim 59, the scoring module is configured to assess a vulnerability and resilience of the third party computer systems.

87. A system of Claim 86, wherein the vulnerability includes a number of IP addresses with malicious behavior.

88. A system of Claim 86, wherein the resilience is inversely proportional to a duration of the malicious behavior.

89. A system of Claim 76, wherein the IP space includes a plurality of IP addresses.

90. A system of Claim 89, further comprising a badness module configured to determine a badness score for each of the IP addresses.

91. A system of Claim 90, wherein the badness score corresponds to an intensity and duration of malicious activity determined from one of the security characterizations.

92. A system of Claim 91, wherein the scoring module is configured to aggregate a plurality of the badness scores.

93. A system of Claim 92, wherein the scoring module is further configured to aggregate the IP addresses associated with the third party computer system.

94. A system of Claim 90, wherein the badness module is further configured to adjust for false positives in the security characterizations.

95. A system of Claim 94, wherein the badness module is further configured to determine an occurrence of an event which includes persistent, reported activity on one of the IP addresses for a predetermined period of time.

96. A system of Claim 95, wherein the badness module is configured to determine an intensity of the IP address for the predetermined period of time.

97. A system of Claim 96, wherein the predetermined period of time is a day.

98. A system of Claim 96, wherein the predetermined period of time accounts for inactive periods.

99. A system of Claim 98, wherein the maximum inactive period is a configurable number.

100. A system of Claim 96, wherein the intensity is in proportion to a number of reporting targets from the security characterizations.

101. A system of Claim 91, wherein the badness module is configured to weight recent events heavier than older events.

102. A system of Claim 90, wherein the badness module is configured to assign a flat score for each of the IP addresses appearing on a block list of one of the security characterizations.

103. A system of Claim 102, wherein the block list does not delist the IP address until requested.

104. A system of Claim 103, wherein the badness module is configured to attenuate the flat score after delisting of the IP address.

105. A system of Claim 104, wherein the badness module is configured to

attenuate the flat score at an exponential decay.

106. A system of Claim 90, wherein the badness module is configured to determine the badness score by generating a flat score in proportion to a CIDR block size.

107. A system of Claim 93, wherein the scoring module is configured to normalize the aggregate of the plurality of badness scores.

108. A system of Claim 107, wherein the scoring module is configured to normalize based on at least one of network size or number of employees.

109. A system of Claim 90, wherein the security characterizations include non-negative information.

110. A system of Claim 59, further comprising an accuracy module configured to correlate the composite security score with statistical outcomes and adjust the scoring module to account for the correlation.

111. A system of Claim 59, further comprising a confidence module configured to determine a confidence range of the composite security score.

112. A system of Claim 111, wherein the confidence range is based on redundancy of the security characterizations.

113. A system of Claim 112, wherein the confidence range is based on a size of the third party computer system.

114. A system of Claim 59, further comprising a predictive module configured to predict future information security performance of the third party computer system using the security characterizations.

115. A system of Claim 59, further comprising an accuracy module configured to determine an accuracy of each of the security characterizations.

116. A system of Claim 115, wherein the accuracy module is configured to determine a level of coverage of the third party security system using the security characterizations.

117. A method of evaluating information security of a third party computer system, the method comprising:

collecting at least one security characterization of the third party computer system;

generating a composite security score using the at least one security characterization;

wherein the at least one security characterization is derived from externally observable characteristics of the third party computer system; and

wherein the composite security score has a relatively high likelihood of corresponding to an internal audit score.

Formatted: Line spacing: 1.5 lines

118. A method of Claim 117, further comprising one or more of a plurality of the methods of Claims 2-58.

Formatted: Indent: Left: 0", Line spacing: 1.5 lines

119. A system for evaluating information security of third party computer systems, the system comprising:

a data collection module configured to receive at least one security characterization, the security characterization describing a security outcome associated with one of the third party computer systems; and

a scoring module connected in communication with the data collection module and configured to use the security characterization to generate a composite security score for the associated third party computer system;

wherein the security outcome of the security characterization is derived from external investigation of the associated third party computer system;

wherein the composite score has a relatively high likelihood of corresponding to an internal audit score.

120. A system of Claim 119, further comprising one or more of a plurality of the systems of Claims 59-116.

Formatted: Indent: Left: 0"

ABSTRACT

A method and system for creating a composite security rating from security characterization data of a third party computer system. The security characterization data is derived from externally observable characteristics of the third party computer system. Advantageously, the composite security score has a relatively high likelihood of corresponding to an internal audit score despite use of externally observable security characteristics. Also, the method and system may include use of multiple security characterizations all solely derived from externally observable characteristics of the third party computer system.

Electronic Patent Application Fee Transmittal

Application Number:	13240572
Filing Date:	22-Sep-2011
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Filer:	Gregory J. Carlin/Cheryl McKinzie
Attorney Docket Number:	10131-002US1

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Late filing fee for oath or declaration	2051	1	65	65
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 1 month with $0 paid	2251	1	75	75
Miscellaneous:				
			Total in USD ($)	**140**

Electronic Acknowledgement Receipt

EFS ID:	11623843
Application Number:	13240572
International Application Number:	
Confirmation Number:	2423
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Customer Number:	96039
Filer:	Gregory J. Carlin/Cheryl McKinzie
Filer Authorized By:	Gregory J. Carlin
Attorney Docket Number:	10131-002US1
Receipt Date:	15-DEC-2011
Filing Date:	22-SEP-2011
Time Stamp:	11:35:32
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		10131_002US1CleanV.pdf	351516 14c2f2dc9292c1c078ba93d7bdd65fb61c7b4fe3	yes	34

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Specification	1	23
	Claims	24	33
	Abstract	34	34

Warnings:					
Information:					
2	Oath or Declaration filed	10131_002US1Dec.pdf	221696 71ade98dbbd1f1c0e70144d667d3afc17c21c735	no	5
Warnings:					
Information:					
3	Drawings-only black and white line drawings	10131_002US1Drawings.pdf	216788 1f57b545429e5d47731e8921f2c3c75e06bd7717	no	3
Warnings:					
Information:					
4	Extension of Time	10131_002US1EOT.pdf	49395 4f3ca1ad4b04a3078cc7574f9680531b11937fc5	no	1
Warnings:					
Information:					
5		10131_002US1Prem.pdf	93408 65ef36cab1f6dd21c8c00a56a076cdb8109c0d6e	yes	14

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Preliminary Amendment	1	1
	Claims	2	13
	Applicant Arguments/Remarks Made in an Amendment	14	14

Warnings:					
Information:					
6	Applicant Response to Pre-Exam Formalities Notice	10131_002US1ResMarkedupVersion.pdf	289735 960312df3e0eca3a4e71bf2e0a7da5af6b4eff27	no	36
Warnings:					
Information:					

7	Fee Worksheet (SB06)	fee-info.pdf	32125 54a78be6af400d7935c76f5651e6ff588d1876d1	no	2

Warnings:	
Information:	
Total Files Size (in bytes):	1254663

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

CLAIMS

1. A method of evaluating information security of a third party computer system, the method comprising:

collecting at least two security characterizations of the third party computer system;

generating a composite security rating using the at least two security characterizations;

wherein the two security characterizations are derived from externally observable characteristics of the third party computer system.

2. A method of Claim 1, wherein each of the security characterizations is from an associated one of a plurality of independent entities.

3. A method of Claim 2, wherein the independent entities include commercial data sources.

4. A method of Claim 2, wherein the security characterizations include at least two data types.

5. A method of Claim 4, wherein the data types include at least one of breach disclosures, block lists, configuration parameters, malware servers, reputation, suspicious activity, spyware, white lists, compromised hosts, malicious activity, spam activity, vulnerable hosts, phishing, or e-mail viruses.

6. A method of Claim 1, wherein the security characterizations are derived without permission of the third party computer system.

7. A method of Claim 1, wherein the externally observable characteristics evidence internal security controls.

8. A method of Claim 1, wherein the externally observable characteristics are outcomes.

9. A method of Claim 1, wherein the externally observable characteristics evidence operational execution of security measures of the third party computer system.

10. A method of Claim 1, wherein the externally observable characteristics include serving of malicious code.

11. A method of Claim 1, wherein the externally observable characteristics include communications with known attacker controlled networks.

12. A method of Claim 1, wherein collecting the data and generating the ratings are repeated to generate a series of ratings.

13. A method of Claim 11, further comprising determining a trend from the series of ratings.

14. A method of Claim 12, further comprising reporting the ratings.

15. A method of Claim 13, wherein reporting includes reporting a warning based on a change in the ratings.

16. A method of Claim 14, wherein reporting includes posting the ratings and warning to a web portal.

17. A method of Claim 1, wherein collecting the security characterizations includes using tools such as WGET, RSYNC or proprietary and manual methods..

18. A method of Claim 1, further comprising mapping the third party computer system to an IP space and using the IP space for collecting the security characterizations.

19. A method of Claim 18, wherein mapping includes querying a regional internet registry.

20. A method of Claim 19, wherein querying includes submitting an entity name.

21. A method of Claim 20, wherein submitting the entity name includes submitting spelling variations of the entity name.

22. A method of Claim 18, wherein mapping includes using a domain name associated with the third party computer system.

23. A method of Claim 22, wherein mapping includes using a dig tool on the domain name to determine a published IP address.

24. A method of Claim 23, wherein mapping includes probing addresses around the published IP address.

25. A method of Claim 24, wherein probing includes probing addresses in powers of 2 around the published IP address.

26. A method of Claim 22, wherein mapping includes adapting the domain name with server naming conventions.

27. A method of Claim 26, wherein mapping includes using nslookup to verify an IP address associated with the domain name.

28. A method of Claim 1, wherein generating the composite security rating includes assessing a vulnerability and resilience of the third party computer systems.

29. A method of Claim 28, wherein vulnerability includes a number of IP addresses with malicious behavior.

30. A method of Claim 28, wherein resilience is inversely proportional to a duration of malicious behavior.

31. A method of Claim 18, wherein the IP space includes a plurality of IP addresses.

32. A method of Claim 31, further comprising determining at least one badness score for each of the IP addresses.

33. A method of Claim 32, wherein the badness score corresponds to an intensity and duration of malicious activity determined from one of the security characterizations.

34. A method of Claim 33, wherein generating the composite security rating includes aggregating a plurality of badness scores.

35. A method of Claim 34, wherein generating the composite security rating includes aggregating the IP addresses associated with the third party computer system.

36. A method of Claim 31, wherein determining the badness score includes adjusting for false positives in the security characterizations.

37. A method of Claim 36, wherein adjusting for false positives includes determining occurrence of an event which includes persistent, reported activity on one of the IP addresses for a predetermined period of time.

38. A method of Claim 37, wherein adjusting for false positives includes determining an intensity of the IP address for the predetermined period of time.

39. A method of Claim 38, wherein the predetermined period of time is at least one day.

40. A method of Claim 38, wherein the predetermined period of time accounts for inactive periods.

41. A method of Claim 40, wherein the maximum inactive period is 3 days.

42. A method of Claim 38, wherein determining an intensity includes increasing intensity in proportion to a number of reporting targets from the security characterizations.

43. A method of Claim 33, wherein determining the badness score includes weighting recent events heavier than older events.

44. A method of Claim 32, wherein determining the badness score includes assigning a raw score for each of the IP addresses appearing on a block list of one of the security characterizations.

45. A method of Claim 44, wherein the block list does not delist the IP address until requested.

46. A method of Claim 45, further comprising attenuating the raw score after delisting of the IP address.

47. A method of Claim 46, wherein attenuating is at an exponential decay.

48. A method of Claim 32, wherein determining the badness score includes generating a raw score in proportion to a CIDR block size.

49. A method of Claim 35, wherein generating the composite security rating includes normalizing the aggregate of the plurality of badness scores.

50. A method of Claim 49, wherein normalizing includes normalizing based on at least one of network size or number of employees.

51. A method of Claim 32, wherein the security characterizations include non-negative information.

52. A method of Claim 1, further comprising correlating the composite security score with statistical outcomes and adjusting the step of generating based on the statistical outcomes.

53. A method of Claim 1, further comprising determining a confidence range of the composite security score.

54. A method of Claim 53, wherein the confidence range is based on redundancy of the security characterizations.

55. A method of Claim 54, wherein the confidence range is based on a size of the third party computer system.

56. A method of Claim 1, further comprising predicting future information security performance of the third party computer system using the security characterizations.

57. A method of Claim 1, further comprising determining an accuracy of each of the security characterizations.

58. A method of Claim 57, wherein determining the accuracy includes determining a level of coverage of the third party computer system by the security characterizations.

59. A system for evaluating information security of third party computer systems, the system comprising:

a data collection module configured to receive at least two security characterizations, each of the security characterizations describing a security outcome associated with one of the third party computer systems; and

a scoring module connected in communication with the data collection module and configured to use the security characterizations to generate a composite security score for the associated third party computer system;

wherein the security outcome is derived from external investigation of the associated third party computer system.

60. A system of Claim 59, wherein each of the security characterizations is from an associated one of a plurality of independent entities.

61. A system of Claim 60, wherein the independent entities include commercial data sources.

62. A system of Claim 60, wherein the security characterizations include at least two data types.

63. A system of Claim 62, wherein the data types include at least one of breach disclosures, block lists, configuration, malware servers, reputation, suspicious activity, spyware, white lists, compromised hosts, malicious activity, spam activity, vulnerable hosts, phishing, or e-mail viruses.

64. A system of Claim 59, wherein the security characterizations are derived without permission of the third party computer system.

65. A system of Claim 59, wherein the externally observable characteristics evidence internal security controls.

66. A system of Claim 59, wherein the externally observable characteristics are outcomes.

67. A system of Claim 59, wherein the externally observable characteristics

evidence operational execution of security measures of the third party computer system.

68. A system of Claim 59, wherein the externally observable characteristics include serving of malicious code.

69. A system of Claim 59, wherein the externally observable characteristics include communications with known attacker controlled networks.

70. A system of Claim 59, wherein the scoring module is configured to generate a series of ratings.

71. A system of Claim 70, further comprising a trend module configured to determine a trend from the series of ratings.

72. A system of Claim 71, further comprising a reporting module configured to report the ratings.

73. A system of Claim 72, wherein the reporting module is configured to report a warning based on a change in the ratings.

74. A system of Claim 74, wherein the reporting module is configured to post the ratings and warning to a web portal.

75. A system of Claim 59, wherein the data collection module is configured to collect the security characterizations includes using tools such as WGET, RSYNC or proprietary and manual methods.

76. A system of Claim 59, further comprising a mapping module configured to map the third party computer system to an IP space and use the IP space for collecting the security characterizations.

77. A system of Claim 76, wherein the mapping module is further configured to submit a query a regional internet registry.

78. A system of Claim 77, wherein the query includes an entity name.

79. A system of Claim 78, wherein the query includes spelling variations of the entity name.

80. A system of Claim 76, wherein the mapping module is configured to obtain a domain name associated with the third party computer system.

81. A system of Claim 80, wherein the mapping module is configured to use a dig tool on the domain name.

82. A system of Claim 81, wherein the mapping module is configured to probe addresses around the published IP address.

83. A system of Claim 82, wherein the mapping module is configured to probe addresses in powers of 2 around the published IP address.

84. A system of Claim 80, wherein the mapping module is configured to adapt the domain name with server naming conventions.

85. A system of Claim 84, wherein the mapping module is configured to use nslookup to verify an IP address associated with the domain name.

86. A system of Claim 59, the scoring module is configured to assess a vulnerability and resilience of the third party computer systems.

87. A system of Claim 86, wherein the vulnerability includes a number of IP addresses with malicious behavior.

88. A system of Claim 86, wherein the resilience is inversely proportional to a duration of the malicious behavior.

89. A system of Claim 76, wherein the IP space includes a plurality of IP addresses.

90. A system of Claim 89, further comprising a badness module configured to determine a badness score for each of the IP addresses.

91. A system of Claim 90, wherein the badness score corresponds to an intensity and duration of malicious activity determined from one of the security characterizations.

92. A system of Claim 91, wherein the scoring module is configured to aggregate a plurality of the badness scores.

93. A system of Claim 92, wherein the scoring module is further configured to aggregate the IP addresses associated with the third party computer system.

94. A system of Claim 90, wherein the badness module is further configured to adjust for false positives in the security characterizations.

95. A system of Claim 94, wherein the badness module is further configured to determine an occurrence of an event which includes persistent, reported activity on one of the IP addresses for a predetermined period of time.

96. A system of Claim 95, wherein the badness module is configured to determine an intensity of the IP address for the predetermined period of time.

97. A system of Claim 96, wherein the predetermined period of time is a day.

98. A system of Claim 96, wherein the predetermined period of time accounts for inactive periods.

99. A system of Claim 98, wherein the maximum inactive period is a configurable number.

100. A system of Claim 96, wherein the intensity is in proportion to a number of reporting targets from the security characterizations.

101. A system of Claim 91, wherein the badness module is configured to weight recent events heavier than older events.

102. A system of Claim 90, wherein the badness module is configured to assign a flat score for each of the IP addresses appearing on a block list of one of the security characterizations.

103. A system of Claim 102, wherein the block list does not delist the IP address until requested.

104. A system of Claim 103, wherein the badness module is configured to attenuate the flat score after delisting of the IP address.

105. A system of Claim 104, wherein the badness module is configured to

attenuate the flat score at an exponential decay.

106. A system of Claim 90, wherein the badness module is configured to determine the badness score by generating a flat score in proportion to a CIDR block size.

107. A system of Claim 93, wherein the scoring module is configured to normalize the aggregate of the plurality of badness scores.

108. A system of Claim 107, wherein the scoring module is configured to normalize based on at least one of network size or number of employees.

109. A system of Claim 90, wherein the security characterizations include non-negative information.

110. A system of Claim 59, further comprising an accuracy module configured to correlate the composite security score with statistical outcomes and adjust the scoring module to account for the correlation.

111. A system of Claim 59, further comprising a confidence module configured to determine a confidence range of the composite security score.

112. A system of Claim 111, wherein the confidence range is based on redundancy of the security characterizations.

113. A system of Claim 112, wherein the confidence range is based on a size of the third party computer system.

114. A system of Claim 59, further comprising a predictive module configured to predict future information security performance of the third party computer system using the security characterizations.

115. A system of Claim 59, further comprising an accuracy module configured to determine an accuracy of each of the security characterizations.

116. A system of Claim 115, wherein the accuracy module is configured to determine a level of coverage of the third party security system using the security characterizations.

117. A method of evaluating information security of a third party computer system, the method comprising:

collecting at least one security characterization of the third party computer system;

generating a composite security score using the at least one security characterization;

wherein the at least one security characterization is derived from externally observable characteristics of the third party computer system; and

wherein the composite security score has a relatively high likelihood of corresponding to an internal audit score.

118. A method of Claim 117, further comprising one or more of a plurality of the methods of Claims 2-58.

119. A system for evaluating information security of third party computer systems, the system comprising:

a data collection module configured to receive at least one security characterization, the security characterization describing a security outcome associated with one of the third party computer systems; and

a scoring module connected in communication with the data collection module and configured to use the security characterization to generate a composite security score for the associated third party computer system;

wherein the security outcome of the security characterization is derived from external investigation of the associated third party computer system;

wherein the composite score has a relatively high likelihood of corresponding to an internal audit score.

