



Planet Depos®
We Make It *Happen™*

Transcript of Seth James Nielson, Ph.D.

Date: March 6, 2024

Case: Iriusrisk, Inc. -v- Threatmodeler Software, Inc. (PTAB)

Planet Depos

Phone: 888.433.3767

Email: transcripts@planetdepos.com

www.planetdepos.com

1 UNITED STATES PATENT AND TRADEMARK OFFICE

2
3 BEFORE THE PATENT TRIAL AND APPEAL BOARD
4

5 IRIUSRISK, INC.,

6 Petitioner,

7 v.

8 THREATMODELER SOFTWARE INC.,

9 Patent Owner.
10

11 IPR2023-00656

12 U.S. Patent No. 10,713,366
13

14
15
16 REMOTE DEPOSITION of SETH JAMES NIELSON, Ph.D.

17 Wednesday, March 6, 2024

18 9:01 a.m. CST
19

20 Job No.: 527767

21 Pages: 1 - 160

22 Reported By: Michelle M. Yohler, CSR, RMR, CRR

1 The deposition of SETH JAMES NIELSON, Ph.D.,
2 held remotely pursuant to notice before
3 Michelle M. Yohler, CSR, RMR, CRR, a certified
4 shorthand reporter, CSR No. 84-4531.

5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22

1 A P P E A R A N C E S

2 ON BEHALF OF IRIUSRISK:

3 MR. MATTHEW MIDDLETON

4 DLA PIPER LLP

5 1650 Market Street

6 Suite 5000

7 Philadelphia, Pennsylvania 19103

8 215.656.3300

9

10 ON BEHALF OF THREATMODELER SOFTWARE INC.:

11 MR. DONALD L. JACKSON

12 RIMON, P.C.

13 8300 Greensboro Drive

14 Suite 500

15 McLean, Virginia 22102

16 571.765.7700

17

18 ALSO PRESENT:

19 Mr. Doru Halip, Technician

20

21

22

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22

E X A M I N A T I O N S

WITNESS	PAGE
SETH JAMES NIELSON, PH.D.	
By Mr. Middleton.....	5

E X H I B I T S

EXHIBITS	PAGE
No. 1001 '366 Patent.....	26
No. 1004 '228 Patent - Keenan.....	101
No. 1005 '907 Patent - Zheng.....	106
No. 1006 Baker Reference.....	129
No. 2009 Declaration of Seth James Nielson, Ph.D.....	7
No. 2010 Supplemental Declaration of Seth James Nielson, Ph.D.....	7

1 P R O C E E D I N G S

2 (Technician read-on.)

3 (WHEREUPON, the witness was duly sworn.)

4 SETH JAMES NIELSON, Ph.D.,

5 called as a witness herein, having been first duly

6 sworn, was examined and testified as follows:

7 EXAMINATION

8 BY MR. MIDDLETON:

9 Q Hi, Dr. Nielson. Just to start off, I
10 understand you've been deposed before; is that
11 correct?

12 A Correct.

13 Q Do you understand you're under oath today?

14 A I do.

15 Q Is there any reason you can't give your
16 best testimony today?

17 A No.

18 Q So a few questions since we're taking this
19 deposition remotely. Do you have any documents
20 with you, physical documents with you today?

21 A No.

22 Q Do you have anything open on your computer

1 right now?

2 A No.

3 Q Other than the Zoom session.

4 A Clearly, yes.

5 Q Right. And where are you located today?

6 A I am in Austin, Texas.

7 Q And do you know where your counsel's
8 located?

9 A Actually, I don't.

10 Q That's fine.

11 MR. MIDDLETON: Can we please mark
12 Exhibit 2009 and 2010.

13 THE TECHNICIAN: Okay. Please stand by.

14 MR. JACKSON: Do you want to remark them
15 or just use the exhibit --

16 MR. MIDDLETON: Yeah, I'm going to use the
17 same exhibit numbering. I don't know if we're
18 going to put the actual marker on them or not, but
19 I'm going to use the same numbering as they are in
20 the proceeding as I go along.

21 MR. JACKSON: Okay.

22 THE TECHNICIAN: Both exhibits are dropped

1 in the chat.

2 (WHEREUPON, Nielson Exhibit Nos. 2009 and
3 2010 were presented to the witness.)

4 BY MR. MIDDLETON:

5 Q Dr. Nielson, do you have both exhibits in
6 front of you?

7 A Just getting the second one.

8 Yes, I have both exhibits in front of me.
9 Thank you.

10 Q All right. So Exhibit 2009 is a copy of
11 your declaration; is that correct?

12 A Of my initial declaration, yes.

13 Q And then Exhibit 2010 is a copy of your
14 supplemental declaration; is that correct?

15 A Yes.

16 Q Did you review these two declarations in
17 preparation for your deposition today?

18 A Yes.

19 Q And do these two declarations represent
20 all the opinions you have in this matter?

21 A They represent my current opinions in this
22 IPR. They are all the opinions that I'm

1 currently -- I understand that I'm currently
2 offering. I don't believe I'm offering any other
3 opinions for this IPR.

4 Q Do you have any other opinions for this
5 IPR that didn't make it into these declarations?

6 A I have obviously -- I mean, there's a lot
7 of opinions that I have, so, I mean, I'm sure I
8 have a number of opinions that are not in this
9 IPR -- declaration.

10 Q Any corrections to your reports today?

11 A Not that I'm aware of.

12 Q Your expertise involves cybersecurity; is
13 that correct?

14 A Yes, at a high level, I am a cybersecurity
15 expert.

16 Q And you're the founder of a firm called
17 Crimson Vista?

18 A Correct.

19 Q And when was this founded?

20 A March 1st, 2016.

21 Q And is it fair to say that Crimson Vista
22 is a computer security research and engineering

1 company?

2 A Yes, that is a fair description.

3 Q And is it correct that as a common
4 consulting service, you provide a source code
5 review?

6 A That is one of the services we provide
7 that is common, yes.

8 Q And you've also performed risk analyses
9 before; is that correct?

10 A Yes, I have performed risk analyses.

11 Q What is a risk analysis?

12 A So it can be a little bit context-specific
13 because risk is a broad area. In one particular
14 instance that I'm thinking of, the client needed
15 to understand the best places to invest their
16 cybersecurity resources.

17 Q And how does investing cybersecurity
18 resources relate to risk?

19 A Well, when you have a limited number of
20 resources, you want to put those resources to
21 where they make the most difference.

22 Q And how do you perform a risk analysis?

1 A Again, that can be somewhat
2 context-specific, but typically a risk analysis
3 requires some form of threat analysis, and then
4 based on the threat analysis, you assess risk
5 that's either quantitative, or it can be
6 qualitative, as in you can prioritize the risks.
7 But it's based on assessment of threats.

8 Q Can you please describe for me your
9 experience with threat modeling.

10 A Sure. I would say that all -- most, if
11 not all, of my cybersecurity career is related to
12 threat modeling in one form or another. So threat
13 modeling involves, for example -- or can involve
14 vulnerability analysis. So even a source code
15 review, for example, I've done source code reviews
16 where we determined vulnerabilities related to
17 cryptography, for example, and then that
18 information is factored into the threat model.

19 I've done threat modeling as part of the
20 risk analysis. I've actually kind of done the
21 reverse from the vulnerability that I mentioned
22 earlier where we did threat modeling as a way to

1 identify where we should prioritize looking for
2 vulnerabilities.

3 So I've done both creating models as well
4 as analysis that goes into models.

5 Q And kind of a broad question, but are you
6 generally familiar with cybersecurity and threat
7 modeling major players, like major players and
8 industries, any government agencies in the area?

9 A Well, you're getting into more of a niche
10 part of threat modeling. So threat modeling has
11 been done by security people for forever. And
12 then some people have preferences for tools and
13 some people have preferences for certain
14 frameworks.

15 As far as frameworks go, I typically rely
16 on NIST for the frame- -- or OWASP would be
17 another example.

18 THE WITNESS: OWASP, for the court
19 reporter, O-W-A-S-P, all capitalized.

20 BY THE WITNESS:

21 A Those are the types of frameworks that I
22 typically go to.

1 As far as tools go, I've used tools less,
2 so I'm not as familiar with the major tools
3 providers. That's kind of a matter of preference.

4 And, actually, I should clarify. Tools,
5 there's obviously a broad set of tools. The sort
6 of tools that we're kind of talking about here in
7 this IPR are for being able to model in some sort
8 of automated fashion certain aspects of a threat
9 model. Obviously there would be tools for
10 collecting data. I am more familiar with tools
11 that collect data, vulnerability data that's then
12 factored into a model.

13 So just pointing out there's a broad range
14 of tools as well, and which ones you use are a
15 matter of preference.

16 BY MR. MIDDLETON:

17 Q And so what are some major cybersecurity
18 technology companies off the top of your head?

19 A For any type of cybersecurity technology?

20 Q Sure. Like, are you familiar with
21 CrowdStrike?

22 A Yes.

1 Q And maybe Palo Alto Networks?

2 A Yes.

3 Q And are you familiar with cybersecurity
4 government agencies as well?

5 A Yes, NIST, for example, is a large one.

6 Q Are you also familiar with the
7 Cybersecurity and Infrastructure Security Agency?

8 A Yes. CISA.

9 Q Yeah, that goes CISA. And you would
10 understand CISA would be the acronym C-I-S-A for
11 the court reporter?

12 A Correct.

13 Q And CISA handles cybersecurity for the
14 U.S. government, right?

15 A "Handles" is a broad term. CISA is
16 definitely an important component for certain
17 identification of problems, publication of
18 responses and recommendations, but I don't know
19 that I would say they alone handle cybersecurity
20 for the U.S. government.

