

UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE PATENT TRIAL AND APPEAL BOARD

-----X

IRIUSRISK, INC.,

Petitioner,

v.

THREATMODELER SOFTWARE, INC.,

Patent Owner.

Case IPR2023-00821

Patent 10,699,008

-----X

DEPOSITION OF ROBERT HURLBUT

Monday, February 5, 2024

Conducted Remotely

REPORTED BY:

Christina Diaz, CRC, CRR, RMR, CSR-NY/NJ, CLR

Job No.: SY8676

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

February 5, 2024
9:58 A.M. E.S.T.

Deposition of ROBERT HURLBUT,
pursuant to notice dated January 23, 2024,
conducted remotely, before Christina Diaz, a
Certified Realtime Captioner, Certified
Realtime and Registered Merit Reporter and
Notary Public within and for the State of
New York.

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

A P P E A R A N C E S

DLA PIPER LLP (US)

Attorneys for Petitioner

1201 North Market Street

Suite 2100

Wilmington, DE 19801

302.468.5675

matthew.middleton@dlapiper.com

BY: MATTHEW MIDDLETON, ESQ.

RIMÔN P.C.

Attorneys for Patent Owner

8300 Greensboro Drive

Suite 500

McLean, VA 22102

571.765.7703

donald.jackson@rimonlaw.com

BY: DONALD JACKSON, ESQ.

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

I N D E X

WITNESS

Robert Hurlbut

EXAMINATION BY

PAGE

Mr. Jackson

6, 115

Mr. Middleton

109

R E F E R E N C E D E X H I B I T S

EXHIBIT PAGE

1001 77

1003 32

1004 32

1005 87

INFORMATION REQUESTS

INSERTED INFORMATION

- NONE -

REQUESTS FOR PRODUCTION

- NONE -

RULING

- NONE -

DIRECTIONS NOT TO ANSWER

- NONE -

1 R. Hurlbut

2 (The following statement was read
3 by the reporter)

4
5 "All parties to this deposition
6 are appearing remotely and have
7 agreed to the witness being sworn in
8 remotely.

9
10 "Due to the nature of remote
11 reporting, please pause briefly before
12 speaking to ensure all parties are
13 heard completely.

14
15 "Counsel, please state your
16 agreement on the record."

17
18 MR. JACKSON: This is Don Jackson
19 for Patent Owner ThreatModeler
20 Software, Inc., and we agree.

21
22 MR. MIDDLETON: This is Matthew
23 Middleton for Petitioner IriusRisk,
24 Inc. I agree.

1 R. Hurlbut

2 R O B E R T H U R L B U T,
3 having been remotely sworn as stipulated
4 by the parties, was examined
5 and testified as follows:
6

7 EXAMINATION

8 BY MR. JACKSON:
9

10 Q. Good morning, Mr. Hurlbut.

11 A. Good morning.

12 Q. Just so the record is clear, we
13 talked about this off-line ahead of time,
14 but I just want to put it on the record.

15 You were deposed in another IPR
16 filed by IriusRisk against different
17 patents owned by ThreatModeler, correct?

18 A. That's correct.

19 Q. And you were deposed in that case
20 in, I think it was December of last year,
21 2023?

22 A. That is correct.

23 Q. So today, if I refer to the other
24 IPR or the prior IPR, will you understand
25 that to be the IPR for which you were

1 R. Hurlbut

2 deposed in December 2023?

3 A. Yes, I will.

4 Q. And if you have any questions
5 about what I am referring to, please,
6 please don't hesitate to speak up. I
7 wanted to go over some of the background,
8 and it's going to be very similar to what
9 we talked about in December. But I just
10 wanted to make it a record in this case, so
11 I apologize for what will seem like repeats
12 of what we have done before.

13 Mr. Hurlbut, am I correct that
14 you spoke at the ThreadModCon 2023
15 conference?

16 A. Yes, I did.

17 Q. And were you paid to attend or
18 speak at that conference?

19 A. No, I was not.

20 Q. And am I correct that your
21 employer paid for all of your expenses
22 associated with that travel to and
23 attendance at that conference, correct?

24 A. That is correct.

25 Q. Your employer is a company called

1 R. Hurlbut

2 Aquia? Did I pronounce that correctly?

3 A. That is correct, yes.

4 Q. Do you own any interest in Aquia?

5 A. Not directly. It is owned by
6 three founders. There are stock options,
7 but outside of that, I do not have direct
8 ownership of the company.

9 Q. So you have stock options in
10 Aquia; is that right?

11 A. Correct.

12 Q. Do you earn those as part of your
13 compensation package as an employee?

14 A. Yes. The company is also
15 pre-IP0. It's not public, so any of the
16 stock options are also not public.

17 Q. Let me ask you, are you also a
18 member of a community called Threat
19 Modeling Connect?

20 A. Yes, I am.

21 Q. And do you contribute articles to
22 that community?

23 A. I have contributed, if I remember
24 correctly, some comments on some articles.

25 I have also contributed a couple of

1 R. Hurlbut

2 opportunities to lead some discussions that
3 were recorded.

4 Q. I guess I should have asked this
5 question. What is Threat Modeling Connect
6 community?

7 A. Sure. Threat Modeling Connect is
8 a community to gather folks who are
9 interested in threat modeling. It's an
10 opportunity for people to register and then
11 log in and be able to see conversations,
12 articles. As I said, they also have these
13 taped discussions every so often. I think
14 typically once a month, but I think it just
15 depends on sometimes what the schedule is,
16 where people just join in and they have a
17 topic and somebody leads it, and they ask
18 questions and discuss. But essentially,
19 it's just a place to be able to communicate
20 and for people to learn more about threat
21 modeling.

22 Q. Is this strictly an online
23 community?

24 A. It is, yes, online.

25 Q. And have you gotten any work

1 R. Hurlbut

2 because of your connection or membership in
3 that community?

4 A. No, I have not.

5 Q. Let me switch gears a little bit
6 and ask you about some of the folks that
7 are associated with IriusRisk and, again, I
8 apologize. I know we covered this in the
9 last deposition.

10 Am I correct that you know a
11 Mr. De Vries at IriusRisk?

12 A. Yes, I do.

13 Q. My understanding is he is a
14 cofounder and CEO of IriusRisk; is that
15 right?

16 A. Yes, that's correct.

17 Q. Am I correct that you have --
18 have you worked with Mr. De Vries? Let me
19 put it that way.

20 A. No, I have not.

21 Q. Am I right, you just met him at
22 various functions relating to Threat
23 Modeling?

24 A. That is correct. Conferences
25 that he has spoken at, or I have attended

1 R. Hurlbut

2 and he has spoken at, or just conferences
3 that we just happen to be at the same place
4 and met and talked.

5 Q. And do you also know Christina
6 Bentue?

7 A. I have met her. I do not know
8 her well, but I have met her.

9 Q. She's the chief operating officer
10 and cofounder of IriusRisk; is that right?

11 A. That's correct.

12 Q. And I don't recall your answers
13 about Mr. Paul Santapau. Do you know
14 Mr. Santapau?

15 A. I do not.

16 Q. What about Fraser Scott. Do you
17 know him?

18 A. Yes, I do know him.

19 Q. Have you ever worked with
20 Mr. Scott?

21 A. I have never worked with him
22 directly. He was at Capital One when I was
23 also at Bank of America, and so through
24 those cooperations between banks, we had
25 opportunity to talk about threat modeling

1 R. Hurlbut

2 programs, but we never worked together.

3 Q. And Mr. Scott -- he is vice
4 president of product development at
5 IriusRisk; is that right?

6 A. That is correct.

7 Q. What about Adam Shostack? I
8 believe you do know Mr. Shostack, correct?

9 A. I do, yes.

10 Q. Have you ever worked with
11 Mr. Shostack?

12 A. No. I have worked -- at Bank of
13 America I was on a contract and then left.
14 Adam Shostack was there, hired as a
15 consultant at Bank of America, and then he
16 left, and I came in full-time. So we have
17 sort of worked together in terms of working
18 at the same organization, but not directly
19 together.

20 Q. And Mr. Shostack -- is he on the
21 technical advisory board at IriusRisk?

22 A. He is, yes.

23 Q. As it relates to Mr. Shostack's
24 involvement with IriusRisk, can you
25 describe your interactions with

1 R. Hurlbut

2 Mr. Shostack?

3 A. Through IriusRisk, I have not had
4 any direct interactions per IriusRisk.

5 Q. Let me change gears and talks
6 about Aquia again.

7 Is Aquia a company that's in the
8 threat modeling business?

9 A. That's just one of the
10 capabilities that it provides for
11 customers.

12 Overall, it's cybersecurity and,
13 in particular, focuses mostly on the public
14 sector. So federal government agencies as
15 well as some commercial organizations as
16 well. But primarily focused on public
17 sector.

18 Q. Cybersecurity for the public
19 sector?

20 A. Exactly. Cybersecurity for the
21 public sector. Threat modeling is one of
22 many, many different things that they
23 offer.

24 Q. What is your title at Aquia
25 currently?

1 R. Hurlbut

2 A. My title is principal
3 applications, security architect and threat
4 modeling lead.

5 Q. So if there is threat modeling
6 business that Aquia has, is it fair to say
7 that you oversee that effort?

8 A. That is correct.

9 Q. Does Aquia have a lot of threat
10 modeling business currently?

11 A. At the moment we have one client
12 that we are working with directly to help
13 them put together a threat modeling
14 program.

15 Q. When did you join Aquia?

16 A. I joined in November of 2021.

17 Q. To serve as an expert in the
18 current IPR or the prior IPR, did you have
19 to get permission from Aquia to take on
20 that project or those projects?

21 A. I did, yes.

22 Q. Who did you get permission from?

23 A. I brought it to the attention of
24 the three founders and they, in turn, ran
25 it by their attorneys, and so together they

1 R. Hurlbut

2 said, yes, you have permission to be able
3 to do this.

4 Q. Did they provide any reasons why
5 they approved that?

6 A. They didn't see a conflict --

7 MR. MIDDLETON: Hold on one
8 second, Robert.

9 I wanted to caution you to not
10 reveal anything that may be privileged
11 between you and Aquia's attorneys as
12 well.

13 THE WITNESS: Yes.

14 MR. MIDDLETON: But you can
15 answer.

16 A. I will just say that they did not
17 foresee or perceive any conflict of
18 interest in the work.

19 BY MR. JACKSON:

20 Q. At Aquia, are you paid a salary,
21 or do you work by the hour?

22 A. I am paid a salary.

23 Q. For the current IPR, you are also
24 being paid by IriusRisk or its counsel for
25 the work you are doing in connection with

1 R. Hurlbut

2 that IPR.

3 Is that right?

4 A. Yes, that is correct.

5 Q. And your compensation -- is that
6 laid out in your declaration that you
7 submitted in this current IPR?

8 A. Yes, it is.

9 Q. And that compensation is
10 accurate?

11 A. That is accurate, yes.

12 Q. I should have asked this
13 question, but sort of a foundation
14 question.

15 Obviously you submitted a
16 declaration in the current IPR, correct?

17 A. That is correct.

18 Q. Before today's deposition, did
19 you have a chance to review that
20 declaration in preparation for the
21 deposition?

22 A. Yes, I did.

23 Q. Did you see any errors or
24 omissions in the declaration when you
25 reviewed it?

1 R. Hurlbut

2 A. No. I did not. Everything
3 looked as it was written.

4 Q. Does your declaration also
5 contain an accurate description of your
6 professional experience?

7 A. Yes, it does.

8 Q. So when you talked to the three
9 founders about working on the two IriusRisk
10 IPRs, what did you tell them about that?

11 A. I shared with them some of the
12 details about the patent, the suit that's
13 been brought, what's public.

14 So I shared that information with
15 them so that they, in turn, could share
16 that with the attorneys.

17 So whatever was public, that's
18 what they saw as well.

19 Q. Did you tell them you wanted to
20 take on these projects or not?

21 A. Well, I did in terms of I was
22 asked by Stephen de Vries directly if I
23 would be willing to participate. And then
24 I brought that to the founders and said, I
25 am interested in doing this.

1 R. Hurlbut

2 Q. Why were you interested in
3 working on these IPRs?

4 A. Based on my expertise. I know
5 threat modeling. And I am just interested
6 in -- really that's my interest is threat
7 modeling.

8 Q. But, in particular, in these
9 IPRs, where as a general matter, you are
10 opining that the patent claims are not
11 valid, what was your reason for being
12 interested in taking those positions?

13 MR. MIDDLETON: Objection. Form.

14 A. Again, I was interested in trying
15 to understand a little bit more about the
16 scenarios and their particular issues there
17 and so that was part of that as well.

18 I also am familiar with threat
19 modeling tools in general, and so, again,
20 interested in learning and how I could
21 contribute. How I could help based on my
22 own understanding and experiences.

23 BY MR. JACKSON:

24 Q. So we have talked about your
25 declaration.

1 R. Hurlbut

2 Let me see if I can figure out
3 how to push a copy out to you
4 electronically.

5 A. Okay.

6 (Discussion off the record)

7 BY MR. JACKSON:

8 Q. Mr. Hurlbut, are you able to see
9 the document?

10 A. Yes.

11 MR. MIDDLETON: Last time,
12 Robert. Make sure you have full access
13 and control of the column document.
14 Whether you have it downloaded or you
15 want to just use the eDepoze software,
16 make sure you have control over it.

17 A. It looks like I do. This is
18 the -- this looks like the right one.

19 (Discussion off the record)

20 BY MR. JACKSON:

21 Q. Mr. Hurlbut, do you have your
22 declaration in the current IPR in front of
23 you?

24 A. I do, yes.

25 Q. And when you wrote your

1 R. Hurlbut

2 declaration, I assume you had studied the
3 '008 Patent, which is the subject of your
4 declaration, correct?

5 A. That is correct.

6 Q. And when you studied the '008
7 Patent, did you understand what the terms
8 used in the '008 Patent meant?

9 A. Yes, I did.

10 Q. And specifically, the claim
11 terms, you had an understanding of what
12 those meant, correct?

13 A. I did, yes.

14 Q. And was your understanding of
15 those terms based on the knowledge of those
16 who have skill in the art as of May of
17 2017?

18 A. Yes.

19 Q. When you did your analysis, did
20 you apply that understanding of those claim
21 terms to your analysis?

22 A. Yes, I did.

23 Q. And some of this again, I
24 apologize, is going to seem like a repeat.
25 I have tried to cut out some of this.

1 R. Hurlbut

2 Just so we have a working
3 definition of some of the terms that are
4 used in the '008 Patent, can you tell us
5 what a threat model is, at least as you
6 understand it?

7 A. Yes.

8 A threat model is a model of the
9 types of threats or potential threats
10 against a system. So security threats
11 typically against a system as well as it
12 may contain any mitigations. Sometimes you
13 may have a diagram, a data flow diagram or
14 related diagram that helps you understand
15 the system better, but ultimately a threat
16 model is a description of the kinds of
17 threats that may be possible against a
18 system as well as mitigations against those
19 threats.

20 Q. And how about the term "threat,"
21 you mentioned that in your answer there.

22 What is a threat in the context
23 of the '008 Patent?

24 A. Sure.

25 A threat is a result of a --

1 R. Hurlbut

2 exploiting a vulnerability. So
3 vulnerabilities may be coding errors and so
4 forth, but the threat is an attack or
5 somebody being able to exploit those.

6 And that's what you are trying to
7 look for or determine when you are thinking
8 about a threat.

9 Q. And then again, this is a term
10 that's used in the '008 Patent.

11 In the context of the '008, what
12 are threat model components?

13 A. Threat model components could be
14 anything that's part of -- that describes
15 parts of a system. So it could be servers.
16 It could be hosts. It could be various
17 applications and so forth. Could be
18 components of a threat model or a threat
19 model diagram.

20 Q. Let me direct you to paragraph 51
21 of your declaration which is on page 19.

22 A. Okay. Okay. Yes. I'm there.

23 Q. Paragraph 51, you have a
24 definition of threat model components,
25 correct?

1 R. Hurlbut

2 A. Okay. Our numbers are different.

3 Sorry. Let me get there.

4 Okay. Here we go. Yes.

5 Q. And what is that definition?

6 A. Yes. So threat model components,
7 potential relevant source for one or more
8 threats.

9 Q. And that's the definition that
10 you applied when you were analyzing the
11 '008 Patent.

12 Is that right?

13 A. That is correct.

14 Q. And that's the same definition
15 that I believe you applied in the prior IPR
16 for that same term, right?

17 A. That is correct, yes.

18 Q. Now a new term that's used in the
19 '008 Patent claims, at least is a term
20 called Attack Paths.

21 Am I correct?

22 A. Yes, that's correct.

23 Q. In the context of the '008
24 Patent, again, as based on the
25 understanding of a person in May of 2017 --

1 R. Hurlbut

2 a person of skill in the art, that is, what
3 is the definition of attack paths?

4 A. As mentioned here, various routes
5 said that all potential attackers to a
6 selected asset or attack vectors. So the
7 various paths an attacker may take to be
8 able to realize the threat against a
9 particular asset or assets.

10 Q. And you are referring to -- the
11 definition you provided in paragraph 52 of
12 your declaration?

13 A. That is correct, yes.

14 Q. And when you say "paths," are
15 these -- I don't want to use the word
16 physical -- I guess either physical or
17 electronic paths.

18 Is that what we are talking
19 about?

20 A. Probably -- it could be physical.
21 It could be electronic, but essentially,
22 different methods or different ways for an
23 attacker to be able to attack. So if you
24 have different threats or different
25 possible ways of realizing a threat against

1 R. Hurlbut

2 an asset, the way you get there is a path
3 or the method that you take is really
4 describing that attack path.

5 Q. When you say "attack," that word
6 by itself, is that referring -- well, let
7 me just ask you openly.

8 A. Sure.

9 Q. What does that word "attack" in
10 the context of attack paths -- what does
11 that mean?

12 A. So the threat as we talked about
13 you can identify a threat but a threat is
14 just that. It's a definition or it's just
15 something you have determined.

16 When a threat becomes an attack
17 is when the threat has actually been
18 realized. So an attacker or somebody who
19 is trying to use that threat to do harm or
20 to extract data, and so forth, that's the
21 attack. They are actually making the
22 threat a reality or realizing the threat as
23 something that does happen or has happened.

24 Q. Correct me if I am wrong, but it
25 sounds like a threat is a potential event,

1 R. Hurlbut

2 I guess?

3 A. Yes.

4 MR. MIDDLETON: Objection. Form.

5 BY MR. JACKSON:

6 Q. And "attack" is when that
7 potential event actually occurs?

8 MR. MIDDLETON: Objection. Form.

9 A. The word "attack" itself, yes.
10 When the event does occur.

11 BY MR. JACKSON:

12 Q. Okay. And then there is -- by
13 the way, did you also review -- you may or
14 may not have done this. Let me just ask
15 you.

16 Did you review the institution
17 decision by the board in the current IPR?

18 A. I did, yes.

19 Q. And in the institution decision
20 -- well, skip that.

21 In your declaration -- let me
22 just ask you directly about another claim
23 term.

24 You quote it in your declaration
25 on pages 43 and 44, if you want to go ahead

1 R. Hurlbut

2 and turn there.

3 A. Okay.

4 Q. Let me know when you are there.

5 A. (Witness reviewing document).

6 Okay. I think so. 43, 44, yes.

7 Q. It's under the heading, Element

8 IF.

9 Do you see that?

10 A. I do see it, yes.

11 Q. Great.

12 You quoted here certain parts of

13 Claim 1 of the '008, correct?

14 A. Yes.

15 Q. Which was the intention, I

16 assume?

17 A. Yes.

18 Q. So there is a phrase in here that

19 reads, "Redefine the first threat model by

20 including in it a second threat model

21 associated with component group."

22 Do you see that?

23 A. I do, yes.

24 Q. What was your understanding of

25 what that phrase meant when you wrote your

1 R. Hurlbut

2 declaration?