120. A system of Claim 119, further comprising one or more of a plurality of the systems of Claims 59-116.

ABSTRACT

A method and system for creating a composite security rating from security characterization data of a third party computer system. The security characterization data is derived from externally observable characteristics of the third party computer system. Advantageously, the composite security score has a relatively high likelihood of corresponding to an internal audit score despite use of externally observable security characteristics. Also, the method and system may include use of multiple security characterizations all solely derived from externally observable characteristics of the third party computer system.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	: Boyer et al.	Art Unit	: 2876
Serial No.	: 13/240,572	Examiner	: Not yet assigned.
Filed	: September 22, 2011	Conf. No.	: 2423
Title	: INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM		

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

DECLARATION BY THE INVENTOR(S)

As a below-named inventor(s), I hereby declare that:

My residence, post office address and citizenship are as stated next to my name.

I believe I am the original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled, INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM, the specification of which was filed on September 22, 2011, and identified as Application Serial No. 13/240,572.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT International filing date of the continuation-in-part application.

I hereby claim the benefit under Title 35, United States Code, §119(e)(1) of any United States provisional application(s) listed below:

U.S. Serial No.	Filing Date	Status
61/386,156	September 24, 2010	
61/492,287	June 1, 2011	

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose all information I know to be material to patentability as defined in Title 37, Code of Federal

Regulations, §1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

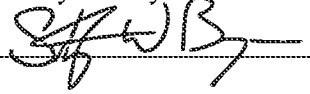
U.S. Serial No.	Filing Date	Status

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate or of any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application for patent or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter having a filing date before that of the application(s) of which priority is claimed:

Country	Application No.	Filing Date	Priority Claimed

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of inventor: Stephen Wayne Boyer

Inventor's signature: 

Date: 12/5/2011

Residence: Waltham, MA

Citizen of: US

Post Office Address: 299 Grove Street
Waltham, MA
02453

Full name of inventor: Nagarjuna Venna

Inventor's signature: Nagarjuna V.

Date: 12/8/2011

Residence: Waltham, MA

Citizen of: India

Post Office Address: 324 Bishops Forest Drive
Waltham, MA
02452

Full name of inventor: Megumi Ando

Inventor's signature: Megumi Ando

Date: December 5, 2011

Residence: Cambridge, MA

Citizen of: US

Post Office Address: 21 Brookline
#207
Cambridge, MA
02139

Global Data Sources 12
Entity ownership collection 14
Data collection mgmt.
Data Collection Processing
Source specific collection modules
Source 1
Source 2
Source 3
Source 4
16
Collected data archive 20
Entity mapped meta-reports repository
28
Raw entity mapped data
Entity Data Join 26 Process
Assign if belongs to Entity
24 Manual Entity Input
Entity Database 22
Ratings Processing
Source specific models
30
Normalization, crossvalidation, & global relative rank 32
Entity Ratings & Analytics
Report Generation 34
Report Archive 36
Report Delivery 38
Deliver Interface (Portal) 40
Deliver Interface (API)
Deliver Interface (Data Feed)
Customers 42
10
18
1
2
3
4
5
6
7
8
9
10
11
12
13
14

FIG. 1

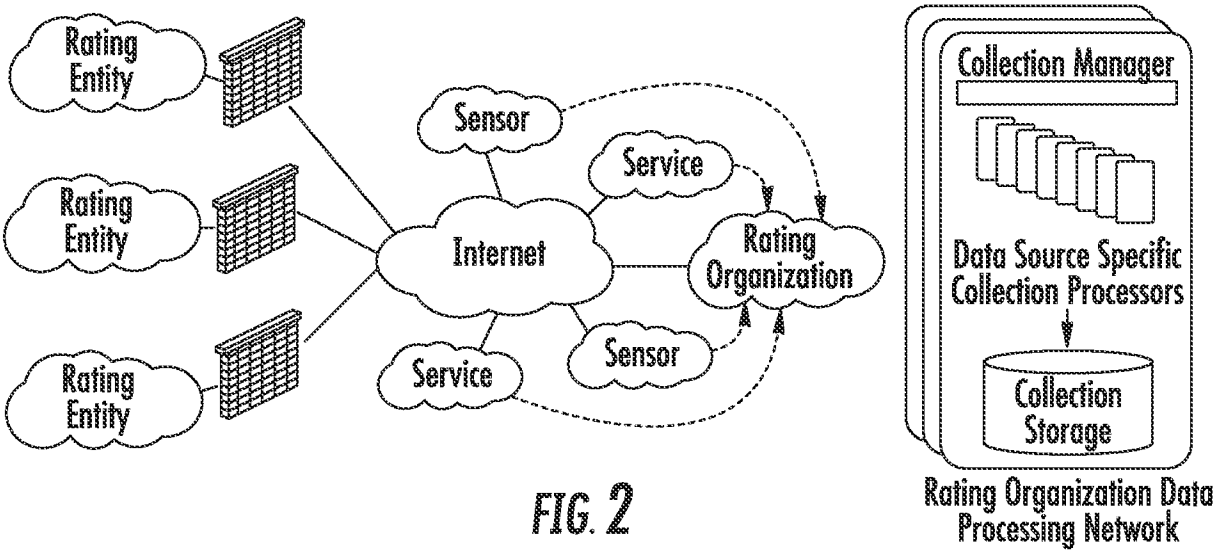

Rating Entity
Rating Entity
Rating Entity
Internet
Sensor
Service
Rating Organization
Service
Sensor
Collection Manager
Data Source Specific Collection Processors
Collection Storage
Rating Organization Data Processing Network

FIG. 2

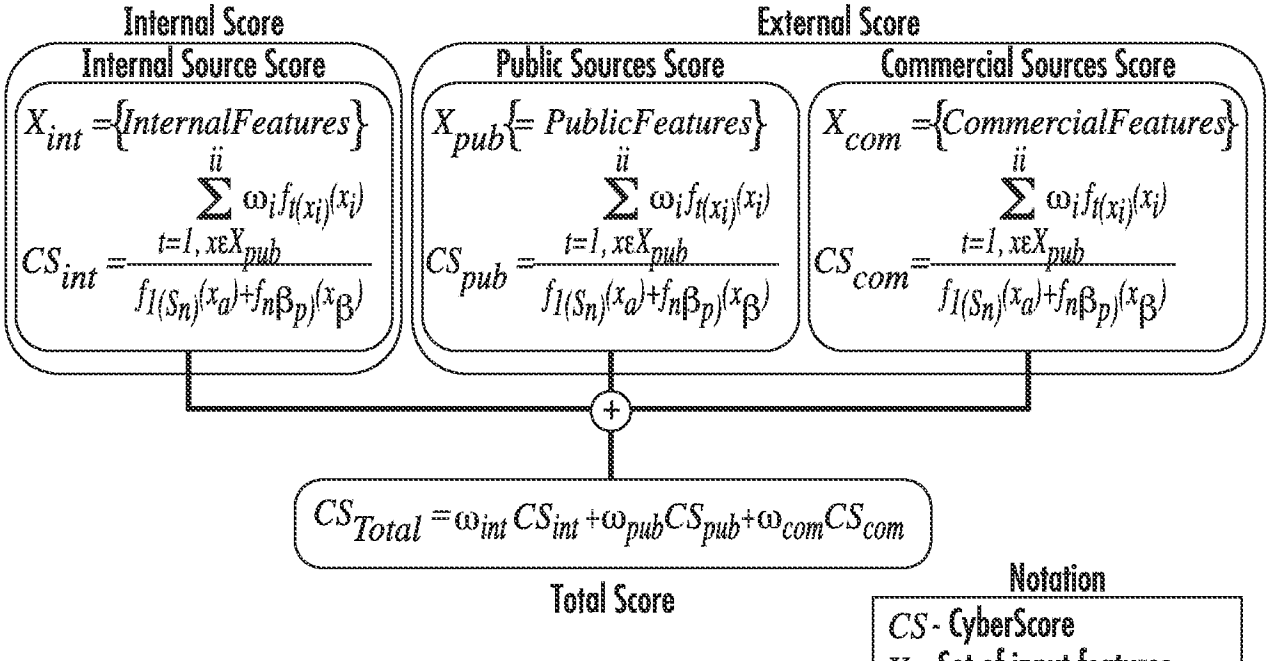

Internal Score
Internal Source Score
$X_{int} = \{InternalFeatures\}$
$CS_{int} = \frac{\sum_{t=1, x \varepsilon X_{pub}}^{ii} \omega_i f_{t(x_i)}(x_i)}{f_{1(S_n)}(x_\alpha) + f_n \beta_p)(x_\beta)}$
External Score
Public Sources Score
$X_{pub} \{= PublicFeatures\}$
$CS_{pub} = \frac{\sum_{t=1, x \varepsilon X_{pub}}^{ii} \omega_i f_{t(x_i)}(x_i)}{f_{1(S_n)}(x_\alpha) + f_n \beta_p)(x_\beta)}$
Commercial Sources Score
$X_{com} = \{CommercialFeatures\}$
$CS_{com} = \frac{\sum_{t=1, x \varepsilon X_{pub}}^{ii} \omega_i f_{t(x_i)}(x_i)}{f_{1(S_n)}(x_\alpha) + f_n \beta_p)(x_\beta)}$
+
$CS_{Total} = \omega_{int} CS_{int} + \omega_{pub} CS_{pub} + \omega_{com} CS_{com}$
Total Score
Notation
CS - CyberScore
X - Set of input features
$\sum^{ii} \omega_i = 1$ - Feature weights
$f_{t(x)}(x)$ - Feature transformation

FIG. 3

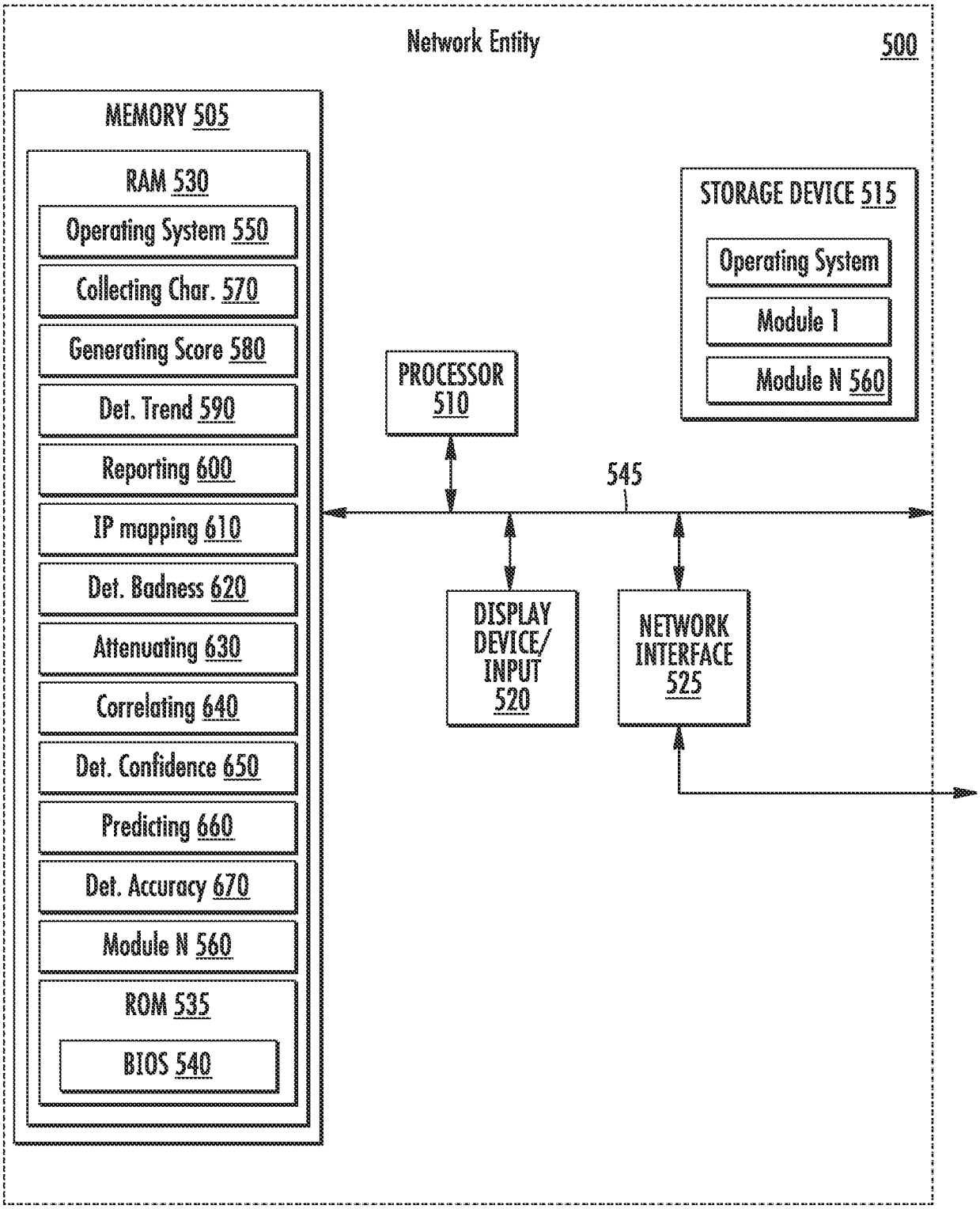

Network Entity
500
MEMORY 505
RAM 530
Operating System 550
Collecting Char. 570
Generating Score 580
Det. Trend 590
Reporting 600
IP mapping 610
Det. Badness 620
Attenuating 630
Correlating 640
Det. Confidence 650
Predicting 660
Det. Accuracy 670
Module N 560
ROM 535
BIOS 540
PROCESSOR 510
STORAGE DEVICE 515
Operating System
Module 1
Module N 560
545
DISPLAY DEVICE/ INPUT 520
NETWORK INTERFACE 525

FIG. 4

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant	:	Boyer, et al.	Art Unit	:	2876
Serial No.	:	13/240,572	Examiner	:	Not yet assigned
Filed	:	September 22, 2011	Conf. No.	:	2423
Title	:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM			

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PETITION FOR ONE-MONTH EXTENSION OF TIME UNDER 37 C.F.R. § 1.136

Please extend the period for response to the action dated October 6, 2011 for One month(s) to and including January 6, 2012.

The required fees are being paid concurrently herewith on the Electronic Filing System (EFS) by way of Electronic Funds Transfer authorization. Please apply any other charges or credits to Deposit Account No. 50-5226.

Respectfully submitted

McKEON MEUNIER CARLIN & CURFMAN, LLC

Date: December 15, 2011

/Gregory J. Carlin/
Gregory J. Carlin
Reg. No. 45,607

Customer No. 96039
docketing@m2iplaw.com
404.645.7700 Phone
404.645.7707 Fax

Electronic Patent Application Fee Transmittal

Application Number:	13240572
Filing Date:	22-Sep-2011
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Filer:	Gregory J. Carlin/Cheryl McKinzie
Attorney Docket Number:	10131-002US1

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Late filing fee for oath or declaration	2051	1	65	65
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension - 1 month with $0 paid	2251	1	75	75
Miscellaneous:				
			Total in USD ($)	**140**

Electronic Acknowledgement Receipt

EFS ID:	11628076
Application Number:	13240572
International Application Number:	
Confirmation Number:	2423
Title of Invention:	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Customer Number:	96039
Filer:	Gregory J. Carlin/Cheryl McKinzie
Filer Authorized By:	Gregory J. Carlin
Attorney Docket Number:	10131-002US1
Receipt Date:	15-DEC-2011
Filing Date:	22-SEP-2011
Time Stamp:	14:36:16
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Electronic Funds Transfer
Payment was successfully received in RAM	$140
RAM confirmation Number	1115
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

Black Kite Ex. 1003, Page 974 of 1060

1	Fee Worksheet (SB06)	fee-info.pdf	32127 3569dd514b40030240e6e9dc982bdbd087f75aff	no	2

Warnings:	
Information:	
Total Files Size (in bytes):	32127

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM

ACKNOWLEDGEMENT

This invention was made with government support under 1127185 awarded by the National Science Foundation. The government has certain rights to this invention.

CROSS-REFERENCE TO RELATED APPLICATIONS

The present application claims priority to U.S. Prov. Pat. App. No. 61/386,156 entitled "Enterprise Information Security Score" and filed on Sept. 24, 2010; and 61/492,287 entitled "Information Technology Security Assessment System" and filed on June 1, 2011 which are hereby incorporated herein in their entirety by reference.

BACKGROUND

The present invention relates to systems for determining the security of information systems and, in particular, for evaluating the security of third-party computer systems.

When a company wants to reduce its cyber security risk of doing business with another company's computer systems, it either performs, or hires an outside firm to perform, a cyber security assessment of the other company to determine if it is following good security practices. The theory is that these good practices make it difficult for attackers to compromise the networks of the other company. If the auditing company is satisfied with the assessment, it may choose to continue doing business with the other company. Or, it may ask the other company to make some improvements to its security systems or terminate the business relationship.

Generally, these audits are slow, expensive and impractical given the high volume of service provider security systems that need to be characterized by the company. And, the inventors have noted that audits are not entirely predictive of the performance of the security systems.

SUMMARY

A method and system is disclosed for creating a composite security rating from security characterization data of a third party computer system. The security

characterization data is derived from externally observable characteristics of the third party computer system. Advantageously, the composite security rating has a relatively high likelihood of corresponding to an internal audit score despite use of externally observable security characteristics. Also, the method and system may include use of multiple security characterizations all solely derived from externally observable characteristics of the third party computer system.

A method of evaluating information security of a third party computer system is disclosed. The method includes collecting at least two security characterizations of the third party computer system. A composite security rating is generated using the at least two security characterizations. Advantageously, the two security characterizations are derived from externally observable characteristics of the third party system.

Each of the security characterizations may be from an associated one of a plurality of independent entities. For example, the independent entities may include commercial data sources. Also, the security characterizations may be derived without permission of the third party system.

The security characterizations may include multiple data types, such as breach disclosures, block lists, configuration parameters, malware servers, reputation metrics, suspicious activity, spyware, white lists, compromised hosts, malicious activity, spam activity, vulnerable hosts, phishing, user-behavior or e-mail viruses. The externally observable characteristics may also include serving of malicious code or communications with known attacker controlled networks.

The externally observable characteristics may be evidence of internal security controls or outcomes or operational execution of security measures of the third party computer system.

The collecting and generating steps may be repeated to generate a series of scores and the series examined to determine a trend. Also, the scores may be reported to a consumer. For instance, reporting may include reporting a warning based on a change in the scores. Or, reporting may include posting the score and warning to a web portal.

Collecting the security characterizations may include using various tools such as WGET, RSYNC, CURL or interfaces that may be characterization specific.

The method may also include mapping the third party computer system to an IP space and using the IP space for collecting the security characterizations. Mapping, for

example, may include querying a Regional Internet Registry (RIR), such as by submitting an entity name to the RIR. Querying an entity name may include querying for variations of the entity name.

Mapping may also include using a domain name associated with the third party computer system. For example, tools such as nslookup or dig may be used on the domain name to determine a published IP address. Mapping may also include probing addresses around the published IP address. For example, IP addresses could be probed in powers of two around the published IP address. Mapping could also include adapting the domain name to server naming conventions and using tools like nslookup to verify an IP address associated with the domain name.