21 Q Have you ever heard of IriusRisk before
22 this case?

1 A No.

2 Q Have you ever heard of ThreatModeler
3 before this case?

4 A No.

5 Q Have you ever heard of Anurag Agarwal
6 before this case?

7 A No.

8 Q He sometimes also goes by Archie Agarwal I
9 believe?

10 A I believe that's correct. But, no, I was
11 unfamiliar with that before this case.

12 Q Have you ever heard of Adam Shostack
13 before this case?

14 A Not that I recall. The name kind of
15 sounds familiar, but it may just be a name that
16 sounds familiar.

17 Q Have you ever heard of a John Steven?

18 A I don't know.

19 Q Do you know anyone that works at
20 ThreatModeler?

21 A Not before this case, no.

22 Q Since you testified that you never heard

1 of IriusRisk and ThreatModeler before, is it safe
2 to say you've never used their tools before
3 either?

4 A Before this case, no.

5 Q And have you ever used the Microsoft
6 threat modeling tool?

7 A I had -- I have heard of the Microsoft
8 threat modeling tool before, but I have not used
9 it.

10 Q Have you ever heard of Threat Modeling
11 Connect?

12 A Threat Modeling Connect before this case,
13 no.

14 Q Have you ever spoken about threat modeling
15 at any conference before?

16 A Yes.

17 Q Which conference?

18 A So when I teach about cybersecurity, I
19 teach about threat models, and I've spoken at
20 Enterprise Data World and Data Architecture -- I'm
21 trying to remember the last letter in it. It's
22 another data conference run by the same

1 organization.

2 Q Can we take a look at your supplemental
3 declaration. That's Exhibit 2010.

4 A Sure.

5 Q And can we please go to Paragraph 6.

6 A Sure. I have it.

7 Q You testify here that in your work as a
8 professional cybersecurity engineer, you worked
9 with clients to develop threat models; is that
10 correct?

11 A That's correct.

12 Q And when exactly did you develop these
13 threat models?

14 A It just -- with the clients, right? So
15 one client in particular was a medical device
16 manufacturer. I believe that was in 2015.

17 Q And do you recall how many clients you've
18 developed threat models for?

19 A Total, no.

20 Q And what types of threats have you
21 included in threat models before?

22 A Well, there's a lot of different levels to

1 threat models. The threat models that we're
2 talking about here in this IPR tend to be more
3 concrete in the sense that they're related to
4 vulnerabilities that you might see in a network or
5 an application, for example.

6 But there's also threat models that they
7 kind of establish at a higher level that kind of
8 can begin an analysis. One of the most important
9 ones, for example, is to decide whether or not you
10 have an insider threat. When we talk about an
11 insider threat, that's a different type of model
12 than if we have an external threat. When you have
13 an insider threat, you have to change the way you
14 look at your security.

15 So a lot of times when I do a threat
16 model, I tend to start with the high level. Like,
17 we need to understand at a high level which types
18 of threats we're dealing with and what we need to
19 be protecting against. And then we work down into
20 more concrete details like, you know, are we
21 worried about buffer overflows because we're
22 writing in C programming and if we have those kind

1 of vulnerabilities, which kind of threats can
2 exploit them.

3 So there's different levels of threat
4 analysis.

5 Q Have you ever included cyber threats in a
6 threat model before?

7 A Well, so cyber threats is more of a
8 category than a specific threat. So unless you're
9 referring to something specific, I'm -- that would
10 be a category, that wouldn't be a specific threat.

11 Q So as part of your work developing threat
12 models, you use the threat tree analysis as one of
13 the approaches in creating threat models; is that
14 right?

15 A That is one approach that I use, yes.

16 Q And the threat tree is diagramed in
17 Paragraph 4 of your supplemental declaration,
18 Exhibit 2010?

19 A This is an illustration of a threat tree,
20 and this is an illustration taken from a book that
21 I sometimes use in my courses.

22 Q Yeah, and that book is the Ross Anderson

1 book?

2 A That's, yes, the Security Engineering.

3 Q Would you consider a threat tree to be the
4 same thing as an attack tree?

5 A Yes, it's sometimes called an attack tree.

6 Q And is this threat tree a threat model?

7 A Yes, at a -- yes, it's a threat model.

8 Q So looking at the diagram, the
9 illustration in Paragraph 4, could you please
10 point out the threats?

11 A Sure. So threats are things that can go
12 wrong. Let me actually -- I just want to pull up
13 from my report here the definition so that we have
14 a context to work in here. One moment.

15 Yes, so I'm just reading from Paragraph 78
16 of -- how do I refer to this exhibit? 2009, did
17 you say?

18 Q Yes.

19 A I'm starting about the middle of the way
20 through. "As explained below, the term 'threat'
21 should be construed to mean one or more potential
22 events that if they occur can cause adverse

1 effects to a target system."

2 So the way a threat tree works is a threat
3 tree starts with kind of first-level set of
4 effects and then shows the cascade down to where
5 there might be a loss.

6 So what you see here in this figure
7 reproduced in my supplementary report is you start
8 to have adverse effects. So cryptanalysis of DES,
9 D-E-S, would be an example of an event that could
10 cause adverse effects to the system. Protocol
11 failure, false auth response.

12 And then these show subsequent negative
13 events that can lead to the successful card
14 forgery, which is an event associated with a loss.

15 Q Would you please also point out the threat
16 model components in this illustration in
17 Paragraph 4 of Exhibit 2010?

18 A Sure. So in this -- so the threat model
19 components were, as I'm using them in my
20 declaration, is that it is sources. And let me
21 just pull this up here, too, so that I have that.

22 So in the context of the '366 patent --

1 and I'm reading again from Exhibit 2009,
2 Paragraph 90 -- "The '366 patent describes each
3 threat model component as a potential relevant
4 source for one or more threats."

5 And so you can see in this threat tree
6 that some of the threats are identified with a
7 potential source. So in the bug in ATM, that
8 would be where the ATM would be a potential source
9 for the bug. Maintenance contractor would also be
10 a potential source. Shoulder surfing implies the
11 source.

12 So there's -- both threats and threat
13 model components would be identified in here.

14 Q In addition to this threat tree analysis,
15 you've used the -- you testified that you used the
16 NIST framework, and you've also used OWASP; is
17 that right?

18 A Yes.

19 Q And what other frameworks have you used
20 before?

21 A NIST is my primary go-to because it's so
22 respected in the industry. OWASP I've used more

1 as just another data point. Those are the two
2 frameworks that I've primarily used.

3 And then, of course, just sources from
4 literature, whether it's papers or books.

5 Q So when you develop threat models, it's
6 mostly from the NIST framework?

7 A Well, I'd actually say that when I develop
8 models, that comes from my expertise and
9 experience. I will typically put together a
10 threat model that I think is appropriate for the
11 client based on client input.

12 The frameworks provide some guidance into
13 what should be considered and how they should be
14 approached, but it's not like they're a do step
15 one, do step two, do step three; that, I have to
16 determine based on my experience and knowledge and
17 what the client's needs are.

18 Q And how many threat models have you
19 developed before?

20 A I don't have a count.

21 Q More than 1,000?

22 A Identifying it by number is also difficult

1 because of where one threat model ends and another
2 begins. I have developed a significant amount of
3 threat models. I'm sure there's been overlap
4 between one or another. I've done threat modeling
5 throughout my career; I don't have a number.

6 Q And I could build a threat model on a
7 white board, right?

8 A You can -- so a threat model is the
9 analysis of the different things that can go wrong
10 in a system, and depending on how detailed you
11 want that model to be, and depending on how big
12 the system is, you could do a white board.

13 I would almost always say that would be a
14 skeleton of a threat model. You'll almost always
15 need some narrative to go along with it to
16 illuminate details. Like, you wouldn't just use
17 this threat tree that we've been talking about and
18 be like: There, threat model, done, we don't need
19 anything else. You'd almost always have to have
20 some explanatory notes, some explanation to help
21 understand what the terms mean.

22 But if you're asking if it needs to be

1 some kind of computer model versus just a
2 document, it can be a document. And, in fact,
3 that's the most common that I've worked with.

4 Q Yeah. And sticking on the same line of
5 computer versus document, I could also just use,
6 you know, any diagramming software tool to build a
7 threat model, right?

8 A Well, I just kind of want to be clear
9 between the distinction, right? Building a threat
10 model is an analysis, right? The documenting
11 system is the way you record and report the
12 analysis.

13 Q So I could record and report the analysis
14 on a diagramming tool, right? An electronic
15 diagramming tool?

16 A So, again, assuming that you've got the
17 analysis all done, right? Like, if you take a
18 look at -- one of the things that, like, the
19 ThreatModeler software does is it both provides
20 some analysis and some documenting, right?