3 A. Redefining. Essentially, you
4 have the first threat model, you have the
5 second threat model. When you are
6 combining or including, as it says, the
7 second threat model, you have now -- by
8 "redefining," essentially, is modifying the
9 first threat model so that now it's a new
10 threat model. It's considered to be
11 essentially a new threat model. So that's
12 the redefining part.

13 Q. So the second threat model -- was
14 that second threat model originally a part
15 of the first threat model?

16 A. No.

17 Q. What the claim language is saying
18 is that you're taking that second threat
19 model and including it in the first threat
20 model?

21 A. That is correct.

22 Q. And by doing so, you're modifying
23 -- I'm trying to follow the claim language
24 here -- you're redefining the first threat
25 model by doing that, correct?

1 R. Hurlbut

2 A. That is correct.

3 Q. Is that understanding based on
4 what's described in the '008 Patent?

5 A. Yes. Yes.

6 Q. Other than what's described in
7 the '008 Patent, did you rely on any other
8 documents or other evidence to support that
9 understanding?

10 A. There is a Swiderski and Window
11 Snyder's book -- Frank Swiderski and Window
12 Snyder's book -- back in 2003, they did
13 talk talking about being able to combine
14 other components into the original threat
15 model and extending. So there is a concept
16 of extending and being able to turn one
17 threat model and two threat models into a
18 new threat model. So that was a concept
19 that's actually been around for a while.
20 So that was not -- it was not confusing to
21 me to read this and understand what it's
22 describing is something that's been known
23 for a while.

24 Q. For this element, 1[f], that we
25 have been talking about -- and again, you

1 R. Hurlbut
2 have the whole thing copied there in your
3 declaration, so you can refer to it if need
4 be -- but for purposes of your analysis in
5 this IPR of that particular claim element,
6 am I correct that you relied only on the
7 Jones reference?

8 A. That's correct, yes.

9 Q. I apologize. I'm actually going
10 to ask you go backward a couple of pages in
11 your declaration to Element 1[e] -- which
12 is on page -- the claim language is
13 repeated on page 41.

14 A. Yes, I'm there.

15 Q. The analysis for this element is
16 in paragraphs 79 and 80, correct?

17 A. Yes.

18 Q. And I just want to make sure that
19 I understand kind of what you based your
20 analysis of this claim element on. And I
21 see the reference there to Jones,
22 obviously, but did you rely on any type of
23 an inherency argument or analysis when
24 analyzing this particular claim element?

25 A. In terms of inherency from --

1 R. Hurlbut

2 could you clarify, please?

3 Q. Yes, I will. I will give it a
4 shot at least.

5 When I say "inherency," I mean
6 something that may be not actually
7 disclosed, but it has to be there or it has
8 to be true that a system worked a certain
9 way or includes some element that's not
10 described.

11 MR. MIDDLETON: Objection to the
12 extent it calls for a legal conclusion.

13 BY MR. JACKSON:

14 Q. Is that clear? Does it make
15 sense?

16 A. I think it does, and I think the
17 answer is no. I use what Jones had written
18 to be able to understand how it was
19 represented there and how it relates to --
20 with this particular patent and how it was
21 written as well.

22 Q. And I have talked about the Jones
23 reference, at least. Let me again push out
24 a copy of that to you so that you have it
25 available to you.

1 R. Hurlbut

2 A. Sure. Do I need to sit back and
3 -- to be able to see it? I imagine so.

4 Q. Matt may have mentioned -- I'm
5 not sure if you can download these and have
6 multiple ones open at the same time or not.
7 But that -- I'm not an expert on this
8 system to be honest with you.

9 A. No, it's fine. If I need to go
10 back, I can do that.

11 MR. JACKSON: In the top-left
12 corner, where you see the "back"
13 button, do you see a number of icons?
14 There is a download icon. That's the
15 second icon from the right.

16 (Reporter clarification)

17 MR. JACKSON: Mr. Hurlbut's
18 declaration is Exhibit 1003. It has
19 been previously submitted in the IPR,
20 and this Jones reference is Exhibit
21 1004, also previously submitted in the
22 IPR.

23 (Exhibit 1003 was referenced for
24 identification)

25 (Exhibit 1004 was referenced for

1 R. Hurlbut

2 identification)

3 BY MR. JACKSON:

4 Q. So, Mr. Hurlbut, were you able to
5 successfully get a copy?

6 A. Yes, I have it open.

7 Q. Okay. Great. If you take a look
8 at Figure 1, please.

9 A. Sure.

10 Q. Let me know when you are there.

11 A. Of course, it's sideways. Let me
12 try to -- there we go, okay. Yes. Got it.

13 Q. So at a high level, just as a
14 general explanation, can you describe what
15 Figure 1 shows?

16 A. Sure. So at a high level, it's
17 determining your data flow diagram. There
18 is the operations of the data flow -- DFD
19 creator as well as the threat indicator,
20 the decomposer decomposing the system, the
21 actual threat analyzer, then reporter. So
22 it looks like these are various components
23 within the system that's doing the work in
24 the Scribe tool of building out a threat
25 model and the various parts of the threat

1 R. Hurlbut

2 model.

3 Q. I was going to walk through some
4 of these sub-elements here, so don't feel
5 like you have got to necessarily get into
6 the detail right now. But I think that
7 Jones describes this system shown here in
8 Figure 1 as a modeling and analysis system.

9 Is that right?

10 A. Yes.

11 Q. And within this system, am I
12 correct that there are these multiple --
13 what I'll call "subsystems" that make up
14 this modeling and analysis system.

15 Is that right?

16 A. That's correct. Yes.

17 Q. And there are a number of arrows
18 that go from one subsystem to another.

19 Do you see that?

20 A. I do, yes.

21 Q. What are those arrows intended to
22 show?

23 A. The arrows are intended to show
24 sort of the flow of work. So criticality,
25 DFD, the creator, threat indicator,

1 R. Hurlbut
2 decomposer, and then back. So really, it's
3 a flow of work. And, of course,
4 ultimately, after the threat analyzer, then
5 to the reporter. So all of those arrows
6 indicate a flow of work through the system.

7 Q. You mentioned "criticality," the
8 first box over on the left labeled 102 is
9 called "criticality establishment."

10 Do you see that?

11 A. Yes, I do.

12 Q. Again, as a general matter -- I
13 am not asking for all the details, but what
14 does the criticality establishment
15 subsystem do?

16 A. I don't recall directly or
17 exactly.

18 Q. Let me see if I can direct you to
19 Jones, Column 4, line 42, to see if that
20 refreshes your memory.

21 A. Okay. Column 4?

22 Q. Yes. Line 42 to -- I have from
23 42 to Column 5, line 3.

24 A. I have it. Okay. "The
25 criticality establishment system may be

1 R. Hurlbut

2 generally configured to provide a desired
3 level of assurance for an information
4 system configured for implementation by a
5 complex-system platform."

6 Q. Again, feel free to read as much
7 of this as you need to. What is the
8 overall purpose of this criticality
9 establishment system 102?

10 A. It looks like, for at least this
11 part of the initial -- it says, "The
12 desired level of assurance may depend on a
13 number of different factors" -- I just lost
14 the page. Let me go back. There we go.
15 "Technologies of the complex-system
16 platform, use cases, regulatory compliance
17 requirements," and so forth.

18 It also mentions a risk sorter,
19 so various aspects of the initial part of
20 the system determining, for example,
21 confidentiality, integrity, availability,
22 the CIA. Let me go on to the next page.

23 Q. Do you understand what it means
24 here in Jones when it says "a desired level
25 of assurance"?

1 R. Hurlbut

2 I was specifically referring to
3 Column 4, line --

4 A. Right.

5 Q. -- 65, I think, but I think it's
6 repeated different places.

7 A. Yes. First time I see it there
8 is on 45. Actually, at 42. I would have
9 to go back and see how that's defined. I'm
10 not remembering how that's defined.

11 Q. We may come across other parts of
12 Jones as we talk that shed some light on
13 that. If we do, would you please just let
14 me know, Oh, by the way, here is where it
15 talks about assurance?

16 A. Sure.

17 Q. Great. Thanks.

18 Let me ask you about the next --
19 well, first of all, let me start with --
20 stay here with this box 102.

21 Okay. We may not know exactly
22 what it means right now by the word
23 "assurance," but is it fair to say that
24 this subsystem 102 is analyzing an
25 information system in Jones?

1 R. Hurlbut

2 A. I would agree with that. It does
3 say down in 65, "Select the desired level
4 of assurance for the information system."
5 So I would agree with that.

6 Q. I guess at a more general level,
7 referring to the system that's in Figure 1
8 as a whole, is the purpose of that system
9 again at a high level to perform certain
10 functions and analysis with respect to the
11 information system that's -- let me strike
12 that. Let me start over. Sorry.

13 In a general matter, at a general
14 level with respect to the system of
15 Figure 1, is it fair to say that that
16 system is analyzing or interpreting in some
17 fashion an information system?

18 MR. MIDDLETON: Objection. Form.

19 A. Yes.

20 Based on what I am seeing here, I
21 would say yes.

22 BY MR. JACKSON:

23 Q. So there is some analysis or
24 assessment that occurs in subsystem 102,
25 and then from there, there is some output,

1 R. Hurlbut

2 presumably, with respect to 102 that flows
3 down to 104.

4 Is that fair?

5 A. Let me see. I would have to see
6 104. 104 is --

7 (Witness reviewing document).

8 When I look back up at 20 --
9 because I'm not looking at the diagram at
10 the moment -- 27, so it talks about
11 criticality establishment system 102, data
12 flow diagram (DFD) level establishment
13 system 104. So when you say 104, you are
14 talking about data flow diagram, level of
15 establishment system?

16 Q. That's right.

17 A. Yes. Sorry. Can you repeat the
18 question again?

19 Q. Sure. I was just trying to get
20 an understanding of -- we may not know all
21 of the details right now, but whatever
22 occurs in the criticality establishment
23 system 102, the results of that flow from
24 102 to the DFD level establishment system
25 104.

1 R. Hurlbut

2 Is that fair?

3 A. Yes.

4 Q. And then that process continues
5 on from 104 to 106.

6 Is that right?

7 A. Yes.

8 Q. So the DFD level establishment
9 system 104, again, at a high level -- can
10 you tell us what that system does?

11 A. Not without checking the
12 references. It's on the next page. I know
13 that.

14 Q. Column 5, maybe starting line 20.

15 A. Right. So "The DFD level
16 establishment system may be configured to
17 assess various criteria of the information
18 system to identify an appropriate level of
19 threat model -- threat-model data flow
20 diagram -- to produce for the information
21 system. In some systems, various criteria
22 of the information system may be associated
23 with various levels, and the appropriate
24 level may identified by matching criteria
25 to a level. For example, the DFD level

1 R. Hurlbut

2 establishment system may identify a level 2
3 threat model as appropriate" --

4 (Reporter clarification)

5 A. "For example, the DFD level
6 establishment system may identify a level 2
7 threat model as appropriate in instances in
8 which the threat model is for any of the
9 following: higher trust level network
10 enclave environments, hybrid access zone,
11 high trust access zone, internet facing
12 applications, and/or systems with
13 transitive access, perimeter-related
14 systems."

15 Q. So is the overall purpose of this
16 particular system, 104, to determine -- I
17 think you used the -- I am looking for it
18 here, but you used the word "level," I
19 think it was?

20 A. Correct. Level 2, and it also
21 later describes a level 1.

22 Q. So the purpose is to determine
23 what level to analyze the system at?

24 A. Or in general -- in this case,
25 and I'm familiar with this -- in this case,

1 R. Hurlbut

2 level -- what type of data flow diagram is
3 this going to be, a level 2 diagram or a
4 level 1?

5 Q. So in that context, what does the
6 word "level" mean, specifically?

7 A. So at about 36 -- line 36 or
8 actually in 34 -- "A level 2 threat model
9 may be appropriate in instances in which it
10 is based on data classification that
11 application or system stores and/or
12 processes for any of the following," and,
13 in particular, it talks about "sensitive"
14 or "highly sensitive personally
15 identifiable information." So I am going
16 to stop there for a moment.

17 If I drop down to what's the
18 difference between that and level 1, about
19 line 41, "And In instances in which none of
20 the forgoing are met, the DFD level
21 establishment system may identify a level 1
22 threat model as appropriate."

23 So based on my understanding of
24 what's written here is that level 2 relates
25 to more sensitive data; a higher

1 R. Hurlbut

2 classification in terms of confidential and
3 so forth; personal identifiable information
4 (PII), and so on. So the sensitivity of
5 the data or information being higher is a
6 level 2. If it's not or unknown or not
7 well known, then it could be a level 1 is
8 my understanding of this paragraph.

9 Q. How does that affect the threat
10 model? How does the level relate to the
11 threat model that's generated?

12 A. Well, based on the definition
13 here, the level 2, if we identify the data
14 flow diagram as a level 2, that indicates
15 to the user that this is a more -- has more
16 highly sensitive data or higher
17 classification, and we might know more
18 about it but certainly it's a more
19 sensitive data versus a level 1. So now
20 what we know about the threat model is that
21 there is -- what we are dealing with is
22 certainly more critical. Let me use that
23 word, critical, than maybe a level 1 in
24 terms of impact of threats and so forth.

25 Q. So the next block in the figure

1 R. Hurlbut

2 one system is called DFD creator, 106?

3 A. Yes.

4 Q. Can you tell me what the DFD
5 creator does again at a high level?

6 A. Sure.

7 So, again, line 45 talks about --
8 may be configured to identify -- the DFD
9 creator may be configured to identify
10 elements of the information system and
11 compose a DFD for the information system
12 from those elements in accordance with the
13 threat model level identified. So matching
14 104 and 106 together. So, essentially,
15 it's allowing you to create -- it's what
16 helps you create the data flow diagram
17 itself.

18 Q. So, again, just for the record,
19 you are referring to Column 5, line 45?

20 A. Yes. I'm sorry. Yes.

21 Q. So this DFD creator is the system
22 that actually creates the data flow diagram
23 of the information system being analyzed?

24 A. That is correct.

25 Q. I know this is asking you to jump

1 R. Hurlbut
2 around in this file, but if you could take
3 a look at figure 8, please.

4 A. Sure.

5 Q. This is figure 8 of Jones, I
6 should say.

7 A. Yes, I can see it.

8 Q. Is that a data flow diagram?

9 A. Yes.

10 Q. So that would be, I guess, an
11 example of what the DFD creator 106 would
12 generate?

13 A. Yes. Or allow the user to
14 generate.

15 Q. What do you mean by allow the
16 user to do it? Like, manually create it?

17 A. Yes.

18 Q. And so, again, referring back to
19 the Figure 1 system from the DFD creator,
20 the next-box or system in the overall flow
21 is threat indicator 108.

22 Is that right?

23 A. Yes.

24 Q. And, again, at a general level,
25 what does the threat indicator 108 do?

1 R. Hurlbut

2 A. So as it indicates in Column 5
3 with line 64, "Threat indicator 108 may be
4 configured to identify a cybersecurity
5 threat to a particular element of the
6 elements of the information system, and add
7 a secondary node representing the security
8 threat to the DFD to thereby produce a
9 threat-model DFD for the information
10 system."

11 So based on that, it's relating
12 now the data flow diagram, the components
13 in the data flow diagram relating threats
14 to those components to make up what they
15 call -- what's referred to here as the
16 threat-model DFD.

17 Q. The phrase "threat-model DFD,"
18 does that actually refer to a threat model?

19 A. (Witness reviewing document).

20 I would say so, yes. I was
21 looking to see, as I mentioned earlier, the
22 -- because there is also the section of 112
23 that does the actual analyzing of threats
24 that makes up the total threat model, but
25 the threat-model DFD is as it mentions here

1 R. Hurlbut

2 combining security threat to a particular
3 element of the data flow diagram. So I
4 would say yes.

5 Q. And Column 6, line 3, there is a
6 parenthetical. It says, "for example,
7 level 2 threat-model DFD."

8 Do you see that?

9 A. I do, yes.

10 Q. Is that -- correct me if I am
11 wrong, but is that referring to a threat
12 model at a particular level -- in this
13 case, level 2?

14 A. Yes.

15 Q. Is it fair to say that Jones
16 describes how its system can generate
17 threat models of the information system at
18 various levels?

19 A. As I understand from Column 5,
20 and starting at line 20, which talked about
21 the DFD level establishment system where a
22 particular level has been determined, from
23 my understanding, that is the level that
24 it's at. So it doesn't necessarily
25 represent multiple -- if it's level 2

1 R. Hurlbut

2 because of the criticality of the data and
3 so forth, that's what it is, a level 2. So
4 that's what defines it as, because of the
5 nature of the data, that's what makes it a
6 level 2, versus a system may be a level 2
7 or it may be a level 1.

8 Q. Okay.

9 A. If that makes sense. So
10 distinguishing between a level 1, because
11 you have less information versus level 2,
12 you have a lot more critical information
13 that needs to be protected. So that's what
14 makes a level 2.

15 Q. Okay. So let me just -- I am
16 going to come back to this thing about
17 levels, but just to round out our
18 discussion of Figure 1, you mentioned -- I
19 am sorry. You did not mention this. Let
20 me start over.

21 So from the DFD creator 106, the
22 flow of this overall system is that the
23 information or results of the DFD creator
24 move to a system called the threat
25 indicator 108.

1 R. Hurlbut

2 Is that right?

3 A. Yes. That's correct.

4 Q. And, again, at a high level, what
5 does the threat indicator 108 do?

6 A. So the threat indicator as it
7 mentions for 108 in Column 5 --

8 Q. I am sorry. You've already
9 answered this question. I apologize.

10 A. I did. That's okay.

11 Q. Basically, it sounds like the
12 threat indicator determines threats
13 associated with the DFD, and then adds some
14 indicator of those threats to the DFD,
15 which results in the threat model?

16 MR. MIDDLETON: Objection. Form.

17 A. Yes.

18 BY MR. JACKSON:

19 Q. And then that resulting -- is it
20 fair to say that that at that point is some
21 sort of a diagram or not?

22 MR. MIDDLETON: Objection. Form.

23 A. I would say so. In Column 6 at
24 around line 7, it talks about secondary
25 node. So that means that there are nodes.

1 R. Hurlbut

2 So that, to me, sounds like a diagram --
3 it's describing a diagram.

4 BY MR. JACKSON:

5 Q. And DFD -- those initials stand
6 for data flow diagram, correct?

7 A. That is correct, yes.

8 Q. So, again, I apologize for having
9 you go backwards in the patent, but if you
10 could look at figure 9, please.

11 A. Sure. Okay. I am looking at it.

12 Q. So is figure 9 an example of the
13 output of this threat indicator 108?

14 A. Let me look at the differences.

15 Of course, you always have to
16 readjust.

17 (Witness reviewing document).

18 I would have to check the
19 references to be able to say for sure. For
20 example, there is addition of 904, 902 and
21 so forth and so on. I would have to check
22 the references to see if those were threats
23 to be able to say that those are the
24 threats represented in this particular
25 diagram as an example.

1 R. Hurlbut

2 Q. If you could go to Column 19,
3 roughly line 12, please.

4 A. Okay. Okay.

5 Q. So this paragraph is a
6 description of figure 9; is that right?

7 A. Yes.

8 Q. And then online 12, it refers to
9 cybersecurity threats 904.

10 Do you see that?

11 A. I do.

12 Q. So when we look back at figure 9,
13 this is showing a data flow diagram with
14 cybersecurity threats 904 added to it; is
15 that right?

16 A. That is correct, yes. Based on
17 this description.

18 Q. Does that sound like what the
19 threat indicator 108 generates?

20 A. Yes. Yes.

21 Q. Then back in Figure 1, the
22 results of the threat indicator 108 flow to
23 the decomposer 110; is that right?

24 A. Yes.

25 Q. At a high level, what does the

1 R. Hurlbut

2 decomposer 110 do?