Generating the composite security rating may include assessing vulnerability and resilience of the third party computer systems. Vulnerability, for example, may include a number of IP addresses with malicious behavior. Resilience may be inversely proportional to a duration of malicious behavior.

The IP space may include a plurality of IP addresses. And, the composite security rating may correspond to an intensity and duration of malicious activity determined from one of the security characterizations. Generation of the composite security rating may include aggregation of a plurality of individual security metrics and/or the IP addresses associated with the third party computer system.

Determination of the individual security metric may include adjusting for false positives in the security characterizations. Correlating data across multiple related security characterizations may help improve the quality of any single security characterization. Further, adjusting for false positives may include determining an occurrence of an event, which includes persistent, reported activity on one of the IP addresses for a predetermined period of time. It may also include determining an intensity of the IP address for the predetermined period of time, such as a day.

Determining the intensity may include increasing intensity in proportion to a number of reporting targets from the security characterizations.

Determining an individual security metric may include assigning a raw score for each of the IP addresses appearing on a block list as one of the security characterizations. After an IP address is delisted, the raw score may be exponentially attenuated.

The individual security metric may also incorporate a raw score in proportion to a

CIDR block size.

Individual security metrics or the composite ratings may be normalized based on, for example, network size or a number of employees.

Security characterizations may also include positive information about an organization that's aggregated into the composite rating.

The method could also include statistically correlating the composite security rating with actual outcomes and adjusting the generating step based on the statistical correlations.

Further, the method may include determining a confidence range of the composite security rating. For example, the confidence range may be based on a redundancy of the security characterizations or a size of the third party computer system.

The method may also include determining an accuracy of each of the security characterizations, such as by determining a level of coverage of the third party computer system by the security characterizations.

Also disclosed herein are a system and computer program product for data collection and scoring, including systems and software for performing the methods described above.

Another method may include generating a composite security rating using at least one security characterization that's derived from externally observable characteristics of the third party computer system wherein the composite security rating has a relatively high likelihood of corresponding to an internal audit score.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

Figure 1 is a schematic of a system for evaluating information security;
Figure 2 is a schematic of a system for gathering security data from external sensors;
Figure 3 is a schematic of a composite security rating calculation; and
Figure 4 is a schematic of a distributed system for evaluating information security.

DETAILED DESCRIPTION

Generally, the present invention includes a method, system and computer program product for creating composite security ratings from security characterization data of a third party computer system. The security characterization data is derived from externally observable characteristics of the third party computer system. Advantageously, the composite security rating has a relatively high likelihood of corresponding to an internal

audit score despite use of externally observable security characteristics. Also, the method and system may include use of multiple security characterizations all solely derived from externally observable characteristics of the third party computer system.

The terminology used herein is for the purpose of describing particular embodiments only and is not intended to be limiting of the invention. As used herein, the singular forms "a", "an" and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the terms "comprises" and/or "comprising," when used in this specification, specify the presence of stated features, integers, steps, operations, elements, and/or components, but do not preclude the presence or addition of one or more other features, integers, steps, operations, elements, components, and/or groups thereof.

The corresponding structures, materials, acts, and equivalents of all means or step plus function elements in the claims below are intended to include any structure, material, or act for performing the function in combination with other claimed elements as specifically claimed. The description of the present invention has been presented for purposes of illustration and description, but is not intended to be exhaustive or limited to the invention in the form disclosed. Many modifications and variations will be apparent to those of ordinary skill in the art without departing from the scope and spirit of the invention. The embodiment was chosen and described in order to best explain the principles of the invention and the practical application, and to enable others of ordinary skill in the art to understand the invention for various embodiments with various modifications as are suited to the particular use contemplated.

Any combination of one or more computer readable medium(s) may be utilized. The computer readable medium may be a computer readable signal medium or a computer readable storage medium. A computer readable storage medium may be, for example, but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, or device, or any suitable combination of the foregoing. More specific examples (a non-exhaustive list) of the computer readable storage medium would include the following: an electrical connection having one or more wires, a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), an optical fiber, a portable compact disc read-only memory (CD-ROM), an optical storage device, a magnetic

storage device, or any suitable combination of the foregoing. In the context of this document, a computer readable storage medium may be any tangible medium that can contain, or store a program for use by or in connection with an instruction execution system, apparatus, or device.

A computer readable signal medium may include a propagated data signal with computer readable program code embodied therein, for example, in baseband or as part of a carrier wave. Such a propagated signal may take any of a variety of forms, including, but not limited to, electro-magnetic, optical, or any suitable combination thereof. A computer readable signal medium may be any computer readable medium that is not a computer readable storage medium and that can communicate, propagate, or transport a program for use by or in connection with an instruction execution system, apparatus, or device.

Program code embodied on a computer readable medium may be transmitted using any appropriate medium, including but not limited to wireless, wireline, optical fiber cable, RF, etc., or any suitable combination of the foregoing.

Computer program code for carrying out operations for aspects of the present invention may be written in any combination of one or more programming languages, including an object oriented programming language such as Java, Smalltalk, C++ or the like and conventional procedural programming languages, such as the "C" programming language or similar programming languages. The program code may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider).

Aspects of the present invention are described below with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems) and computer program products according to embodiments of the invention. It will be understood that each block of the flowchart illustrations and/or block diagrams, and combinations of blocks in the flowchart illustrations and/or block diagrams, can be implemented by computer program instructions. These computer program instructions may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data

processing apparatus to produce a machine, such that the instructions, which execute via the processor of the computer or other programmable data processing apparatus, create means for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

These computer program instructions may also be stored in a computer readable medium that can direct a computer, other programmable data processing apparatus, or other devices to function in a particular manner, such that the instructions stored in the computer readable medium produce an article of manufacture including instructions which implement the function/act specified in the flowchart and/or block diagram block or blocks.

The computer program instructions may also be loaded onto a computer, other programmable data processing apparatus, or other devices to cause a series of operational steps to be performed on the computer, other programmable apparatus or other devices to produce a computer implemented process such that the instructions which execute on the computer or other programmable apparatus provide processes for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

Referring again to Fig. 1, a system 10 for evaluating information security of a third party computer system includes the following systems: a global data source 12, an entity ownership collector 14, a data collection processor 16, a data collection management 18, a data archive 20, an entity database 22, a manual entity input 24, an entity data join process 26, an entity mapped meta-reports repository 28, a ratings processing 30, a normalization, consolidation and global relative rank 32, a report generation 34, a report archive 36 and a report delivery 38 systems. Different delivery modules 40 are configured to use different methods to deliver the reports to customers 42.

The global data source system 12 obtains data sources that characterize any observation about an entity (e.g., a third party computer system) and these sources can be highly varied and disparate. Each data source has a particular vantage point of the security related characteristics of entities.

The entity ownership collection system 14 gathers information about an entity. This includes information about which IT assets an entity owns, controls, uses, or is affiliated with. Examples of asset ownership include control and operation of an Internet Protocol (IP) network address range or computer services such as web servers residing within that address block. Information about entities also includes relationships such as subsidiaries,

affiliates, etc., that describe entity association.

The data collection processing system 16 includes custom modules configured to collect and process unique data sources.

The data collection management system 18 is configured to schedule and coordinate the constant collection of the different data sources.

The data archive 20 is configured to store all of the terabytes of data constantly collected by the data collection management system 18.

The entity database 22 holds all of the information about an entity such as its name, address, web site address, industry sector, IP address ranges owned, etc. This data base includes the "Entity Map" which maps data back to an entity. For example, if observations are made about a particular IP address, the IP address can be looked up in the entity map to determine which entity controls or owns that address. This database is populated by automatic or manual data collection methods, or combinations thereof.

The manual entity input system is configured to place non-automatic data on an entity into the entity database 22.

The entity data join process or system 26 is configured to match the collected data to the entity. In most instances, this is a computationally expensive operation because it requires going though all of the data collected and performing the map operation. Any evidence of security outcomes or configurations in the larger data collection pool is then assigned to an entity based on the entity map.

The entity mapped meta-reports repository 28 contains data summaries of observations made with respect to a particular entity for each data set after the map/join process is complete.

The ratings processing system 30 may include custom models for applying data source specific ratings to determine an entity rating. Each data source generally requires a custom model due to the unique nature of that data source. Each model accounts for the custom attributes and idiosyncrasies of the different data sources that have been mapped to the entity being rated. Custom data source models can account for any data source feature including temporal and cross-data source behaviors.

The ratings normalization, cross-validation, and relative ranking system 32 is configured to normalize ratings so appropriate entity-to-entity comparisons can be made and the ratings are normalized and ranked within sectors or peer-groups and globally.

An entity and rating analytics repository or archive 36 is configured to hold all of the ratings data and resulting analytics produced by the ratings process.

A report generation system 34 takes the ratings and analytics and generates report objects. These objects are not rendered into any particular presentation format at this stage but are in a generic intermediary format that can be then transformed into a specific deliverable format.

A report delivery system 38 is configured to translate generic reports into a specific report format. Examples of these formats include HTML, PDF, text, and XML. Delivery modules 40 are different methods for delivering the reports include by web portal, API or data feed.

Advantages include ratings based on the quality of outcomes of the information security practices of the third party computer systems and enablement of comparisons of ratings across organizations. The system 10 can be entirely, or to a large extent, automated and need not have the permission of the entity being rated. The reports will allow risk management professionals to monitor, assess and mitigate partner risk by up-to-date ratings due to its persistent monitoring of the third party computer systems. Also, the portal may provide for location of new partners, such as suppliers, with lower risk profiles and improved security postures.

Unlike internal audit systems, the system 10 is not relying upon a correlation between practices and outcomes. Instead, evidence of actual security outcomes is collected through the data source partners.

Also advantageously, trial data on 50 entities revealed that rankings produced using the system 10 matched internal evaluations. In some cases the system 10 revealed problems with the entities not revealed by internal evaluations.

Data Sources

External ratings from data sources available outside an entity provide an information security based view into internal workings of the organization. For example, infection by malicious software can be determined using non-invasive website scanning technology. Communication between the entity computer system and known attacker controlled networks may reveal when the computer system has been compromised. Also, if an entity computer system is serving malicious code to visitors the system was compromised at some

point. The entity may not have the capability to detect such compromises or cannot quickly react operationally to resolve the issue. External observations also can measure operational execution, which may not occur despite good internal policies.

A diverse set of network sensors and services around the Internet collect and observe information about the third party entity computer systems. The system 10 then gathers, processes, and stores the data collected about entities from the sensors and service providers using custom developed data source specific collection processors. The collection manager 18 automates the scheduling and execution of the different collectors.

The global data source system 12 includes hundreds of potential data sources, including, for example during experimental testing, 97 data sources owned by 37 organizations. At least 82 data sources are on active collection, being stored on the data archive 20. Trial ratings were performed on at least 11 data sources from 7 organizations. Rankings were produced on nearly 600 different entities.

A data source is a single type of data from a single organization. For example, if two organizations provide a list of hosts that participate in phishing attacks, they are counted as two data sources. The 15 types of data in Table 3 all provide different information security related views of an organization. New types of data and new sources of existing data types are constantly added to the data sources used to characterize the performance of the entity. Breach disclosures for example indicate that an organization has experienced a particular kind of data or integrity breach. Configuration data on the other hand provides any number of configuration related information and could for example state the type of encryption used on the organization's website.

Table 1 Data Sources Summary

Total Data Sources	97
Total Sourcing Organizations	37
Total Sources on Active Collection	82
Total Different Source Types	15

Table 3 Data Source Types

Breach Disclosures	Spam Activity

Block Lists	Vulnerable Hosts
Configuration Parameters	Spyware
Compromised Hosts	Whitelists
Malicious Activity	Email viruses
Malware Servers	Multi-type
Reputation	Phishing
Suspicious Activity	User Behavior

Of the 97 data sources identified, 82 are on "Active Collection" meaning there is a method for obtaining the data source and that its collection is automated. The high degree of automation helps to satisfy the methodology objective for adoption of techniques that are principally automated.

Table 2 lists the 6 collections methods employed for data acquisition with the "Unknown" category meaning that the sources are identified but the method and ability to collect that data source has yet be determined. The method Instances are the number of data sources that are collected using that particular method. For example, 32 of the sources are collected using the network file transfer and synchronization tool rsync (http://samba.anu.edu.au/rsync/).

Table 2 Data Collection Methods

Methods	Instances	Methods	Instances
WGET	35	WHOIS	1
RSYNC	32	HTTP GET	1
API	13	UNKNOWN	9
MANUAL	6		

A collection processing infrastructure 50, configured to build and validate composite security ratings, is shown in Fig. 2. A plurality of different clouds represents different network segments. Rated Entity clouds 52 are organizations for which the system 10 generates a rating. Those entities include an entity perimeter or boundary, indicated by the firewall that connects to the Internet. Services clouds 54 provide data or reports on observed activity from a rated entity 52. An example of a report from a Service 54 could be a list of hosts that have been participating in malicious activity. Services use Sensor networks 56 to

observe the behavior of entities. For example, a sensor could observe SPAM messages sent from a rated entity network 52 to the Internet 58.

Entity Mapping

There is no single central repository that holds information about the IP address allocation. Determining the correct and complete IP address space owned by a given entity improves the reliability and robustness of a rating.

In general, Regional Internet Registries (RIRs) manage the allocation and registration of Internet number resources (IP Addresses, Autonomous System Numbers, etc.) within a particular region of the world. There are five RIRs - ARIN for North America, AfriNIC for Africa, APNIC for Asia Pacific, RIPE for Europe, Middle East, Central Asia, and LACNIC for Latin America.

The RIRs allocate the address space to service providers, corporations, universities, etc. The RIRs provide various interfaces that enable queries of the RIR to determine who owns a given IP address. It is also possible to query the database by an entity name and get a list of IP addresses allocated to that entity. Despite lack of standardization of entity names in the RIR databases, well chosen queries can result in a very high coverage of addresses owned by an entity.

Another problem is that RIRs often allocate large chunks of addresses to Internet Service Providers (ISPs) who go on to allocate smaller address spaces to their customers. ISPs are under no obligation to report this data back to anyone. Most small companies contract with their local ISP for Internet access and don't obtain addresses from RIRs.

These problems are addressed by the entity ownership collection system 14 being configured to execute various heuristic processes including the following non-limiting list of examples:

1. Using the 'dig' (http://linux.die.net/man/1/dig) tool to determine any IP information published by an entity. The dig tool takes the domain name of the entity as an argument. For example, execution of 'dig a.com ANY' returns all IP information published by the entity a.com.

2. Use the IP addresses and domain names published to find ranges of IP addresses actually used. ISPs almost always allocate addresses in size of powers of 2 (2, 4, 8 etc.). Knowing one IP address allows probing around that space. The 'whois'

(http://linux.die.net/man/1/whois) tool can be used to determine ownership of neighborhood addresses.

3. Even if the entity does not publish any IP information that can be retrieved through dig, most entities have servers whose names may be guessed. Mail servers for the domain a.com often have the name mail.a.com, SMTP servers tend to be smtp.a.com, FTP servers tend to be ftp.a.com etc. Using a tool like nslookup, the entity ownership collection system 14 can verify if any of these common names are in use by the entity.

4. If an IP address is found, the system 14 is configured to probe around the address (such as in step 2) to determine any addresses in the neighborhood owned by that entity.

5. Searching around the website of the company often gives a hint of other servers hosted by the company (ex: reports.a.com) which can be used as a starting point for search.

Rating Methodology

Organizational security risk may be measured along two vectors: vulnerability and resilience. An entity's vulnerability is defined as its "physical, technical, organizational, and cultural states," which can be exploited to create a security breach. An entity's resilience is defined to be its ability to recover from a security breach.

The system 10 uses the concepts of vulnerability and resilience by examining externally observable proxies for them. An example proxy for entity vulnerability is the number of entity-owned IP addresses, which are reported to be malicious. The higher the number of reports the more likely the entity was vulnerable and had been compromised. Resilience is inversely proportional to the duration of detected malicious activity. The shorter the duration of the malicious activity, the higher level of resilience the entity demonstrates as it can quickly identify and remove malicious infections.

To compute the ratings for an entity, the system 10 aggregates all of the data collected pertaining to the IT assets owned by that organization, such as the IP addresses controlled by the entity and the associated activity of those IP addresses. The types of activities depend on the types of data. The data sources may include false positives and the system 10 is configured to account for those uncertainties.

To determine quality metrics for IP address based assets, every IP address is uniquely mapped to an entity. Processing the data from a data source yields a list of IPs for each organization that has demonstrated suspicious or malicious behavior. The processing

steps are as follows:

1. For each IP address, determine a security quality metric called "badness".
2. Badness is a number between 0 and 1 that corresponds to the extent and duration of malicious activity that was reported.
3. For each data source in which the IP address is reported, determine a data source specific badness score for that IP.
4. Consolidate the badness score for a given IP across all data sources by cross validating data to determine the aggregate Badness for that IP.
5. Aggregate the badness scores of IPs from an entity to determine the entity's IP asset based security quality metric.

The ratings processing system 30 is configured to account for differences in data sources and types. Given each data source's potentially unique view of an entity, there is not a universal technique that treated them all the same way. Data source specific modeling techniques, for example, were developed for 11 of the 97 data sources in experimental trials in order to demonstrate feasibility and validate the approach. The data sources incorporated accounted for five different data source types: Block Lists, Suspicious Activity, Malicious Servers, Compromised Hosts, and Spamming.

The following two sections give detailed examples of modeling techniques developed for calculating IP address badness for two different data sources that are representative of the data collected.

One of the data sources is a daily updated list of IP addresses that were reported by volunteer hosts from across the Internet. IP Addresses are reported in this data source if they have communicated with hosts that do not expect any inbound communication from them. It lists many more IP addresses on a given day compared with the other data sources and therefore, provides a significant amount of information contained only in this data source. However, this data source has a high incidence of false positives, where a false positive is an unwarranted report due to an incorrectly configured reporting host (i.e., the target) or a listing of an incorrect IP address due to backscatter.

False positives are accounted for by identifying events – where an event is defined as persistent, reported activity on a single IP address within a time period. For each event, heuristics are applied to determine the average intensity for the event. The intensity of an IP address on a given day is a measure of the confidence that malicious activity originated

from the IP address on that day.

For the case where an event spans multiple days, the IP address is generally reported on each day in the event. However, if an IP address is listed on one day but not the next, this omission does not necessarily signify that the host has stopped its malicious behavior; rather, it could be that the host was offline for the day. For example, many corporate hosts are offline for weekends and holidays. Thus, an event is allowed to have short inactive periods, or days without any reports on the IP address. To generate the IP address quality metric, a maximum inactive period of three days is used.

The intensity of an IP address for a given day is calculated dynamically and increases both with the number of reporting targets as well as the duration of the event. Reports with a larger number of targets have larger intensities. This is because false positives due to mis-configured hosts are less likely to have occurred when multiple targets report the same IP address on the same day. Likewise, reports that belong to a persistent event have larger intensities, since persistent reports also signal the legitimacy of the malicious activity on the IP address.