21 So you can take these third-party
22 components and you bring them in, and it provides

1 this automated analysis system. And that also
2 includes some built-in documentation.

3 But there would be nothing to stop you
4 from taking all of the output that you got from
5 your ThreatModeler tool, going over to a Word
6 document, and drawing a bunch of diagrams, writing
7 down all the information. There's -- you know,
8 you could clearly transfer all of that information
9 to a document.

10 Q Okay. And I just want to walk through how
11 to build a threat model in the context of the '366
12 patent.

13 So let's say I want to build a threat
14 model for my everyday life. I'm using a laptop
15 for work right now. My laptop has a Bluetooth
16 port that can connect to Bluetooth devices. So
17 one threat to my laptop could be bluejacking
18 through the Bluetooth port, correct?

19 A Yeah, I think you're actually -- you're
20 almost quoting out of the '366. Is that something
21 we can open?

22 Q Absolutely. Yeah.

1 THE TECHNICIAN: Please stand by.

2 MR. MIDDLETON: Can we do Exhibit 1001?

3 THE TECHNICIAN: Yes. One second.

4 (WHEREUPON, Nielson Exhibit No. 1001 was
5 presented to the witness.)

6 THE TECHNICIAN: The exhibit is in the
7 chat.

8 BY THE WITNESS:

9 A Yes, I see it now. Give me just one
10 second.

11 Yes, I have it open now. Would you like
12 me to go to the part of the specification you were
13 talking about?

14 BY MR. MIDDLETON:

15 Q Sure. Column 10...

16 A Yes, column 10.

17 Q Line 13 -- no, 12 is where it starts.

18 A Sure. I have that part of the
19 specification.

20 I'm sorry, would you mind repeating what
21 your question was?

22 Q Sure. Actually, let's just go over what

1 it says in the '366 patent.

2 So you see column 10, it says,
3 "Accordingly" -- you know -- "using the above
4 example, the Bluetooth port may be defined as a
5 relevant source for a bluejacking threat"; is that
6 correct?

7 A Yes.

8 Q So there, you know, the '366 patent is
9 saying bluejacking is a threat and the Bluetooth
10 port is the threat model component; is that
11 correct?

12 A Sure. That's a fair reading of that.

13 Q So going back to my question before, you
14 know, I was kind of building this hypothetical
15 world where, you know, I'm using -- it's not so
16 much hypothetical because it's true also. I'm
17 using my laptop for work right now. My laptop has
18 a Bluetooth port that can connect to Bluetooth
19 devices. So one threat to my laptop could be
20 bluejacking through the Bluetooth port; is that
21 right?

22 A Well, it could be. I mean, it would have

1 to take some context into consideration, but, I
2 mean, that's potentially reasonable.

3 Q What additional context would you need?

4 A Well, this kind of goes back to what I was
5 saying earlier that, for the type of analysis that
6 you do, there's different levels, right?

7 So one of the very first questions that I
8 would be interested if you were my client would
9 be, well, what type of data are you trying to
10 protect and based on the way you use your laptop
11 and where you use your laptop, what do we identify
12 as the most likely types of threats such as
13 insider threats or external threat.

14 Bluetooth, for example, has a fairly
15 limited range, and that can vary. So maybe even
16 in your case, we would want to measure the range
17 of the Bluetooth because that will help us to
18 understand how significant of a threat that's
19 going to be in your particular circumstance.

20 What's being described here in the '366 is
21 kind of already taking some of those assumptions
22 into consideration, right? That's why it even

1 says "may," right? It doesn't say "must be" or
2 "is," right? It says the Bluetooth port may be
3 defined as a relevant source, and that's why I'm
4 putting some of this other context as an example
5 around that.

6 Q That's fair. So what if I added, you
7 know, to my hypothetical and said I do all my work
8 in a coffee shop, how about that? Would
9 bluejacking be a threat to my Bluetooth port in my
10 laptop?

11 A That seems more likely. That seems more
12 likely, but I'm hesitant to give you an absolute
13 on a hypothetical. If there were, you know -- if
14 there were concrete data, then I could perform the
15 analysis. But I will agree that the coffee shop
16 makes that threat more reasonable to consider in a
17 model than you sitting in your office in the law
18 office.

19 Q Yeah, we have some pretty good protections
20 here. At least I hope we do.

21 Okay. So then let's just assume, you
22 know, for the sake of argument, because it's in

1 the '366 patent, you know, bluejacking -- well,
2 let me go back up.

3 Bluejacking is a threat described in the
4 '366 patent, right?

5 A Bluejacking is a threat as I describe in
6 the '366 patent, yes.

7 Q And a Bluetooth port is a threat model
8 component described in the '366 patent?

9 A That is correct.

10 Q So if I wanted to build a threat model
11 based on bluejacking and the Bluetooth port, to
12 start could I take a white board and draw a circle
13 with the word "bluejacking" in it and then, you
14 know, draw -- someone else on the white board draw
15 a square with the word "Bluetooth port" on it and
16 then draw a line between the two?

17 A I mean, once you've done the analysis,
18 there are a lot of different ways you could choose
19 to document it. I think that's a little bit
20 different from what's being described in the '366
21 patent, but, yeah, if you want to document it
22 using your own diagramming or whatever else, you

1 could document that however you want.

2 Q How is it being done in the '366 patent?

3 A Well, first of all, what's being done in
4 the '366 patent isn't just about creating a threat
5 model. If you look to what the '366 says in terms
6 of its -- what it's describing as its advance over
7 the prior art, it's not suggesting that nobody has
8 ever designed models before.

9 Instead, what it's saying is there's a lot
10 of tools that are used to document things that are
11 not threat models, and they produce these
12 electronic documents that document things that are
13 not threat models. And that's commonly done.

14 In particular, you might, for example,
15 document your network architecture. This is very
16 common. All right, we want to know where all of
17 our routers are, we want to know where our Wi-Fi
18 points are, and we document that. And that is
19 commonly done through the IT department so that
20 they know how to troubleshoot so that they know
21 this, they know that.

22 And the '366 says we can take that

1 information and we can, in an automated fashion,
2 derive a threat model from it.

3 Q I understand that, but I think what my
4 question is getting at is just the different ways
5 you could document your threat model.

6 So we talked about, you know, white
7 boarding could be one way where you have a circle
8 and square and draw a line between the two. That
9 could be one way to document it. How is the '366
10 patent documenting the threat model itself?

11 A Well, again, once the '366 has done --
12 what's described in here has done the analysis,
13 the documentation is somewhat inherent in the
14 system. They have it -- they have their own kind
15 of documentation -- right? -- these kind of native
16 components. But the analysis was the -- you know,
17 was the derivation of the threat model from the
18 input information.

19 Q Are you familiar at all with Lucidchart?

20 A Yes.

21 Q And you could draw diagrams on Lucidchart;
22 is that right?

1 A You can draw diagrams in Lucidchart, yes.

2 Q So the same way I would document a threat
3 model on a white board the way we described, I
4 could document it the same way on Lucidchart,
5 right?

6 A Yes. And I think the '366 would consider
7 that to be another example of a type of input that
8 it would be able to pull in.

9 Q And you can import Visio diagrams into
10 Lucidchart; is that right?

11 A I'm trying to remember. It's been a while
12 since I've used it. I'd have to double-check.
13 But it wouldn't surprise me if that were the case.
14 A lot of charting tools have ways of converting a
15 chart from one form to another.

16 Q Sure. And why don't we pull up the '366
17 patent again.

18 A Yes, I have it.

19 Q And let's just go to column 2, line 47.

20 A I have column 2.

21 Q Line 47?

22 A Yes.

1 Q So that says, [as read] "Software exists
2 for converting a diagram file of one type to
3 another type of a diagram file but not to a threat
4 model. For example, Lucidchart, SmartDraw, and
5 Edraw Soft are programs which will convert a
6 Microsoft Visio file to another file type (for
7 example, importing the visual elements and
8 retaining some diagram features of the original
9 Visio file) but without creating an associated
10 threat model," right?

11 A Correct.

12 Q So does that confirm for you that
13 Lucidchart can import Visio diagrams?

14 A It definitely can convert for sure.

15 Q Well, it does say, "For example, importing
16 the visual elements and retaining the diagram
17 features," right?

18 A Yeah. I'm only being hyper precise to the
19 point it mentions multiple things here. Just
20 because I haven't worked with it, I'm just saying
21 what I know for absolute certain. It says for
22 absolute certain it will convert a Microsoft Visio

1 file into another file type.

2 The "for example" I'm -- you know, that
3 probably applies to all three, but I'm just, you
4 know, being hyper accurate.

5 Q That's fair. But you would assume at the
6 very least, the "for example" applies to at least
7 one of Lucidchart, SmartDraw, or Edraw Soft?

8 A Yes.

9 Q So at least one of Lucidchart, SmartDraw,
10 and/or Edraw Soft can import visual elements and
11 retaining some diagram features of the original
12 Visio file?

13 A Yes.

14 Q And you testified -- sorry.

15 You testified that you can pretty much
16 document how -- your threat model however you
17 like. Let's say I have that simple threat model
18 that we discussed with the circle and the square
19 and the lines connected to them. Let's say I want
20 to add, you know, another threat to my threat
21 model. You know, can I pretty much do that also
22 however I'd like?