3 A. So per Column 6, line 16 -- 15,
4 16 -- 15. "In these examples, the
5 decomposer 110 may be configured to
6 decompose one or more components of the
7 information system modeled by the DFD into
8 its nested components and data flows
9 therebetween. The decomposer may then
10 provide feedback of its decomposition to
11 the DFD creator 106, which may then modify
12 or which may modify the threat-model DFD
13 for the decomposed components to include
14 their nested components and data flows,
15 thereby producing a level n+1 threat-model
16 DFD."

17 So the decomposer is able to
18 split components into nested components and
19 data flows, so representing that a higher
20 level component may be split into or broken
21 into, instead, nested or smaller components
22 and data flows -- related data flows.

23 Q. So just to take an example.
24 Let's say the original component in
25 the information systems was a bank, for

1 R. Hurlbut

2 example --

3 A. (Nodding affirmatively).

4 Q. And correct me if I am wrong or
5 tell me if I am right, is it fair to say
6 what the decomposer is doing is taking the
7 bank as a whole and then breaking it apart
8 to see its internal components?

9 A. Based on my understanding of this
10 paragraph, yes. I would say so.

11 Q. And in the context of the bank
12 example, what would be some of the internal
13 components?

14 A. I would say the various sections
15 of the bank, so it could be the tellers.
16 It could be the various places where
17 somebody is opening an account maybe. The
18 vault. And of course the personnel, as
19 well, but the various operations within
20 that bank.

21 Q. Okay. Assuming there was an ATM
22 in the bank, would that be another
23 subcomponent?

24 A. Sure. Sure.

25 Q. And the cash drawers for the

1 R. Hurlbut

2 tellers? Would that be another one?

3 A. Cash drawers, yes.

4 Q. Before the decomposition, is it
5 fair to say that the threats associated
6 with those subcomponents were modeled at
7 the overall bank level?

8 A. Yes. Related to the particular
9 component at whatever level it was. So at
10 the higher level, threats that are given
11 are at that level, and then after
12 decomposition, then threats would be also
13 then related to the various decomposed
14 components.

15 Q. So I was just trying to
16 understand the relationship between the
17 bank and its subcomponents. If you look at
18 a particular threat associated with a
19 subcomponent, let's just take an ATM for
20 example.

21 A. (Nodding affirmatively).

22 Q. The ATM is in the bank. There
23 are certain threats associated with that
24 ATM, correct?

25 A. Yes. Correct.

1 R. Hurlbut

2 Q. If you are looking at the overall
3 bank branch at that higher level component,
4 are the risks that are associated with the
5 ATM reflected in the threats that are
6 associated with the bank as a whole?

7 A. If I understand your question and
8 I'm going to make sure -- would I know the
9 threats for, let's say, the ATM, if I am
10 looking at the bank as a whole?

11 Q. No. Not that you would know
12 them, but just that the effect of the
13 threat to the ATM particularly is reflected
14 in -- to whatever degree, it's reflected in
15 the overall threat scenario for the bank as
16 a whole.

17 Is that correct?

18 MR. MIDDLETON: Objection. Form.

19 A. Again, as I understand this
20 document and the description here, as you
21 decompose, then the threats sort of become
22 part of, or revealed, or are now a part of
23 the larger threat model, so I would say so.

24 BY MR. JACKSON:

25 Q. I am sorry for asking vague

1 R. Hurlbut

2 questions.

3 A. It's okay. I am trying to make
4 sure I understand it and as well as
5 understand it, how this is described as
6 well.

7 Q. Absolutely. I appreciate that.
8 And maybe, just to make it a little easier
9 to refer to the different levels, let's
10 assume we are just looking at a bank, and
11 the bank is one component of this overall
12 threat model diagram, DFD, okay?

13 A. (Nodding affirmatively).

14 Q. And so if we are looking at the
15 bank as a whole, from the outside --

16 A. Right.

17 Q. -- can we call that level 1 just
18 for discussion purposes?

19 A. (Nodding affirmatively).

20 Q. And then when we go into the bank
21 and look at its subcomponents, we can call
22 that level 2?

23 A. I would say so. I mean, it does
24 mention the hierarchy there in Column 6,
25 line 31.

1 R. Hurlbut

2 So there is a hierarchy which
3 seems to indicate with the levels that you
4 are moving down in terms of degree of
5 decomposition and understanding and so
6 forth. So yes, I would say so. Different
7 levels related.

8 Q. And in line 31 of Column 6, it
9 refers to level of the hierarchy, right?

10 A. Yes, it does.

11 Q. So it's implying that there is a
12 hierarchy of levels, right?

13 A. Yes.

14 Q. And I just picked level one and
15 level two just as a way of referring to
16 them. But if we assume the bank as a whole
17 is a single component in the threat model
18 is at level one --

19 A. (Nodding affirmatively).

20 Q. -- and we -- then using, I guess,
21 the decomposer, we then look at the
22 subcomponents of the bank, for example,
23 looking at the ATM or the cash drawers or
24 the tellers, can we describe those
25 components at being at level two?

1 R. Hurlbut

2 A. So this is what's interesting is
3 that over in Column 5, it describes level
4 two as something related to criticality and
5 so forth. So when you say level two, it's
6 almost redefining it.

7 Q. Right. I agree. I understand
8 what you are saying.

9 I was thinking about here in
10 Column 6, for example, at line 23 --

11 A. (Nodding affirmatively).

12 Q. -- it talks about a Level n+1
13 threat-model DFD?

14 A. Right.

15 Q. And then there is also, I think,
16 another instance where it talks about -- up
17 above actually, at line 2 and 3, it refers
18 to a Level N threat-model DFD.

19 Do you see that?

20 A. Yes.

21 Q. The N is just a placeholder for a
22 number, correct?

23 A. Correct, yes.

24 Q. So we could maybe so as to avoid
25 confusion with one and two over in

1 R. Hurlbut

2 Column 5, what if we said the bank as a
3 whole is at level five, and then when we
4 use the decomposer to look at the
5 subcomponents of the bank, those
6 subcomponents are at level six.

7 Would that be reasonable?

8 A. Yes. I would agree with that.

9 Q. So when -- I forgot where I
10 started. I apologize.

11 So when you look at the -- this
12 may be retreading some of the ground. I
13 apologize.

14 When you look at the bank at
15 level five, are the threats associated with
16 the components -- the subcomponents at
17 level six, are they reflected in the
18 threats associated with the level five
19 bank?

20 A. If you are looking at level 6,
21 then yes, because you are also seeing level
22 five and then level 6, if I understand your
23 question.

24 Q. So let's go on through -- there
25 is only a couple more blocks of this

1 R. Hurlbut

2 Figure 1.

3 A. Okay.

4 Q. Is it fair to say the decomposer
5 outputs data in one of two directions, if
6 you will.

7 The first one being that it can
8 feedback results into the DFD creator 106?

9 Is that right?

10 A. Yes, yes.

11 Q. Or, alternatively, it can output
12 its results to threat analyzer 112; is that
13 right?

14 A. Yes, that's correct.

15 Q. So let's talk about threat
16 analyzer 112.

17 A. Okay.

18 Q. Again, at a high level, what does
19 threat analyzer 112 do?

20 A. So Column 6, line 35, threat
21 analyzer 112 may be configured to perform
22 an analysis of the cybersecurity threat
23 based on the threat-model DFD and metadata
24 associated with the nodes edges and
25 secondary node thereof.

1 R. Hurlbut

2 So it's doing the work of
3 determining the threats based on, at that
4 point, what components are present. Any
5 nodes, edges, as it says, and then it also
6 indicates, Identify a measure of current
7 risk, suggested mitigations and so on.

8 Going down to 46. Threat
9 analyzer 112 may also provide metadata
10 associated with a secondary node.

11 Q. The secondary node, is that
12 referring to the actual threats themselves
13 that were added by the threat indicator at
14 roughly Column 5, line 65?

15 A. That's a great question. And,
16 unfortunately, they don't really specify.
17 But that the node as used elsewhere seems
18 to refer to the nodes in the data flow
19 diagram which relate to components, the
20 various decomposed components as it
21 mentions up there in 26, Column 6 about
22 decomposed components and appropriate
23 secondary nodes representing those threats.

24 Q. Right. So --

25 A. I am sorry. To answer your

1 R. Hurlbut

2 question, that does seem to refer to the
3 threats.

4 Q. Just to clarify, and also in
5 fairness to you, if I could have you take a
6 look at Column 5 starting at roughly line
7 -- it looks like 66.

8 A. Okay. Sure.

9 The information system and add a
10 secondary node representing the
11 cybersecurity threat. Yes.

12 So it is -- secondary node is
13 representing the threat -- a security
14 threat.

15 Q. Okay.

16 A. Okay.

17 (Witness reviewing document).

18 So I apologize, could you ask the
19 question again?

20 Q. That's okay. I don't have a
21 question pending, I think. I was trying to
22 figure out what to ask next.

23 Okay. I think you had just
24 explained that in Column 6, line 46, the
25 threat analyzer also provides metadata

1 R. Hurlbut

2 associated with the secondary note, right?

3 A. Correct.

4 Q. And that's where I asked you,
5 does the secondary node correspond to the
6 threat?

7 A. Right.

8 Q. And you said yes?

9 A. Yes. Based on looking back at 66
10 on Column 5.

11 Q. And looking here at this
12 description of the threat analyzer, does it
13 tell you what the purpose of that analysis
14 is?

15 You mentioned referring to or
16 determining -- I'm not sure -- referring to
17 a current risk and suggested mitigation,
18 and then now we also have the addition of
19 metadata associated with threats.

20 Does this tell us what the
21 purpose of that effort is?

22 A. (Witness reviewing document).

23 Well, one, it does mention -- 38,
24 line 38 in Column 6.

25 In some examples, this may

1 R. Hurlbut

2 include the threat analyzer being
3 configured to identify a measure of current
4 risk of the cybersecurity threat to a
5 particular element, sometimes being
6 referred to as a current risk rating and
7 identify a suggested mitigation
8 implementable to reduce the current risk
9 rating to a lower measure, a residual risk.

10 So it looks like the purpose is
11 as it's analyzing the threat or determining
12 the threat, ultimately leading to make
13 recommendations or determine a risk rating
14 as well as recommendations for mitigations
15 that could reduce that risk rating. So
16 that seems to be the purpose of the threat
17 analyzer.

18 Q. Okay. And then from the threat
19 analyzer, the output of that threat
20 analyzer in Figure 1 flows to the reporter
21 114.

22 Is that right?

23 A. That's correct.

24 Q. And, again, at a high level, what
25 does the reporter 114 do?

1 R. Hurlbut

2 A. As indicates starting at line 59
3 on Column 6, configured to generate one or
4 more reports from the threat analysis.
5 So -- and report could be just a summary of
6 that data or information.

7 Q. So it can extract metadata, for
8 example?

9 A. Correct, yes. Metadata.

10 Q. And this would be in -- is the
11 output of the reporter a DFD?

12 A. No. No. Let's see.

13 (Witness reviewing document).

14 It says, An organized arrangement
15 of at least some of the attributes of at
16 least some of the components, data flows,
17 or cybersecurity threat.

18 So it's not really another data
19 flow diagram, but more metadata or other
20 data, and then organized to give some -- as
21 it says, at least some of the attributes of
22 at least some of the components, data flows
23 or cybersecurity threat.

24 So it's -- it would appear here
25 that it's a written description of that

1 R. Hurlbut

2 data versus a diagram itself. It's not a
3 diagram. It's just a listing or organized
4 listing of information.

5 Q. This listing of information -- is
6 that a threat model?

7 A. No. It's a way of communicating
8 the results of the threat model exercise.

9 Q. And I should have asked you to
10 take a look at these earlier, but figures
11 10A and 10B in Jones --

12 A. Sure.

13 Q. -- I think these are described as
14 being examples of reports, but I will let
15 you confirm whether that's true or not?

16 A. Sure. So 10A and 10B. Yes.
17 Yes.

18 Q. These are reports?

19 A. These are reports.

20 Q. So we can take one of them, if
21 you would like. Actually, I did have a
22 question about these two.

23 Is there a relationship between
24 these two reports, or are these two
25 separate reports?

1 R. Hurlbut

2 What I am wondering is, is 10B
3 supposed to be additional columns for
4 what's shown in 10A, or are these supposed
5 to be two different reports?

6 A. To me, it looks like two
7 different reports mainly because of the
8 reference numbers. If it was a
9 continuation, for example, I think the
10 numbers would be continual. So nine and so
11 forth.

12 So I think, to me, these look
13 like two separate reports.

14 Q. I was wondering if maybe 10B
15 could be put to the right of 10A. So the
16 row continues through 10A over to 10B, the
17 same row?

18 A. Oh, I see.

19 Q. I am not sure. I am asking.

20 A. I am looking at it again. It's
21 hard to see because I have to keep --

22 Q. Toggling?

23 A. Toggling and making it from
24 upside down to not upside down type of
25 thing.

1 R. Hurlbut

2 If you look at the columns,
3 Vulnerability Threat Impact and then you
4 look at the next one, those columns are not
5 there. So it is the same report. It's
6 just, as you said, two parts of the same
7 report. So next door to each other.

8 Q. And believe me, I am not trying
9 suggest it is or it isn't. I just honestly
10 didn't know.

11 So I thought I would ask you
12 whether that's the way it's supposed to be
13 laid out or not?

14 A. That's what it looks like to me,
15 based on my understanding and seeing
16 reports like this before. That's what it
17 looks like to me.

18 Q. And then the reporter is the end
19 point of the system of Figure 1, right?

20 A. Correct.

21 Q. So earlier we talked about --
22 when we were talking about, I guess it was
23 threat indicator and we were talking about
24 hierarchies and levels, and that sort of
25 thing. And I mentioned, I think I wanted

1 R. Hurlbut
2 to come back to that topic.
3 And going back to Column 5, there
4 is a discussion there in a paragraph that
5 goes from line 4 to roughly line 19 where
6 it talks about hierarchy and levels.
7 Let me know when you are there.
8 A. Yes. I'm at 4.
9 Q. Column 5?
10 A. Column 5, yes. Yes.
11 Q. So the sentence that starts at
12 roughly line 10 --
13 A. Okay.
14 Q. -- it says the information system
15 for starters. That's the system will go
16 analyzed by the system of Figure 1?
17 A. Yes, correct.
18 Q. The information system may be
19 describable in terms of a hierarchal
20 breakdown herein after referred to as a
21 hierarchy of its components.
22 Do you see that?
23 A. Yes.
24 Q. I am sorry. I didn't finish the
25 sentence. I thought I did.

1 R. Hurlbut

2 A hierarchical breakdown of its
3 components at different levels.

4 Do you see that?

5 A. I do, yes.

6 Q. What does that tell you about the
7 information system being analyzed?

8 A. That the information system can
9 be broken down, that there is a hierarchy,
10 various components, and at different
11 levels.

12 So what it's saying is that a
13 system is comprised of potentially multiple
14 levels and multiple components on each
15 level.

16 Q. So at a top level, there are
17 components of the information system,
18 right?

19 A. Yes.

20 Q. And then at least some of those
21 components may have subcomponents.

22 Is that right?

23 A. That's correct.

24 Q. And when you go to a level --
25 whatever the next lower level is or higher,

1 R. Hurlbut

2 depending, I guess, on how you look at it,
3 when you go down to the subcomponent level,
4 at least some of those subcomponents may
5 have -- may further have their own
6 subcomponents.

7 Is that right?

8 A. That's correct, yes.

9 Q. And those are part of this
10 overall information system that's being
11 analyzed, right?

12 A. That is correct, yes.

13 Q. And that's what Jones refers this
14 as multiple nested components; is that
15 right?

16 It's at line 16.

17 A. Yes. Multiple nested components,
18 yes.

19 Q. And that's what Jones is talking
20 about, is that you can go from one
21 component, its subcomponents, and then at
22 least some of those subcomponents may have
23 their own further subcomponents, right?

24 A. Yes. That's correct.

25 Q. And all of that is part of that

1 R. Hurlbut
2 information system that's being analyzed?

3 A. Yes. Correct.

4 MR. JACKSON: I apologize. We
5 have been going for over an hour. Did
6 you want to take a break?

7 THE WITNESS: Maybe five minutes
8 or so.

9 MR. JACKSON: Let's go off the
10 record.

11 (Recess: 11:23 to 11:31 a.m.)

12 BY MR. JACKSON:

13 Q. Mr. Hurlbut, let me ask you to
14 take a look at your declaration, which is
15 Exhibit 1003, and I'm going to ask you
16 specifically about a sentence on page 45.
17 It's part of a paragraph that actually --
18 and a section that actually starts on page
19 44. So feel free to look at as much of
20 that as you need to for context.

21 A. Okay.

22 Q. The sentence I wanted to ask you
23 about ask at the top of page 45. It's the
24 first full sentence right before the figure
25 that you have there. It begins with the

1 R. Hurlbut

2 phrase "a POSITA would."

3 Do you see that?

4 A. Yes, I do.

5 Q. And I just want to ask you a
6 little bit about what you meant in this
7 sentence, just so that I'm sure I
8 understand what's being said here. So
9 please take your time to read that sentence
10 to yourself, and then let me know when you
11 are finished.

12 A. Okay.

13 (Witness reviewing document).

14 Okay.

15 Q. Okay. So, specifically, I want
16 to ask you about the phrase, "identifying
17 elements of the information system."

18 Do you see that phrase?

19 A. I do, yes.

20 Q. My question is really, is the
21 word "identifying" there being used as an
22 adjective or as a verb? And if that
23 doesn't make sense, I'll try to change my
24 question.

25 A. Sure. I would say as an

1 R. Hurlbut

2 adjective. So the differences between
3 various elements within the system knowing
4 that this is one thing versus another
5 thing-type of thing.

6 Q. So as an adjective?

7 A. Yes.

8 Q. And then the last clause in this
9 sentence reads, "when Jones' system is
10 applied."

11 Do you see that there?

12 A. Yes, I do.

13 Q. In the context of this overall
14 sentence, what did you mean by that phrase?

15 A. Part of the -- again, the work
16 here is determining with a deep
17 composition, what are the components, how
18 are they connected, and so on. So in terms
19 of applying Jones' system of that
20 decomposition, various levels and so forth
21 to make up the whole.

22 Q. I'm sorry. Were you finished
23 with your answer?

24 A. I am, yes.

25 Q. I apologize. Okay. So I'm

1 R. Hurlbut

2 sorry. I'm just a little -- still a little
3 confused. So let me back up a little bit
4 more in that sentence.

5 A. (Nodding affirmatively).

6 Q. The larger phrase says "which
7 would be dependent on a predefined system
8 when Jones' system is applied."

9 The predefined system, are you
10 referring there to the information system
11 that's being analyzed in Jones?

12 A. Correct, yes. So we have a
13 particular information system that we're
14 looking at, yes.

15 Q. And the information system --
16 just to clarify, the information system is
17 not a DFD or a threat-model DFD, right?

18 A. That's correct, right.

19 Q. It's the actual real world system
20 that's being analyzed?

21 A. Correct, yes.

22 Q. Okay. So in that real world
23 system, what you're saying is it itself is
24 predefined before Jones' system is applied,
25 right?

1 R. Hurlbut

2 A. Or it's determined this is a
3 system you want to analyze, so that's the
4 pre-definition aspect of it.

5 Q. And so when you refer up above in
6 the sentence to "the interrelated group of
7 two or more threat model components in
8 Jones" and that they "may be predefined,"
9 that's saying that when you apply or
10 generate, rather, a threat model using the
11 Jones system --

12 A. (Nodding affirmatively).

13 Q. -- from the information system,
14 that at least two threat model components
15 are interrelated because the information
16 system has defined those elements, if you
17 will, to be interrelated.

18 Is that right?

19 A. Yes. That's correct.

20 Q. Okay. I just wanted to make sure
21 I understood that. I think I do. Thank
22 you.

23 A. Okay. You are welcome.

24 MR. JACKSON: Let me show you or
25 push out to you the actual patent that

1 R. Hurlbut

2 we are -- that's at issue in this IPR,
3 the '008 Patent.