The intensity, I(s) is calculated as follows:

$$I(s) = \begin{cases} 0.1, & if\ s < 2 \\ 0.01e^{\frac{\ln(10)(s-1)}{4}}, & if\ 2 \le s < 5 \\ 0.8 - 0.7e^{-\frac{\ln(10)(s-5)}{4}}, & if\ s \le 5 \end{cases}$$

where s is the number of hosts reporting the IP address. Thus, the average intensity, I_{avg}, of an event is the average of the intensities calculated per active day (a day with reports) and is determined as follows:

$$I_{avg} = \frac{I(s)}{T} + \frac{A \cdot I_{prev}}{T},$$

where T is the list time, A is T minus the number of days since the last update, and I_{prev} is the average intensity at the last update. The Badness, B_{IP}, of an IP address is derived from the intensity and duration of the events for the IP, such that recent events are weighted heavier than historical events and is calculated as follows:

$$B_{IP} = min(1, \frac{I_{avg}(1-e^{-0.02})}{1-e^{-0.12}} \sum_{t_1}^{t_n} e^{-0.02}),$$

where t_1 and t_n denote time lapsed from the end and beginning of an event, respectively; and

the average intensity is readjusted if the persistence surpasses a threshold.

The second data source example is a host block list that lists IP addresses that have been compromised. Based on an analysis of the data sources collection methods, the block list is considered very reliable in the sense that a listing implies that malicious activity originated from the listed address. This block list removes IP addresses from the list if no malicious activity is detected for a small window of time. Because of the high confidence in the data source's accuracy, any IP address on the block list is assigned a raw Badness of 0.8.

Once an IP address is delisted and is no longer on the block list, its Badness decays exponentially with respect to the time since it was last listed. Thus, the Badness is:

$$B_{IP} = 0.8e^{-\frac{\ln(2)T}{182.625}},$$

where T is the time in days since the last listing. This decay rate corresponds to a half-life of six months.

Various other data sources are handled similarly but the raw score is based on the confidence in the data source's collection methods. Other data sources track CIDR blocks as opposed to individual IP addresses, and so the Badness assigned to a listing on these lists are weighted by the CIDR block size as follows:

$$B_{IP} = 0.8We^{-\frac{\ln(2)T}{182.625}},$$

where W is the natural log of the block size.

The total IP space badness of an entity is an aggregation of the badness of the entity's individual IP addresses and/or CIDR blocks. In the simplest model where all data sources are IP address based, the entity badness is the total badness of the IP addresses owned by the entity. To normalize ratings across entities of different sizes, the entity's network size defined as the number of active IP addresses owned by the entity is used:

$$B_{entity} = \frac{\sum_{IP \in entity} B_{IP}}{\ln(N)},$$

where N denotes the network size. Normalizing avoids penalizing of smaller entities allowing fair comparisons between entities of differing sizes.

Enhancements to the Ratings Methodology

The system 10 may also include expanded the methodology to support additional

and different types of data sources. It could identify data sources that indicate different levels of IT sophistication - such information is a measure of the level of IT practice maturity.

Entity normalization methods can also account for differences in entity size beyond network size. For example, the use of other normalization methods such as number of employees may help produce more robust normalizations under certain circumstances.

Also, statistical properties of the model's internal parameters may be analyzed and adjust based on the findings. For example, certain inputs or features may be disproportionately skewing the ratings and such inputs or features may be modulated through weighting factors.

The composite security rating described above measured, amongst other things, how much, to what extent, and how recently malicious activity was detected on an entity's cumulative IP space. The score could also be adapted to show a level of confidence. For example, a failure to detect malicious activity on an entity's IP space does not necessarily imply non-malicious behavior. Rather, the data sources may lack coverage on the entity's IP space. By outputting a range as opposed to a number, the system 10 is able to convey its confidence in a rating where a larger range necessarily implies a lower confidence, and a smaller range necessarily implies a higher confidence.

Such a range could be computed from a mean score and a confidence range, which could be determined from a developed discrete choice model. Features such as the Badness scores from each data source could help determine the mean score. Features such as redundancy between data sources and network size could also help determine the confidence range.

Entity mapping may also be improved through other data sources and functions. Data sharing relationships with Internet Service Providers might provide additional data on security outcomes and practices at entity computer systems. Also, consumers of the scoring reports may already have partner-mapping data through the nature of their relationship with the entity or may be able to request the information.

Entity mapping may also be facilitated by persistent updates of the heuristics, such as updating prefixes from BGP announcements and data from Regional Internet Registries.

Data storage used by the system 10 may be improved to minimize the disk space required while supporting rapid inclusion of new entity ratings. For example, high-speed

data access layers may be created for daily ratings computation.

Speed and scale can be accomplished through distributed or parallel processing on different systems. A distributed data source query interface may be implemented so that massive and expensive centralized data storage is not required.

The system 10 may also be configured to develop and evaluate predictive capabilities of information security ratings and incorporate them into the rating methodology.

The ability to demonstrate predictability has a dependency on data reliability. For example, improving coverage of malicious events improves data reliability. Statistical evaluations may be used to disambiguate strong entity performance (e.g., no malicious activity) from low coverage (e.g., lack of information on the malicious activity). These evaluations can then be used in the rating methodology.

Statistical evaluations of data coverage may include a data accuracy assessment wherein levels of coverage assurance associated with a particular adopted data source are determined. Also, observations across data sources may be compared to determine data sources of high probability or low probability of coverage for a given entity.

Predictive modeling may include determination of entity historical trends to display and predict future performance. Regression and machine learning based models may be developed to predict information security performance. Models may be evaluated and further developed for predictive capability through a series of prediction experiments.

Also, the data source features may be analyzed for correlations of high and low performance. For example, entities with behavior "X" tend to perform well and entities that demonstrate property "Y" tend to behave poorly.

Use of External and Internal Security Data

The system 10 may also include internally derived security assessments. For example, such a score computation is shown in Fig. 3. The final score S_{Total} has two components, the Internal score and the External score.

The Internal score, S_{int}, is derived from data collected and observed from inside the enterprise. Data sources that provide inputs to the internal scoring function could include, but are not limited to, the following:

- Vulnerability scans
- Firewall Rules
- Incident Reports
- Configurations
- Software inventory
- Policies
- Controls
- User Behavior

The features from each of the data sources are extracted to create a feature vector. This feature vector is $X_{\text{int}} = \{InternalFeatures\}$ in the "Internal Source Score," as shown in Fig. 3. Features include, but are not limited to, derived metrics from the data sources (e.g., the number of remotely exploitable vulnerabilities from outside the entity, the number of incidents, or the number of vulnerable versions of software).

Each feature x_i in X_{INT} has a corresponding transformation function $f_{t(x_i)}(x_i)$ that performs a normalization transformation such that the resultants can be summed.

Each feature x_i in X_{INT} also has corresponding weight ω_i such that different weights can be placed on the resultant feature transformation where the sum of the weights equal is unity $\sum_{i=1}^{n} \omega_i = 1$. The sum of the transformed and weighted feature vector is computed by summing each resultant for each of the features $\sum_{i=1, x \in X_{\text{int}}}^{n} \omega_i f_{t(x_i)}(x_i)$.

The final score S_{int} is the summation normalized by a set of normalization factors given as $f_{t(x_\alpha)}(x_\alpha) + f_{t(x_\beta)}(x_\beta)$ where each normalization factor $x_\alpha, x_\beta, \ldots$ also has a factor normalization transformation function.

The computation of the Internal Score is given as: $S_{\text{int}} = \dfrac{\sum_{i=1, x \in X_{\text{int}}}^{n} \omega_i f_{t(x_i)}(x_i)}{f_{t(x_\alpha)}(x_\alpha) + f_{t(x_\beta)}(x_\beta)}$

Black Kite Ex. 1002, Page 994 of 1060

The External Score is the combination of the Public Sources Score (S_{pub}) and the Commercial Sources (S_{com}). S_{pub} and S_{com} are derived using the same heuristic combinatorial functions as the Internal Score. However, the input data sources, weights, transformation functions and normalization factors are different.

S_{pub} and S_{com} have their own feature vectors $X_{pub} = \{PublicFeatures\}$ and $X_{com} = \{CommercialFeatures\}$ based on the data input sources used.

Data sources in X_{pub} that provide inputs to the S_{pub} score could include but are not limited to the following:

- Industry reports
- Internet monitoring web sites that publish reports (ex: *www.malwareurl.com*)
- News articles
- Court records

Data sources in X_{com} that provide inputs to the S_{com} score could include but are not limited to the following:

- Company proprietary data collected during operations
- Renesys
- Arbor Networks
- Business intelligence bought from corporations and services
- User Behavior

With the Internal and External Scores computed, the final total score is computed and the weighted sum of the three: $S_{Total} = \omega_{int} S_{int} + \omega_{pub} S_{pub} + \omega_{com} S_{com}$

It is possible that the algorithm does not have the same inputs for all entities. More information may be available for some entities compared to other entities. Given this, each data source is assigned a normalized confidence level based on how much they contribute to the computation of the enterprise score. Depending on the actual data that went into rating the company, the confidence level is assigned as a sum of the confidence levels associated with the data sources. The confidence level can be used to assign a range of scores for an enterprise. For instance, if an enterprise is rated as 750 with a confidence level of 0.8, the

entity's actual score is reported as (750 – (1 – 0.8) * 100, 750) = (730 – 750). An entity's score is deemed to be unavailable if the confidence level is below a minimum threshold of 0.5.

It should be noted that the S_{int} may be zero due to a lack of available information or permission, wherein S_{total} becomes characteristic only of externally observable characteristics. Also, characteristics for the calculation can be used in conjunction, or vice versa, with functions and aspects of the remaining systems described hereinabove and below.

Distributed System

Referring now to Fig. 4, a schematic diagram of a central server 500, or similar network entity, configured to implement a system for creating a composite security score is provided. As used herein, the designation "central" merely serves to describe the common functionality the server provides for multiple clients or other computing devices and does not require or infer any centralized positioning of the server relative to other computing devices. As may be understood from Fig. 4, the central server 500 may include a processor 510 that communicates with other elements within the central server 500 via a system interface or bus 545. Also included in the central server 500 may be a display device/input device 520 for receiving and displaying data. This display device/input device 520 may be, for example, a keyboard or pointing device that is used in combination with a monitor. The central server 500 may further include memory 505, which may include both read only memory (ROM) 535 and random access memory (RAM) 530. The server's ROM 535 may be used to store a basic input/output system 540 (BIOS), containing the basic routines that help to transfer information across the one or more networks.

In addition, the central server 500 may include at least one storage device 515, such as a hard disk drive, a floppy disk drive, a CD Rom drive, or optical disk drive, for storing information on various computer-readable media, such as a hard disk, a removable magnetic disk, or a CD-ROM disk. As will be appreciated by one of ordinary skill in the art, each of these storage devices 515 may be connected to the system bus 545 by an appropriate interface. The storage devices 515 and their associated computer-readable media may provide nonvolatile storage for a central server. It is important to note that the computer-readable media described above could be replaced by any other type of computer-readable

media known in the art. Such media include, for example, magnetic cassettes, flash memory cards and digital video disks.

A number of program modules may be stored by the various storage devices and within RAM 530. Such program modules may include an operating system 550 and a plurality of one or more (N) modules 560. The modules 560 may control certain aspects of the operation of the central server 500, with the assistance of the processor 510 and the operating system 550. For example, the modules may perform the functions described above and illustrated by the figures and other materials disclosed herein, such as collecting security characterizations 570, generating a composite rating 580, determining a trend 590, reporting the ratings 600, IP mapping 610, determining a badness quality metric 620, attenuating a raw score 630, correlating with statistical outcomes 640, determining a confidence range 650, predicting future performance 660 and determining an accuracy 670.

The flowchart and block diagrams in the figures illustrate the architecture, functionality, and operation of possible implementations of systems, methods and computer program products according to various embodiments of the present invention. In this regard, each block in the flowchart or block diagrams may represent a module, segment, or portion of code, which comprises one or more executable instructions for implementing the specified logical function(s). It should also be noted that, in some alternative implementations, the functions noted in the block may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams and/or flowchart illustration, and combinations of blocks in the block diagrams and/or flowchart illustration, can be implemented by special purpose hardware-based systems that perform the specified functions or acts, or combinations of special purpose hardware and computer instructions.

The corresponding structures, materials, acts, and equivalents of all means or step plus function elements in the claims below are intended to include any structure, material, or act for performing the function in combination with other claimed elements as specifically claimed. The description of the present invention has been presented for purposes of illustration and description, but is not intended to be exhaustive or limited to the invention in the form disclosed. Many modifications and variations will be apparent to

Black Kite Ex. 1002, Page 997 of 1060

those of ordinary skill in the art without departing from the scope and spirit of the invention. The embodiment was chosen and described in order to best explain the principles of the invention and the practical application, and to enable others of ordinary skill in the art to understand the invention for various embodiments with various modifications as are suited to the particular use contemplated.

Black Kite Ex. 1002, Page 998 of 1060

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/240,572	Filing Date 09/22/2011	☐ To be Mailed

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☒		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT	12/15/2011	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 20	Minus	** 120	= 0	X $30 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 1	Minus	***4	= 0	X $125 =	0	OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

AMENDMENT		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/THERESA LINDSAY/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/240,572	09/22/2011	2876	462	10131-002US1	120	4

CONFIRMATION NO. 2423

96039
McKeon Meunier Carlin & Curfman LLC
817 W. Peachtree Street, Suite 900
Atlanta, GA 30308

FILING RECEIPT

OC000000050194875

Date Mailed: 10/06/2011

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Stephen Wayne Boyer, Waltham, MA;
Nagarjuna Venna, Waltham, MA;
Megumi Ando, Cambridge, MA;

Assignment For Published Patent Application

BITSIGHT TECHNOLOGIES, INC., Waltham, MA

Power of Attorney: None

Domestic Priority data as claimed by applicant

This appln claims benefit of 61/492,287 06/01/2011
and claims benefit of 61/386,156 09/24/2010

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)

If Required, Foreign Filing License Granted: 10/03/2011

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/240,572**

Projected Publication Date: Request for Non-Publication Acknowledged

Non-Publication Request: Yes

Early Publication Request: No
**** SMALL ENTITY ****

Title

INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM

Preliminary Class

235

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as

set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 13/240,572

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A	95		N/A	
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A	310		N/A	
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A	125		N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	120 minus 20 =	* 100	x 30 =	3000	OR		
INDEPENDENT CLAIMS (37 CFR 1.16(h))	4 minus 3 =	* 1	x 125 =	125			
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $310 ($155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			0.00			
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))				0.00			
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	3655		TOTAL	

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)		RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/240,572	09/22/2011	Stephen Wayne Boyer	10131-002US1

CONFIRMATION NO. 2423

96039
McKeon Meunier Carlin & Curfman LLC
817 W. Peachtree Street, Suite 900
Atlanta, GA 30308

FORMALITIES LETTER

OC000000050194876

Date Mailed: 10/06/2011

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The oath or declaration is missing.
  A properly signed oath or declaration in compliance with 37 CFR 1.63, identifying the application by the above Application Number and Filing Date, is required.
  Note: If a petition under 37 CFR 1.47 is being filed, an oath or declaration in compliance with 37 CFR 1.63 signed by all available joint inventors, or if no inventor is available by a party with sufficient proprietary interest, is required.

The application is informal since it does not comply with the regulations for the reason(s) indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- A substitute specification in compliance with 37 CFR 1.52, 1.121(b)(3), and 1.125, is required. The substitute specification must be submitted with markings and be accompanied by a clean version (without markings) as set forth in 37 CFR 1.125(c) and a statement that the substitute specification contains no new matter (see 37 CFR 1.125(b)). The specification, claims, and/or abstract page(s) submitted is not acceptable and cannot be scanned or properly stored because:
  - The line spacing on the specification, claims, and/or abstract is not 1½ or double spaced (see 37 CFR 1.52(b)).
- Replacement drawings in compliance with 37 CFR 1.84 and 37 CFR 1.121(d) are required. The drawings submitted are not acceptable because:
  - The drawings submitted to the Office are not electronically reproducible because portions of figures 1-3 are missing and/or blurry.

Applicant is cautioned that correction of the above items may cause the specification and drawings page count to exceed 100 pages. If the specification and drawings exceed 100 pages, applicant will need to submit the required application size fee.

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- Additional claim fees of $**3125** as a small entity, including any required multiple dependent claim fee, are required. Applicant must submit the additional claim fees or cancel the additional claims for which fees are due.
- A surcharge (for late submission of filing fee, search fee, examination fee or oath or declaration) as set forth in 37 CFR 1.16(f) of $**65** for a small entity in compliance with 37 CFR 1.27, must be submitted.

SUMMARY OF FEES DUE:

Total fee(s) required within **TWO MONTHS** from the date of this Notice is $**3190** for a small entity

- $**65** Surcharge.
- Total additional claim fee(s) for this application is $**3125**
  - $**125** for **1** independent claims over 3.
  - $**3000** for **100** total claims over 20.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

Registered users of EFS-Web may alternatively submit their reply to this notice via EFS-Web.
https://sportal.uspto.gov/authenticate/AuthenticateUserLocalEPF.html

For more information about EFS-Web please call the USPTO Electronic Business Center at **1-866-217-9197** or visit our website at http://www.uspto.gov/ebc.

If you are not using EFS-Web to submit your reply, you must include a copy of this notice.

/atesfaye/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Doc Code: FAI.REQ
Document Description: Request First Action Interview

PTO/SB/413C (05-11)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

REQUEST FOR FIRST ACTION INTERVIEW (FULL PILOT PROGRAM)

Attorney Docket Number: 10131-002US1	Application Number (if known): To Be Assigned	Filing date: 2011-09-22
First Named Inventor: Stephen Boyer	Title: Information Technology Security Assessment System	

APPLICANT HEREBY REQUESTS A FIRST ACTION INTERVIEW IN THE ABOVE-IDENTIFIED APPLICATION. See Instruction Sheet on page 2.

1. The application must contain three (3) or fewer independent claims and twenty (20) or fewer total claims.

2. The application must not contain any multiple dependent claims.

3. By filing this request:

   Applicant is agreeing to make an election without traverse if the Office determines that the claims are not obviously directed to a single invention; and

   Applicant is agreeing not to request for a refund of the search fee and any excess claims fee paid in the application after the mailing or notification of the pre-interview communication prepared by the examiner.

4. Other attachments: Preliminary Amendment

Signature	Date 2011-09-22
Name (Print/Typed): Gregory J. Carlin	Registration Number 45,607

Note: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required in accordance with 37 CFR 1.33 and 11.18. Please see 37 CFR 1.4(d) for the form of the signature. If necessary, submit multiple forms for more than one signature, see below.*

[X] *Total of 1 forms are submitted.

This information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Instruction Sheet for Request for First Action Interview (Full Pilot Program)

(Not to be Submitted to the USPTO)

A grantable request must meet the following conditions:

1. The application must be a new non-reissue utility application filed under 35 U.S.C. 111(a) or an international application that has entered the national stage in compliance with 35 U.S.C. 371(c).

2. The application must contain three (3) or fewer independent claims and twenty (20) or fewer total claims. The application may not contain any multiple dependent claims.

3. The request must be filed electronically using the Office's electronic filing system, EFS-Web.

4. The claims must be directed to a single invention. If the Office determines that the claims are directed to multiple inventions (*e.g.*, in a restriction requirement), the applicant must make an election without traverse.