1 A Well, I want to make sure I back up and --
2 I don't know that I ever agreed with you that the
3 thing drawn on a white board was a threat model.
4 So I just don't want to have that be accepted into
5 this hypothetical.

6 Do you want to ask the question again, or
7 do you want me to answer with that caveat?

8 Q Well, what makes the white board not a
9 threat model?

10 A Well, you're providing me a hypothetical,
11 and I'm trying to work with that. I'm just
12 saying, like, I have not come to a conclusion that
13 what you described is a threat model.

14 Q So what about the -- you know, going back
15 to Exhibit 2009 in that illustration in
16 Paragraph 4 of Exhibit 2009, you testified that
17 that was a threat model, right?

18 A I'm sorry. Do you mean Exhibit --

19 Q 2010. Paragraph 4 of 2010. That's right.

20 A Yes, I would say that this is an example
21 of a threat model, maybe a skeletal example, but
22 I'd say this is an example of a threat model.

1 Q And I could draw that on a white board,
2 right?

3 A You absolutely could draw this on a white
4 board.

5 Q So you agree that I could draw a threat
6 model on a white board?

7 A I agree that you could draw -- you could
8 document your threat model on a white board, yes.

9 Q So let's stick with the example in
10 Paragraph 4, the illustration of that threat model
11 then.

12 Let's say I wanted to add a new threat to
13 this threat tree, and let's say I drew it on a
14 white board and I want to add a new threat. Can I
15 just, you know, draw another threat on a piece of
16 paper and then take a piece of tape and just tape
17 it to my white board?

18 A You're obviously physically capable of
19 taping a piece of paper to your white board. The
20 key question of course is about the threat model.

21 So one of the things I've been
22 distinguishing is the threat model versus the

1 representation of the threat model. So just
2 drawing things and attaching them is not by
3 itself, you know, adding things to a threat model.
4 That would be some kind of analysis, and then you
5 might document it by changing the drawing.

6 Q So I think I understand what you mean.
7 And when I'm asking my questions, I'm really just
8 thinking with the assumption that the analysis has
9 already been performed.

10 And that's kind of how we discuss the '366
11 patent goes, right? Because it's talking about
12 bluejacking and Bluetooth port, so the '366 makes
13 some assumptions when it describes potential
14 threats and threat model components that these --
15 that this analysis has already been performed;
16 isn't that right? Just for exemplary purposes.

17 A Well, but I feel like that takes all of
18 the whole context of the patent out, right? Like,
19 you know, yes, within this one paragraph it's
20 talking about bluejacking, but that is meant to be
21 understood in the context of the whole patent.

22 I don't think the '366 patent is in any

1 way suggesting that, you know, well, just draw
2 bluejacking on the white board and you've got
3 a -- you know, a threat model, right? There is
4 analysis that has to be done, and the '366 patent
5 is pretty explicit about that.

6 Q Can we go back to Exhibit 2009 of your
7 report -- your declaration.

8 A Yes.

9 Q And then Paragraph 78.

10 A Yes, I have that.

11 Q And here you testified earlier that you
12 construed the term "threat" to mean one or more
13 potential events that, if they occur, can cause
14 adverse effects to a target system; is that right?

15 A Correct.

16 Q And this is the definition that you
17 applied in your report?

18 A Yes.

19 Q And you agree with this definition?

20 A Yes.

21 Q What do you mean by "target system"?

22 A Threat analysis is performed within the

1 context of some type of system. Whatever that
2 system is, these events would cause adverse
3 effects to that system.

4 Q And what's an example of a target system?

5 A I mean, whatever the system is being
6 analyzed. That can include humans. It can be
7 just an application.

8 The '366, in particular, emphasizes the
9 need to be broader than an application and that
10 that's one of the places that it emphasizes its
11 automation is valuable.

12 But in terms of understanding a threat,
13 the threat can apply to any system that --
14 wherever you want to divide something up, you can
15 identify threats to that -- whatever that object
16 is.

17 Q And by target system, do you also mean --
18 sorry. Scratch that.

19 Target systems are called threat model
20 components in the '366 patent, right?

21 A Can you point me to the part of the
22 specification you're referring to?

1 Q Well, you testified earlier that you
2 defined threat model components as relevant
3 sources of threats, right?

4 A Yes.

5 Q So a target system would be a relevant
6 source of a threat, right?

7 A I do not believe that that is how the '366
8 patent would use those terms.

9 Q So if the threat is bluejacking, what's
10 the target system?

11 A Well, I'd say that that would depend. In
12 your case, it might be your laptop. The way the
13 '366 patent refers to it -- I'm starting at the
14 bottom of column 8, starting on line 65.

15 [As read] "Referring to Figure 2 a
16 representative example of a threat modeling
17 process (process) (method) 200 includes generating
18 a threat model 208 for any application, process,
19 or system under consideration."

20 And I'm going to skip here just a little
21 bit to get to the part I was -- that was the
22 background.

1 Then it says -- and this is in column 9 at
2 line 17 -- "Process 200 in implementations
3 includes a user selecting from among the available
4 components those components which are relevant to
5 any given system, process, or application."

6 So the system that the '366 is talking
7 about is made up of components. The components
8 may be sources of threats.

9 Q Could a target system and a component be
10 the same thing?

11 A I could conceive of a circumstance, for
12 example, where we might want to call the Bluetooth
13 port a system using the example from before, but
14 it's still the fact that it's a component that
15 we're talking about sources, and I would not
16 generically say that systems are sources of
17 threats. At least as how it's used in the '366.

18 Q So if I have bluejacking as a threat and
19 Bluetooth port as one component, couldn't I also
20 put laptop as another component?

21 A Well, given the examples I've just talked
22 through, I'd say I would need context to determine

1 that. If you have a specific example from the
2 '366, I can answer that if you want to point me to
3 one.

4 Q Well, what more context would you need?

5 A I'd need to see how the term "system" and
6 "components" are being used. In the paragraphs
7 that I read, for example, they're being treated
8 differently. If there's a place where they're
9 being treated in a different way, then I'm happy
10 to look at that part and discuss it with you.

11 Q So you want to look at Figure 10 of the
12 '366 patent?

13 A All right. I'm looking at Figure 10.

14 Q Okay. And then you see there's a large
15 box, and it seems to be labeled "Office Network."
16 Is office network here a component?

17 A You cut out for just a second. Which part
18 did you talk about?

19 Q Right under the heading "End Point
20 Security," so right in the diagram part, there's a
21 big --

22 A Yes.

1 Q -- box and a bunch of little tinier boxes
2 inside that bigger box. The larger box is labeled
3 "Office Network"; is that right?

4 A Yes.

5 Q Is office network a component?

6 A It may just be a matter of perspective.
7 If we are trying to model the threats to -- if
8 we're trying to model the threats to -- I'm going
9 back to the figure -- the threats to office
10 network, that analysis is going to be useful only
11 if we have a better granularity in the components
12 that can be analyzed. With that said, if you had
13 a larger system for which office network became a
14 component, that would be reasonable.

15 I guess, so it depends on what the target
16 system is. If office network is a target system,
17 its model will need to be analyzed in terms of its
18 components. But if there's a larger target
19 system, an office network is a component to that,
20 then that level of granularity -- office network
21 level of granularity, it may be a component.

22 Q You see sort of in the center of

1 Figure 10, you see where it says -- there's a
2 little box that says "BT port"?

3 A Yes.

4 Q And that's the Bluetooth port, right?

5 A Yes, it has the Bluetooth symbol next to
6 it.

7 Q You agree that's a component, right?

8 A From the perspective of office network,
9 that is a component where there is a source of a
10 potential threat.

11 Q And then BT port is included in a larger
12 box labeled "Laptop"; is that right?

13 A That's correct.

14 Q Is laptop a component?

15 A From the perspective of office network...

16 Well, let me talk about this then in
17 context of this specific threat, the bluejacking.
18 The laptop is only a component, meaning a source,
19 for the bluejacking if it has a Bluetooth port.

20 So, for example, if you were to just erase
21 everything in the laptop box and just say I have a
22 laptop; I can't tell if that's a source, which

1 would be a component, for a bluejacking threat
2 unless I knew it had a Bluetooth port, at which
3 point it would end up maybe being this Bluetooth
4 port component.

5 So I can see laptop -- laptop could
6 potentially be a component; it just depends on how
7 we're using it and the context.

8 Q So is it right that what is and isn't a
9 component changes based on context?

10 A Well, within the '366, components, for
11 example, are things that can be put into a
12 database and identified as a source of a threat.
13 So that -- as an example, right? I'm not saying
14 it has to have that, but, as an example, it says
15 components can be put into a database where it
16 identifies the component and the threat.

17 Obviously how you choose to set that up is
18 going to depend a little bit on the modeler, but
19 you could accept a kind of standard set. So we're
20 going to -- as a standard set say that Bluetooth
21 port is going to be in, like, the standard
22 database as a source for a bluejacking threat.

1 If the modeler wanted to change the
2 granularity and say, look, we're just going to
3 assume that all of our laptops have Bluetooth
4 ports, maybe every laptop they're ever going to
5 buy is going to have a Bluetooth port, the '366
6 patent talks about adjusting your models based on
7 context.