4 THE WITNESS: Okay.

5 (Exhibit 1001 was referenced for
6 identification)

7 BY MR. JACKSON:

8 Q. So you should have that. The
9 '008 Patent is identified as Exhibit 1001
10 in this IPR. The patent is there for your
11 reference if you want to look at a larger
12 context, but I want to specifically ask you
13 about paragraph 85 of your declaration,
14 which relates to claim 3. That's on
15 page 48. It starts on page 48.

16 A. Okay. Okay. I lost my place
17 again. Sorry.

18 MR. JACKSON: I don't know if
19 it's easier or not, but you may want to
20 try downloading the document, and then
21 maybe using Adobe to navigate pages.
22 It might be easier.

23 MR. MIDDLETON: That's what I
24 have been doing. I think it is easier.

25 THE WITNESS: Okay. It says

1 R. Hurlbut
 2 "save," but it's not saving. I
 3 have a PDF of this -- of all of
 4 these, but I was trying to pull the one
 5 down from what you provided, unless
 6 there's --

7 MR. MIDDLETON: Are you okay if
 8 Mr. Hurlbut pulls up his version of
 9 Exhibit 1001?

10 MR. JACKSON: Yes.

11 BY MR. JACKSON:

12 Q. And actually, Exhibit 1001 and
 13 1003, have you added -- let me just ask you
 14 about 1003, your copy.

15 Does your copy include any
 16 information that isn't reflected in the
 17 official Exhibit 1003?

18 A. No.

19 Q. No annotations or anything like
 20 that?

21 A. No annotations or anything, no.

22 Q. How about with respect to the
 23 '008 Patent, which is Exhibit 1001, are
 24 there any annotations or additional
 25 information on your copy?

1 R. Hurlbut

2 A. No annotations or additional
3 information.

4 Q. Feel free to pull those up, then,
5 please.

6 A. Thank you. So this is 1003 and
7 1001. Okay. I have got both open.

8 Q. So it should be page 48 of your
9 declaration. I'm not sure what PDF page
10 that is. But it's page 48.

11 MR. MIDDLETON: It's PDF page 55.

12 THE WITNESS: Okay. I think I'm
13 there. Page 55. Yes. I'm there.

14 BY MR. JACKSON:

15 Q. You're going to think this is a
16 lot of work for a simple question. But I
17 wanted to -- I guess I could have asked you
18 about the claim from the patent, but you
19 have it quoted here on page 48 of your
20 declaration.

21 A. (Nodding affirmatively).

22 Q. Do you see Claim 3? It is in the
23 heading.

24 A. Yes.

25 Q. And the claim begins, "The threat

1 R. Hurlbut

2 model chaining method of Claim 1, further
3 comprising," and then there is a lot of
4 language after that.

5 Do you see that?

6 A. Yes.

7 Q. When you wrote your declaration,
8 was it your understanding that claim 3 was
9 adding additional method steps to what's
10 recited in claim 1?

11 MR. MIDDLETON: Objection. Form
12 and objection to the extent it calls
13 for a legal conclusion.

14 A. As I recall, it's essentially
15 similar to Claim 1. Yes. One or more
16 interfaces receiving one or more user
17 inputs. So, yes, there is some addition,
18 but, essentially, it's still Claim 1 -- or
19 mostly Claim 1.

20 BY MR. JACKSON:

21 Q. I apologize.

22 So are you saying that parts of
23 claim 3 -- when you did your analysis that
24 parts of claim 3 were satisfied because of
25 some malls you did with respect to Claim 1.

1 R. Hurlbut

2 Is that right?

3 A. Correct, but also I looked at 3
4 on its own as well.

5 Q. Sorry. I am not following you.

6 Is that an alternative analysis
7 you did? You said I looked at claim 3 as
8 well.

9 A. Right.

10 So I understood Claim 1, and I
11 looked at what's similar or the same as
12 Claim 1 for claim 3?

13 Q. So what parts of claim 3 were
14 already addressed in your analysis of
15 Claim 1?

16 A. I have to go back and look at
17 Claim 1 for a moment. Actually let me look
18 at the patent. It's easier to see them
19 side by side.

20 (Witness reviewing document).

21 Yes. So I saw it as an extension
22 or an additional inputs, additional
23 components, additional, and so on to what
24 is one.

25 Q. So you mentioned additional.

1 R. Hurlbut

2 There are several uses of the
3 word additional in claim 3, right?

4 A. Correct, yes.

5 Q. Right. So, for example, claim 3
6 refers to additional threat model
7 components, right?

8 A. Yes.

9 Q. And is it your understanding that
10 the additional threat model components
11 recited in claim 3 are separate from the
12 threat model components recited in Claim 1?

13 Maybe "separate" isn't the right
14 word. There are at least an additional
15 two.

16 A. Right. Additional.

17 Q. So the additional threat model
18 components of claim 3 are not satisfied by
19 the threat model components of Claim 1,
20 right?

21 A. Correct.

22 Q. And then claim 3 also refers to
23 additional threats, right?

24 A. Correct.

25 Q. And the same logic holds true,

1 R. Hurlbut

2 that the additional threats are threats in
3 addition to the threats that were recited
4 in Claim 1, right?

5 A. Correct.

6 Q. And then just to round things out
7 here, claim 3 refers to additional
8 compensating controls.

9 Do you see that?

10 A. Yes.

11 Q. And the same is true for those
12 additional compensating controls are in
13 addition to whatever compensating controls
14 are recited in Claim 1, right?

15 A. Yes, that's correct.

16 Q. And is that the analysis that you
17 used when you -- I am sorry. Strike that.

18 Is that the understanding you
19 used when you analyzed claim 3 here in, it
20 looks like paragraph 85?

21 A. Let me go back there again. But
22 yes. That was 35.

23 (Witness reviewing document).

24 Right. The last statement there,
25 each of these steps could be performed an

1 R. Hurlbut

2 additional time. One or more of each of
3 these functions in creating one or more
4 DFDs including the claimed element. So
5 yes. That was my understanding in
6 analyzing claim 3.

7 Q. And just for the record, what
8 were you referring to?

9 A. I am sorry. So if we are looking
10 at 85.

11 Q. Paragraph 85 of your declaration?

12 A. Paragraph 85, the last sentence
13 there. I will go one above that.

14 "Jones discloses that each of
15 these steps could be performed an
16 additional time. Jones refers consistently
17 to one or more of each of its functions and
18 creating one or more DFDs including the
19 claimed elements."

20 Q. That's the sentence -- it's
21 actually the end of one sentence on page 48
22 rather?

23 A. And going into, yes, the first of
24 page 49.

25 Q. Okay. And then you also cite to

1 R. Hurlbut

2 the figures 7 through 9 of Jones as
3 support, correct?

4 A. Yes.

5 Q. And you have figure 9 there
6 obviously embedded in your paragraph 85,
7 correct?

8 A. Yes. Yes.

9 Q. If I could direct you to
10 paragraph 87 of your declaration.

11 A. (Nodding affirmatively).

12 Q. Let me know when you are there.
13 This relates to claim 2.

14 A. Yes, I am there.

15 Q. Just, again, so I understand kind
16 of where you are coming from on this, is it
17 correct to say that you relied on Zheng or
18 disclosing the elements of claim 2?

19 A. Yes.

20 Q. Did you rely on any other
21 reference is in analyzing claim 2 here in
22 paragraphs 87 and 88?

23 A. No. Just Zheng. Yes. Right.
24 This is attack paths.

25 Q. Let me have you move over to

1 R. Hurlbut
2 paragraphs 95 and 96 of your declaration.

3 A. Okay.

4 Q. This relates to claim 5.

5 A. Okay. I am there.

6 Q. And claim 5 is a dependent claim
7 off of claim 4, right?

8 A. Yes.

9 Q. And so as support for the
10 evidentiary support you point to in Zheng
11 as disclosing this claim element or it's
12 actually a claim is Column 5, lines 6 to 24
13 and at the very end of 96, paragraph 96,
14 Column 10 lines 43 to 49.

15 Correct?

16 A. That's correct.

17 MR. JACKSON: Let me push out
18 Zheng.

19 BY MR. JACKSON:

20 Q. Do you have a clean copy of
21 Zheng?

22 A. I do.

23 Q. Let me just, for the record, push
24 out a clean copy of that as well.

25 A. Sure.

1 R. Hurlbut

2 Q. You said you had your own clean
3 copy of Zheng, right?

4 A. I do. I have it open.

5 MR. JACKSON: For the record,
6 Zheng is Exhibit 1005 in the IPR we are
7 talking about.

8 (Exhibit 1005 was referenced for
9 identification)

10 BY MR. JACKSON:

11 Q. So let me, if I could, direct you
12 to that first cite, Zheng, Column 5, lines
13 6 to 24.

14 A. (Nodding affirmatively).

15 Q. And if you want to read that to
16 refresh yourself, please do so and just let
17 me know when you are finished.

18 A. Sure.

19 So Column 5 -- sorry, one more
20 time.

21 Q. Yes. Line 6 to line 24.

22 A. Okay.

23 (Witness reviewing document).

24 Okay. I read it.

25 Q. Zheng refers to vector multiple

1 R. Hurlbut

2 times, including in this paragraph, right?

3 A. Yes.

4 Q. And a vector -- is it fair to say
5 in Zheng, a vector connects two end points
6 together?

7 A. No. Not necessarily. Just go
8 back to threat target -- line 16, Column 5,
9 a threat target application, displayable
10 vector connecting the two to represent and
11 visualize a particular attack methodology.

12 So Zheng is using a vector as an
13 attack path essentially. It's not just
14 connecting point to point, but it's
15 actually -- the display of a vector is
16 representing a particular attack.

17 In this case, it calls it attack
18 methodology, but essentially, it's an
19 attack path.

20 Q. What about this sentence or
21 phrase that you refer to here says that the
22 vector connects to more than two end
23 points?

24 A. Which one is that? In the Zheng
25 patent?

1 R. Hurlbut

2 Q. In Zheng.

3 A. Okay.

4 Q. You pointed to roughly lines --
5 it looks like maybe 17 and 18 of Column 5.

6 Maybe starting at 16. I think
7 it's 17 and 18.

8 A. 17 and 18, yes.

9 (Witness reviewing document).

10 Q. I am just curious -- maybe there
11 is other parts of this paragraph. Feel
12 free to refer to that as well.

13 Particularly what you pointed to
14 was a phrase in lines 16 and 17.

15 What about that phrase tells you
16 that an attack vector in Zheng connects
17 more than just two end points?

18 A. I think it's further down. But
19 vector connection could be a data flow path
20 between one or more cities between one or
21 more buildings. So I think it's a little
22 further down.

23 Let me go back and look at the --
24 one-to-one mapping between a threat actor
25 and threat target as well as one-to-one,

1 R. Hurlbut

2 one-to-many, many-to-one, many-to-many
3 mapping of threats and threat actors.

4 So that refers really towards the
5 end of that, lines 20 through 24, it looks
6 like.

7 Is that what you are asking
8 about?

9 Q. Yes. I think this is the same
10 idea. Okay.

11 So let me just ask you
12 specifically about these examples here in
13 this paragraph of Column 5 of Zheng.

14 So that sentence at line 18
15 begins for example, a vector connection can
16 be a data flow path between one or more
17 cities. Let me just stop there.

18 A. Okay.

19 Q. So if -- it gives the alternative
20 one or more cities. So in the case of one
21 city, a vector would connect from the city
22 to itself, right?

23 A. No. I don't think so, if I
24 understand the question. Let's just go
25 back up for a moment to line 14, Column 5.

1 R. Hurlbut

2 Each threat can be visually associated with
3 at least one threat actor application, a
4 threat target application and displayable
5 vector connecting the two.

6 So then when you go back to your
7 question about one or more cities, based on
8 what Zheng is saying here is that there
9 could be a threat actor. There needs to be
10 a threat actor, the target application in
11 this case it could be a city or multiple
12 cities.

13 And then the displayable vector
14 that's connecting one or more or
15 essentially two. But based on my
16 understanding here, I don't think it would
17 be city to city, if I understand what you
18 were asking.

19 Q. Okay. Go ahead. I am sorry.

20 A. I was going to say, I wonder if
21 it would help to look at the diagram -- let
22 me just look up here.

23 What figure is this referring to?
24 If that helps.

25 Q. I see a reference to Figure 1 in

1 R. Hurlbut

2 Column 4 at line 31 -- I am sorry.

3 I think it's referring to
4 Figure 2 if you go back to the bottom of
5 column 3.

6 A. Right. I think it is. Figure 2
7 doesn't look quite right.

8 (Witness reviewing document).

9 I guess it would be Figure 2.

10 All right.

11 (Witness reviewing document).

12 We are on 5? Yes. 5. Okay.

13 (Witness reviewing document).

14 Back to your question about one
15 or more cities, I think you said does that
16 mean a city could have a vector connected
17 to itself?

18 Q. Right. So Zheng says one or more
19 cities.

20 So I was just taking for starters
21 the situation where it's just a single
22 city?

23 A. Right.

24 Q. So is that saying that you have a
25 vector that connects from that city back to

1 R. Hurlbut

2 itself?

3 A. Again, I would say no based on
4 Column 5 and starting at line 14 that each
5 threat can be visually associated with at
6 least one threat actor, application, a
7 threat target application and a displayable
8 vector.

9 So the city itself would not be
10 the threat actor in the question that you
11 are asking. The city is actually the
12 target.

13 Q. Okay. But in the next sentence
14 after that, it says, for example, a vector
15 connection, so now it seems to be focusing
16 on the vector itself, right?

17 A. Okay. Sure.

18 Q. It says a vector connection can
19 be a data flow path between one or more
20 cities.

21 I stopped right at the one just
22 to start there.

23 A. (Nodding affirmatively).

24 Q. I was trying to understand in the
25 case of the one city, what does that vector

1 R. Hurlbut

2 connection look like?

3 A. Again, I think it would show --
4 based online 14 that there is going to be a
5 threat actor application that connects or a
6 threat actor that connects to the one, the
7 city, and then, in turn, connects to
8 another city. And so on.

9 Is there a vector between city to
10 city to city? I think that's what you are
11 asking, if I understand correctly.

12 Q. Well, that would seem to be the
13 case of more than one city, right, which is
14 the second alternative here?

15 A. However that's --

16 (Witness reviewing document).

17 Also in line 20, Column 5, a
18 threat can provide one-to-one matching
19 between a threat actor and a threat target.
20 A one-to-many, so a threat actor to many
21 targets, let's say. So that goes back
22 maybe to your cities, one to two or more
23 cities. And then a many-to-one mapping or
24 many-to-many mapping depending on the
25 nature of the threat.

1 R. Hurlbut

2 So there may be additional -- I
3 think the -- as I understand it, based on
4 my reading of this and especially going
5 back again to line 14, Column 5, it says a
6 vector is one, a threat actor application;
7 two, a threat target; and three, the
8 displayable vector or that connection
9 between two of these parts. The first
10 part, the threat actor; the second part,
11 the threat target; and then the line
12 between or the -- as it says, the
13 displayable vector between those two.
14 That's the two. However, the one-to-one,
15 one-to-many is the threat actor to many
16 targets, potentially many threat actors to
17 one target and many threat actors to many
18 threat targets. So with that understanding
19 from, again, based on the definition as
20 it's described of what a vector is -- what
21 it's trying to represent with a vector is
22 always connected between a threat actor and
23 a threat target versus a -- a city to city
24 is really a threat target and that's not
25 how I understand the definition here of a

1 R. Hurlbut

2 threat vector or displayable vector here.

3 Q. Okay.

4 A. Does that make sense?

5 Q. I think it does. Seems as though
6 -- again, you tell me if I am misconstruing
7 what you are saying, but it seems like in
8 the context of the discussion of one or
9 more cities or one or more buildings, that
10 that doesn't really -- that sentence
11 doesn't really describe the situation where
12 you have the threat actor, the vector, and
13 the target. It's only -- if I understand
14 you correctly, it's only describing the
15 targets, correct?

16 A. If it's -- well, one to more
17 cities, yes, correct. It's describing the
18 targets. In this case, the cities or the
19 buildings, correct, yes.

20 Q. Okay.

21 A. As opposed to a city would be the
22 attacker, a threat actor, and another city
23 would be the threat target. That's what I
24 was a little bit confused on when you were
25 asking that question. Would you have a

1 R. Hurlbut

2 vector to itself if it's one. But no. I
3 think these are all referring to the
4 targets, which makes sense in terms of
5 components, in terms of -- typically, when
6 you are separating the threat actor from
7 the threat target. I don't know if that
8 made sense. Going back to the declaration,
9 I say one or more attack paths which pass
10 through multiple diagram components.
11 Looking at paragraph 95, a vector
12 connection can be a data flow path between
13 one or more cities or between one or more
14 buildings, and one-to-one mapping between a
15 threat actor and a target. And, again, as
16 well as one-to-many, many-to-one,
17 many-to-many mapping the threats and threat
18 actors.

19 So I think the clarification is
20 the threat actor and the threat target so
21 that last sentence is one-to-many,
22 many-to-one, many-to-many, mapping of
23 threats, which -- in terms of determining
24 or understanding threats or threat actors
25 against threat targets and the vector in

1 R. Hurlbut
2 between based on the definitions.

3 Is that clear, or are you
4 still --

5 Q. Yes, I think it is clear. When
6 Zheng refers to vectors, are vectors
7 typically depicted as an arrow from some
8 starting point to an ending point?

9 A. As Zheng describes it?

10 Q. As Zheng uses that phrase,
11 "vector," vectors are throughout in Zheng,
12 right?

13 A. Right.

14 Q. So vectors in that context, in
15 the context of Zheng, are they typically
16 depicted as an arrow from a starting point
17 to some ending point?

18 A. I would say yes. I'm looking
19 for, like, for example, the cities and so
20 forth, but that's not featured, but the
21 vector itself or the characterization of
22 it, I would say, is an arrow.

23 Q. Okay.

24 A. It talks about data flow path,
25 and if you talk about data flows, are

1 R. Hurlbut
2 usually represented as arrows or showing
3 the path from one point to another.

4 MR. MIDDLETON: Did we lose Don?
5 We can go off the record.

6 (Discussion off the record)

7 BY MR. JACKSON:

8 Q. I guess we need to go back on the
9 record. Let's go back on the record.
10 Thanks.

11 So, Mr. Hurlbut, let me ask you
12 about the second passage of Zheng that you
13 cite, and this is in -- you cite it in
14 paragraph 96 of your declaration.

15 A. Yes.

16 Q. But you refer to Column 10, line
17 43 to 48?

18 A. (Nodding affirmatively).

19 Q. And so in Zheng at Column 10,
20 line 43 to 48, I want to ask you about
21 that --

22 A. Okay.

23 Q. -- section.

24 A. Okay.

25 Q. So at Column 10 -- let me ask you

1 R. Hurlbut

2 just to go ahead and read that section of
3 Zheng, if you would, please.

4 A. Sure.

5 Q. Let me know when you are
6 finished.

7 A. Okay.

8 (Witness reviewing document).

9 Okay. I am.

10 Q. Is it fair to say that that
11 portion of Zheng, Column 10, line 43 to 48
12 describes the breadth of the impact that a
13 vulnerability or an attack can have on a
14 system?

15 A. Yes, it does.

16 Q. This passage here is not specific
17 to any particular vectors or attack
18 paths -- right? -- it's just describing
19 sort of the, if you will -- not only the
20 immediate effect of a vulnerability or an
21 attack, but perhaps secondary and tertiary
22 effects of that attack, right?