5. The request must be filed at least one day before a first Office action on the merits of the application appears in the Patent Application Information Retrieval (PAIR) system (*i.e.*, at least one day prior to the date when a first Office action on the merits, notice of allowability or allowance, or action under Ex parte Quayle, 1935 Dec. Comm'r Pat. 11 (1935) appears in the PAIR system). Applicant may check the status of the application using the PAIR system.

6. The request for a first action interview must include a statement that applicant agrees not to file a request for a refund of the search fee and any excess claims fees paid in the application after the mailing or notification of the Pre-Interview Communication. Any petition for express abandonment under 37 CFR 1.138(d), and request for a refund of the search fee and any excess claims fees, filed after the mailing or notification of the Pre-Interview Communication will not be granted.

For more information, see notice "Full First Action Interview Pilot Program" available on the USPTO web site at http://www.uspto.gov/patents/init_events/fairp_full.jsp

Doc Code: FAI.REQ
Document Description: Request First Action Interview

PTO/SB/413C (05-11)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

REQUEST FOR FIRST ACTION INTERVIEW (FULL PILOT PROGRAM)

Attorney Docket Number: 10131-002US1	Application Number (if known): To Be Assigned	Filing date: 2011-09-22
First Named Inventor: Stephen Boyer	Title: Information Technology Security Assessment System	

APPLICANT HEREBY REQUESTS A FIRST ACTION INTERVIEW IN THE ABOVE-IDENTIFIED APPLICATION. See Instruction Sheet on page 2.

1. The application must contain three (3) or fewer independent claims and twenty (20) or fewer total claims.

2. The application must not contain any multiple dependent claims.

3. By filing this request:

   Applicant is agreeing to make an election without traverse if the Office determines that the claims are not obviously directed to a single invention; and

   Applicant is agreeing not to request for a refund of the search fee and any excess claims fee paid in the application after the mailing or notification of the pre-interview communication prepared by the examiner.

4. Other attachments: Preliminary Amendment

Signature	Date 2011-09-22
Name (Print/Typed): Gregory J. Carlin	Registration Number 45,607

Note: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required in accordance with 37 CFR 1.33 and 11.18. Please see 37 CFR 1.4(d) for the form of the signature. If necessary, submit multiple forms for more than one signature, see below.*

[X] *Total of 1 forms are submitted.

This information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Instruction Sheet for Request for First Action Interview (Full Pilot Program)

(Not to be Submitted to the USPTO)

A grantable request must meet the following conditions:

1. The application must be a new non-reissue utility application filed under 35 U.S.C. 111(a) or an international application that has entered the national stage in compliance with 35 U.S.C. 371(c).

2. The application must contain three (3) or fewer independent claims and twenty (20) or fewer total claims. The application may not contain any multiple dependent claims.

3. The request must be filed electronically using the Office's electronic filing system, EFS-Web.

4. The claims must be directed to a single invention. If the Office determines that the claims are directed to multiple inventions (*e.g.*, in a restriction requirement), the applicant must make an election without traverse.

5. The request must be filed at least one day before a first Office action on the merits of the application appears in the Patent Application Information Retrieval (PAIR) system (*i.e.*, at least one day prior to the date when a first Office action on the merits, notice of allowability or allowance, or action under Ex parte Quayle, 1935 Dec. Comm'r Pat. 11 (1935) appears in the PAIR system). Applicant may check the status of the application using the PAIR system.

6. The request for a first action interview must include a statement that applicant agrees not to file a request for a refund of the search fee and any excess claims fees paid in the application after the mailing or notification of the Pre-Interview Communication. Any petition for express abandonment under 37 CFR 1.138(d), and request for a refund of the search fee and any excess claims fees, filed after the mailing or notification of the Pre-Interview Communication will not be granted.

For more information, see notice "Full First Action Interview Pilot Program" available on the USPTO web site at http://www.uspto.gov/patents/init_events/faipp_full.jsp

Electronic Patent Application Fee Transmittal

Application Number:	
Filing Date:	
Title of Invention:	Information Technology Security Assessment System
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Filer:	Gregory J. Carlin/Carla Key
Attorney Docket Number:	10131-002US1

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	82	82
Utility Search Fee	2111	1	270	270
Utility Examination Fee	2311	1	110	110
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	462

Electronic Acknowledgement Receipt

EFS ID:	11019096
Application Number:	13240572
International Application Number:	
Confirmation Number:	2423
Title of Invention:	Information Technology Security Assessment System
First Named Inventor/Applicant Name:	Stephen Wayne Boyer
Customer Number:	96039
Filer:	Gregory J. Carlin/Carla Key
Filer Authorized By:	Gregory J. Carlin
Attorney Docket Number:	10131-002US1
Receipt Date:	22-SEP-2011
Filing Date:	
Time Stamp:	16:56:40
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Electronic Funds Transfer
Payment was successfully received in RAM	$462
RAM confirmation Number	6168
Deposit Account	
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)

Black Kite Ex. 1002, Page 1012 of 1060

1	Transmittal of New Application	10131-002US1_Transmittal.pdf	349422 63940bd2a5de1d36cfd4fe4848e3e7594db8d64e	no	2
Warnings:					
Information:					
2	Application Data Sheet	10131-002US1_ADS.pdf	1420379 576a35347b4b32b482cd6b4c9d629abcd347c22e	no	5
Warnings:					
Information:					
3		10131-002US1_Application.pdf	913434 9fc2a550072bfc37604adf06e73f68ad1d725102	yes	36

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	23
Claims	24	31
Abstract	32	32
Drawings-other than black and white line drawings	33	36

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

4	Nonpublication request from applicant.	10131-002US1_Nonpublication Request.pdf	676061 77da4ae09eb1c63840b6a165362eefcdfd5ad5b3	no	2

Warnings:

The page size in the PDF is too large. The pages should be 8.5 x 11 or A4. If this PDF is submitted, the pages will be resized upon entry into the Image File Wrapper and may affect subsequent processing

Information:

5	First Action Interview - Enrollment Request	10131-002US1_Request_FirstActionInterview.pdf	400372 bb3913fcc81c9c25210ea4f29fa0f69193a48ab8	no	2
Warnings:					
Information:					
6	Fee Worksheet (SB06)	fee-info.pdf	32614 d648e486309701d631305bd706a662e6ec184274	no	2
Warnings:					
Information:					

Total Files Size (in bytes):	3792282

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/05 (08-08)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office. U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	10131-002US1
First Inventor	Stephen Boyer
Title	Information Technology Security Ass
Express Mail Label No.	N/A

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1. ☐ **Fee Transmittal Form** (e.g., PTO/SB/17)
2. ☑ **Applicant claims small entity status.** See 37 CFR 1.27.
3. ☑ **Specification** [*Total Pages* 32]
   Both the claims and abstract must start on a new page
   (For information on the preferred arrangement, see MPEP 608.01(a))
4. ☑ **Drawing(s)** (*35 U.S.C. 113*) [*Total Sheets* 4]
5. **Oath or Declaration** [*Total Sheets* _____]
   a. ☐ Newly executed (original or copy)
   b. ☐ A copy from a prior application (37 CFR 1.63(d))
   (for continuation/divisional with Box 18 completed)
   i. ☐ DELETION OF INVENTOR(S)
   Signed statement attached deleting inventor(s) name in the prior application, see 37 CFR 1.63(d)(2) and 1.33(b).
6. ☑ **Application Data Sheet.** See 37 CFR 1.76
7. ☐ **CD-ROM or CD-R** in duplicate, large table or Computer Program *(Appendix)*
   ☐ Landscape Table on CD
8. **Nucleotide and/or Amino Acid Sequence Submission**
   (if applicable, items a. – c. are required)
   a. ☐ Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
      i. ☐ CD-ROM or CD-R (2 copies); or
      ii. ☐ Paper
   c. ☐ Statements verifying identity of above copies

ADDRESS TO:
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

ACCOMPANYING APPLICATION PARTS

9. ☐ **Assignment Papers** (cover sheet & document(s))
   Name of Assignee _____
10. ☐ **37 CFR 3.73(b) Statement** *(when there is an assignee)* ☐ **Power of Attorney**
11. ☐ **English Translation Document** *(if applicable)*
12. ☐ **Information Disclosure Statement** (PTO/SB/08 or PTO-1449)
    ☐ Copies of citations attached
13. ☑ **Preliminary Amendment**
14. ☐ **Return Receipt Postcard** (MPEP 503)
    (*Should be specifically itemized)*
15. ☐ **Certified Copy of Priority Document(s)**
    (if foreign priority is claimed)
16. ☑ **Nonpublication Request** under 35 U.S.C. 122(b)(2)(B)(i). Applicant must attach form PTO/SB/35 or equivalent.
17. ☑ Other: Request for First Action Interview

18. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in the first sentence of the specification following the title, or in an Application Data Sheet under 37 CFR 1.76:*

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.: .....

Prior application information: *Examiner* _____ *Art Unit:* _____

19. CORRESPONDENCE ADDRESS

☑ The address associated with Customer Number: 96039 ***OR*** ☐ Correspondence address below

Name					
Address					
City		State		Zip Code	
Country		Telephone		Email	

Signature	/Gregory J. Carlin/	Date	2011-09-22
Name (Print/Type)	Gregory J. Carlin	Registration No. (Attorney/Agent)	45607

This collection of information is required by 37 CFR 1.53(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PTO/SB/14 (11-08)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10131-002US1
	Application Number	
Title of Invention	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM	

The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76.
This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.

Secrecy Order 37 CFR 5.2

☐ Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Applicant Information:

Applicant 1 Remove

Applicant Authority ◉ Inventor ○ Legal Representative under 35 U.S.C. 117 ○ Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
	Stephen	Wayne	Boyer	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Waltham	State/Province	MA	Country of Residence[i]	US

Citizenship under 37 CFR 1.41(b)[i]: US

Mailing Address of Applicant:

Address 1	299 Grove Street		
Address 2			
City	Waltham	State/Province	MA
Postal Code	02453	Country[i]	US

Applicant 2 Remove

Applicant Authority ◉ Inventor ○ Legal Representative under 35 U.S.C. 117 ○ Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
	Nagarjuna		Venna	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Waltham	State/Province	MA	Country of Residence[i]	US

Citizenship under 37 CFR 1.41(b)[i]: IN

Mailing Address of Applicant:

Address 1	324 Bishops Forest Drive		
Address 2			
City	Waltham	State/Province	MA
Postal Code	02452	Country[i]	US

Applicant 3 Remove

Applicant Authority ◉ Inventor ○ Legal Representative under 35 U.S.C. 117 ○ Party of Interest under 35 U.S.C. 118

Prefix	Given Name	Middle Name	Family Name	Suffix
	Megumi		Ando	

Residence Information (Select One) ◉ US Residency ○ Non US Residency ○ Active US Military Service

City	Cambridge	State/Province	MA	Country of Residence[i]	US

PTO/SB/14 (11-08)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10131-002US1
	Application Number	
Title of Invention	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM	

Citizenship under 37 CFR 1.41(b) [i]	US		
Mailing Address of Applicant:			
Address 1	21 Brookline Street #207		
Address 2			
City	Cambridge	**State/Province**	MA
Postal Code	02139	**Country**[i]	US

All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the **Add** button. Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below.
For further information see 37 CFR 1.33(a).

☐ **An Address is being provided for the correspondence Information of this application.**

Customer Number	96039		
Email Address	docketing@m2iplaw.com	Add Email	Remove Email

Application Information:

Title of the Invention	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM		
Attorney Docket Number	10131-002US1	**Small Entity Status Claimed**	☒
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		**Sub Class (if any)**	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)	4	**Suggested Figure for Publication (if any)**	

Publication Information:

☐ Request Early Publication (Fee required at time of Request 37 CFR 1.219)

☒ **Request Not to Publish.** I hereby request that the attached application not be published under 35 U.S. C. 122(b) and certify that the invention disclosed in the attached application **has not and will not** be the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32).
Enter either Customer Number or complete the Representative Name section below. If both sections are completed the Customer Number will be used for the Representative Information during processing.

Please Select One:	◉ Customer Number	○ US Patent Practitioner	○ Limited Recognition (37 CFR 11.9)

PTO/SB/14 (11-08)
Approved for use through 01/31/2014. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10131-002US1
	Application Number	
Title of Invention	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM	

Customer Number	96039

Domestic Benefit/National Stage Information:

This section allows for the applicant to either claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c) or indicate National Stage entry from a PCT application. Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.

Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	61/492287	2011-06-01
Prior Application Status	Pending		Remove
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)
	non provisional of	61/386156	2010-09-24

Additional Domestic Benefit/National Stage Data may be generated within this form by selecting the **Add** button. Add

Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).

Remove

Application Number	Country [i]	Parent Filing Date (YYYY-MM-DD)	Priority Claimed
			○ Yes ◉ No

Additional Foreign Priority Data may be generated within this form by selecting the **Add** button. Add

Assignee Information:

Providing this information in the application data sheet does not substitute for compliance with any requirement of part 3 of Title 37 of the CFR to have an assignment recorded in the Office.

Assignee 1 Remove

If the Assignee is an Organization check here. ☒

Organization Name	BitSight Technologies, Inc.		
Mailing Address Information:			
Address 1	738 Main Street, No. 388		
Address 2			
City	Waltham	**State/Province**	MA
Country [i]	US	Postal Code	02451-0616
Phone Number		Fax Number	
Email Address			

Additional Assignee Data may be generated within this form by selecting the **Add** button. Add

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	10131-002US1
	Application Number	
Title of Invention	INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM	

Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/Gregory J. Carlin/			Date (YYYY-MM-DD)	2011-09-22
First Name	Gregory	Last Name	Carlin	Registration Number	45607

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.

2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.

3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.

4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).

5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.

6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).

7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.

8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.

9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

CLAIMS

1. A method of evaluating information security of a third party computer system, the method comprising:

collecting at least two security characterizations of the third party computer system;

generating a composite security rating using the at least two security characterizations;

wherein the two security characterizations are derived from externally observable characteristics of the third party computer system.

2. A method of Claim 1, wherein each of the security characterizations is from an associated one of a plurality of independent entities.

3. A method of Claim 2, wherein the independent entities include commercial data sources.

4. A method of Claim 2, wherein the security characterizations include at least two data types.

5. A method of Claim 4, wherein the data types include at least one of breach disclosures, block lists, configuration parameters, malware servers, reputation, suspicious activity, spyware, white lists, compromised hosts, malicious activity, spam activity, vulnerable hosts, phishing, or e-mail viruses.

6. A method of Claim 1, wherein the security characterizations are derived without permission of the third party computer system.

7. A method of Claim 1, wherein the externally observable characteristics evidence internal security controls.

8. A method of Claim 1, wherein the externally observable characteristics are outcomes.

9. A method of Claim 1, wherein the externally observable characteristics evidence operational execution of security measures of the third party computer system.

10. A method of Claim 1, wherein the externally observable characteristics include serving of malicious code.

11. A method of Claim 1, wherein the externally observable characteristics include communications with known attacker controlled networks.

12. A method of Claim 1, wherein collecting the data and generating the ratings are repeated to generate a series of ratings.

13. A method of Claim 11, further comprising determining a trend from the series of ratings.

14. A method of Claim 12, further comprising reporting the ratings.

15. A method of Claim 13, wherein reporting includes reporting a warning based on a change in the ratings.

16. A method of Claim 14, wherein reporting includes posting the ratings and warning to a web portal.

17. A method of Claim 1, wherein collecting the security characterizations includes using tools such as WGET, RSYNC or proprietary and manual methods..

18. A method of Claim 1, further comprising mapping the third party computer system to an IP space and using the IP space for collecting the security characterizations.

19. A method of Claim 18, wherein mapping includes querying a regional internet registry.

20. A method of Claim 19, wherein querying includes submitting an entity name.

21. A method of Claim 20, wherein submitting the entity name includes submitting spelling variations of the entity name.

22. A method of Claim 18, wherein mapping includes using a domain name associated with the third party computer system.

23. A method of Claim 22, wherein mapping includes using a dig tool on the domain name to determine a published IP address.

24. A method of Claim 23, wherein mapping includes probing addresses around the published IP address.

25. A method of Claim 24, wherein probing includes probing addresses in powers of 2 around the published IP address.

26. A method of Claim 22, wherein mapping includes adapting the domain name with server naming conventions.

27. A method of Claim 26, wherein mapping includes using nslookup to verify an IP address associated with the domain name.

28. A method of Claim 1, wherein generating the composite security rating includes assessing a vulnerability and resilience of the third party computer systems.

29. A method of Claim 28, wherein vulnerability includes a number of IP addresses with malicious behavior.

30. A method of Claim 28, wherein resilience is inversely proportional to a duration of malicious behavior.

31. A method of Claim 18, wherein the IP space includes a plurality of IP addresses.

32. A method of Claim 31, further comprising determining at least one badness score for each of the IP addresses.

33. A method of Claim 32, wherein the badness score corresponds to an intensity and duration of malicious activity determined from one of the security characterizations.

34. A method of Claim 33, wherein generating the composite security rating includes aggregating a plurality of badness scores.

35. A method of Claim 34, wherein generating the composite security rating includes aggregating the IP addresses associated with the third party computer system.

36. A method of Claim 31, wherein determining the badness score includes adjusting for false positives in the security characterizations.

37. A method of Claim 36, wherein adjusting for false positives includes determining occurrence of an event which includes persistent, reported activity on one of the IP addresses for a predetermined period of time.

38. A method of Claim 37, wherein adjusting for false positives includes determining an intensity of the IP address for the predetermined period of time.

39. A method of Claim 38, wherein the predetermined period of time is at least one day.

40. A method of Claim 38, wherein the predetermined period of time accounts for inactive periods.

41. A method of Claim 40, wherein the maximum inactive period is 3 days.

42. A method of Claim 38, wherein determining an intensity includes increasing intensity in proportion to a number of reporting targets from the security characterizations.

43. A method of Claim 33, wherein determining the badness score includes weighting recent events heavier than older events.

44. A method of Claim 32, wherein determining the badness score includes assigning a raw score for each of the IP addresses appearing on a block list of one of the security characterizations.

45. A method of Claim 44, wherein the block list does not delist the IP address until requested.

46. A method of Claim 45, further comprising attenuating the raw score after delisting of the IP address.

47. A method of Claim 46, wherein attenuating is at an exponential decay.

48. A method of Claim 32, wherein determining the badness score includes generating a raw score in proportion to a CIDR block size.

49. A method of Claim 35, wherein generating the composite security rating includes normalizing the aggregate of the plurality of badness scores.

50. A method of Claim 49, wherein normalizing includes normalizing based on at least one of network size or number of employees.

51. A method of Claim 32, wherein the security characterizations include non-negative information.

52. A method of Claim 1, further comprising correlating the composite security score with statistical outcomes and adjusting the step of generating based on the statistical outcomes.

53. A method of Claim 1, further comprising determining a confidence range of the composite security score.

54. A method of Claim 53, wherein the confidence range is based on redundancy of the security characterizations.

55. A method of Claim 54, wherein the confidence range is based on a size of the third party computer system.

56. A method of Claim 1, further comprising predicting future information security performance of the third party computer system using the security characterizations.

57. A method of Claim 1, further comprising determining an accuracy of each of the security characterizations.

58. A method of Claim 57, wherein determining the accuracy includes determining a level of coverage of the third party computer system by the security characterizations.