8 It mentions if everything is HTTPS, you
9 may remove things related to HTTP issues because
10 you just don't need to deal with those. Well,
11 similarly, it would be like, well, all of our
12 laptops are going to have Bluetooth ports, so
13 we'll have laptop be the source of bluejacking.
14 From the perspective of office network, if laptop
15 is already identified as having a Bluetooth port
16 and, hence, a bluejacking threat that is possible,
17 from the perspective of office network, laptop
18 with that Bluetooth port could be a source of the
19 bluejacking threat.

20 Q So you testified earlier that, you know, a
21 laptop, depending on context, could be a target
22 system; is that right?

1 A Yes, a laptop could be the system you're
2 modeling.

3 Q And to just take a real world example,
4 depending on the context again, you know, a house
5 could be a target system, right?

6 A I know you said depending on context
7 already in your question, but I guess I'd have to
8 see it. I'd have to see the scenario. I haven't
9 thought through that.

10 Q Well, let's go back to your definition
11 first then. You used the term "adverse effects"
12 in your definition. What do you mean by "adverse
13 effects"?

14 A I'm sorry, are we going back to definition
15 of threat?

16 Q The definition of threat in Paragraph 78
17 of Exhibit 2009.

18 A Yes.

19 Well, adverse effects is also
20 context-dependent. It depends on what it is
21 you're trying to protect and what properties you
22 need to maintain.

1 Q So just to come up with a scenario, I want
2 to go back to my real world example of a house.
3 Just one potential -- let's say I want a threat --
4 I want to model the threat of a natural disaster
5 to my house. How would that look like in the
6 context of your definition of a threat?

7 A Okay. So we are not necessarily talking
8 about threats that involve technology or hackers
9 or anything like that?

10 Q Right. So let's back up based on your
11 response there.

12 The '366 patent isn't limited to
13 technology and hackers, right?

14 MR. JACKSON: Object to the form.

15 BY MR. MIDDLETON:

16 Q The '366 patent isn't limited to threats
17 that involve technology, right?

18 MR. JACKSON: Object to the form.

19 BY THE WITNESS:

20 A Well, you've got two parts in there, so
21 let me try and deal with each one separately.

22 So you asked if whether or not it needed

1 to include attackers. Threat modeling is usually
2 done differently from safety modeling. So threat
3 modeling usually is dealing with attacks. The
4 '366 patent also includes language to that effect.

5 BY MR. MIDDLETON:

6 Q So I -- I didn't mean to interrupt. You
7 go ahead.

8 A I was done with the first one. If you
9 want to ask a question before I go on to whether
10 or not it has to be computer-based, we can talk
11 about threats and attacks first if you'd like.

12 Q Sure. Let's go to column 9 and line 66.

13 A Yes, I see that.

14 Q So it says, "For example, if one is
15 modeling the threats involved in commuting to
16 work" -- and then going to the next column -- "for
17 example, if one is modeling the threats involving
18 commuting to work safely, one threat may be
19 freeway collision and one component, which would
20 be correlated with this threat through the
21 database, would be merging onto the freeway,"
22 right?

1 A Yes. I'm aware of this part of the
2 patent. I had interpreted this to be
3 illustrative.

4 But even if we're taking this as a literal
5 threat, I think you would still see the freeway
6 collision from the perspective of threat modeling
7 as attack. Which doesn't necessarily mean malice,
8 but it could mean drunk driver, it could mean
9 somebody that is behaving in a way that's unsafe,
10 but it's not just random chance or a natural
11 disaster.

12 Q A freeway collision can be an accident,
13 right?

14 A It can be, yes.

15 Q And, I mean, an accident can be based on
16 random chance?

17 A Yes, but I'm saying that I think what
18 would make this part of your threat analysis is
19 the fact that there is another human actor
20 involved that is making decisions.

21 When I explain to my students the
22 difference between safety and security, I'm, like,

1 it is true that security has to deal with all the
2 safety issues, it's not like -- but for -- it's
3 for different reasons. What changes security from
4 safety is that security is dealing with conscious
5 actors that are working against you. It's not
6 just like what are the odds that I'll get cancer
7 based on my -- you know, my profile? It is: We
8 are dealing with adversaries.

9 We do include safety issues for sure, but
10 a lot of times those are looked at from the
11 perspective of how would a system become insecure
12 because this safety thing happened.

13 Q So you do include safety issues in threat
14 models, though, right?

15 A Yes.

16 Q And your definition of threat is one or
17 more potential events, right? That, if they
18 occur, can cause adverse effects to a target
19 system?

20 A Yes, adverse effects, in my mind, are
21 relevant to the security of the system, however
22 that's defined.

1 Q I mean, a natural disaster, that could be
2 one or more potential events, right?

3 A It could be, yes.

4 Q And a natural disaster could cause adverse
5 effects, right?

6 A There is the potential that an earthquake,
7 for example, a natural disaster would have an
8 adverse effect on the security of the system. So
9 in that circumstance, yes, I would agree that
10 could be part of a threat model.

11 Q And just to throw out a real world
12 hypothetical here, let's say, like, I'm in
13 California. You know, there's a lot of tech
14 companies in California. And I built my data
15 infrastructure right on a fault line. Wouldn't I
16 want that in my threat model?

17 A It depends. And the reason I say that is
18 even if you built it right on the fault line, that
19 is more understandable with -- it's almost a
20 perfect -- perfectly represented by the statistics
21 in the sense that you can determine what you want
22 to do with that risk from the fault line and the

1 resulting damage and the loss can be calculated in
2 a fairly straightforward manner.

3 Threat modeling deals with a higher degree
4 of unpredictability because you are dealing with
5 humans. You still use probabilities. You still
6 use likelihood when you -- if you're calculating
7 risk and you do your loss event times likelihood.

8 But the thing about a threat model is you
9 are trying to understand how another human being
10 is going to exploit your system.

11 And that may happen because there was a
12 natural disaster. For example, if your system
13 that's sitting on the fault line provides some
14 kind of key security feature, then when that goes
15 down, you may have security vulnerabilities that
16 are a result because of it. But you don't
17 mitigate -- you don't mitigate earthquakes like
18 you mitigate humans.

19 Q So in this scenario then you're talking
20 about in your last example, the -- the target
21 system is the building that I built on the fault
22 line and the adverse effect is that when, you

1 know, that key security feature that I built on
2 the fault line goes down, I might have security
3 vulnerabilities that result because of it?

4 A Sure. That's a -- that's possible.

5 Also, because I referenced it just a
6 little bit earlier, I wanted to point out that
7 what I'm describing here is also language that is
8 discussed in the '366. So I'm looking at
9 column 1, and I'm looking at starting at line 60.
10 "Threat modeling allows a user to analyze
11 potential attack vectors and prioritize
12 vulnerabilities."

13 I'm not saying that you can't include
14 natural disasters and other safety issues in here,
15 but that sentence that I just read is correct; the
16 primary purpose of threat modeling is to analyze
17 potential attack vectors and prioritize
18 vulnerabilities.

19 Q Right. And so the very next sentence of
20 that same paragraph it says, "While some threat
21 modeling involves threats related to computing
22 networks and systems, threat modeling in general

1 encompasses a broader scope and may involve
2 modeling threats and non-computer-related systems
3 and processes."

4 A That's correct. If you recall, earlier I
5 mentioned that I felt like you had two questions
6 for me, and we really only got into the first one
7 which is, you know, does it involve some kind of
8 attacker, right? Does it involve some kind of
9 human agency approach.

10 The second half of your question that I
11 recall from earlier was does it have to be
12 computer systems, and the answer's no. And this
13 is an example where it says, yes, we -- the '366
14 is encompassing threats that go beyond computer
15 systems.

16 Q Understood. I didn't mean to cut you off
17 before. I'm sorry about that.

18 A No, it's fine. I told you we were dealing
19 with two at a time, so I'm just letting you know
20 there was question one, which I gave my answer
21 for, and question two, which is, you know, can it
22 be outside of computer systems, and the answer is

1 yes.

2 Q And can we skip right over to column 2.

3 A Right.

4 Q Line 3. This says, "With regards to
5 modeling computing networks, traditional threat
6 modeling systems and methods exist for assessing
7 risk from potential cyber threats at an individual
8 application level without fully accounting for
9 application-to-application interactions thereby
10 miscalculating organizational risks."

11 Did I read that correctly?

12 A Yes, you read that correctly.

13 Q Now, it says methods exist for assessing
14 risk from potential cyber threats. What are cyber
15 threats?

16 A Well, again, it's a category -- right? --
17 where -- I mean, it's basically just kind of an
18 extension of the question we were just talking
19 about, right? Threats that are in computers and
20 computer networks would be in the category of
21 cyber threats.

22 Q Would malware be another example of a

1 cyber threat?

2 A Well, again, going with the definition
3 that I'm using here for this patent, which is an
4 event, I'd say it would have to be the malware
5 being active; it would have to be actually doing
6 whatever the malicious payload is that it's
7 designed to do.

8 Q Okay. And then so they use another
9 example. Phishing, but the specific act of
10 phishing, so, like, sending an email to an
11 employee's Outlook would be an --

12 A That would be a --

13 Q Sorry. I didn't mean to -- go ahead.

14 A Yes, so the email arriving in -- so,
15 actually, there could be different levels of
16 threat -- right? -- depending on how significant
17 it will be if it happens, right?