23 A. Yes, but in line 46, it does say,
24 not only does an attack impact directly
25 targeted applications, which indicates that

1 R. Hurlbut

2 that is a -- that's essentially how it
3 defines vectors earlier about directly
4 targeted applications. But then beyond
5 that. So it's both, really. It's about
6 how the vectors work and how they are
7 showing those attacks and those attack
8 paths, but also how does that, and again,
9 potentially impact beyond that. But that
10 particular part right there, the attack
11 impact directly targeted applications is a
12 call back to earlier about the relationship
13 with the vectors.

14 Q. Okay. So this is implicitly
15 referring back to the fact that there is a
16 threat and a vector and a target?

17 A. Right.

18 Q. And then it's saying that when
19 that attack actually occurs, that not only
20 is the target immediately affected, but
21 there can also be other, what I call,
22 secondary impacts on the overall system,
23 right?

24 A. Yes. Correct.

25 Q. Is there an example you can think

1 R. Hurlbut

2 of to describe that situation?

3 A. Sure. Let me see.

4 Q. My old standby is a bank.

5 A. Yes. Sure. I can -- in fact,
6 that's my original example is related to a
7 bank, as well, and I am familiar with some
8 of the types of attacks.

9 In terms of, let's say, a bank,
10 for example, if someone was able to -- some
11 financial centers have iPads or other kind
12 of devices. You come in and say, let me
13 check you in and expedite everything. If
14 somebody -- an associate put the iPad or
15 whatever they are using down and somebody
16 then took it, what would they be able to do
17 with it? If they are able to compromise
18 it, then maybe they just compromise that
19 one device and try to figure out how it
20 works and see what's happening, but if they
21 are able to compromise -- able to figure
22 out a few things, would that have far
23 reaching consequences, other data that's
24 moving through that device? There is
25 certainly some mitigations around that.

1 R. Hurlbut

2 But that's just one in particular in terms
3 of if you are able to attack something
4 that's important, but it has dependencies
5 as well, it allows you to get into the rest
6 of the system, other customers, other
7 accounts and so on. So that's -- those are
8 an example of how just attacking one item,
9 one place, one target then could have
10 multiple residual impacts to them being
11 able to get to other data, other
12 information and so forth.

13 Q. Okay. What about an example
14 where, let's say an attacker attacks the --
15 I will call it the Internet connection of a
16 particular branch, the branch's connection
17 to the outside world?

18 A. Sure.

19 Q. And is able to successfully cut
20 off that connection between the branch and
21 the outside world. So that would be the
22 attacker, the vector is some sort of
23 Internet connection and then the target is,
24 let's say, the branch's firewall.

25 Is that a reasonable example of a

1 R. Hurlbut

2 threat in an attack?

3 A. Yes. I think so. I think so.

4 Q. And so if the attacker is able to
5 successfully shut down the branch's
6 firewall, would there be potentially other
7 secondary effects that would occur at the
8 bank branch, like, for example, maybe the
9 tellers can't -- not the tellers, but maybe
10 whoever it is at the bank that has access
11 to the vault can no longer access the vault
12 because of some security protocol that's
13 implicitly affected?

14 A. Sure. Sure. Is there a
15 lockdown, for example. Maybe if you are
16 not able to connect out. As you said,
17 maybe the vault shuts down or other kinds
18 of things that might happen as a result.
19 Sure.

20 Q. And that would be an example of
21 this situation that's being described here
22 in Column 10?

23 A. Yes. Yes. Yes.

24 Q. So in the '008 Patent --

25 A. (Nodding affirmatively).

1 R. Hurlbut

2 Q. -- first of all, let me find my
3 copy.

4 In claim 19, so this is on the
5 last page of the '008 Patent?

6 A. Yes.

7 Q. In claim 19, it refers to
8 communication protocol -- a communication
9 protocol.

10 Do you see that?

11 A. I do.

12 Q. What is a communication protocol?

13 A. A communication protocol -- it's
14 just a way or a software system that is
15 defined to help two end points to be able
16 to communicate. So, for example, when you
17 go to a website, you type in http or https,
18 and the "s" basically is a more secure
19 version. It's encrypted and so forth for
20 your connection to a website. Http is a
21 communication protocol. Https is also a
22 communication protocol. It's a standard, a
23 way of communicating from one point to
24 another. In this case, in this example
25 from the browser on your local computer to

1 R. Hurlbut

2 the web application or web server that you
3 are connecting to where that web
4 application resides. And so that's your
5 communication protocol. That's standard.
6 It helps you then communicate between those
7 two points.

8 Q. Would it be fair to call -- if
9 you tried to explain this maybe to a
10 layperson, not somebody such as yourself,
11 but to a layperson, could you describe a
12 communication protocol as being analogous
13 to a language?

14 A. It could be. It could be. I
15 think maybe, hopefully, it's a little
16 simpler maybe is the difference between
17 telephone calls, what they call the
18 landline. I pick up a receiver and I can
19 see an actual telephone line that's going
20 from my handset, my phone to the wall that
21 I think I can look out and I see it goes to
22 a pole, and that goes somewhere else, and
23 finally it connects to somebody else who
24 also has an actual physical line, and now
25 they are able to communicate. Now you give

1 R. Hurlbut

2 somebody a cell phone. Where is the line?
3 How am I communicating with other people?
4 Those are radio waves, and so the radio
5 waves are the communication protocol in
6 that case. The first one was an actual
7 physical line. Now for a cell phone, your
8 communication protocol are the radio waves.
9 In both cases, you are talking but
10 different ways to communicate. So I guess
11 languages could be another way of
12 describing two people speaking French, two
13 people are speaking German. Two different
14 ways to communicate but they are both
15 communicating. So yes. I will go with
16 that.

17 Q. Okay. I know it can't be a
18 perfect analogy. No analogy is perfect.
19 Just as a more simple way of thinking about
20 what a protocol is. That's what I was
21 trying to drive at, I guess.

22 A. Right.

23 Q. So a protocol has certain rules,
24 if you will, about what the signals on the
25 communication line mean to a recipient, is

1 R. Hurlbut

2 that fair?

3 A. That's correct, yes.

4 Q. So is it fair to say that the
5 protocol doesn't necessarily define the
6 information that's transmitted? It defines
7 how the information is transmitted?

8 A. That is correct, yes.

9 Q. So if a user, for example, on a
10 computer -- let's say, I was trying to log
11 in to my bank account over the Internet?

12 A. Right.

13 Q. And I enter my user name and
14 password. Is the user name and password a
15 communication protocol?

16 A. No.

17 Q. It's transmitted using a
18 communication protocol, is that right?

19 A. That's correct.

20 In that case, the user name and
21 the password are just data that you are
22 transmitting, but the communication
23 protocol is what actually moves the data
24 from one point to another.

25 MR. JACKSON: I think those are

1 R. Hurlbut
2 all the questions I have, Mr. Hurlbut.
3 Thank you.

4 THE WITNESS: Okay. Thank you.

5 MR. JACKSON: Pass the witness.

6

7 EXAMINATION

8 BY MR. MIDDLETON:

9

10 Q. Mr. Hurlbut, you spoke with
11 Counsel earlier about Threat Modeling
12 Connect; is that right?

13 A. That's correct, yes.

14 Q. Just a couple questions on
15 that.

16 Is Threat Modeling Connect a for
17 profit or nonprofit organization?

18 A. As far as I know, it's just a
19 nonprofit organization.

20 Q. Are you paid for your work at
21 Threat Modeling Connect?

22 A. I am not.

23 Q. Can you take a look at Jones?

24 A. Sure.

25 Q. That is Exhibit 1004.

1 R. Hurlbut

2 A. (Nodding affirmatively).

3 Q. Do you remember discussing with
4 Counsel, Figure 1?

5 A. Yes, I do.

6 Q. And Counsel asked you for a high
7 level description of what Figure 1 is
8 doing.

9 Is that correct?

10 A. That's correct.

11 Q. Can we go to Column 3, line 13
12 through 16.

13 A. Sure.

14 Okay. Column 3. I am sorry.
15 Which lines again?

16 Q. Line 13 through 16.

17 A. Sure.

18 Q. So this says, "Figure 1 is an
19 illustration of a system for modeling and
20 analysis of cybersecurity threats in a
21 complex-system platform, in accordance with
22 example implementations of the present
23 disclosure."

24 A. Yes.

25 Q. Can we also go to Column 4,

1 R. Hurlbut

2 line 6.

3 A. Yes.

4 Q. And this says essentially the
5 same thing -- right? -- referring now to
6 Figure 1, "A modeling and analysis system
7 of cybersecurity threats."

8 Is that right?

9 A. That's correct.

10 Q. Does this refresh your memory on
11 a high level description of what Figure 1
12 is directed to?

13 MR. JACKSON: Object to the
14 form.

15 A. Yes.

16 BY MR. MIDDLETON:

17 Q. And, in your opinion, what is
18 Figure 1 directed to at a high level?

19 A. It's a way or showing how the
20 system can help model and analyze the
21 system. So for a threat model analysis,
22 determining security -- cybersecurity
23 threats.

24 Q. And still referring to
25 Figure 1, you spoke with Counsel about DFD

1 R. Hurlbut

2 creator.

3 Is that right?

4 A. That's correct, yes.

5 Q. Can we go to Column 6.

6 A. Okay.

7 Q. At about line 18. This sentence
8 starts, "The decomposer may then provide
9 feedback of its decomposition to the DFD
10 creator 106" --

11 A. Yes.

12 Q. -- "which may modify the
13 threat-model DFD, the decomposed
14 components to include their nested
15 components and data flows (and appropriate
16 metadata) thereby producing a level n+1
17 threat-model DFD."

18 A. Yes.

19 Q. What is your understanding of
20 that passage?

21 A. My understanding is that the DFD
22 creator can take a look at the top level
23 and be able to decompose, and so now you
24 have not just the original threat model,
25 which, in DFD, that contained the high

1 R. Hurlbut

2 level, but also additional subcomponents
3 that then turned this into a level n+1
4 threat-model DFD, essentially a new threat
5 model.

6 Q. And the very next sentence, to
7 start off -- you also spoke with Counsel
8 about the threat indicator 108.

9 Is that correct?

10 A. That's correct.

11 Q. The next sentence says, "Again,
12 the threat indicator 108 may be applied to
13 identify any cybersecurity threats to
14 elements (nested components and data flows)
15 of the decomposed components, and add
16 appropriate secondary nodes (and
17 appropriate metadata) representing those
18 threats."

19 A. Yes.

20 Q. What is your understanding of
21 that passage?

22 A. My understanding is that as it
23 decomposes those components into additional
24 subcomponents, there are also threats that
25 are determined and analyzed to be present

1 R. Hurlbut

2 as well with those subcomponents, and now
3 they become part of the threat-model DFD as
4 well.

5 Q. And then the next sentence says,
6 "Or instead of modifying the existing
7 threat-model DFD, in some examples, the DFD
8 creator and threat indicator may begin
9 again to compose a new DFD and threat-model
10 DFD for this level of hierarchy."

11 A. (Nodding affirmatively).

12 Q. What is your understanding of
13 this sentence?

14 A. My understanding is that you have
15 some options here that may incorporate them
16 into the original threat-model DFD to
17 create a larger new threat model or a
18 completely new threat model out of those
19 subcomponents into the components and the
20 related threats.

21 So you now have a second threat
22 model.

23 MR. MIDDLETON: I have no further
24 questions.

25 MR. JACKSON: Okay.

1 R. Hurlbut

2

3 FURTHER EXAMINATION

4 BY MR. JACKSON:

5

6 Q. Mr. Hurlbut, first of all, over
7 the break that we took, did you communicate
8 with anybody over the break?

9 A. No, I did not.

10 Q. Thank you. And then in response
11 to Counsel's redirect questioning that you
12 just went through as it relates to this
13 Column 6 of Jones, did any of the answers
14 that you gave change any of your earlier
15 testimony as it relates to this same
16 column?

17 A. I don't think so.

18 Q. Okay. And the Threat Modeling
19 Connect community, is that -- isn't that a
20 community that's paid for by IriusRisk?

21 A. Yes. It is supported by
22 IriusRisk.

23 Q. Are there any other financial
24 supporters of that community?

25 A. Not that I'm aware. I am not at

1 R. Hurlbut

2 a level to know all the behind the scenes,
3 but, as far as I know, IriusRisk is the
4 sole supporter of Threat Modeling Connect.

5 Q. And then going back here to
6 Jones, as it relates to these nested
7 components, is it still your testimony that
8 when it talks about nested components,
9 these are components that are essentially
10 subcomponents of higher level components of
11 the threat model?

12 A. Initially, yes. But as we also
13 talked about, it could create a second
14 threat model as well.

15 Q. Would it be fair to describe that
16 decomposition process as sort of getting
17 like an exploded view of the higher level
18 component?

19 MR. MIDDLETON: Objection to
20 form.

21 BY MR. JACKSON:

22 Q. Are you familiar with that
23 phrase?

24 A. Yes. It makes sense. It makes
25 sense.

1 R. Hurlbut

2 Q. So did you agree with my question
3 or statement?

4 A. As described, initially, you're
5 looking at a system, you're decomposing
6 components of an original system that had
7 many nested or subcomponents, so, yes.

8 MR. JACKSON: Those are all the
9 questions I have. Thank you.

10 Anything else, Matt?

11 MR. MIDDLETON: Nothing from me.

12 (Proceedings concluded at 12:32
13 P.M. E.S.T.)

14

15

16

17

18

19

20

21

22

23

24

25

- 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

ACKNOWLEDGMENT OF DEPONENT

[illegible]

I, ROBERT HURLBUT, hereby certify, that I have read the transcript of my testimony taken under oath in my deposition of February 5, 2024; that the transcript is a true, complete and correct record of what was asked, answered and said during this deposition, and that the answers on the record as given by me are true and correct.

ROBERT HURLBUT

SUBSCRIBED AND SWORN BEFORE ME
THIS _____ DAY OF _____ 2024.

Notary Public

My Commission Expires: _____

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21

C E R T I F I C A T E

STATE OF NEW YORK)
) ss.
COUNTY OF NEW YORK)

I, Christina Diaz, a Certified Realtime
Captioner, Certified Realtime and Registered
Merit Reporter and Notary Public within and for
the State of New York, do hereby certify:

That ROBERT HURLBUT, the witness whose
deposition is hereinbefore set forth, was duly
sworn by me and that such deposition is a true
record of the testimony given by such witness on
February 5, 2024.

I further certify that I am not related
to any of the parties to this action by blood or
marriage and that I am in no way interested in
the outcome of this matter.

Dated: February 7, 2024

CHRISTINA DIAZ, CRC, CRR, RMR, CSR-NY/NJ, CLR
NCRA Certified Realtime Captioner
NCRA Certified Realtime Reporter
NCRA Registered Merit Reporter
NYS Certified Shorthand Reporter Lic. #001046-1
NJ Certified Shorthand Reporter Lic. #30XI00244900
West Certified LiveNote Reporter

1

2

E R R A T A S H E E T

3

Case Name: IriusRisk, Inc. v.
 ThreatModeler Software, Inc.

4

Deposition Date: Monday, February 5, 2024

5

Deponent: Robert Hurlbut

6

Page/Line	Now Reads	Should Read	Reason
-----------	-----------	-------------	--------

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

Date

Signature

A				
able 9:11,19 15:2 19:8 22:5 24:8,23 29:13,16 31:18 32:3 33:4 50:19 50:23 52:17 102:10,16,17,21 102:21 103:3,11 103:19 104:4,16 105:15 106:25 112:23 Absolutely 56:7 access 19:12 41:10 41:11,13 104:10 104:11 account 53:17 108:11 accounts 103:7 accurate 16:10,11 17:5 ACKNOWLED... 118:2 action 119:16 actor 89:24 91:3,9 91:10 93:6,10 94:5,6,19,20 95:6 95:10,15,22 96:12 96:22 97:6,15,20 actors 90:3 95:16 95:17 97:18,24 actual 33:21 46:23 61:12 75:19 76:25 106:19,24 107:6 Adam 12:7,14 add 46:6 62:9 113:15 added 51:14 61:13 78:13 adding 80:9 addition 50:20 63:18 80:17 83:3 83:13 additional 67:3 78:24 79:2 80:9 81:22,22,23,25 82:3,6,10,14,16 82:17,23 83:2,7	83:12 84:2,16 95:2 113:2,23 addressed 81:14 adds 49:13 adjective 73:22 74:2,6 Adobe 77:21 advisory 12:21 affect 43:9 affirmatively 53:3 54:21 56:13,19 57:19 58:11 75:5 76:12 79:21 85:11 87:14 93:23 99:18 104:25 110:2 114:11 agencies 13:14 agree 5:20,24 38:2 38:5 58:7 59:8 117:2 agreed 5:7 agreement 5:16 ahead 6:13 26:25 91:19 100:2 allow 45:13,15 allowing 44:15 allows 103:5 alternative 81:6 90:19 94:14 alternatively 60:11 America 11:23 12:13,15 analogous 106:12 analogy 107:18,18 analysis 20:19,21 30:4,15,20,23 34:8,14 38:10,23 60:22 63:13 65:4 80:23 81:6,14 83:16 110:20 111:6,21 analyze 41:23 76:3 111:20 analyzed 44:23 69:16 70:7 71:11 72:2 75:11,20 83:19 113:25	analyzer 33:21 35:4 60:12,16,19 60:21 61:9 62:25 63:12 64:2,17,19 64:20 analyzing 23:10 30:24 37:24 38:16 46:23 64:11 84:6 85:21 and/or 41:12 42:11 annotations 78:19 78:21,24 79:2 answer 4:23 15:15 21:21 31:17 61:25 74:23 answered 49:9 118:13 answers 11:12 115:13 118:14 anybody 115:8 apart 53:7 apologize 7:11 10:8 20:24 30:9 49:9 50:8 59:10,13 62:18 72:4 74:25 80:21 APPEAL 1:2 appear 65:24 appearing 5:6 application 42:11 88:9 91:3,4,10 93:6,7 94:5 95:6 106:2,4 applications 14:3 22:17 41:12 100:25 101:4,11 applied 23:10,15 74:10 75:8,24 113:12 apply 20:20 76:9 applying 74:19 appreciate 56:7 appropriate 40:18 40:23 41:3,7 42:9 42:22 61:22 112:15 113:16,17 approved 15:5	Aquia 8:2,4,10 13:6,7,24 14:6,9 14:15,19 15:20 Aquia's 15:11 architect 14:3 argument 30:23 arrangement 65:14 arrow 98:7,16,22 arrows 34:17,21,23 35:5 99:2 art 20:16 24:2 articles 8:21,24 9:12 asked 9:4 16:12 17:22 63:4 66:9 79:17 110:6 118:13 asking 35:13 44:25 55:25 67:19 90:7 91:18 93:11 94:11 96:25 aspect 76:4 aspects 36:19 assess 40:17 assessment 38:24 asset 24:6,9 25:2 assets 24:9 associate 102:14 associated 7:22 10:7 27:21 40:22 49:13 54:5,18,23 55:4,6 59:15,18 60:24 61:10 63:2 63:19 91:2 93:5 assume 20:2 27:16 56:10 57:16 Assuming 53:21 assurance 36:3,12 36:25 37:15,23 38:4 ATM 53:21 54:19 54:22,24 55:5,9 55:13 57:23 attack 22:4 23:20 24:3,6,23 25:4,5,9 25:10,16,21 26:6 26:9 85:24 88:11	88:13,16,17,19 89:16 97:9 100:13 100:17,21,22,24 101:7,10,19 103:3 104:2 attacker 24:7,23 25:18 96:22 103:14,22 104:4 attackers 24:5 attacking 103:8 attacks 101:7 102:8 103:14 attend 7:17 attendance 7:23 attended 10:25 attention 14:23 attorneys 3:5,14 14:25 15:11 17:16 attributes 65:15,21 availability 36:21 available 31:25 avoid 58:24 aware 115:25 a.m 2:8 72:11
				B
				B 4:11 6:2,2 back 29:12 32:2,10 32:12 35:2 36:14 37:9 39:8 45:18 48:16 51:12,21 63:9 69:2,3 75:3 81:16 83:21 88:8 89:23 90:25 91:6 92:4,14,25 94:21 95:5 97:8 99:8,9 101:12,15 116:5 background 7:7 backward 30:10 backwards 50:9 bank 11:23 12:12 12:15 52:25 53:7 53:11,15,20,22 54:7,17,22 55:3,6 55:10,15 56:10,11 56:15,20 57:16,22 59:2,5,14,19