59. A system for evaluating information security of third party computer systems, the system comprising:

a data collection module configured to receive at least two security characterizations, each of the security characterizations describing a security outcome associated with one of the third party computer systems; and

a scoring module connected in communication with the data collection module and configured to use the security characterizations to generate a composite security score for the associated third party computer system;

wherein the security outcome is derived from external investigation of the associated third party computer system.

60. A system of Claim 59, wherein each of the security characterizations is from an associated one of a plurality of independent entities.

61. A system of Claim 60, wherein the independent entities include commercial data sources.

62. A system of Claim 60, wherein the security characterizations include at least two data types.

63. A system of Claim 62, wherein the data types include at least one of breach disclosures, block lists, configuration, malware servers, reputation, suspicious activity, spyware, white lists, compromised hosts, malicious activity, spam activity, vulnerable hosts, phishing, or e-mail viruses.

64. A system of Claim 59, wherein the security characterizations are derived without permission of the third party computer system.

65. A system of Claim 59, wherein the externally observable characteristics evidence internal security controls.

66. A system of Claim 59, wherein the externally observable characteristics are outcomes.

67. A system of Claim 59, wherein the externally observable characteristics evidence operational execution of security measures of the third party computer system.

68. A system of Claim 59, wherein the externally observable characteristics include serving of malicious code.

69. A system of Claim 59, wherein the externally observable characteristics include communications with known attacker controlled networks.

70. A system of Claim 59, wherein the scoring module is configured to generate a series of ratings.

71. A system of Claim 70, further comprising a trend module configured to determine a trend from the series of ratings.

72. A system of Claim 71, further comprising a reporting module configured to report the ratings.

73. A system of Claim 72, wherein the reporting module is configured to report a warning based on a change in the ratings.

74. A system of Claim 74, wherein the reporting module is configured to post the ratings and warning to a web portal.

75. A system of Claim 59, wherein the data collection module is configured to collect the security characterizations includes using tools such as WGET, RSYNC or proprietary and manual methods.

76. A system of Claim 59, further comprising a mapping module configured to map the third party computer system to an IP space and use the IP space for collecting the security characterizations.

77. A system of Claim 76, wherein the mapping module is further configured to submit a query a regional internet registry.

78. A system of Claim 77, wherein the query includes an entity name.

79. A system of Claim 78, wherein the query includes spelling variations of the entity name.

80. A system of Claim 76, wherein the mapping module is configured to obtain a domain name associated with the third party computer system.

81. A system of Claim 80, wherein the mapping module is configured to use a dig tool on the domain name.

82. A system of Claim 81, wherein the mapping module is configured to probe addresses around the published IP address.

83. A system of Claim 82, wherein the mapping module is configured to probe addresses in powers of 2 around the published IP address.

84. A system of Claim 80, wherein the mapping module is configured to adapt

the domain name with server naming conventions.

85. A system of Claim 84, wherein the mapping module is configured to use nslookup to verify an IP address associated with the domain name.

86. A system of Claim 59, the scoring module is configured to assess a vulnerability and resilience of the third party computer systems.

87. A system of Claim 86, wherein the vulnerability includes a number of IP addresses with malicious behavior.

88. A system of Claim 86, wherein the resilience is inversely proportional to a duration of the malicious behavior.

89. A system of Claim 76, wherein the IP space includes a plurality of IP addresses.

90. A system of Claim 89, further comprising a badness module configured to determine a badness score for each of the IP addresses.

91. A system of Claim 90, wherein the badness score corresponds to an intensity and duration of malicious activity determined from one of the security characterizations.

92. A system of Claim 91, wherein the scoring module is configured to aggregate a plurality of the badness scores.

93. A system of Claim 92, wherein the scoring module is further configured to aggregate the IP addresses associated with the third party computer system.

94. A system of Claim 90, wherein the badness module is further configured to adjust for false positives in the security characterizations.

95. A system of Claim 94, wherein the badness module is further configured to determine an occurrence of an event which includes persistent, reported activity on one of the IP addresses for a predetermined period of time.

96. A system of Claim 95, wherein the badness module is configured to determine an intensity of the IP address for the predetermined period of time.

97. A system of Claim 96, wherein the predetermined period of time is a day.

98. A system of Claim 96, wherein the predetermined period of time accounts for inactive periods.

99. A system of Claim 98, wherein the maximum inactive period is a configurable number.

100. A system of Claim 96, wherein the intensity is in proportion to a number of

reporting targets from the security characterizations.

101. A system of Claim 91, wherein the badness module is configured to weight recent events heavier than older events.

102. A system of Claim 90, wherein the badness module is configured to assign a flat score for each of the IP addresses appearing on a block list of one of the security characterizations.

103. A system of Claim 102, wherein the block list does not delist the IP address until requested.

104. A system of Claim 103, wherein the badness module is configured to attenuate the flat score after delisting of the IP address.

105. A system of Claim 104, wherein the badness module is configured to attenuate the flat score at an exponential decay.

106. A system of Claim 90, wherein the badness module is configured to determine the badness score by generating a flat score in proportion to a CIDR block size.

107. A system of Claim 93, wherein the scoring module is configured to normalize the aggregate of the plurality of badness scores.

108. A system of Claim 107, wherein the scoring module is configured to normalize based on at least one of network size or number of employees.

109. A system of Claim 90, wherein the security characterizations include non-negative information.

110. A system of Claim 59, further comprising an accuracy module configured to correlate the composite security score with statistical outcomes and adjust the scoring module to account for the correlation.

111. A system of Claim 59, further comprising a confidence module configured to determine a confidence range of the composite security score.

112. A system of Claim 111, wherein the confidence range is based on redundancy of the security characterizations.

113. A system of Claim 112, wherein the confidence range is based on a size of the third party computer system.

114. A system of Claim 59, further comprising a predictive module configured to predict future information security performance of the third party computer system using the security characterizations.

115. A system of Claim 59, further comprising an accuracy module configured to determine an accuracy of each of the security characterizations.

116. A system of Claim 115, wherein the accuracy module is configured to determine a level of coverage of the third party security system using the security characterizations.

117. A method of evaluating information security of a third party computer system, the method comprising:

collecting at least one security characterization of the third party computer system;

generating a composite security score using the at least one security characterization;

wherein the at least one security characterization is derived from externally observable characteristics of the third party computer system; and

wherein the composite security score has a relatively high likelihood of corresponding to an internal audit score.

118. A method of Claim 117, further comprising one or more of a plurality of the methods of Claims 2-58.

119. A system for evaluating information security of third party computer systems, the system comprising:

a data collection module configured to receive at least one security characterization, the security characterization describing a security outcome associated with one of the third party computer systems; and

a scoring module connected in communication with the data collection module and configured to use the security characterization to generate a composite security score for the associated third party computer system;

wherein the security outcome of the security characterization is derived from external investigation of the associated third party computer system;

wherein the composite score has a relatively high likelihood of corresponding to an internal audit score.

120. A system of Claim 119, further comprising one or more of a plurality of the systems of Claims 59-116.

ABSTRACT

A method and system for creating a composite security rating from security characterization data of a third party computer system. The security characterization data is derived from externally observable characteristics of the third party computer system. Advantageously, the composite security score has a relatively high likelihood of corresponding to an internal audit score despite use of externally observable security characteristics. Also, the method and system may include use of multiple security characterizations all solely derived from externally observable characteristics of the third party computer system.

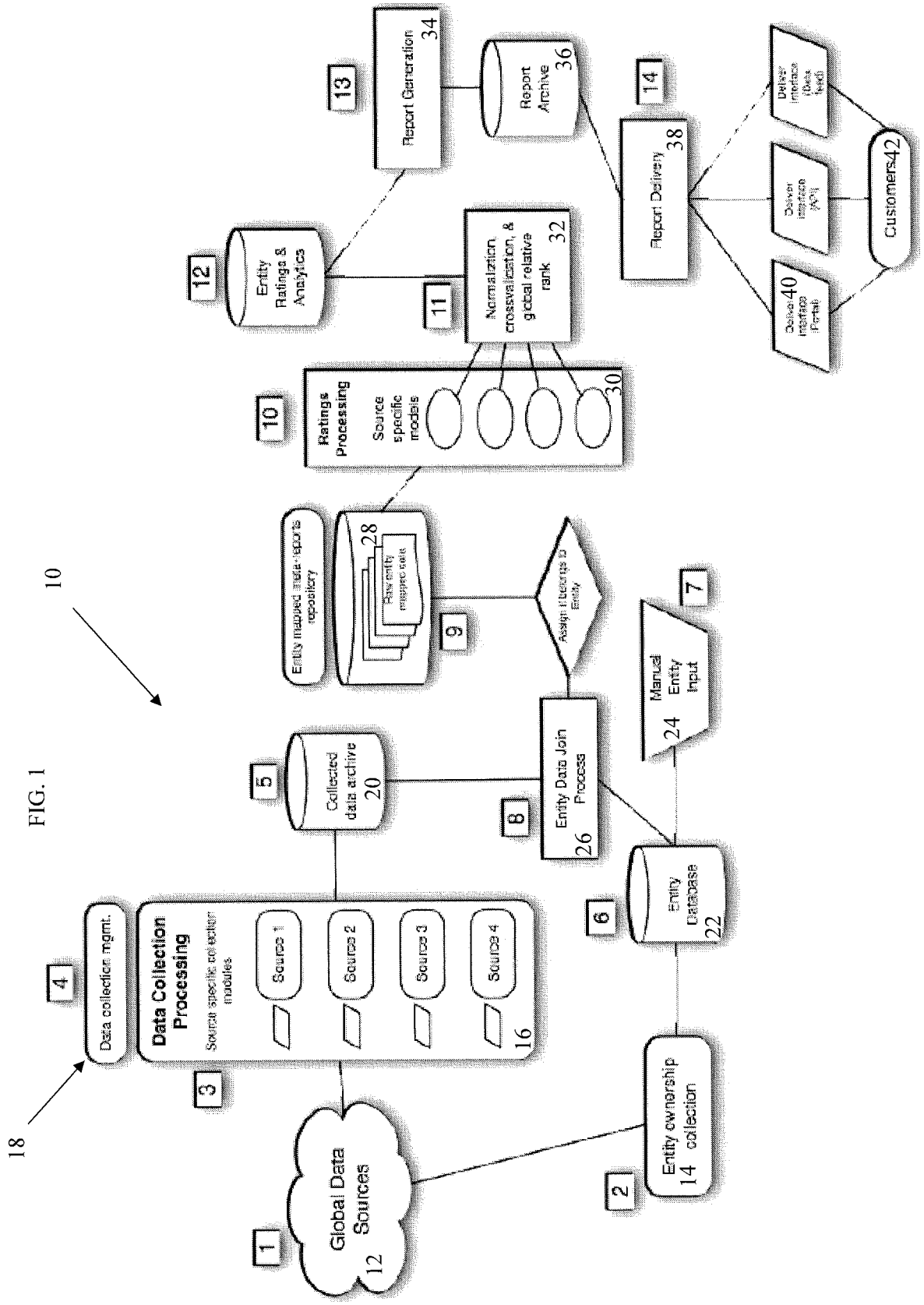


FIG. 1

Black Kite Ex. 1002, Page 1031 of 1060

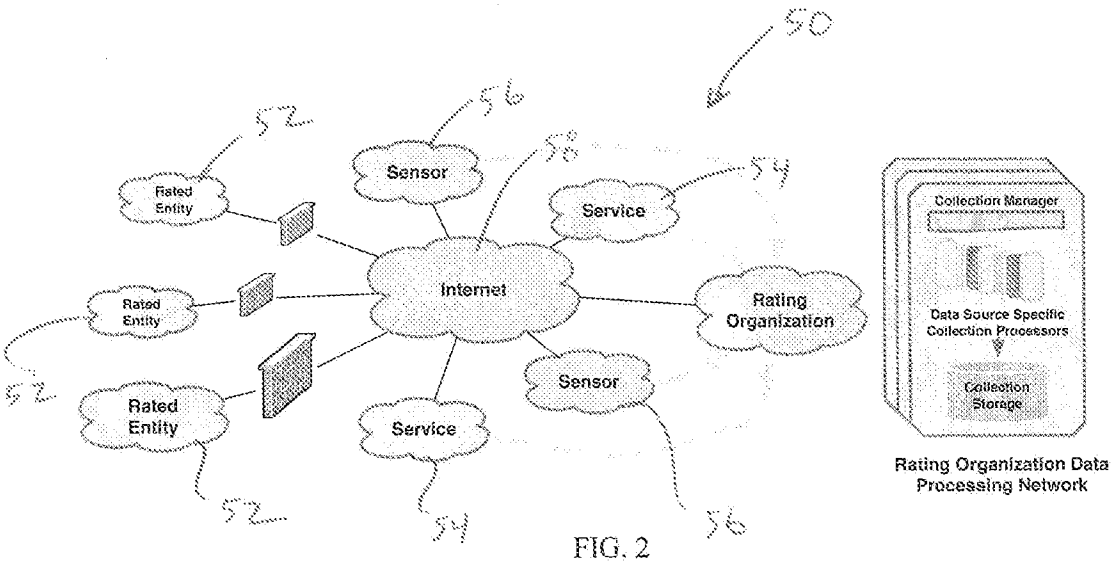


FIG. 2

Black Kite Ex. 1002, Page 1032 of 1060

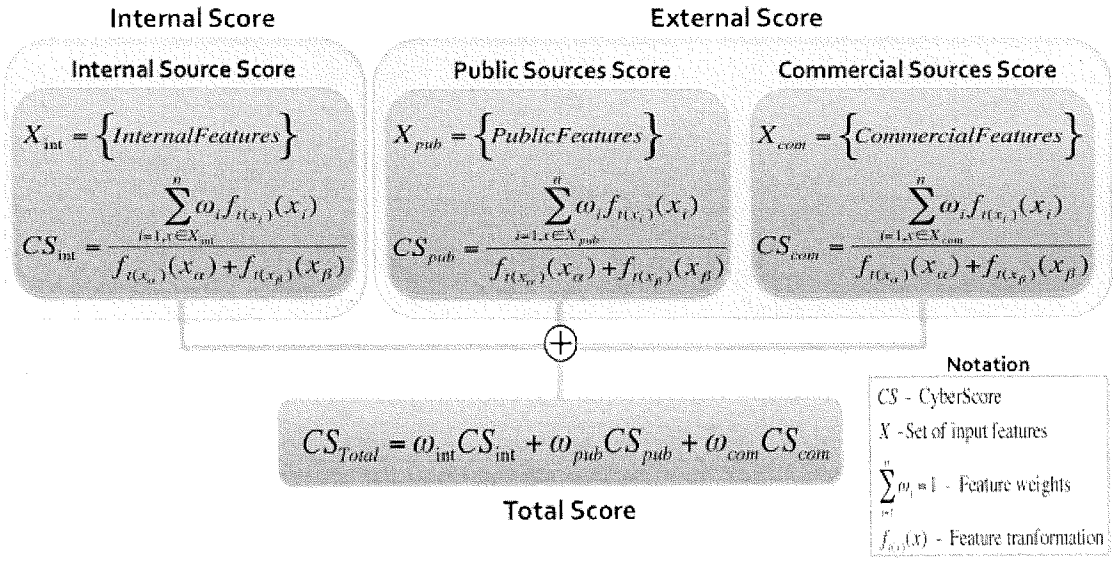
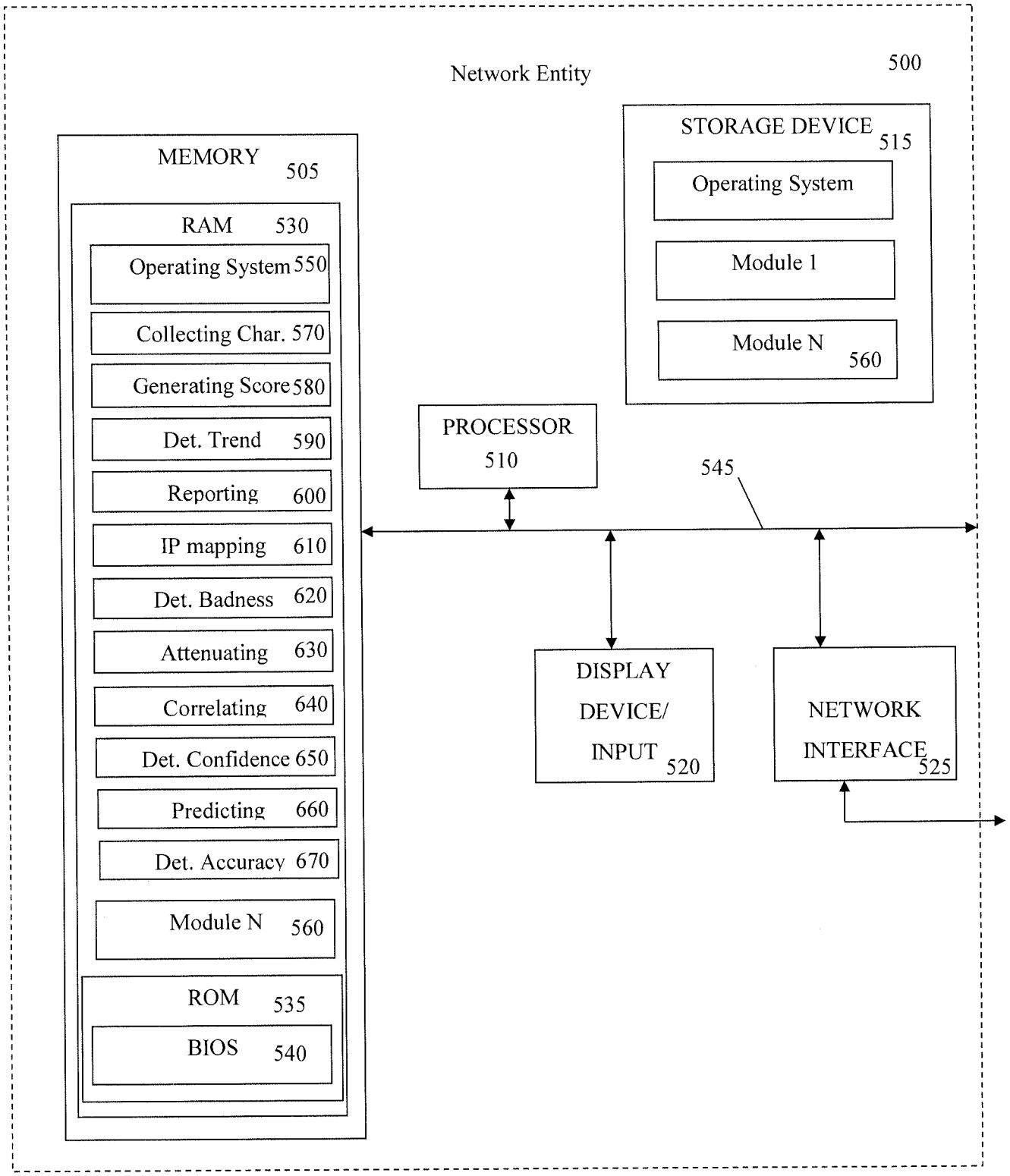


FIG. 3

Black Kite Ex. 1002, Page 1033 of 1060

FIG. 4


Network Entity
500
MEMORY
505
RAM
530
Operating System
550
Collecting Char.
570
Generating Score
580
Det. Trend
590
Reporting
600
IP mapping
610
Det. Badness
620
Attenuating
630
Correlating
640
Det. Confidence
650
Predicting
660
Det. Accuracy
670
Module N
560
ROM
535
BIOS
540
STORAGE DEVICE
515
Operating System
Module 1
Module N
560
PROCESSOR
510
545
DISPLAY
DEVICE/
INPUT
520
NETWORK
INTERFACE
525

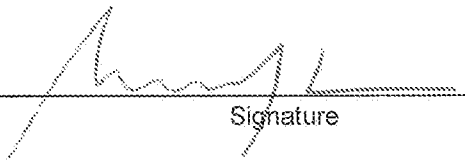
PTO/SB/35 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

NONPUBLICATION REQUEST UNDER 35 U.S.C. 122(b)(2)(B)(i)

First Named Inventor	Stephen Boyer
Title	Information Technology Security Assessment System
Attorney Docket Number	10131-002US1

I hereby certify that the invention disclosed in the attached application **has not and will not be** the subject of an application filed in another country, or under a multilateral international agreement, that requires publication at eighteen months after filing.