18 Like, if it gets to the server, that may
19 be -- it's kind of like the attack tree chain,
20 right? It shouldn't even get to the local mail
21 server, but if it does, it's even worse if it gets
22 down to the user's inbox, and it's even worse if

1 the user then sees it, right? And then of course
2 it's even worse if the user clicks on whatever
3 link is in the phishing email.

4 So there's -- so identifying threats does
5 depend a little bit on how you're modeling it and
6 at what levels you want to, but anywhere along the
7 way, there was an event, right? The mail server
8 received it. That's an event. And that could
9 lead to adverse effects because it may go all the
10 way down the rest of the chain we were just
11 talking about, right? All the way down to the
12 user clicking on it.

13 But you could also choose to model it when
14 it hits the user's inbox. You could choose to
15 model it when the user clicks on it. You know,
16 your model could include all of that.

17 Q And the threat isn't the specific event
18 happening -- maybe that's a bad way to put it.
19 It's not a real example of it happening so much
20 that it is, like, the potential for it happening,
21 right?

22 A Well, I did use in my definition that it

1 is the potential event. Obviously that can
2 include the actual event -- right? -- because the
3 potential is now, you know, 100 percent, I guess.

4 But, yes, so the reason why I was still
5 taking malware out unless it was doing something
6 is because it's not even necessarily potential
7 unless there are other situations that may be
8 true, right?

9 Like, if you've got malware in a form
10 where it can't operate and it will only operate if
11 certain -- I mean, I don't know, maybe receiving
12 it is still an event; it just depends on how you
13 choose to slice up the modeling is all.

14 Q And would the potential for a distributed
15 denial-of-service attack be another example of a
16 cyber threat?

17 A That is a potential event that, if it
18 occurred, would cause adverse effects to the
19 target system, so, yes, that would be a threat.

20 MR. MIDDLETON: Okay. Let's take a
21 ten-minute break.

22 (WHEREUPON, a recess was had.)

1 BY MR. MIDDLETON:

2 Q Dr. Nielson, a few questions about risk.

3 Can we look at Paragraph 80 of Exhibit 2009.

4 A Yes, I have it.

5 Q And here you're discussing the '366
6 patent; is that right?

7 A Yes.

8 Q And this Paragraph 80, you write,
9 "Whereas, risk is the potential impact on a system
10 due to a threat that occurs coupled with the
11 likelihood that a threat will occur"; is that
12 right?

13 A Correct.

14 Q Is this the definition of risk that the
15 '366 patent uses?

16 A The '366 patent does not provide a
17 definition, but this definition is compatible with
18 how it is used.

19 Q So you agree with this definition?

20 A The definition of -- I just want to --
21 risk likelihood times impact is the way I've been
22 using "risk," both in my career and in this

1 patent.

2 Q And that's the definition you applied in
3 your report?

4 A Yes.

5 Q And going back to, you know, the
6 earthquake example where I build a key security
7 feature on a fault line, what would be the risk
8 associated with that example?

9 A Well, I don't have the numbers to build
10 that from, especially given that it's
11 hypothetical, but, again, this definition would
12 apply.

13 Q And, sorry, what more information would
14 you need?

15 A Well, I'd need to have a calculation for
16 likelihood, and I'd need to have a calculation for
17 impact.

18 Q And what calculation of impact would you
19 use?

20 A That would depend, but a couple of
21 examples could be financial. So you could just
22 start with what would be the financial damage to

1 the building. But then, again, as I said earlier,
2 we're talking about a threat analysis we're
3 probably more concerned with what the security
4 impact would be. And so you'd need a calculation
5 for the costs associated with the loss of the
6 security features.

7 Q So one example of a risk would be that the
8 likelihood of loss of the security feature due to
9 the earthquake is very high; would that be one
10 example?

11 A Of a likelihood?

12 Q The likelihood of loss of the security
13 feature due to an earthquake is very high, could
14 that be one example of a risk?

15 A Well, remember, risk is not the
16 likelihood.

17 Q Sure. Provide me one example of risk in
18 this scenario then.

19 A Well, so one way you could do it is if you
20 calculate likelihood as a percentage. And you'd
21 get that maybe from actuarial tables or something
22 like that. Then you would have a percentage. And

1 if your impact was measured in dollars, then you
2 could calculate risk strictly as, like, a -- with
3 a dollar sign.

4 Now, in the '366 patent -- and maybe this
5 is what you were getting at a little bit -- they
6 have quantized risk into things like high-risk and
7 low risk, but if you look at how that's used --
8 and let me turn over here to a place where this is
9 discussed in the '366 patent.

10 Yes, so if you look at column 25, starting
11 in line 8. I can read it if you'd like me to, but
12 I'm going to just kind of summarize here because
13 it's kind of long. It talks about having a list
14 of components. The components are sorted based on
15 their vulnerability level. But separate from
16 that, there is a risk value associated with each
17 one, and that risk has been quantized. So they
18 refer to some of them as very high risks, some as
19 high risks, medium risks, and so forth.

20 So there's both the vulnerability level,
21 which you could derive a likelihood from
22 perhaps -- it doesn't say that, but a person of

1 skill in the art might do that. And then from
2 looking at the impact that would happen if, in
3 fact, the threat resulted in a loss, then you
4 would create some kind of multiplication that
5 gives you a value, and then you quantize that down
6 to these levels of very high risk or high risk and
7 medium risk.

8 Q So you said -- you testified earlier
9 though that risk isn't just the likelihood, right?

10 A Correct.

11 Q So this quantized risk, I mean, is that
12 still risk as you're defining it?

13 A Well, yes. What I'm telling you is that
14 this risk is including in it impact.

15 Q And it's including impact of a threat?

16 A It's including impact of loss based on the
17 threat. So, remember, we talk about threat as
18 potential events, right? But there's only a loss
19 when the adverse impact actually occurs. So one
20 way of looking at impact is to look at actual
21 loss, right?

22 So if we go back to the malware example,

1 if there is an actual loss that results from
2 malware deleting a bunch of really valuable data,
3 then you can talk about the impact. You can also
4 look at impact in terms of expected loss. So you
5 might also base that on other risk analysis,
6 right? But however you look at it, there's the
7 likelihood and the impact from the damage
8 happening.

9 Q What do you mean by looking at impact in
10 terms of expected loss?

11 A Well, you can't always wait for the bad
12 thing to happen in order to calculate risk or else
13 you'd end up with a lot of zero risk, right?
14 Because you multiply by zero, nothing bad has
15 happened yet and, therefore, the risk is zero.
16 But of course it doesn't work that way, right?

17 So if we go back to our example of
18 phishing, there might not be an actual loss until
19 the user who receives the email clicks on the link
20 and loses their credentials, right?

21 But let's say that we're looking at a
22 phishing email reaching the local mail delivery

1 server. Well, we -- there's a number of different
2 ways of doing this. You can -- and that's both in
3 terms of likelihood and in terms of the way you
4 calculate impact, right? But let's just take
5 impact by itself.

6 If you know from experience that across
7 your 1,000 employees, there's 2 employees a
8 year -- sometimes it's calculated on an annualized
9 basis -- 2 employees a year click on phishing
10 emails if they get them. They don't recognize
11 them. They're tricked by them, whatever, right?

12 So now if you receive the phishing email
13 at the delivery server, you could potentially
14 calculate a risk calculation right there and then,
15 right? Which is what's our expected loss? Well,
16 our expected loss is take however much damage we
17 experienced and multiply it by 2 one-thousandths.
18 I mean, it's annualized, so my numbers are a
19 little bit -- I'm kind of doing them off the cuff
20 here without writing them all out.

21 But the main idea is that you're coming up
22 with a likelihood, and you're using that to

1 determine your risk of letting this phishing email
2 land on the delivery server.

3 If you have an organization where 500 out
4 of 1,000 people are clicking on things, then, you
5 know, you can end up with being like, okay, our
6 impact is much higher and so our risk is much
7 higher and we need to deal with this issue more
8 aggressively.

9 Another example would be, like, let's say
10 we're taking a server with data on it. Well, if
11 the data is really valuable data, our risk is
12 higher than another server with exactly the same
13 threats but with lower-value data.

14 And so we can make calculations about that
15 even before the loss occurs, but, I don't know, my
16 preference, I prefer to find as much actual data
17 as possible where it is available.

18 Q So you testified if you have an
19 organization where 500 out of 1,000 people are
20 clicking on things, then you know your risk is
21 much higher and we need to deal with that issue
22 more aggressively. Is that a fair statement of

1 what you testified?

2 A Yes, but make sure you're understanding
3 the context that I testified that in. I was
4 talking about the context of calculating the risk
5 at the delivery server.

6 Q Okay.

7 A Not calculating the risk at the location
8 of the individual click, right?

9 So, here, what I'm talking about is you
10 may do a risk calculation at one level where you
11 take your likelihood times impact and you come up
12 with numbers, and that becomes your impact number
13 if you look at an earlier step in the process
14 where you're, like, well, what's the probability
15 we get to this step? And then from this step, we
16 multiply that by the impact if we have numbers
17 that tell us what's happening or estimating or
18 evaluating what's happening at a later step.