102:4,7,9 104:8 104:10 108:11 banks 11:24 based 18:4,21 20:15 23:24 29:3 30:19 38:20 42:10 42:23 43:12 46:11 51:16 53:9 60:23 61:3 63:9 68:15 91:7,15 93:3 94:4 95:3,19 98:2 basically 49:11 105:18 begins 72:25 79:25 90:15 believe 12:8 23:15 68:8 Bentue 11:6 better 21:15 beyond 101:4,9 bit 10:5 18:15 73:6 75:3 96:24 block 43:25 blocks 59:25 blood 119:16 board 1:2 12:21 26:17 book 29:11,12 bottom 92:4 box 35:8 37:20 branch 55:3 103:16 103:20 104:8 branch's 103:16,24 104:5 breadth 100:12 break 72:6 115:7,8 breakdown 69:20 70:2 breaking 53:7 briefly 5:11 broken 52:20 70:9 brought 14:23 17:13,24 browser 105:25 building 33:24 buildings 89:21 96:9,19 97:14	business 13:8 14:6 14:10 button 32:13 C C 3:2 4:11 119:2,2 call 34:13 46:15 56:17,21 101:12 101:21 103:15 106:8,17 called 7:25 8:18 23:20 35:9 44:2 48:24 calls 31:12 80:12 88:17 106:17 capabilities 13:10 Capital 11:22 Captioner 2:13 119:7,22 case 1:8 6:19 7:10 41:24,25 47:13 88:17 90:20 91:11 93:25 94:13 96:18 105:24 107:6 108:20 120:3 cases 36:16 107:9 cash 53:25 54:3 57:23 caution 15:9 cell 107:2,7 centers 102:11 CEO 10:14 certain 27:12 31:8 38:9 54:23 107:23 certainly 43:18,22 102:25 Certified 2:13,13 119:6,7,22,23,24 119:24,25 certify 118:8 119:9 119:15 chaining 80:2 chance 16:19 change 13:5 73:23 115:14 characterization 98:21	check 50:18,21 102:13 checking 40:11 chief 11:9 Christina 1:24 2:12 11:5 119:6,22 CIA 36:22 cite 84:25 87:12 99:13,13 cities 89:20 90:17 90:20 91:7,12 92:15,19 93:20 94:22,23 96:9,17 96:18 97:13 98:19 city 90:21,21 91:11 91:17,17 92:16,22 92:25 93:9,11,25 94:7,8,9,10,10,13 95:23,23 96:21,22 claim 20:10,20 26:22 27:13 28:17 28:23 30:5,12,20 30:24 77:14 79:18 79:22,25 80:2,8 80:10,15,18,19,23 80:24,25 81:7,10 81:12,12,13,15,17 82:3,5,11,12,18 82:19,22 83:4,7 83:14,19 84:6 85:13,18,21 86:4 86:6,6,7,11,12 105:4,7 claimed 84:4,19 claims 18:10 23:19 clarification 32:16 41:4 97:19 clarify 31:2 62:4 75:16 classification 42:10 43:2,17 clause 74:8 clean 86:20,24 87:2 clear 6:12 31:14 98:3,5 client 14:11 CLR 1:24 119:22	coding 22:3 cofounder 10:14 11:10 column 19:13 35:19,21,23 37:3 40:14 44:19 46:2 47:5,19 49:7,23 51:2 52:3 56:24 57:8 58:3,10 59:2 60:20 61:14,21 62:6,24 63:10,24 65:3 69:3,9,10 86:12,14 87:12,19 88:8 89:5 90:13 90:25 92:2,5 93:4 94:17 95:5 99:16 99:19,25 100:11 104:22 110:11,14 110:25 112:5 115:13,16 columns 67:3 68:2 68:4 combine 29:13 combining 28:6 47:2 come 37:11 48:16 69:2 102:12 coming 85:16 comments 8:24 commercial 13:15 Commission 118:23 communicate 9:19 105:16 106:6,25 107:10,14 115:7 communicating 66:7 105:23 107:3 107:15 communication 105:8,8,12,13,21 105:22 106:5,12 107:5,8,25 108:15 108:18,22 community 8:18,22 9:6,8,23 10:3 115:19,20,24 company 7:25 8:8	8:14 13:7 compensating 83:8 83:12,13 compensation 8:13 16:5,9 complete 118:12 completely 5:13 114:18 complex-system 36:5,15 110:21 compliance 36:16 component 27:21 52:20,24 54:9 55:3 56:11 57:17 71:21 116:18 components 22:12 22:13,18,24 23:6 29:14 33:22 46:12 46:14 52:6,8,13 52:14,18,18,21 53:8,13 54:14 57:25 59:16 61:4 61:19,20,22 65:16 65:22 69:21 70:3 70:10,14,17,21 71:14,17 74:17 76:7,14 81:23 82:7,10,12,18,19 97:5,10 112:14,15 113:14,15,23 114:19 116:7,8,9 116:10 117:6 compose 44:11 114:9 composition 74:17 comprised 70:13 comprising 80:3 compromise 102:17,18,21 computer 105:25 108:10 concept 29:15,18 concluded 117:12 conclusion 31:12 80:13 conducted 1:16 2:12
--	--	---	---	--

conference 7:15,18 7:23 conferences 10:24 11:2 confidential 43:2 confidentiality 36:21 configured 36:2,4 40:16 44:8,9 46:4 52:5 60:21 64:3 65:3 confirm 66:15 conflict 15:6,17 confused 75:3 96:24 confusing 29:20 confusion 58:25 connect 8:19 9:5,7 90:21 104:16 109:12,16,21 115:19 116:4 connected 74:18 92:16 95:22 connecting 88:10 88:14 91:5,14 106:3 connection 10:2 15:25 89:19 90:15 93:15,18 94:2 95:8 97:12 103:15 103:16,20,23 105:20 connects 88:5,22 89:16 92:25 94:5 94:6,7 106:23 consequences 102:23 considered 28:10 consistently 84:16 consultant 12:15 contain 17:5 21:12 contained 112:25 context 21:22 22:11 23:23 25:10 42:5 53:11 72:20 74:13 77:12 96:8 98:14,15	continual 67:10 continuation 67:9 continues 40:4 67:16 contract 12:13 contribute 8:21 18:21 contributed 8:23 8:25 control 19:13,16 controls 83:8,12,13 conversations 9:11 cooperations 11:24 copied 30:2 copy 19:3 31:24 33:5 78:14,15,25 86:20,24 87:3 105:3 corner 32:12 correct 6:17,18,22 7:13,20,23,24 8:3 8:11 10:10,16,17 10:24 11:11 12:6 12:8 14:8 16:4,16 16:17 20:4,5,12 22:25 23:13,17,21 23:22 24:13 25:24 27:13 28:21,25 29:2 30:6,8,16 34:12,16 41:20 44:24 47:10 49:3 50:6,7 51:16 53:4 54:24,25 55:17 58:22,23 60:14 63:3 64:23 65:9 68:20 69:17 70:23 71:8,12,24 72:3 75:12,18,21 76:19 81:3 82:4,21,24 83:5,15 85:3,7,17 86:15,16 96:15,17 96:19 101:24 108:3,8,19 109:13 110:9,10 111:9 112:4 113:9,10 118:12,15 correctly 8:2,24	94:11 96:14 correspond 63:5 counsel 5:15 15:24 109:11 110:4,6 111:25 113:7 Counsel's 115:11 COUNTY 118:6 119:5 couple 8:25 30:10 59:25 109:14 course 33:11 35:3 50:15 53:18 covered 10:8 CRC 1:24 119:22 create 44:15,16 45:16 114:17 116:13 creates 44:22 creating 84:3,18 creator 33:19 34:25 44:2,5,9,21 45:11,19 48:21,23 52:11 60:8 112:2 112:10,22 114:8 criteria 40:17,21 40:24 critical 43:22,23 48:12 criticality 34:24 35:7,9,14,25 36:8 39:11,22 48:2 58:4 CRR 1:24 119:22 CSR-NY/NJ 1:24 119:22 curious 89:10 current 14:18 15:23 16:7,16 19:22 26:17 61:6 63:17 64:3,6,8 currently 13:25 14:10 customers 13:11 103:6 cut 20:25 103:19 cybersecurity 13:12,18,20 46:4	51:9,14 60:22 62:11 64:4 65:17 65:23 110:20 111:7,22 113:13 D D 4:2,11 data 21:13 25:20 33:17,18 39:11,14 40:19 42:2,10,25 43:5,13,16,19 44:16,22 45:8 46:12,13 47:3 48:2,5 50:6 51:13 52:8,14,19,22,22 60:5 61:18 65:6 65:16,18,20,22 66:2 89:19 90:16 93:19 97:12 98:24 98:25 102:23 103:11 108:21,23 112:15 113:14 Date 120:4,25 dated 2:11 119:19 DAY 118:20 de 3:8 10:11,18 17:22 dealing 43:21 December 6:20 7:2 7:9 decision 26:17,19 declaration 16:6,16 16:20,24 17:4 18:25 19:22 20:2 20:4 22:21 24:12 26:21,24 28:2 30:3,11 32:18 72:14 77:13 79:9 79:20 80:7 84:11 85:10 86:2 97:8 99:14 decompose 52:6 55:21 112:23 decomposed 52:13 54:13 61:20,22 112:13 113:15 decomposer 33:20	35:2 51:23 52:2,5 52:9,17 53:6 57:21 59:4 60:4 112:8 decomposes 113:23 decomposing 33:20 117:5 decomposition 52:10 54:4,12 57:5 74:20 112:9 116:16 deep 74:16 define 108:5 defined 37:9,10 76:16 105:15 defines 48:4 101:3 108:6 definition 21:3 22:24 23:5,9,14 24:3,11 25:14 43:12 95:19,25 definitions 98:2 degree 55:14 57:4 depend 36:12 dependencies 103:4 dependent 75:7 86:6 depending 71:2 94:24 depends 9:15 depicted 98:7,16 Deponent 118:2 120:5 deposed 6:15,19 7:2 deposition 1:14 2:10 5:5 10:9 16:18,21 118:10 118:14 119:11,12 120:4 describable 69:19 describe 12:25 33:14 57:24 96:11 102:2 106:11 116:15 described 29:4,6
---	--	--	--	---

31:10 56:5 66:13 95:20 104:21 117:4 describes 22:14 34:7 41:21 47:16 58:3 98:9 100:12 describing 25:4 29:22 50:3 96:14 96:17 100:18 107:12 description 17:5 21:16 51:6,17 55:20 63:12 65:25 110:7 111:11 desired 36:2,12,24 38:3 detail 34:6 details 17:12 35:13 39:21 determine 22:7 41:16,22 64:13 determined 25:15 47:22 76:2 113:25 determines 49:12 determining 33:17 36:20 61:3 63:16 64:11 74:16 97:23 111:22 development 12:4 device 102:19,24 devices 102:12 DFD 33:18 34:25 39:12,24 40:8,15 40:25 41:5 42:20 44:2,4,8,11,21 45:11,19 46:8,9 46:16,17,25 47:7 47:21 48:21,23 49:13,14 50:5 52:7,11,12,16 56:12 58:13,18 60:8,23 65:11 75:17,17 111:25 112:9,13,17,21,25 113:4 114:3,7,9 114:10,16 DFDs 84:4,18	diagram 21:13,13 21:14 22:19 33:17 39:9,12,14 40:20 42:2,3 43:14 44:16,22 45:8 46:12,13 47:3 49:21 50:2,3,6,25 51:13 56:12 61:19 65:19 66:2,3 91:21 97:10 Diaz 1:24 2:12 119:6,22 difference 42:18 106:16 differences 50:14 74:2 different 6:16 13:22 23:2 24:22 24:22,24,24 36:13 37:6 56:9 57:6 67:5,7 70:3,10 107:10,13 direct 8:7 13:4 22:20 35:18 85:9 87:11 directed 111:12,18 directions 4:23 60:5 directly 8:5 11:22 12:18 14:12 17:22 26:22 35:16 100:24 101:3,11 disclosed 31:7 discloses 84:14 disclosing 85:18 86:11 disclosure 110:23 discuss 9:18 discussing 110:3 discussion 19:6,19 48:18 56:18 69:4 96:8 99:6 discussions 9:2,13 display 88:15 displayable 88:9 91:4,13 93:7 95:8 95:13 96:2	distinguishing 48:10 DLA 3:4 document 19:9,13 27:5 39:7 46:19 50:17 55:20 62:17 63:22 65:13 73:13 77:20 81:20 83:23 87:23 89:9 92:8 92:11,13 94:16 100:8 documents 29:8 doing 15:25 17:25 28:22,25 33:23 53:6 61:2 77:24 110:8 Don 5:18 99:4 DONALD 3:20 donald.jackson... 3:19 door 68:7 download 32:5,14 downloaded 19:14 downloading 77:20 drawers 53:25 54:3 57:23 drive 3:15 107:21 drop 42:17 Due 5:10 duly 119:11	either 24:16 electronic 24:17,21 electronically 19:4 element 27:7 29:24 30:5,11,15,20,24 31:9 46:5 47:3 64:5 84:4 86:11 elements 44:10,12 46:6 73:17 74:3 76:16 84:19 85:18 113:14 embedded 85:6 employee 8:13 employer 7:21,25 enclave 41:10 encrypted 105:19 ensure 5:12 enter 108:13 environments 41:10 errors 16:23 22:3 especially 95:4 ESQ 3:11,20 essentially 9:18 24:21 28:3,8,11 44:14 80:14,18 88:13,18 91:15 101:2 111:4 113:4 116:9 establishment 35:9 35:14,25 36:9 39:11,12,15,22,24 40:8,16 41:2,6 42:21 47:21 event 25:25 26:7,10 evidence 29:8 evidentiary 86:10 exactly 13:20 35:17 37:21 EXAMINATION 4:5 6:7 109:7 115:3 examined 6:4 example 36:20 40:25 41:5 45:11 47:6 50:12,20,25 52:23 53:2,12	54:20 57:22 58:10 65:8 67:9 82:5 90:15 93:14 98:19 101:25 102:6,10 103:8,13,25 104:8 104:15,20 105:16 105:24 108:9 110:22 examples 52:4 63:25 66:14 90:12 114:7 exercise 66:8 Exhibit 4:12 32:18 32:20,23,25 72:15 77:5,9 78:9,12,17 78:23 87:6,8 109:25 existing 114:6 expedite 102:13 expenses 7:21 experience 17:6 experiences 18:22 expert 14:17 32:7 expertise 18:4 Expires 118:23 explain 106:9 explained 62:24 explanation 33:14 exploded 116:17 exploit 22:5 exploiting 22:2 extending 29:15,16 extension 81:21 extent 31:12 80:12 extract 25:20 65:7 E.S.T 2:8 117:13
---	--	--	---	---

108:2,4 116:15 fairness 62:5 familiar 18:18 41:25 102:7 116:22 far 102:22 109:18 116:3 fashion 38:17 featured 98:20 February 1:15 2:7 118:11 119:14,19 120:4 federal 13:14 feedback 52:10 60:8 112:9 feel 34:4 36:6 72:19 79:4 89:11 figure 19:2 33:8,15 34:8 38:7,15 43:25 45:3,5,19 48:18 50:10,12 51:6,12,21 60:2 62:22 64:20 68:19 69:16 72:24 85:5 91:23,25 92:4,6,9 102:19,21 110:4,7 110:18 111:6,11 111:18,25 figures 66:10 85:2 file 45:2 filed 6:16 finally 106:23 financial 102:11 115:23 find 105:2 fine 32:9 finish 69:24 finished 73:11 74:22 87:17 100:6 firewall 103:24 104:6 first 27:19 28:4,9 28:15,19,24 35:8 37:7,19 60:7 72:24 84:23 87:12 95:9 105:2 107:6 115:6	five 59:3,15,18,22 72:7 flow 21:13 33:17,18 34:24 35:3,6 39:12,14,23 40:19 42:2 43:14 44:16 44:22 45:8,20 46:12,13 47:3 48:22 50:6 51:13 51:22 61:18 65:19 89:19 90:16 93:19 97:12 98:24 flows 39:2 52:8,14 52:19,22,22 64:20 65:16,22 98:25 112:15 113:14 focused 13:16 focuses 13:13 focusing 93:15 folks 9:8 10:6 follow 28:23 following 5:2 41:9 42:12 81:5 follows 6:5 foresee 15:17 forgoing 42:20 forgot 59:9 form 18:13 26:4,8 38:18 49:16,22 55:18 80:11 111:14 116:20 forth 22:4,17 25:20 36:17 43:3,24 48:3 50:21 57:6 58:5 67:11 74:20 98:20 103:12 105:19 119:11 foundation 16:13 founders 8:6 14:24 17:9,24 Frank 29:11 Fraser 11:16 free 36:6 72:19 79:4 89:12 French 107:12 front 19:22 full 19:12 72:24	full-time 12:16 functions 10:22 38:10 84:3,17 further 71:5,23 80:2 89:18,22 114:23 115:3 119:15 G gather 9:8 gears 10:5 13:5 general 18:9,19 33:14 35:12 38:6 38:13,13 41:24 45:24 generally 36:2 generate 45:12,14 47:16 65:3 76:10 generated 43:11 generates 51:19 German 107:13 getting 116:16 give 31:3 65:20 106:25 given 54:10 118:15 119:13 gives 90:19 go 7:7 23:4 26:25 30:10 32:9 33:12 34:18 36:14,14,22 37:9 50:9 51:2 56:20 59:24 69:15 70:24 71:3,20 72:9 81:16 83:21 84:13 88:7 89:23 90:24 91:6,19 92:4 99:5,8,9 100:2 105:17 107:15 110:11,25 112:5 goes 69:5 94:21 106:21,22 going 7:8 20:24 30:9 34:3 42:3,15 48:16 55:8 61:8 69:3 72:5,15 79:15 84:23 91:20	94:4 95:4 97:8 106:19 116:5 Good 6:10,11 gotten 9:25 government 13:14 great 27:11 33:7 37:17 61:15 Greensboro 3:15 ground 59:12 group 27:21 76:6 guess 9:4 24:16 26:2 38:6 45:10 57:20 68:22 71:2 79:17 92:9 99:8 107:10,21 H H 4:11 6:2 120:2 handset 106:20 happen 11:3 25:23 104:18 happened 25:23 happening 102:20 hard 67:21 harm 25:19 heading 27:7 79:23 heard 5:13 help 14:12 18:21 91:21 105:15 111:20 helps 21:14 44:16 91:24 106:6 hereinbefore 119:11 hesitate 7:6 hierarchal 69:19 hierarchical 70:2 hierarchies 68:24 hierarchy 56:24 57:2,9,12 69:6,21 70:9 114:10 high 33:13,16 38:9 40:9 41:11 44:5 49:4 51:25 60:18 64:24 110:6 111:11,18 112:25 higher 41:9 42:25	43:5,16 52:19 54:10 55:3 70:25 116:10,17 highly 42:14 43:16 hired 12:14 Hold 15:7 holds 82:25 honest 32:8 honestly 68:9 hopefully 106:15 hosts 22:16 hour 15:21 72:5 http 105:17,20 https 105:17,21 Hurlbut 1:14 2:10 4:4 5:1 6:1,10 7:1 7:13 8:1 9:1 10:1 11:1 12:1 13:1 14:1 15:1 16:1 17:1 18:1 19:1,8 19:21 20:1 21:1 22:1 23:1 24:1 25:1 26:1 27:1 28:1 29:1 30:1 31:1 32:1 33:1,4 34:1 35:1 36:1 37:1 38:1 39:1 40:1 41:1 42:1 43:1 44:1 45:1 46:1 47:1 48:1 49:1 50:1 51:1 52:1 53:1 54:1 55:1 56:1 57:1 58:1 59:1 60:1 61:1 62:1 63:1 64:1 65:1 66:1 67:1 68:1 69:1 70:1 71:1 72:1,13 73:1 74:1 75:1 76:1 77:1 78:1,8 79:1 80:1 81:1 82:1 83:1 84:1 85:1 86:1 87:1 88:1 89:1 90:1 91:1 92:1 93:1 94:1 95:1 96:1 97:1 98:1 99:1,11
--	---	--	--	---