I hereby request that the attached application not be published under 35 U.S.C. 122(b).



Signature

9/22/11

Date

Gregory J. Carlin

Typed or printed name

45,607

Registration Number, if applicable

(404) 645-7700

Telephone Number

This request must be signed in compliance with 37 CFR 1.33(b) and submitted with the application **upon filing.**

Applicant may rescind this nonpublication request at any time. If applicant rescinds a request that an application not be published under 35 U.S.C. 122(b), the application will be scheduled for publication at eighteen months from the earliest claimed filing date for which a benefit is claimed.

If applicant subsequently files an application directed to the invention disclosed in the attached application in another country, or under a multilateral international agreement, that requires publication of applications eighteen months after filing, the applicant **must** notify the United States Patent and Trademark Office of such filing within forty-five (45) days after the date of the filing of such foreign or international application. **Failure to do so will result in abandonment of this application (35 U.S.C. 122(b)(2)(B)(iii)).**

This collection of information is required by 37 CFR 1.213(a). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 6 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

SCORE Placeholder Sheet for IFW Content

Application Number: 13240572 Document Date: 9/22/2011

The presence of this form in the IFW record indicates that the following document type was received in electronic format on the date identified above. This content is stored in the SCORE database.

- Drawings

Since this was an electronic submission, there is no physical artifact folder, no artifact folder is recorded in PALM, and no paper documents or physical media exist. The TIFF images in the IFW record were created from the original documents that are stored in SCORE.

To access the documents in the SCORE database, refer to instructions developed by SIRA.

At the time of document entry (noted above):

- Examiners may access SCORE content via the eDAN interface using the Supplemental Content tab.
- Other USPTO employees can bookmark the current SCORE URL (http://es/ScoreAccessWeb/).
- External customers may access SCORE content via the Public and Private PAIR interfaces using the Supplemental Content tab.

Form Revision Date: May 1, 2009

INFORMATION TECHNOLOGY SECURITY ASSESSMENT SYSTEM

ACKNOWLEDGEMENT

This invention was made with government support under 1127185 awarded by the National Science Foundation. The government has certain rights to this invention.

CROSS-REFERENCE TO RELATED APPLICATIONS

The present application claims priority to U.S. Prov. Pat. App. No. 61/386,156 entitled "Enterprise Information Security Score" and filed on Sept. 24, 2010; and 61/492,287 entitled "Information Technology Security Assessment System" and filed on June 1, 2011 which are hereby incorporated herein in their entirety by reference.

BACKGROUND

The present invention relates to systems for determining the security of information systems and, in particular, for evaluating the security of third-party computer systems.

When a company wants to reduce its cyber security risk of doing business with another company's computer systems, it either performs, or hires an outside firm to perform, a cyber security assessment of the other company to determine if it is following good security practices. The theory is that these good practices make it difficult for attackers to compromise the networks of the other company. If the auditing company is satisfied with the assessment, it may choose to continue doing business with the other company. Or, it may ask the other company to make some improvements to its security systems or terminate the business relationship.

Generally, these audits are slow, expensive and impractical given the high volume of service provider security systems that need to be characterized by the company. And, the inventors have noted that audits are not entirely predictive of the performance of the security systems.

SUMMARY

A method and system is disclosed for creating a composite security rating from security characterization data of a third party computer system. The security

characterization data is derived from externally observable characteristics of the third party computer system. Advantageously, the composite security rating has a relatively high likelihood of corresponding to an internal audit score despite use of externally observable security characteristics. Also, the method and system may include use of multiple security characterizations all solely derived from externally observable characteristics of the third party computer system.

A method of evaluating information security of a third party computer system is disclosed. The method includes collecting at least two security characterizations of the third party computer system. A composite security rating is generated using the at least two security characterizations. Advantageously, the two security characterizations are derived from externally observable characteristics of the third party system.

Each of the security characterizations may be from an associated one of a plurality of independent entities. For example, the independent entities may include commercial data sources. Also, the security characterizations may be derived without permission of the third party system.

The security characterizations may include multiple data types, such as breach disclosures, block lists, configuration parameters, malware servers, reputation metrics, suspicious activity, spyware, white lists, compromised hosts, malicious activity, spam activity, vulnerable hosts, phishing, user-behavior or e-mail viruses. The externally observable characteristics may also include serving of malicious code or communications with known attacker controlled networks.

The externally observable characteristics may be evidence of internal security controls or outcomes or operational execution of security measures of the third party computer system.

The collecting and generating steps may be repeated to generate a series of scores and the series examined to determine a trend. Also, the scores may be reported to a consumer. For instance, reporting may include reporting a warning based on a change in the scores. Or, reporting may include posting the score and warning to a web portal.

Collecting the security characterizations may include using various tools such as WGET, RSYNC, CURL or interfaces that may be characterization specific.

The method may also include mapping the third party computer system to an IP space and using the IP space for collecting the security characterizations. Mapping, for

example, may include querying a Regional Internet Registry (RIR), such as by submitting an entity name to the RIR. Querying an entity name may include querying for variations of the entity name.

Mapping may also include using a domain name associated with the third party computer system. For example, tools such as nslookup or dig may be used on the domain name to determine a published IP address. Mapping may also include probing addresses around the published IP address. For example, IP addresses could be probed in powers of two around the published IP address. Mapping could also include adapting the domain name to server naming conventions and using tools like nslookup to verify an IP address associated with the domain name.

Generating the composite security rating may include assessing vulnerability and resilience of the third party computer systems. Vulnerability, for example, may include a number of IP addresses with malicious behavior. Resilience may be inversely proportional to a duration of malicious behavior.

The IP space may include a plurality of IP addresses. And, the composite security rating may correspond to an intensity and duration of malicious activity determined from one of the security characterizations. Generation of the composite security rating may include aggregation of a plurality of individual security metrics and/or the IP addresses associated with the third party computer system.

Determination of the individual security metric may include adjusting for false positives in the security characterizations. Correlating data across multiple related security characterizations may help improve the quality of any single security characterization. Further, adjusting for false positives may include determining an occurrence of an event, which includes persistent, reported activity on one of the IP addresses for a predetermined period of time. It may also include determining an intensity of the IP address for the predetermined period of time, such as a day.

Determining the intensity may include increasing intensity in proportion to a number of reporting targets from the security characterizations.

Determining an individual security metric may include assigning a raw score for each of the IP addresses appearing on a block list as one of the security characterizations. After an IP address is delisted, the raw score may be exponentially attenuated.

The individual security metric may also incorporate a raw score in proportion to a

CIDR block size.

Individual security metrics or the composite ratings may be normalized based on, for example, network size or a number of employees.

Security characterizations may also include positive information about an organization that's aggregated into the composite rating.

The method could also include statistically correlating the composite security rating with actual outcomes and adjusting the generating step based on the statistical correlations.

Further, the method may include determining a confidence range of the composite security rating. For example, the confidence range may be based on a redundancy of the security characterizations or a size of the third party computer system.

The method may also include determining an accuracy of each of the security characterizations, such as by determining a level of coverage of the third party computer system by the security characterizations.

Also disclosed herein are a system and computer program product for data collection and scoring, including systems and software for performing the methods described above.

Another method may include generating a composite security rating using at least one security characterization that's derived from externally observable characteristics of the third party computer system wherein the composite security rating has a relatively high likelihood of corresponding to an internal audit score.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

Figure 1 is a schematic of a system for evaluating information security;
Figure 2 is a schematic of a system for gathering security data from external sensors;
Figure 3 is a schematic of a composite security rating calculation; and
Figure 4 is a schematic of a distributed system for evaluating information security.

DETAILED DESCRIPTION

Generally, the present invention includes a method, system and computer program product for creating composite security ratings from security characterization data of a third party computer system. The security characterization data is derived from externally observable characteristics of the third party computer system. Advantageously, the composite security rating has a relatively high likelihood of corresponding to an internal

audit score despite use of externally observable security characteristics. Also, the method and system may include use of multiple security characterizations all solely derived from externally observable characteristics of the third party computer system.

The terminology used herein is for the purpose of describing particular embodiments only and is not intended to be limiting of the invention. As used herein, the singular forms "a", "an" and "the" are intended to include the plural forms as well, unless the context clearly indicates otherwise. It will be further understood that the terms "comprises" and/or "comprising," when used in this specification, specify the presence of stated features, integers, steps, operations, elements, and/or components, but do not preclude the presence or addition of one or more other features, integers, steps, operations, elements, components, and/or groups thereof.

The corresponding structures, materials, acts, and equivalents of all means or step plus function elements in the claims below are intended to include any structure, material, or act for performing the function in combination with other claimed elements as specifically claimed. The description of the present invention has been presented for purposes of illustration and description, but is not intended to be exhaustive or limited to the invention in the form disclosed. Many modifications and variations will be apparent to those of ordinary skill in the art without departing from the scope and spirit of the invention. The embodiment was chosen and described in order to best explain the principles of the invention and the practical application, and to enable others of ordinary skill in the art to understand the invention for various embodiments with various modifications as are suited to the particular use contemplated.

Any combination of one or more computer readable medium(s) may be utilized. The computer readable medium may be a computer readable signal medium or a computer readable storage medium. A computer readable storage medium may be, for example, but not limited to, an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, or device, or any suitable combination of the foregoing. More specific examples (a non-exhaustive list) of the computer readable storage medium would include the following: an electrical connection having one or more wires, a portable computer diskette, a hard disk, a random access memory (RAM), a read-only memory (ROM), an erasable programmable read-only memory (EPROM or Flash memory), an optical fiber, a portable compact disc read-only memory (CD-ROM), an optical storage device, a magnetic

storage device, or any suitable combination of the foregoing. In the context of this document, a computer readable storage medium may be any tangible medium that can contain, or store a program for use by or in connection with an instruction execution system, apparatus, or device.

A computer readable signal medium may include a propagated data signal with computer readable program code embodied therein, for example, in baseband or as part of a carrier wave. Such a propagated signal may take any of a variety of forms, including, but not limited to, electro-magnetic, optical, or any suitable combination thereof. A computer readable signal medium may be any computer readable medium that is not a computer readable storage medium and that can communicate, propagate, or transport a program for use by or in connection with an instruction execution system, apparatus, or device.

Program code embodied on a computer readable medium may be transmitted using any appropriate medium, including but not limited to wireless, wireline, optical fiber cable, RF, etc., or any suitable combination of the foregoing.

Computer program code for carrying out operations for aspects of the present invention may be written in any combination of one or more programming languages, including an object oriented programming language such as Java, Smalltalk, C++ or the like and conventional procedural programming languages, such as the "C" programming language or similar programming languages. The program code may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider).

Aspects of the present invention are described below with reference to flowchart illustrations and/or block diagrams of methods, apparatus (systems) and computer program products according to embodiments of the invention. It will be understood that each block of the flowchart illustrations and/or block diagrams, and combinations of blocks in the flowchart illustrations and/or block diagrams, can be implemented by computer program instructions. These computer program instructions may be provided to a processor of a general purpose computer, special purpose computer, or other programmable data

processing apparatus to produce a machine, such that the instructions, which execute via the processor of the computer or other programmable data processing apparatus, create means for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

These computer program instructions may also be stored in a computer readable medium that can direct a computer, other programmable data processing apparatus, or other devices to function in a particular manner, such that the instructions stored in the computer readable medium produce an article of manufacture including instructions which implement the function/act specified in the flowchart and/or block diagram block or blocks.

The computer program instructions may also be loaded onto a computer, other programmable data processing apparatus, or other devices to cause a series of operational steps to be performed on the computer, other programmable apparatus or other devices to produce a computer implemented process such that the instructions which execute on the computer or other programmable apparatus provide processes for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

Referring again to Fig. 1, a system 10 for evaluating information security of a third party computer system includes the following systems: a global data source 12, an entity ownership collector 14, a data collection processor 16, a data collection management 18, a data archive 20, an entity database 22, a manual entity input 24, an entity data join process 26, an entity mapped meta-reports repository 28, a ratings processing 30, a normalization, consolidation and global relative rank 32, a report generation 34, a report archive 36 and a report delivery 38 systems. Different delivery modules 40 are configured to use different methods to deliver the reports to customers 42.

The global data source system 12 obtains data sources that characterize any observation about an entity (e.g., a third party computer system) and these sources can be highly varied and disparate. Each data source has a particular vantage point of the security related characteristics of entities.

The entity ownership collection system 14 gathers information about an entity. This includes information about which IT assets an entity owns, controls, uses, or is affiliated with. Examples of asset ownership include control and operation of an Internet Protocol (IP) network address range or computer services such as web servers residing within that address block. Information about entities also includes relationships such as subsidiaries,

affiliates, etc., that describe entity association.

The data collection processing system 16 includes custom modules configured to collect and process unique data sources.

The data collection management system 18 is configured to schedule and coordinate the constant collection of the different data sources.

The data archive 20 is configured to store all of the terabytes of data constantly collected by the data collection management system 18.

The entity database 22 holds all of the information about an entity such as its name, address, web site address, industry sector, IP address ranges owned, etc. This data base includes the "Entity Map" which maps data back to an entity. For example, if observations are made about a particular IP address, the IP address can be looked up in the entity map to determine which entity controls or owns that address. This database is populated by automatic or manual data collection methods, or combinations thereof.

The manual entity input system is configured to place non-automatic data on an entity into the entity database 22.

The entity data join process or system 26 is configured to match the collected data to the entity. In most instances, this is a computationally expensive operation because it requires going though all of the data collected and performing the map operation. Any evidence of security outcomes or configurations in the larger data collection pool is then assigned to an entity based on the entity map.

The entity mapped meta-reports repository 28 contains data summaries of observations made with respect to a particular entity for each data set after the map/join process is complete.

The ratings processing system 30 may include custom models for applying data source specific ratings to determine an entity rating. Each data source generally requires a custom model due to the unique nature of that data source. Each model accounts for the custom attributes and idiosyncrasies of the different data sources that have been mapped to the entity being rated. Custom data source models can account for any data source feature including temporal and cross-data source behaviors.

The ratings normalization, cross-validation, and relative ranking system 32 is configured to normalize ratings so appropriate entity-to-entity comparisons can be made and the ratings are normalized and ranked within sectors or peer-groups and globally.

An entity and rating analytics repository or archive 36 is configured to hold all of the ratings data and resulting analytics produced by the ratings process.

A report generation system 34 takes the ratings and analytics and generates report objects. These objects are not rendered into any particular presentation format at this stage but are in a generic intermediary format that can be then transformed into a specific deliverable format.

A report delivery system 38 is configured to translate generic reports into a specific report format. Examples of these formats include HTML, PDF, text, and XML. Delivery modules 40 are different methods for delivering the reports include by web portal, API or data feed.

Advantages include ratings based on the quality of outcomes of the information security practices of the third party computer systems and enablement of comparisons of ratings across organizations. The system 10 can be entirely, or to a large extent, automated and need not have the permission of the entity being rated. The reports will allow risk management professionals to monitor, assess and mitigate partner risk by up-to-date ratings due to its persistent monitoring of the third party computer systems. Also, the portal may provide for location of new partners, such as suppliers, with lower risk profiles and improved security postures.

Unlike internal audit systems, the system 10 is not relying upon a correlation between practices and outcomes. Instead, evidence of actual security outcomes is collected through the data source partners.

Also advantageously, trial data on 50 entities revealed that rankings produced using the system 10 matched internal evaluations. In some cases the system 10 revealed problems with the entities not revealed by internal evaluations.

Data Sources

External ratings from data sources available outside an entity provide an information security based view into internal workings of the organization. For example, infection by malicious software can be determined using non-invasive website scanning technology. Communication between the entity computer system and known attacker controlled networks may reveal when the computer system has been compromised. Also, if an entity computer system is serving malicious code to visitors the system was compromised at some

point. The entity may not have the capability to detect such compromises or cannot quickly react operationally to resolve the issue. External observations also can measure operational execution, which may not occur despite good internal policies.

A diverse set of network sensors and services around the Internet collect and observe information about the third party entity computer systems. The system 10 then gathers, processes, and stores the data collected about entities from the sensors and service providers using custom developed data source specific collection processors. The collection manager 18 automates the scheduling and execution of the different collectors.

The global data source system 12 includes hundreds of potential data sources, including, for example during experimental testing, 97 data sources owned by 37 organizations. At least 82 data sources are on active collection, being stored on the data archive 20. Trial ratings were performed on at least 11 data sources from 7 organizations. Rankings were produced on nearly 600 different entities.

A data source is a single type of data from a single organization. For example, if two organizations provide a list of hosts that participate in phishing attacks, they are counted as two data sources. The 15 types of data in Table 3 all provide different information security related views of an organization. New types of data and new sources of existing data types are constantly added to the data sources used to characterize the performance of the entity. Breach disclosures for example indicate that an organization has experienced a particular kind of data or integrity breach. Configuration data on the other hand provides any number of configuration related information and could for example state the type of encryption used on the organization's website.

Table 1 Data Sources Summary

Total Data Sources	97
Total Sourcing Organizations	37
Total Sources on Active Collection	82
Total Different Source Types	15

Table 3 Data Source Types

Breach Disclosures	Spam Activity

Block Lists	Vulnerable Hosts
Configuration Parameters	Spyware
Compromised Hosts	Whitelists
Malicious Activity	Email viruses
Malware Servers	Multi-type
Reputation	Phishing
Suspicious Activity	User Behavior

Of the 97 data sources identified, 82 are on "Active Collection" meaning there is a method for obtaining the data source and that its collection is automated. The high degree of automation helps to satisfy the methodology objective for adoption of techniques that are principally automated.

Table 2 lists the 6 collections methods employed for data acquisition with the "Unknown" category meaning that the sources are identified but the method and ability to collect that data source has yet be determined. The method Instances are the number of data sources that are collected using that particular method. For example, 32 of the sources are collected using the network file transfer and synchronization tool rsync (http://samba.anu.edu.au/rsync/).

Table 2 Data Collection Methods

Methods	Instances	Methods	Instances
WGET	35	WHOIS	1
RSYNC	32	HTTP GET	1
API	13	UNKNOWN	9
MANUAL	6		

A collection processing infrastructure 50, configured to build and validate composite security ratings, is shown in Fig. 2. A plurality of different clouds represents different network segments. Rated Entity clouds 52 are organizations for which the system 10 generates a rating. Those entities include an entity perimeter or boundary, indicated by the firewall that connects to the Internet. Services clouds 54 provide data or reports on observed activity from a rated entity 52. An example of a report from a Service 54 could be a list of hosts that have been participating in malicious activity. Services use Sensor networks 56 to

observe the behavior of entities. For example, a sensor could observe SPAM messages sent from a rated entity network 52 to the Internet 58.