19 Q Understood. But when you're looking at an
20 organization of 500 out of 1,000 people are
21 clicking on these links and the reason you want to
22 look at a risk and look at a risk model is so you

1 can deal with the underlying issue; is that right?

2 A Well, it's so you can prioritize.

3 Q And prioritize what exactly?

4 A Your cybersecurity resources. You only
5 have so many. So if you're in an organization
6 where 2 out of 1,000 are click -- and obviously
7 this is all hypothetical -- if the 2 out of the
8 1,000 are clicking on things is the CEO and CTO,
9 maybe that's still a huge problem.

10 But I'm just providing a hypothetical
11 where I'm just trying to show with numbers how
12 risk can vary based on impact, right? So if we
13 have 2 people out of 1,000, all things being
14 equal, losing their credentials and an
15 organization with 500 out of 1,000 losing their
16 credentials to a phishing attack, then when we
17 look at the risk associated with it coming to the
18 local delivery server -- right? -- before it's
19 delivered, then we can start to say, well, what's
20 the likelihood that it lands on the server, right?
21 It got past some kind of defense. It wasn't even
22 supposed to get onto the server, right? There's

1 some probability that it gets to the local
2 delivery server and that's our likelihood.

3 But at that stage, at that particular
4 place, calculating your potential risk is, well,
5 assuming these emails get delivered, how much
6 damage are we looking at, right? Then you've
7 got -- you know, if you're dealing with an
8 organization where you're losing 500 credentials,
9 that's a higher risk than if you're in an
10 organization where you're losing 2 credentials,
11 all other things being equal.

12 Q So the point of all that -- all the risk
13 analysis is to prioritize your cybersecurity
14 resources; is that correct?

15 A You need to prioritize the cybersecurity
16 resources that go into mitigating threats, and
17 that is based on a risk analysis.

18 Now, it is also true that you can have
19 determinations by executives or by other
20 responsible parties that they're going to accept
21 risk, so -- I should maybe qualify that with it's
22 used in making informed decisions about how you

1 deal with, you know -- well, as you look at risks,
2 without understanding them, it's difficult to
3 address them.

4 Q And what do you mean by "looking at risks
5 without understanding them"?

6 A Well, if I don't know if one risk is a
7 bigger problem than another or if I can't grasp
8 the nature of the risk, then it's fairly
9 meaningless to decide whether you're going to
10 mitigate the risk or accept the risk or transfer
11 the risk.

12 There's a number of different solutions to
13 dealing with risk, but -- you know, for example,
14 like, I refer to the NIST framework quite a bit.
15 You start by identifying the risk, and then once
16 you've identified and kind of analyzed the risk,
17 then you have the information you need to make an
18 informed decision about what you're going to do
19 about it.

20 Q So just to go back to your example of, you
21 know, I have 500 out of 1,000 employees every year
22 clicking on suspicious links, in that scenario, it

1 would probably be, you know, a high priority to
2 deal with that threat by -- and you would
3 understand that by looking at the risk; is that
4 right?

5 A Well, again, I only did this as a
6 comparison -- right? -- so I'm saying I don't know
7 what all their other risks are, so I'm just saying
8 that compared to 2 out of 1,000, it's a bigger
9 issue.

10 When you look at risk, risk is a -- risk
11 is the way that you quantify the challenges that
12 you're facing in an organization, okay? And so if
13 you have an identified risk, that may tell you
14 where you need to go investigate.

15 Now, I want to emphasize this because I
16 know this has come up in this IPR, but a risk
17 doesn't identify your vulnerability, or not
18 necessarily. So if you have a risk that you've
19 calculated, say, from actuarial tables or from
20 other hard data, you may just say, like, well, we
21 know we're losing this many credentials a year,
22 right?

1 And then from that, then it's, like, well,
2 we can choose to mitigate with insurance or we can
3 choose to mitigate with this or we may decide to
4 go do an investigation to try to understand why
5 we're losing all these credentials.

6 But it's the impact times likelihood,
7 however you identify those values for which there
8 are multiple methods.

9 So I just want to emphasize with the risk
10 value by itself, that is an indication of loss or
11 expected loss that is being experienced, and then
12 the organization knows how to deal -- well, or
13 will choose how to deal with that information.

14 Q So in another example you just gave, you
15 gave the example that if you have a risk that you
16 calculated from actuarial tables or from other
17 hard data, you can just say, you know, you're
18 losing this many credentials per year. In that
19 scenario, the losing the credentials is the
20 threat, right?

21 A In that situation, I would say losing the
22 credentials is the adverse impact, not the threat.

1 Q And how would you mitigate losing the
2 credentials?

3 A Well, you couldn't unless you knew the way
4 those were being lost. But if you understood that
5 you were, in fact, having a significant risk --
6 right? -- that there was -- or you were
7 experiencing loss or you were calculating risk
8 based on this likelihood times impact, then if you
9 chose to mitigate, you could dig deeper into
10 identifying sources, and once you identified those
11 sources, then you could mitigate.

12 Q And the matter in which the credentials
13 are being lost is the threat, right?

14 A The event that is causing the loss
15 would -- or the events, there could be more than
16 one -- is what is causing the loss of the
17 credentials.

18 Q So, just to clarify, the event that's
19 causing the loss is the threat?

20 A The event, potential or otherwise, that
21 results in the adverse impact is the threat. So
22 in this case where the adverse impact is losing

1 the credentials, the events, potential events,
2 et cetera, whether it's potential or actual that
3 is resulting in that loss is the threat.

4 Q And loss of credentials could occur
5 through phishing attempts, right?

6 A There are a number of ways that can occur.
7 Phishing attacks could be one. Stolen password
8 file is another. There are a number of different
9 ways that could happen.

10 Q What are some other different ways?

11 A Social engineering, drive-by download,
12 redirected -- what's the word for it? -- it's
13 where you have a fake web page that looks like the
14 real web page. That can be done with DNS
15 redirection or ARP poisoning or some of these
16 other situations. That could result in lost
17 credentials. I mean, even a buffer overflow
18 attack could, depending on what's in memory.

19 Q And buffer flow is a form of distributed
20 denial-of-service; is that right?

21 A No.

22 Q No?

1 A I mean, I suppose there may be -- that's
2 not normally how a distributed denial-of-service
3 attack works. Not normally. I'm not saying it's
4 never happened, but that's not the normal --
5 that's not normally how it works.

6 Q What is a buffer overflow?

7 A So a buffer overflow attack is where you
8 have a computer system that needs to read in some
9 input from the user. So if you have a username
10 and password field, the system needs to have a
11 place set aside in memory to store what the user
12 inputs.

13 So although it may sound just really
14 strange, the language that was used the most for
15 years and years and years and years -- and that's
16 the C programming language, and it still underlies
17 libraries even for other languages -- does not do
18 what's called bounds checking.

19 And so let's say that the C program set up
20 2,000 bytes for somebody to put in their username.
21 Usually it's only going to take 16 bytes, maybe
22 20. So 2,000 is more than enough, right? Well,

1 if the adversary knows -- and there's different
2 ways the adversary finds out -- the adversary can
3 potentially, if there's no manual bounds checking,
4 put in more than 2,000 characters in a way that
5 can potentially overwrite other parts of memory.

6 And overwriting the other parts of memory,
7 you can take control of the system if -- there's a
8 number of caveats. I'm giving you the basic,
9 basic, basic overview. But if you overwrite a
10 certain part of memory that has to do with what's
11 called control flow, then you now can actually put
12 your own code into the system and take control.

13 And a lot of times, the goal is -- it's
14 manifold. Once you have control, you can examine
15 memory, and if there's data in memory, even if
16 you're not running the program, you can pull data
17 right out of memory. Sometimes you're just taking
18 control of the box to turn it into a system that
19 you can use as a foothold to attack other systems
20 on the network.

21 But it -- buffer overflows are some of the
22 worst in terms of if an attacker figures out how

1 to exploit one, that can usually be very, very,
2 very bad.

3 Q I can't recall if you testified about this
4 already, but what is a risk model?

5 A Well, the risk model, that would depend.
6 So actually let me ask you this question first:
7 Do you have a specific part of my report where I
8 refer to a risk model? I just want to see if I'm
9 referring to a specific context before I answer.

10 Q No, I don't have a specific context in
11 mind; I'm just asking for your understanding.

12 A Well, it's -- it depends, and so I'm just
13 trying to understand context.

14 Q What does it depend on?

15 A Well, so, for example, I do discuss in my
16 report that Keenan is disclosing a risk modeling
17 system. So in Keenan, for example, Keenan is
18 providing some systems and methods in order to
19 analyze risk in a system in order to -- as I say
20 in my report, in order to determine insurance
21 premiums, for example.

22 So when we talk about a model, the model

1 is the approaches that we're using in order to
2 talk about and act on risk.

3 Q And by "act on risk," do you mean mitigate
4 risk?

5 A Well, let me give you this as an example
6 of a risk modeling, all right?

7 So we've just read in the newspapers that
8 there was a huge leak of intelligence out of
9 Germany and it leaked and it got to Russia. They
10 don't know how it happened yet, or at least
11 according to the newspapers, they don't know how
12 it happened yet. It's possible they don't know
13 how it happened yet.