100:1 101:1 102:1 103:1 104:1 105:1 106:1 107:1 108:1 109:1,2,10 110:1 111:1 112:1 113:1 114:1 115:1,6 116:1 117:1 118:8 118:18 119:10 120:5 Hurlbut's 32:17 hybrid 41:10	104:13 implying 57:11 important 103:4 include 52:13 64:2 78:15 112:14 includes 31:9 including 27:20 28:6,19 84:4,18 88:2 incorporate 114:15 indicate 35:6 57:3 indicates 43:14 46:2 61:6 65:2 100:25 indicator 33:19 34:25 45:21,25 46:3 48:25 49:5,6 49:12,14 50:13 51:19,22 61:13 68:23 113:8,12 114:8 information 4:19 4:20 17:14 36:3 37:25 38:4,11,17 40:17,20,22 42:15 43:3,5 44:10,11 44:23 46:6,9 47:17 48:11,12,23 52:7,25 62:9 65:6 66:4,5 69:14,18 70:7,8,17 71:10 72:2 73:17 75:10 75:13,15,16 76:13 76:15 78:16,25 79:3 103:12 108:6 108:7 inherency 30:23,25 31:5 initial 36:11,19 initially 116:12 117:4 initials 50:5 inputs 80:17 81:22 INSERTED 4:20 instance 58:16 instances 41:7 42:9 42:19	institution 26:16 26:19 integrity 36:21 intended 34:21,23 intention 27:15 interactions 12:25 13:4 interest 8:4 15:18 18:6 interested 9:9 17:25 18:2,5,12 18:14,20 119:17 interesting 58:2 interfaces 80:16 internal 53:8,12 internet 41:11 103:15,23 108:11 interpreting 38:16 interrelated 76:6 76:15,17 involvement 12:24 iPad 102:14 iPads 102:11 IPR 6:15,24,24,25 14:18,18 15:23 16:2,7,16 19:22 23:15 26:17 30:5 32:19,22 77:2,10 87:6 IPRs 17:10 18:3,9 IPR2023-00821 1:8 IriusRisk 1:4 5:23 6:16 10:7,11,14 11:10 12:5,21,24 13:3,4 15:24 17:9 115:20,22 116:3 120:3 issue 77:2 issues 18:16 item 103:8	38:22 49:18 50:4 55:24 72:4,9,12 76:24 77:7,18 78:10,11 79:14 80:20 86:17,19 87:5,10 99:7 108:25 109:5 111:13 114:25 115:4 116:21 117:8 January 2:11 Job 1:25 join 9:16 14:15 joined 14:16 Jones 30:7,21 31:17,22 32:20 34:7 35:19 36:24 37:12,25 45:5 47:15 66:11 71:13 71:19 74:9,19 75:8,11,24 76:8 76:11 84:14,16 85:2 109:23 115:13 116:6 jump 44:25	labeled 35:8 laid 16:6 68:13 landline 106:18 language 28:17,23 30:12 80:4 106:13 languages 107:11 larger 55:23 75:6 77:11 114:17 layperson 106:10 106:11 lead 9:2 14:4 leading 64:12 leads 9:17 learn 9:20 learning 18:20 left 12:13,16 35:8 legal 31:12 80:13 let's 52:24 54:19 55:9 56:9 59:24 60:15 65:12 72:9 90:24 94:21 99:9 102:9 103:14,24 108:10 level 33:13,16 36:3 36:12,24 38:3,6,9 38:14 39:12,14,24 40:8,9,15,18,24 40:25,25 41:2,5,6 41:9,18,20,21,23 42:2,3,4,6,8,18,20 42:21,24 43:6,7 43:10,13,14,19,23 44:5,13 45:24 47:7,12,13,21,22 47:23,25 48:3,6,6 48:7,10,11,14 49:4 51:25 52:15 52:20 54:7,9,10 54:11 55:3 56:17 56:22 57:9,14,15 57:18,25 58:3,5 58:12,18 59:3,6 59:15,17,18,20,21 59:22 60:18 64:24 70:15,16,24,25 71:3 110:7 111:11 111:18 112:16,22
I icon 32:14,15 icons 32:13 idea 90:10 identifiable 42:15 43:3 identification 32:24 33:2 77:6 87:9 identified 40:24 44:13 77:9 identify 25:13 40:18 41:2,6 42:21 43:13 44:8 44:9 46:4 61:6 64:3,7 113:13 identifying 73:16 73:21 illustration 110:19 imagine 32:3 immediate 100:20 immediately 101:20 impact 43:24 68:3 100:12,24 101:9 101:11 impacts 101:22 103:10 implementable 64:8 implementation 36:4 implementations 110:22 implicitly 101:14		J Jackson 3:20 4:6 5:18,18 6:8 15:19 18:23 19:7,20 26:5,11 31:13 32:11,17 33:3	K keep 67:21 kind 30:19 85:15 102:11 kinds 21:16 104:17 know 10:8,10 11:5 11:7,13,17,18 12:8 18:4 27:4 33:10 37:14,21 39:20 40:12 43:17 43:20 44:25 55:8 55:11 68:10 69:7 73:10 77:18 85:12 87:17 97:7 100:5 107:17 109:18 116:2,3 knowing 74:3 knowledge 20:15 known 29:22 43:7	
			L L 6:2	

113:2,3 114:10 116:2,10,17 levels 40:23 47:18 48:17 56:9 57:3,7 57:12 68:24 69:6 70:3,11,14 74:20 Lic 119:24,24 light 37:12 line 35:19,22,23 37:3 40:14 42:7 42:19 44:7,19 46:3 47:5,20 49:24 51:3 52:3 56:25 57:8 58:10 58:17 60:20 61:14 62:6,24 63:24 65:2 69:5,5,12 71:16 87:21,21 88:8 90:14,25 92:2 93:4 94:17 95:5,11 99:16,20 100:11,23 106:19 106:24 107:2,7,25 110:11,16 111:2 112:7 lines 86:12,14 87:12 89:4,14 90:5 110:15 listing 66:3,4,5 little 10:5 18:15 56:8 73:6 75:2,2,3 89:21 96:24 106:15 LiveNote 119:25 LLP 3:4 local 105:25 lockdown 104:15 log 9:11 108:10 logic 82:25 longer 104:11 look 22:7 33:7 39:8 45:3 50:10,14 51:12 54:17 56:21 57:21 59:4,11,14 62:6 66:10 67:12 68:2,4 71:2 72:14 72:19 77:11 81:16	81:17 89:23 91:21 91:22 92:7 94:2 106:21 109:23 112:22 looked 17:3 81:3,7 81:11 looking 39:9 41:17 46:21 50:11 55:2 55:10 56:10,14 57:23 59:20 63:9 63:11 67:20 75:14 84:9 97:11 98:18 117:5 looks 19:17,18 33:22 36:10 62:7 64:10 67:6 68:14 68:17 83:20 89:5 90:5 lose 99:4 lost 36:13 77:16 lot 14:9 48:12 79:16 80:3 lower 64:9 70:25 M making 25:21 67:23 malls 80:25 manually 45:16 many-to-many 90:2 94:24 97:17 97:22 many-to-one 90:2 94:23 97:16,22 mapping 89:24 90:3 94:23,24 97:14,17,22 Market 3:6 marriage 119:17 matching 40:24 44:13 94:18 Matt 32:4 117:10 matter 18:9 35:12 38:13 119:18 Matthew 3:11 5:22 matthew.middlet... 3:10	McLean 3:17 mean 25:11 31:5 42:6 45:15 56:23 74:14 92:16 107:25 means 36:23 37:22 49:25 meant 20:8,12 27:25 73:6 measure 61:6 64:3 64:9 member 8:18 membership 10:2 memory 35:20 111:10 mention 48:19 56:24 63:23 mentioned 21:21 24:4 32:4 35:7 46:21 48:18 63:15 68:25 81:25 mentions 36:18 46:25 49:7 61:21 Merit 2:14 119:8 119:23 met 10:21 11:4,7,8 42:20 metadata 60:23 61:9 62:25 63:19 65:7,9,19 112:16 113:17 method 25:3 80:2,9 methodology 88:11 88:18 methods 24:22 Middleton 3:11 4:7 5:22,23 15:7,14 18:13 19:11 26:4 26:8 31:11 38:18 49:16,22 55:18 77:23 78:7 79:11 80:11 99:4 109:8 111:16 114:23 116:19 117:11 minutes 72:7 misconstruing 96:6 mitigation 63:17	64:7 mitigations 21:12 21:18 61:7 64:14 102:25 model 21:5,8,8,16 22:12,13,18,19,24 23:6 27:19,20 28:4,5,7,9,10,11 28:13,14,15,19,20 28:25 29:15,17,18 33:25 34:2 40:19 41:3,7,8 42:8,22 43:10,11,20 44:13 46:18,24 47:12 49:15 55:23 56:12 57:17 66:6,8 76:7 76:10,14 80:2 82:6,10,12,17,19 111:20,21 112:24 113:5 114:17,18 114:22 116:11,14 modeled 52:7 54:6 modeling 8:19 9:5 9:7,9,21 10:23 11:25 13:8,21 14:4,5,10,13 18:5 18:7,19 34:8,14 109:11,16,21 110:19 111:6 115:18 116:4 models 29:17 47:17 modify 52:11,12 112:12 modifying 28:8,22 114:6 moment 14:11 39:10 42:16 81:17 90:25 Monday 1:15 120:4 month 9:14 morning 6:10,11 move 48:24 85:25 moves 108:23 moving 57:4 102:24 multiple 32:6 34:12 47:25 70:13,14	71:14,17 87:25 91:11 97:10 103:10 N N 3:2 4:2,11 58:18 58:21 name 108:13,14,20 120:3 nature 5:10 48:5 94:25 navigate 77:21 NCRA 119:22,23 119:23 necessarily 34:5 47:24 88:7 108:5 need 30:3 32:2,9 36:7 72:20 99:8 needs 48:13 91:9 nested 52:8,14,18 52:21 71:14,17 112:14 113:14 116:6,8 117:7 network 41:9 never 11:21 12:2 new 2:16 23:18 28:9,11 29:18 113:4 114:9,17,18 118:4,6 119:3,5,9 next-box 45:20 nine 67:10 NJ 119:24 Nodding 53:3 54:21 56:13,19 57:19 58:11 75:5 76:12 79:21 85:11 87:14 93:23 99:18 104:25 110:2 114:11 node 46:7 49:25 60:25 61:10,11,17 62:10,12 63:5 nodes 49:25 60:24 61:5,18,23 113:16 nonprofit 109:17 109:19 North 3:6
--	--	--	--	--

Notary 2:15 118:22 119:8 note 63:2 notice 2:11 November 14:16 number 32:13 34:17 36:13 58:22 numbers 23:2 67:8 67:10 NYS 119:24 n+1 52:15 58:12 112:16 113:3	84:25 86:3,5 87:22,24 89:3 90:10,18 91:19 92:12 93:13,17 96:3,20 98:23 99:22,24 100:7,9 101:14 103:13 107:17 109:4 110:14 112:6 114:25 115:18 old 102:4 omissions 16:24 once 9:14 ones 32:6 one-to-many 90:2 94:20 95:15 97:16 97:21 one-to-one 89:24 89:25 94:18 95:14 97:14 online 9:22,24 51:8 94:4 open 32:6 33:6 79:7 87:4 opening 53:17 openly 25:7 operating 11:9 operations 33:18 53:19 opining 18:10 opinion 111:17 opportunities 9:2 opportunity 9:10 11:25 opposed 96:21 options 8:6,9,16 114:15 organization 12:18 109:17,19 organizations 13:15 organized 65:14,20 66:3 original 29:14 52:24 102:6 112:24 114:16 117:6	originally 28:14 outcome 119:18 output 38:25 50:13 60:11 64:19 65:11 outputs 60:5 outside 8:7 56:15 103:17,21 overall 13:12 36:8 41:15 45:20 48:22 54:7 55:2,15 56:11 71:10 74:13 101:22 oversee 14:7 owned 6:17 8:5 Owner 1:7 3:14 5:19 ownership 8:8	74:15 95:10,10 101:10 114:3 participate 17:23 particular 13:13 18:8,16 24:9 30:5 30:24 31:20 41:16 42:13 46:5 47:2 47:12,22 50:24 54:8,18 64:5 75:13 88:11,16 100:17 101:10 103:2,16 particularly 55:13 89:13 parties 5:5,12 6:4 119:16 parts 22:15 27:12 33:25 37:11 68:6 80:22,24 81:13 89:11 95:9 pass 97:9 109:5 passage 99:12 100:16 112:20 113:21 password 108:14 108:14,21 patent 1:1,2,7,9 3:14 5:19 17:12 18:10 20:3,7,8 21:4,23 22:10 23:11,19,24 29:4 29:7 31:20 50:9 76:25 77:3,9,10 78:23 79:18 81:18 88:25 104:24 105:5 patents 6:17 path 25:2,4 88:13 88:19 89:19 90:16 93:19 97:12 98:24 99:3 paths 23:20 24:3,7 24:14,17 25:10 85:24 97:9 100:18 101:8 Paul 11:13 pause 5:11	PDF 78:3 79:9,11 pending 62:21 people 9:10,16,20 107:3,12,13 perceive 15:17 perfect 107:18,18 perform 38:9 60:21 performed 83:25 84:15 perimeter-related 41:13 permission 14:19 14:22 15:2 person 23:25 24:2 personal 43:3 personally 42:14 personnel 53:18 Petitioner 1:5 3:5 5:23 phone 106:20 107:2,7 phrase 27:18,25 46:17 73:2,16,18 74:14 75:6 88:21 89:14,15 98:10 116:23 physical 24:16,16 24:20 106:24 107:7 pick 106:18 picked 57:14 PII 43:4 PIPER 3:4 place 9:19 11:3 77:16 103:9 placeholder 58:21 places 37:6 53:16 platform 36:5,16 110:21 please 5:11,15 7:5 7:6 31:2 33:8 37:13 45:3 50:10 51:3 73:9 79:5 87:16 100:3 point 49:20 61:4 68:19 86:10 88:14 88:14 98:8,8,16
---	---	--	---	--

98:17 99:3 105:23 108:24 pointed 89:4,13 points 88:5,23 89:17 105:15 106:7 pole 106:22 portion 100:11 POSITA 73:2 positions 18:12 possible 21:17 24:25 potential 21:9 23:7 24:5 25:25 26:7 potentially 70:13 95:16 101:9 104:6 predefined 75:7,9 75:24 76:8 preparation 16:20 present 61:4 110:22 113:25 president 12:4 presumably 39:2 previously 32:19 32:21 pre-definition 76:4 pre-IPO 8:15 primarily 13:16 principal 14:2 prior 6:24 14:18 23:15 privileged 15:10 Probably 24:20 Proceedings 117:12 process 40:4 116:16 processes 42:12 produce 40:20 46:8 producing 52:15 112:16 product 12:4 PRODUCTION 4:21 professional 17:6 profit 109:17 program 14:14	programs 12:2 project 14:20 projects 14:20 17:20 pronounce 8:2 protected 48:13 protocol 104:12 105:8,9,12,13,21 105:22 106:5,12 107:5,8,20,23 108:5,15,18,23 provide 15:4 36:2 52:10 61:9 94:18 112:8 provided 24:11 78:5 provides 13:10 62:25 public 2:15 8:15,16 13:13,16,18,21 17:13,17 118:22 119:8 pull 78:4 79:4 pulls 78:8 purpose 36:8 38:8 41:15,22 63:13,21 64:10,16 purposes 30:4 56:18 pursuant 2:11 push 19:3 31:23 76:25 86:17,23 put 6:14 10:19 14:13 67:15 102:14 P.C 3:13 P.M 117:13	questions 7:4 9:18 56:2 109:2,14 114:24 117:9 quite 92:7 quote 26:24 quoted 27:12 79:19	120:2 radio 107:4,4,8 ran 14:24 rating 64:6,9,13,15 reaching 102:23 read 5:2 29:21 36:6 73:9 87:15,24 100:2 118:9 120:6 reading 95:4 readjust 50:16 reads 27:19 74:9 120:6 real 75:19,22 reality 25:22 realize 24:8 realized 25:18 realizing 24:25 25:22 really 18:6 25:3 35:2 61:16 65:18 73:20 90:4 95:24 96:10,11 101:5 Realtime 2:13,14 119:6,7,22,23 reason 18:11 120:6 reasonable 59:7 103:25 reasons 15:4 recall 11:12 35:16 80:14 receiver 106:18 receiving 80:16 Recess 72:11 recipient 107:25 recited 80:10 82:11 82:12 83:3,14 recommendations 64:13,14 record 5:16 6:12,14 7:10 19:6,19 44:18 72:10 84:7 86:23 87:5 99:5,6 99:9,9 118:12,15 119:13 recorded 9:3 Redefine 27:19 redefining 28:3,8	28:12,24 58:6 redirect 115:11 reduce 64:8,15 refer 6:23 30:3 46:18 56:9 61:18 62:2 76:5 88:21 89:12 99:16 reference 30:7,21 31:23 32:20 67:8 77:11 85:21 91:25 referenced 32:23 32:25 77:5 87:8 references 40:12 50:19,22 referred 46:15 64:6 69:20 referring 7:5 24:10 25:6 37:2 38:7 44:19 45:18 47:11 57:15 61:12 63:15 63:16 75:10 84:8 91:23 92:3 97:3 101:15 111:5,24 refers 51:8 57:9 58:17 71:13 82:6 82:22 83:7 84:16 87:25 90:4 98:6 105:7 reflected 55:5,13 55:14 59:17 78:16 refresh 87:16 111:10 refreshes 35:20 register 9:10 Registered 2:14 119:7,23 regulatory 36:16 relate 43:10 61:19 related 21:14 52:22 54:8,13 57:7 58:4 102:6 114:20 119:15 relates 12:23 31:19 42:24 77:14 85:13 86:4 115:12,15 116:6 relating 10:22
---	--	--	---	---