Entity Mapping

There is no single central repository that holds information about the IP address allocation. Determining the correct and complete IP address space owned by a given entity improves the reliability and robustness of a rating.

In general, Regional Internet Registries (RIRs) manage the allocation and registration of Internet number resources (IP Addresses, Autonomous System Numbers, etc.) within a particular region of the world. There are five RIRs - ARIN for North America, AfriNIC for Africa, APNIC for Asia Pacific, RIPE for Europe, Middle East, Central Asia, and LACNIC for Latin America.

The RIRs allocate the address space to service providers, corporations, universities, etc. The RIRs provide various interfaces that enable queries of the RIR to determine who owns a given IP address. It is also possible to query the database by an entity name and get a list of IP addresses allocated to that entity. Despite lack of standardization of entity names in the RIR databases, well chosen queries can result in a very high coverage of addresses owned by an entity.

Another problem is that RIRs often allocate large chunks of addresses to Internet Service Providers (ISPs) who go on to allocate smaller address spaces to their customers. ISPs are under no obligation to report this data back to anyone. Most small companies contract with their local ISP for Internet access and don't obtain addresses from RIRs.

These problems are addressed by the entity ownership collection system 14 being configured to execute various heuristic processes including the following non-limiting list of examples:

1. Using the 'dig' (http://linux.die.net/man/1/dig) tool to determine any IP information published by an entity. The dig tool takes the domain name of the entity as an argument. For example, execution of 'dig a.com ANY' returns all IP information published by the entity a.com.

2. Use the IP addresses and domain names published to find ranges of IP addresses actually used. ISPs almost always allocate addresses in size of powers of 2 (2, 4, 8 etc.). Knowing one IP address allows probing around that space. The 'whois'

(http://linux.die.net/man/1/whois) tool can be used to determine ownership of neighborhood addresses.

3. Even if the entity does not publish any IP information that can be retrieved through dig, most entities have servers whose names may be guessed. Mail servers for the domain a.com often have the name mail.a.com, SMTP servers tend to be smtp.a.com, FTP servers tend to be ftp.a.com etc. Using a tool like nslookup, the entity ownership collection system 14 can verify if any of these common names are in use by the entity.

4. If an IP address is found, the system 14 is configured to probe around the address (such as in step 2) to determine any addresses in the neighborhood owned by that entity.

5. Searching around the website of the company often gives a hint of other servers hosted by the company (ex: reports.a.com) which can be used as a starting point for search.

Rating Methodology

Organizational security risk may be measured along two vectors: vulnerability and resilience. An entity's vulnerability is defined as its "physical, technical, organizational, and cultural states," which can be exploited to create a security breach. An entity's resilience is defined to be its ability to recover from a security breach.

The system 10 uses the concepts of vulnerability and resilience by examining externally observable proxies for them. An example proxy for entity vulnerability is the number of entity-owned IP addresses, which are reported to be malicious. The higher the number of reports the more likely the entity was vulnerable and had been compromised. Resilience is inversely proportional to the duration of detected malicious activity. The shorter the duration of the malicious activity, the higher level of resilience the entity demonstrates as it can quickly identify and remove malicious infections.

To compute the ratings for an entity, the system 10 aggregates all of the data collected pertaining to the IT assets owned by that organization, such as the IP addresses controlled by the entity and the associated activity of those IP addresses. The types of activities depend on the types of data. The data sources may include false positives and the system 10 is configured to account for those uncertainties.

To determine quality metrics for IP address based assets, every IP address is uniquely mapped to an entity. Processing the data from a data source yields a list of IPs for each organization that has demonstrated suspicious or malicious behavior. The processing

steps are as follows:

1. For each IP address, determine a security quality metric called "badness".
2. Badness is a number between 0 and 1 that corresponds to the extent and duration of malicious activity that was reported.
3. For each data source in which the IP address is reported, determine a data source specific badness score for that IP.
4. Consolidate the badness score for a given IP across all data sources by cross validating data to determine the aggregate Badness for that IP.
5. Aggregate the badness scores of IPs from an entity to determine the entity's IP asset based security quality metric.

The ratings processing system 30 is configured to account for differences in data sources and types. Given each data source's potentially unique view of an entity, there is not a universal technique that treated them all the same way. Data source specific modeling techniques, for example, were developed for 11 of the 97 data sources in experimental trials in order to demonstrate feasibility and validate the approach. The data sources incorporated accounted for five different data source types: Block Lists, Suspicious Activity, Malicious Servers, Compromised Hosts, and Spamming.

The following two sections give detailed examples of modeling techniques developed for calculating IP address badness for two different data sources that are representative of the data collected.

One of the data sources is a daily updated list of IP addresses that were reported by volunteer hosts from across the Internet. IP Addresses are reported in this data source if they have communicated with hosts that do not expect any inbound communication from them. It lists many more IP addresses on a given day compared with the other data sources and therefore, provides a significant amount of information contained only in this data source. However, this data source has a high incidence of false positives, where a false positive is an unwarranted report due to an incorrectly configured reporting host (i.e., the target) or a listing of an incorrect IP address due to backscatter.

False positives are accounted for by identifying events – where an event is defined as persistent, reported activity on a single IP address within a time period. For each event, heuristics are applied to determine the average intensity for the event. The intensity of an IP address on a given day is a measure of the confidence that malicious activity originated

from the IP address on that day.

For the case where an event spans multiple days, the IP address is generally reported on each day in the event. However, if an IP address is listed on one day but not the next, this omission does not necessarily signify that the host has stopped its malicious behavior; rather, it could be that the host was offline for the day. For example, many corporate hosts are offline for weekends and holidays. Thus, an event is allowed to have short inactive periods, or days without any reports on the IP address. To generate the IP address quality metric, a maximum inactive period of three days is used.

The intensity of an IP address for a given day is calculated dynamically and increases both with the number of reporting targets as well as the duration of the event. Reports with a larger number of targets have larger intensities. This is because false positives due to mis-configured hosts are less likely to have occurred when multiple targets report the same IP address on the same day. Likewise, reports that belong to a persistent event have larger intensities, since persistent reports also signal the legitimacy of the malicious activity on the IP address.

The intensity, I(s) is calculated as follows:

$$I(s) = \begin{cases} 0.1, & if\ s < 2 \\ 0.01e^{\frac{\ln(10)(s-1)}{4}}, & if\ 2 \le s < 5 \\ 0.8 - 0.7e^{-\frac{\ln(10)(s-5)}{4}}, & if\ s \le 5 \end{cases}$$

where s is the number of hosts reporting the IP address. Thus, the average intensity, I_{avg}, of an event is the average of the intensities calculated per active day (a day with reports) and is determined as follows:

$$I_{avg} = \frac{I(s)}{T} + \frac{A \cdot I_{prev}}{T},$$

where T is the list time, A is T minus the number of days since the last update, and I_{prev} is the average intensity at the last update. The Badness, B_{IP}, of an IP address is derived from the intensity and duration of the events for the IP, such that recent events are weighted heavier than historical events and is calculated as follows:

$$B_{IP} = min(1, \frac{I_{avg}(1-e^{-0.02})}{1-e^{-0.12}} \sum_{t_1}^{t_n} e^{-0.02}),$$

where t_1 and t_n denote time lapsed from the end and beginning of an event, respectively; and

the average intensity is readjusted if the persistence surpasses a threshold.

The second data source example is a host block list that lists IP addresses that have been compromised. Based on an analysis of the data sources collection methods, the block list is considered very reliable in the sense that a listing implies that malicious activity originated from the listed address. This block list removes IP addresses from the list if no malicious activity is detected for a small window of time. Because of the high confidence in the data source's accuracy, any IP address on the block list is assigned a raw Badness of 0.8.

Once an IP address is delisted and is no longer on the block list, its Badness decays exponentially with respect to the time since it was last listed. Thus, the Badness is:

$$B_{IP} = 0.8e^{-\frac{\ln(2)T}{182.625}},$$

where T is the time in days since the last listing. This decay rate corresponds to a half-life of six months.

Various other data sources are handled similarly but the raw score is based on the confidence in the data source's collection methods. Other data sources track CIDR blocks as opposed to individual IP addresses, and so the Badness assigned to a listing on these lists are weighted by the CIDR block size as follows:

$$B_{IP} = 0.8We^{-\frac{\ln(2)T}{182.625}},$$

where W is the natural log of the block size.

The total IP space badness of an entity is an aggregation of the badness of the entity's individual IP addresses and/or CIDR blocks. In the simplest model where all data sources are IP address based, the entity badness is the total badness of the IP addresses owned by the entity. To normalize ratings across entities of different sizes, the entity's network size defined as the number of active IP addresses owned by the entity is used:

$$B_{entity} = \frac{\sum_{IP \in Entity} B_{IP}}{\ln(N)},$$

where N denotes the network size. Normalizing avoids penalizing of smaller entities allowing fair comparisons between entities of differing sizes.

Enhancements to the Ratings Methodology

The system 10 may also include expanded the methodology to support additional

and different types of data sources. It could identify data sources that indicate different levels of IT sophistication - such information is a measure of the level of IT practice maturity.

Entity normalization methods can also account for differences in entity size beyond network size. For example, the use of other normalization methods such as number of employees may help produce more robust normalizations under certain circumstances.

Also, statistical properties of the model's internal parameters may be analyzed and adjust based on the findings. For example, certain inputs or features may be disproportionately skewing the ratings and such inputs or features may be modulated through weighting factors.

The composite security rating described above measured, amongst other things, how much, to what extent, and how recently malicious activity was detected on an entity's cumulative IP space. The score could also be adapted to show a level of confidence. For example, a failure to detect malicious activity on an entity's IP space does not necessarily imply non-malicious behavior. Rather, the data sources may lack coverage on the entity's IP space. By outputting a range as opposed to a number, the system 10 is able to convey its confidence in a rating where a larger range necessarily implies a lower confidence, and a smaller range necessarily implies a higher confidence.

Such a range could be computed from a mean score and a confidence range, which could be determined from a developed discrete choice model. Features such as the Badness scores from each data source could help determine the mean score. Features such as redundancy between data sources and network size could also help determine the confidence range.

Entity mapping may also be improved through other data sources and functions. Data sharing relationships with Internet Service Providers might provide additional data on security outcomes and practices at entity computer systems. Also, consumers of the scoring reports may already have partner-mapping data through the nature of their relationship with the entity or may be able to request the information.

Entity mapping may also be facilitated by persistent updates of the heuristics, such as updating prefixes from BGP announcements and data from Regional Internet Registries.

Data storage used by the system 10 may be improved to minimize the disk space required while supporting rapid inclusion of new entity ratings. For example, high-speed

data access layers may be created for daily ratings computation.

Speed and scale can be accomplished through distributed or parallel processing on different systems. A distributed data source query interface may be implemented so that massive and expensive centralized data storage is not required.

The system 10 may also be configured to develop and evaluate predictive capabilities of information security ratings and incorporate them into the rating methodology.

The ability to demonstrate predictability has a dependency on data reliability. For example, improving coverage of malicious events improves data reliability. Statistical evaluations may be used to disambiguate strong entity performance (e.g., no malicious activity) from low coverage (e.g., lack of information on the malicious activity). These evaluations can then be used in the rating methodology.

Statistical evaluations of data coverage may include a data accuracy assessment wherein levels of coverage assurance associated with a particular adopted data source are determined. Also, observations across data sources may be compared to determine data sources of high probability or low probability of coverage for a given entity.

Predictive modeling may include determination of entity historical trends to display and predict future performance. Regression and machine learning based models may be developed to predict information security performance. Models may be evaluated and further developed for predictive capability through a series of prediction experiments.

Also, the data source features may be analyzed for correlations of high and low performance. For example, entities with behavior "X" tend to perform well and entities that demonstrate property "Y" tend to behave poorly.

Use of External and Internal Security Data

The system 10 may also include internally derived security assessments. For example, such a score computation is shown in Fig. 3. The final score S_{Total} has two components, the Internal score and the External score.

The Internal score, S_{int}, is derived from data collected and observed from inside the enterprise. Data sources that provide inputs to the internal scoring function could include, but are not limited to, the following:

- Vulnerability scans
- Firewall Rules
- Incident Reports
- Configurations
- Software inventory
- Policies
- Controls
- User Behavior

The features from each of the data sources are extracted to create a feature vector. This feature vector is $X_{\text{int}} = \{InternalFeatures\}$ in the "Internal Source Score," as shown in Fig. 3. Features include, but are not limited to, derived metrics from the data sources (e.g., the number of remotely exploitable vulnerabilities from outside the entity, the number of incidents, or the number of vulnerable versions of software).

Each feature x_i in X_{INT} has a corresponding transformation function $f_{I(x_i)}(x_i)$ that performs a normalization transformation such that the resultants can be summed.

Each feature x_i in X_{INT} also has corresponding weight ω_i such that different weights can be placed on the resultant feature transformation where the sum of the weights equal is unity $\sum_{i=1}^{n} \omega_i = 1$. The sum of the transformed and weighted feature vector is computed by summing each resultant for each of the features $\sum_{i=1, x \in X_{\text{int}}}^{n} \omega_i f_{I(x_i)}(x_i)$.

The final score S_{int} is the summation normalized by a set of normalization factors given as $f_{I(x_\alpha)}(x_\alpha) + f_{I(x_\beta)}(x_\beta)$ where each normalization factor $x_\alpha, x_\beta, \ldots$ also has a factor normalization transformation function.

The computation of the Internal Score is given as: $S_{\text{int}} = \dfrac{\sum_{i=1, x \in X_{\text{int}}}^{n} \omega_i f_{I(x_i)}(x_i)}{f_{I(x_\alpha)}(x_\alpha) + f_{I(x_\beta)}(x_\beta)}$.

The External Score is the combination of the Public Sources Score (S_{pub}) and the Commercial Sources (S_{com}). S_{pub} and S_{com} are derived using the same heuristic combinatorial functions as the Internal Score. However, the input data sources, weights, transformation functions and normalization factors are different.

S_{pub} and S_{com} have their own feature vectors $X_{pub} = \{PublicFeatures\}$ and $X_{com} = \{CommercialFeatures\}$ based on the data input sources used.

Data sources in X_{pub} that provide inputs to the S_{pub} score could include but are not limited to the following:

- Industry reports
- Internet monitoring web sites that publish reports (ex: *www.malwareurl.com*)
- News articles
- Court records

Data sources in X_{com} that provide inputs to the S_{com} score could include but are not limited to the following:

- Company proprietary data collected during operations
- Renesys
- Arbor Networks
- Business intelligence bought from corporations and services
- User Behavior

With the Internal and External Scores computed, the final total score is computed and the weighted sum of the three: $S_{Total} = \omega_{int} S_{int} + \omega_{pub} S_{pub} + \omega_{com} S_{com}$

It is possible that the algorithm does not have the same inputs for all entities. More information may be available for some entities compared to other entities. Given this, each data source is assigned a normalized confidence level based on how much they contribute to the computation of the enterprise score. Depending on the actual data that went into rating the company, the confidence level is assigned as a sum of the confidence levels associated with the data sources. The confidence level can be used to assign a range of scores for an enterprise. For instance, if an enterprise is rated as 750 with a confidence level of 0.8, the

entity's actual score is reported as (750 – (1 – 0.8) * 100, 750) = (730 – 750). An entity's score is deemed to be unavailable if the confidence level is below a minimum threshold of 0.5.

It should be noted that the S_{int} may be zero due to a lack of available information or permission, wherein S_{total} becomes characteristic only of externally observable characteristics. Also, characteristics for the calculation can be used in conjunction, or vice versa, with functions and aspects of the remaining systems described hereinabove and below.

Distributed System

Referring now to Fig. 4, a schematic diagram of a central server 500, or similar network entity, configured to implement a system for creating a composite security score is provided. As used herein, the designation "central" merely serves to describe the common functionality the server provides for multiple clients or other computing devices and does not require or infer any centralized positioning of the server relative to other computing devices. As may be understood from Fig. 4, the central server 500 may include a processor 510 that communicates with other elements within the central server 500 via a system interface or bus 545. Also included in the central server 500 may be a display device/input device 520 for receiving and displaying data. This display device/input device 520 may be, for example, a keyboard or pointing device that is used in combination with a monitor. The central server 500 may further include memory 505, which may include both read only memory (ROM) 535 and random access memory (RAM) 530. The server's ROM 535 may be used to store a basic input/output system 540 (BIOS), containing the basic routines that help to transfer information across the one or more networks.

In addition, the central server 500 may include at least one storage device 515, such as a hard disk drive, a floppy disk drive, a CD Rom drive, or optical disk drive, for storing information on various computer-readable media, such as a hard disk, a removable magnetic disk, or a CD-ROM disk. As will be appreciated by one of ordinary skill in the art, each of these storage devices 515 may be connected to the system bus 545 by an appropriate interface. The storage devices 515 and their associated computer-readable media may provide nonvolatile storage for a central server. It is important to note that the computer-readable media described above could be replaced by any other type of computer-readable

media known in the art. Such media include, for example, magnetic cassettes, flash memory cards and digital video disks.

A number of program modules may be stored by the various storage devices and within RAM 530. Such program modules may include an operating system 550 and a plurality of one or more (N) modules 560. The modules 560 may control certain aspects of the operation of the central server 500, with the assistance of the processor 510 and the operating system 550. For example, the modules may perform the functions described above and illustrated by the figures and other materials disclosed herein, such as collecting security characterizations 570, generating a composite rating 580, determining a trend 590, reporting the ratings 600, IP mapping 610, determining a badness quality metric 620, attenuating a raw score 630, correlating with statistical outcomes 640, determining a confidence range 650, predicting future performance 660 and determining an accuracy 670.

The flowchart and block diagrams in the figures illustrate the architecture, functionality, and operation of possible implementations of systems, methods and computer program products according to various embodiments of the present invention. In this regard, each block in the flowchart or block diagrams may represent a module, segment, or portion of code, which comprises one or more executable instructions for implementing the specified logical function(s). It should also be noted that, in some alternative implementations, the functions noted in the block may occur out of the order noted in the figures. For example, two blocks shown in succession may, in fact, be executed substantially concurrently, or the blocks may sometimes be executed in the reverse order, depending upon the functionality involved. It will also be noted that each block of the block diagrams and/or flowchart illustration, and combinations of blocks in the block diagrams and/or flowchart illustration, can be implemented by special purpose hardware-based systems that perform the specified functions or acts, or combinations of special purpose hardware and computer instructions.

The corresponding structures, materials, acts, and equivalents of all means or step plus function elements in the claims below are intended to include any structure, material, or act for performing the function in combination with other claimed elements as specifically claimed. The description of the present invention has been presented for purposes of illustration and description, but is not intended to be exhaustive or limited to the invention in the form disclosed. Many modifications and variations will be apparent to

those of ordinary skill in the art without departing from the scope and spirit of the invention. The embodiment was chosen and described in order to best explain the principles of the invention and the practical application, and to enable others of ordinary skill in the art to understand the invention for various embodiments with various modifications as are suited to the particular use contemplated.

Black Kite Ex. 1002, Page 1060 of 1060