46:11,13 relationship 54:16 66:23 101:12 relevant 23:7 relied 30:6 85:17 rely 29:7 30:22 85:20 remember 8:23 110:3 remembering 37:10 remote 5:10 remotely 1:16 2:12 5:6,8 6:3 repeat 20:24 39:17 repeated 30:13 37:6 repeats 7:11 report 65:5 68:5,7 REPORTED 1:23 reporter 2:14 5:3 32:16 33:21 35:5 41:4 64:20,25 65:11 68:18 119:8 119:23,23,24,24 119:25 reporting 5:11 reports 65:4 66:14 66:18,19,24,25 67:5,7,13 68:16 represent 47:25 88:10 95:21 represented 31:19 50:24 99:2 representing 46:7 52:19 61:23 62:10 62:13 88:16 113:17 REQUESTS 4:19 4:21 requirements 36:17 resides 106:4 residual 64:9 103:10 respect 38:10,14 39:2 78:22 80:25	response 115:10 rest 103:5 result 21:25 104:18 resulting 49:19 results 39:23 48:23 49:15 51:22 60:8 60:12 66:8 retreading 59:12 reveal 15:10 revealed 55:22 review 16:19 26:13 26:16 reviewed 16:25 reviewing 27:5 39:7 46:19 50:17 62:17 63:22 65:13 73:13 81:20 83:23 87:23 89:9 92:8 92:11,13 94:16 100:8 right 8:10 10:15,21 11:10 12:5 16:3 19:18 23:12,16 32:15 34:6,9,15 37:4,22 39:16,21 40:6,15 45:22 49:2 51:6,15,23 53:5 56:16 57:9 57:12 58:7,14 60:9,13 61:24 63:2,7 64:22 67:15 68:19 70:18 70:22 71:7,11,15 71:23 72:24 75:17 75:18,25 76:18 81:2,9 82:3,5,7,13 82:16,20,23 83:4 83:14,24 85:23 86:7 87:3 88:2 90:22 92:6,7,10 92:18,23 93:16,21 94:13 98:12,13 100:18,22 101:10 101:17,23 107:22 108:12,18 109:12 111:5,8 112:3 RIMÓN 3:13	risk 36:18 61:7 63:17 64:4,6,8,9 64:13,15 risks 55:4 RMR 1:24 119:22 Robert 1:14 2:10 4:4 15:8 19:12 118:8,18 119:10 120:5 roughly 51:3 61:14 62:6 69:5,12 89:4 round 48:17 83:6 routes 24:4 row 67:16,17 rules 107:23 RULING 4:22	99:12 114:21 116:13 secondary 46:7 49:24 60:25 61:10 61:11,23 62:10,12 63:2,5 100:21 101:22 104:7 113:16 section 46:22 72:18 99:23 100:2 sections 53:14 sector 13:14,17,19 13:21 secure 105:18 security 14:3 21:10 46:7 47:2 62:13 104:12 111:22 see 9:11 15:6 16:23 19:2,8 27:9,10,22 30:21 32:3,12,13 34:19 35:10,18,19 37:7,9 39:5,5 45:7 46:21 47:8 50:22 51:10 53:8 58:19 65:12 67:18,21 69:22 70:4 73:3 73:18 74:11 79:22 80:5 81:18 83:9 91:25 102:3,20 105:10 106:19,21 seeing 38:20 59:21 68:15 Select 38:3 selected 24:6 sense 31:15 48:9 73:23 96:4 97:4,8 116:24,25 sensitive 42:13,14 42:25 43:16,19 sensitivity 43:4 sentence 69:11,25 72:16,22,24 73:7 73:9 74:9,14 75:4 76:6 84:12,20,21 88:20 90:14 93:13 96:10 97:21 112:7 113:6,11 114:5,13	separate 66:25 67:13 82:11,13 separating 97:6 serve 14:17 server 106:2 servers 22:15 set 119:11 share 17:15 shared 17:11,14 shed 37:12 Shorthand 119:24 119:24 Shostack 12:7,8,11 12:14,20 13:2 Shostack's 12:23 shot 31:4 show 34:22,23 76:24 94:3 showing 51:13 99:2 101:7 111:19 shown 34:7 67:4 shows 33:15 shut 104:5 shuts 104:17 side 81:19,19 sideways 33:11 signals 107:24 Signature 120:25 similar 7:8 80:15 81:11 simple 79:16 107:19 simpler 106:16 single 57:17 92:21 sit 32:2 situation 92:21 96:11 102:2 104:21 six 59:6,17 skill 20:16 24:2 skip 26:20 smaller 52:21 Snyder's 29:11,12 software 1:6 5:20 19:15 105:14 120:3 sole 116:4
--	---	---	--	--

somebody 9:17 22:5 25:18 53:17 102:14,15 106:10 106:23 107:2 sorry 23:3 38:12 39:17 44:20 48:19 49:8 55:25 61:25 69:24 74:22 75:2 77:17 81:5 83:17 84:9 87:19 91:19 92:2 110:14 sort 12:17 16:13 34:24 49:21 55:21 68:24 100:19 103:22 116:16 sorter 36:18 sound 51:18 sounds 25:25 49:11 50:2 source 23:7 speak 7:6,18 speaking 5:12 107:12,13 specific 100:16 specifically 20:10 37:2 42:6 72:16 73:15 77:12 90:12 specify 61:16 split 52:18,20 spoke 7:14 109:10 111:25 113:7 spoken 10:25 11:2 ss 118:5 119:4 stand 50:5 standard 105:22 106:5 standby 102:4 start 37:19 38:12 48:20 93:22 113:7 started 59:10 starters 69:15 92:20 starting 40:14 47:20 62:6 65:2 89:6 93:4 98:8,16 starts 69:11 72:18 77:15 112:8	state 2:15 5:15 118:4 119:3,9 statement 5:2 83:24 117:3 STATES 1:1 stay 37:20 Stephen 17:22 steps 80:9 83:25 84:15 stipulated 6:3 stock 8:6,9,16 stop 42:16 90:17 stopped 93:21 stores 42:11 Street 3:6 strictly 9:22 strike 38:11 83:17 studied 20:2,6 subcomponent 53:23 54:19 71:3 subcomponents 54:6,17 56:21 57:22 59:5,6,16 70:21 71:4,6,21 71:22,23 113:2,24 114:2,19 116:10 117:7 subject 20:3 submitted 16:7,15 32:19,21 SUBSCRIBED 118:19 subsystem 34:18 35:15 37:24 38:24 subsystems 34:13 sub-elements 34:4 successfully 33:5 103:19 104:5 suggest 68:9 suggested 61:7 63:17 64:7 suit 17:12 Suite 3:7,16 summary 65:5 support 29:8 85:3 86:9,10 supported 115:21	supporter 116:4 supporters 115:24 supposed 67:3,4 68:12 sure 9:7 19:12,16 21:24 25:8 30:18 32:2,5 33:9,16 37:16 39:19 44:6 45:4 50:11,19 53:24,24 55:8 56:4 62:8 63:16 66:12,16 67:19 73:7,25 76:20 79:9 86:25 87:18 93:17 100:4 102:3 102:5 103:18 104:14,14,19 109:24 110:13,17 Swiderski 29:10,11 switch 10:5 sworn 5:7 6:3 118:19 119:12 system 21:10,11,15 21:18 22:15 31:8 32:8 33:20,23 34:7,8,11,14 35:6 35:25 36:4,9,20 37:25 38:4,7,8,11 38:14,16,17 39:11 39:13,15,23,24 40:9,10,16,18,21 40:22 41:2,6,16 41:23 42:11,21 44:2,10,11,21,23 45:19,20 46:6,10 47:16,17,21 48:6 48:22,24 52:7 62:9 68:19 69:14 69:15,16,18 70:7 70:8,13,17 71:10 72:2 73:17 74:3,9 74:19 75:7,8,9,10 75:13,15,16,19,23 75:24 76:3,11,13 76:16 100:14 101:22 103:6 105:14 110:19	111:6,20,21 117:5 117:6 systems 40:21 41:12,14 52:25 SY8676 1:25 T T 4:11 6:2,2 119:2 119:2 120:2,2 take 14:19 17:20 24:7 25:3 33:7 45:2 52:23 54:19 62:5 66:10,20 72:6,14 73:9 109:23 112:22 taken 118:10 talk 11:25 29:13 37:12 60:15 98:25 talked 6:13 7:9 11:4 17:8 18:24 25:12 31:22 47:20 68:21 116:13 talking 24:18 29:13 29:25 39:14 68:22 68:23 71:19 87:7 107:9 talks 13:5 37:15 39:10 42:13 44:7 49:24 58:12,16 69:6 98:24 116:8 taped 9:13 target 88:8,9 89:25 91:4,10 93:7,12 94:19 95:7,11,17 95:23,24 96:13,23 97:7,15,20 101:16 101:20 103:9,23 targeted 100:25 101:4,11 targets 94:21 95:16 95:18 96:15,18 97:4,25 technical 12:21 Technologies 36:15 telephone 106:17 106:19 tell 17:10,19 21:4	40:10 44:4 53:5 63:13,20 70:6 96:6 tellers 53:15 54:2 57:24 104:9,9 tells 89:15 term 21:20 22:9 23:16,18,19 26:23 terms 12:17 17:21 20:7,11,15,21 21:3 30:25 43:2 43:24 57:4 69:19 74:18 97:4,5,23 102:9 103:2 tertiary 100:21 testified 6:5 testimony 115:15 116:7 118:9 119:13 Thank 76:21 79:6 109:3,4 115:10 117:9 Thanks 37:17 99:10 therebetween 52:9 thereof 60:25 thing 30:2 48:16 67:25 68:25 74:4 74:5 111:5 things 13:22 83:6 102:22 104:18 thing-type 74:5 think 6:20 9:13,14 27:6 31:16,16 34:6 37:5,5 41:17 41:19 58:15 62:21 62:23 66:13 67:9 67:12 68:25 76:21 77:24 79:12,15 89:6,18,21 90:9 90:23 91:16 92:3 92:6,15 94:3,10 95:3 96:5 97:3,19 98:5 101:25 104:3 104:3 106:15,21 108:25 115:17 thinking 22:7 58:9
---	---	--	--	---

107:19 thought 68:11 69:25 ThreadModCon 7:14 threat 8:18 9:5,7,9 9:20 10:22 11:25 13:8,21 14:3,5,9 14:13 18:5,6,18 21:5,8,15,20,22 21:25 22:4,8,12 22:13,18,18,24 23:6 24:8,25 25:12,13,13,16,17 25:19,22,22,25 27:19,20 28:4,5,7 28:9,10,11,13,14 28:15,18,19,24 29:14,17,17,18 33:19,21,24,25 34:25 35:4 40:19 41:3,7,8 42:8,22 43:9,11,20 44:13 45:21,25 46:3,5,8 46:18,24 47:2,11 47:17 48:24 49:5 49:6,12,15 50:13 51:19,22 54:18 55:13,15,23 56:12 57:17 60:12,15,19 60:20,22 61:8,13 62:11,13,14,25 63:6,12 64:2,4,11 64:12,16,18,19 65:4,17,23 66:6,8 68:3,23 76:7,10 76:14 79:25 82:6 82:10,12,17,19 88:8,9 89:24,25 90:3 91:2,3,4,9,10 93:5,6,7,10 94:5,6 94:18,19,19,20,25 95:6,7,10,11,15 95:16,17,18,22,23 95:24 96:2,12,22 96:23 97:6,7,15 97:17,20,20,24,25	101:16 104:2 109:11,16,21 111:21 112:24 113:4,8,12 114:8 114:17,18,21 115:18 116:4,11 116:14 ThreatModeler 1:6 5:19 6:17 120:3 threats 21:9,9,10 21:17,19 23:8 24:24 43:24 46:13 46:23 49:12,14 50:22,24 51:9,14 54:5,10,12,23 55:5,9,21 59:15 59:18 61:3,12,23 62:3 63:19 82:23 83:2,2,3 90:3 97:17,23,24 110:20 111:7,23 113:13,18,24 114:20 threat-model 40:19 46:9,16,17,25 47:7 52:12,15 58:13,18 60:23 75:17 112:13,17 113:4 114:3,7,9 114:16 three 8:6 14:24 17:8 95:7 time 6:13 19:11 32:6 37:7 73:9 84:2,16 87:20 times 88:2 title 13:24 14:2 today 6:23 today's 16:18 Toggling 67:22,23 tool 33:24 tools 18:19 top 70:16 72:23 112:22 topic 9:17 69:2 top-left 32:11 total 46:24	TRADEMARK 1:1 transcript 118:9,11 transitive 41:13 transmitted 108:6 108:7,17 transmitting 108:22 travel 7:22 TRIAL 1:2 tried 20:25 106:9 true 31:8 66:15 82:25 83:11 118:12,15 119:12 trust 41:9,11 try 33:12 73:23 77:20 102:19 trying 18:14 22:6 25:19 28:23 39:19 54:15 56:3 62:21 68:8 78:4 93:24 95:21 107:21 108:10 turn 14:24 17:15 27:2 29:16 94:7 turned 113:3 two 17:9 29:17 57:15,25 58:4,5 58:25 60:5 66:22 66:24,24 67:5,6 67:13 68:6 76:7 76:14 82:15 88:5 88:10,22 89:17 91:5,15 94:22 95:7,9,13,14 105:15 106:7 107:12,12,13 type 30:22 42:2 67:24 105:17 types 21:9 102:8 typically 9:14 21:11 97:5 98:7 98:15	35:4 64:12 understand 6:24 18:15 20:7 21:6 21:14 29:21 30:19 31:18 36:23 47:19 54:16 55:7,19 56:4,5 58:7 59:22 73:8 85:15 90:24 91:17 93:24 94:11 95:3,25 96:13 understanding 10:13 18:22 20:11 20:14,20 23:25 27:24 29:3,9 39:20 42:23 43:8 47:23 53:9 57:5 68:15 80:8 82:9 83:18 84:5 91:16 95:18 97:24 112:19,21 113:20 113:22 114:12,14 understood 76:21 81:10 unfortunately 61:16 UNITED 1:1 unknown 43:6 upside 67:24,24 use 19:15 24:15 25:19 31:17 36:16 43:22 59:4 user 43:15 45:13,16 80:16 108:9,13,14 108:20 uses 82:2 98:10 usually 99:2	61:20 70:10 74:3 74:20 vault 53:18 104:11 104:11,17 vector 87:25 88:4,5 88:10,12,15,22 89:16,19 90:15,21 91:5,13 92:16,25 93:8,14,16,18,25 94:9 95:6,8,13,20 95:21 96:2,2,12 97:2,11,25 98:11 98:21 101:16 103:22 vectors 24:6 98:6,6 98:11,14 100:17 101:3,6,13 verb 73:22 version 78:8 105:19 versus 43:19 48:6 48:11 66:2 74:4 95:23 vice 12:3 view 116:17 visualize 88:11 visually 91:2 93:5 Vries 10:11,18 17:22 vulnerabilities 22:3 vulnerability 22:2 68:3 100:13,20
W				
walk 34:3 wall 106:20 want 6:14 19:15 24:15 26:25 30:18 72:6 73:5,15 76:3 77:11,12,19 87:15 99:20 wanted 7:7,10 15:9 17:19 68:25 72:22 76:20 79:17 waves 107:4,5,8 way 10:19 25:2 26:13 31:9 37:14				
V				
v 1:5 120:3 VA 3:17 vague 55:25 valid 18:11 various 10:22 22:16 24:4,7 33:22,25 36:19 40:17,21,23 47:18 53:14,16,19 54:13				
U				
U 6:2,2 ultimately 21:15				

57:15 66:7 68:12 105:14,23 107:11 107:19 111:19 119:17 ways 24:22,25 107:10,14 web 106:2,2,3 website 105:17,20 welcome 76:23 went 115:12 West 119:25 we're 75:13 willing 17:23 Wilmington 3:8 Window 29:10,11 witness 4:3 5:7 15:13 27:5 39:7 46:19 50:17 62:17 63:22 65:13 72:7 73:13 77:4,25 79:12 81:20 83:23 87:23 89:9 92:8 92:11,13 94:16 100:8 109:4,5 119:10,13 wonder 91:20 wondering 67:2,14 word 24:15 25:5,9 26:9 37:22 41:18 42:6 43:23 73:21 82:3,14 work 9:25 15:18,21 15:25 33:23 34:24 35:3,6 61:2 74:15 79:16 101:6 109:20 worked 10:18 11:19,21 12:2,10 12:12,17 31:8 working 12:17 14:12 17:9 18:3 21:2 works 102:20 world 75:19,22 103:17,21 written 17:3 31:17 31:21 42:24 65:25	wrong 25:24 47:11 53:4 wrote 19:25 27:25 80:7 X X 1:3,10 4:2,11 Y year 6:20 York 2:16 118:4,6 119:3,5,9 Z Zheng 85:17,23 86:10,18,21 87:3 87:6,12,25 88:5 88:12,24 89:2,16 90:13 91:8 92:18 98:6,9,10,11,15 99:12,19 100:3,11 zone 41:10,11 # #001046-1 119:24 #30XI00244900 119:24 0 008 20:3,6,8 21:4 21:23 22:10,11 23:11,19,23 27:13 29:4,7 77:3,9 78:23 104:24 105:5 1 1 27:13 33:8,15 34:8 38:7,15 41:21 42:4,18,21 43:7,19,23 45:19 48:7,10,18 51:21 56:17 60:2 64:20 68:19 69:16 80:2 80:10,15,18,19,25 81:10,12,15,17 82:12,19 83:4,14 91:25 110:4,7,18	111:6,11,18,25 1 30:11 1 29:24 10 69:12 86:14 99:16,19,25 100:11 104:22 10A 66:11,16 67:4 67:15,16 10B 66:11,16 67:2 67:14,16 10,699,008 1:9 1001 4:13 77:5,9 78:9,12,23 79:7 1003 4:14 32:18,23 72:15 78:13,14,17 79:6 1004 4:15 32:21,25 109:25 1005 4:16 87:6,8 102 35:8 36:9 37:20 37:24 38:24 39:2 39:11,23,24 104 39:3,6,6,13,13 39:25 40:5,9 41:16 44:14 106 40:5 44:2,14 45:11 48:21 52:11 60:8 112:10 108 45:21,25 46:3 48:25 49:5,7 50:13 51:19,22 113:8,12 109 4:7 11:23 72:11 11:31 72:11 110 51:23 52:2,5 112 46:22 60:12,16 60:19,21 61:9 114 64:21,25 115 4:6 12 51:3,8 12:32 117:12 1201 3:6 13 110:11,16 14 90:25 93:4 94:4 95:5 15 52:3,4	16 52:3,4 71:16 88:8 89:6,14 110:12,16 17 89:5,7,8,14 18 89:5,7,8 90:14 112:7 19 22:21 51:2 69:5 105:4,7 19801 3:8 2 2 41:2,6,20 42:3,8 42:24 43:6,13,14 47:7,13,25 48:3,6 48:6,11,14 56:22 58:17 85:13,18,21 92:4,6,9 20 39:8 40:14 47:20 90:5 94:17 2003 29:12 2017 20:17 23:25 2021 14:16 2023 6:21 7:2,14 2024 1:15 2:7,11 118:11,20 119:14 119:19 120:4 2100 3:7 22102 3:17 23 2:11 58:10 24 86:12 87:13,21 90:5 26 61:21 27 39:10 3 3 35:23 47:5 58:17 77:14 79:22 80:8 80:23,24 81:3,7 81:12,13 82:3,5 82:11,18,22 83:7 83:19 84:6 92:5 110:11,14 302.468.5675 3:9 31 56:25 57:8 92:2 32 4:14,15 34 42:8 35 60:20 83:22 36 42:7,7	38 63:23,24 4 4 35:19,21 37:3 69:5,8 86:7 92:2 110:25 41 30:13 42:19 42 35:19,22,23 37:8 43 26:25 27:6 86:14 99:17,20 100:11 44 26:25 27:6 72:19 45 37:8 44:7,19 72:16,23 46 61:8 62:24 100:23 48 77:15,15 79:8,10 79:19 84:21 99:17 99:20 100:11 49 84:24 86:14 5 5 1:15 2:7 35:23 40:14 44:19 46:2 47:19 49:7 58:3 59:2 61:14 62:6 63:10 69:3,9,10 86:4,6,12 87:12 87:19 88:8 89:5 90:13,25 92:12,12 93:4 94:17 95:5 118:11 119:14 120:4 500 3:16 51 22:20,23 52 24:11 55 79:11,13 571.765.7703 3:18 59 65:2 6 6 4:6 47:5 49:23 52:3 56:24 57:8 58:10 59:20,22 60:20 61:21 62:24 63:24 65:3 86:12 87:13,21 111:2 112:5 115:13 64 46:3
--	--	--	--	---

65 37:5 38:3 61:14

66 62:7 63:9

7

7 49:24 85:2 119:19

77 4:13

79 30:16

8

8 45:3,5

80 30:16

8300 3:15

85 77:13 83:20

84:10,11,12 85:6

87 4:16 85:10,22

88 85:22

9

9 50:10,12 51:6,12

85:2,5

9:58 2:8

902 50:20

904 50:20 51:9,14

95 86:2 97:11

96 86:2,13,13 99:14