14 The thing is, you can look over time at
15 the number of information leaks that you have, and
16 you can calculate a risk model. Okay, we don't
17 know how this information leaked, but we see that
18 we are having these amount of secrets leaked this
19 many times per year over the last 20 years. You
20 construct a risk model where you're, like, okay,
21 let's use this to determine our frequency.

22 And that frequency can also be based on,

1 well, if we know about this many, let's model how
2 many we think are happening that we don't know
3 about based on how many are happening that we do
4 know about.

5 And then you look at the impact. This one
6 that just happened was pretty massive impact. You
7 calculate all of your consequences for that, and
8 you put together a risk model.

9 Now, if you look at the risk model, you
10 will have to decide what are you going to do with
11 it. Based on what the executives in charge
12 decide, they may be, like, you know what? There's
13 always going to be some amount of leaks that
14 happened, and we're not going to do better than
15 this.

16 Or they may be like, wow, we're having a
17 large amount of secrets that gets leaked every
18 year; this might mean we have some systemic
19 issues.

20 From there, mitigation might require
21 investigation; we don't know how the leaks
22 happened yet, but we have to figure them out. So

1 you may conduct an audit, trace things out, run
2 experiments, you may do this, may do that, in
3 order to determine what your actual threats are
4 and then mitigate those threats.

5 Q And the threat in that scenario is the
6 information leak, right?

7 A The adverse impact was the information.

8 Q And the threat is the event that caused
9 the information leak?

10 A The threat is, again, the potential or
11 actual event that results in -- or could result in
12 the adverse impact to the target system.

13 Q Wouldn't the adverse effect be the loss of
14 information to an adversary?

15 A I mean, I -- that's the information leak.

16 Q Sure. The information leak is the event,
17 and the loss of information to Russia is the
18 impact?

19 MR. JACKSON: Object to the form.

20 BY THE WITNESS:

21 A No, the adverse effect was the information
22 leak. We do not know the event that caused that.

1 BY MR. MIDDLETON:

2 Q In the --

3 A Even in your way of phrasing it, there is
4 no identifiable event. All we're describing are
5 the adverse outcomes.

6 Q I'm sorry. Doesn't the term "leak" imply
7 a specific event?

8 A No, that's also a noun, right? It's also
9 the data. It's also the -- this is the leak. So
10 there is data that got to where it should not go,
11 and that was the adverse impact. How that
12 happened, unknown.

13 Q So the adverse impact is that data got to
14 where it should not go; is that right?

15 A That was an adverse impact, the data went
16 where it shouldn't.

17 Q And the thing that caused the data to go
18 where it shouldn't is the information leak?

19 A Well, the event -- I guess in this case
20 there would be multiple events -- the events that
21 obtained the information and the events that
22 transmitted the information would be part -- would

1 be at least two events that were the causes. What
2 exactly caused those, we don't know.

3 Q So another example of a risk model could
4 be the risk of damage to houses due to Atlantic
5 hurricanes in the United States; is that fair?

6 A You could narrow a model down, a risk
7 model down to where this was only one potential
8 threat that is being identified, right? You could
9 arbitrarily be, like, I'm only going to consider
10 one threat and build a risk model around it.

11 Generically risk models look at the impact
12 and the likelihood but do not necessarily limit
13 the sources. So taking your example, we can talk
14 about threats that are -- threats -- we can talk
15 about risks that are damage to houses.

16 We can break that down further. Maybe
17 there's different reasons to have it broken down
18 further, and maybe we would break it all the way
19 down to hurricanes. But risk models in general
20 are not so limited.

21 Q If I did break it down just to that, you
22 know, that sort of risk model to the risk of

1 Atlantic hurricanes in the United States, that
2 risk model is identifying the threat, right?

3 A No, I wouldn't say that that's the case.

4 Q So maybe I should rephrase my question.

5 The risk of damage to houses due to
6 Atlantic hurricanes in the United States, that
7 risk model is identifying Atlantic hurricanes as
8 the threat, right?

9 A It's certainly naming it. I guess the
10 key thing, like, going back to what a threat model
11 is, a threat model is attempting to identify where
12 "identify" has maybe a stronger connotation than
13 just to name it.

14 So if you look at threat modeling, for
15 example, threat modeling attempts to understand
16 the causes, what's going on, why is it going on.
17 The identification is understanding the nature of
18 the threat.

19 Risk models, even when they're narrowed
20 down to a single threat, have no requirements in
21 understanding the threat. At this point, it is
22 simply an impact times likelihood, and that's what

1 the model is built around.

2 Q So you testified in your report that
3 threats and risks are different concepts; is that
4 right?

5 A I did.

6 Q But people in the cybersecurity industry
7 sometimes use the words "threats" and "risk"
8 interchangeably; isn't that right?

9 A I think people in the cybersecurity
10 community understand that those terms are
11 distinct, and that's well-documented.

12 Q But sometimes in publications, someone in
13 the cybersecurity industry might identify risk
14 when they really mean threats; isn't that right?

15 A Well, I mean, I don't know that I think
16 this concept is particularly controversial. I
17 mean, I note in my report that even IriusRisk's
18 expert Mr. Hurlbut agreed with my definition --
19 not my definition, but the definition I used of
20 likelihood times impact and agreed that there's
21 not a one-to-one relationship.

22 I just don't think this is a controversial

1 concept that threat and risk are different.

2 Q Sure. And I'm not asking you whether
3 threats and risk are different; I'm just asking
4 you whether people in the cybersecurity industry
5 sometimes use the words "threats" and "risks"
6 interchangeably?

7 A I am sure that somewhere out there
8 somebody somewhere has done the word "risk" when
9 they meant "threat" and vice-versa. But that's
10 not that the cybersecurity community has that
11 view; it's that somebody maybe was misspeaking or
12 speaking quickly or not assuming that the words
13 they were talking about would be used in
14 litigation.

15 MR. MIDDLETON: I think this is a good
16 time for another break. Can we take a slightly
17 longer break, maybe 20, 25 minutes for lunch?

18 MR. JACKSON: Is that okay with you, Seth?

19 THE WITNESS: Fine with me.

20 MR. JACKSON: Okay. I don't know if I'll
21 have time to get lunch in that time, but --

22 MR. MIDDLETON: If you want to take

1 longer, Don, we can.

2 THE WITNESS: Well, I don't know if we
3 want to go off the record for a discussion about
4 schedule, but I'd like to ask --

5 MR. JACKSON: Let's go off.

6 MR. MIDDLETON: Let's go off.

7 (WHEREUPON, a recess was had.)

8 BY MR. MIDDLETON:

9 Q Dr. Nielson, just to go back to your
10 definition of risk and just to confirm again, your
11 definition of risk is the likelihood of a threat
12 by the impact of that threat; is that correct?

13 A No.

14 Q Let's go to Paragraph 80 of your report --
15 your declaration, I'm sorry. And it's
16 Exhibit 2009.

17 A Yes.

18 Q And there you testified about the '366
19 patent, and you mentioned earlier that you agreed
20 with the definition below where risk is the
21 potential impact on a system due to a threat that
22 occurs coupled with the likelihood that a threat

1 will occur, correct?

2 A Yes. So risk is the impact of a loss --
3 like in this case where we're talking about a loss
4 from a threat -- occurred with the likelihood of
5 that loss, in this case where a threat is likely
6 to occur.

7 Q So if you were trying to determine risk,
8 you would need to know the likelihood of a threat,
9 right?

10 A If the threat is what you are dealing
11 with, then you would need to know -- well, it's
12 the likelihood of loss due to the threat.

13 Q So you would need to know the likelihood
14 of loss due to the threat, right?

15 A So, again, in the situation where you're
16 talking about risks related to threats --
17 right? -- so we talked about risks where you don't
18 know exactly what the threat was, right? So in
19 situations where you are talking about risks
20 associated with threats, then you would need
21 information such as how likely is this threat to
22 actually result in a loss.

1 Q Can we look at Figure 8 of the '366
2 patent?

3 A Sure.

4 Yes, I have it.

5 Q Okay. And Figure 8 is showing the risks
6 associated with certain threats, right?

7 A There is a risk that is associated with
8 threat, yes.

9 Q And that middle column there that just
10 says "Risk" --

11 A Actually, you know what? I misspoke. I
12 misspoke. It's not associated with threat. If we
13 look down in the text, the text says it's
14 associated with a component. So let me pull that
15 up here.

16 Well, they're not specifically citing
17 Figure 8. Let me read this out, and then I'm
18 going to go see if it has a different narrative
19 for Figure 8. But this is in column 25 -- I
20 mentioned this earlier -- it starts in line 8.
21 "In implementations an interface of the system may
22 list the most vulnerable in ascending/descending

1 order along with the risk level for each listed
2 component."

3 Q If we go to column 14, line 5.

4 A Yes.

5 Yes, here in line 5, it says, "For
6 example, Figure 8 shows interface 800 which is
7 accessed by selecting 'threats' sub-menu item.
8 The title 'threats' is shown near the top of a
9 list of threats which are organized into rows and
10 columns showing each threat's name, risk level,
11 and attached labels."

12 Q So the risk here is associated with the
13 threat, right?

14 A For Figure 8, it -- this says it's
15 associated with the threat.

16 Q Now, if I was just to take that middle
17 column, the column that just says "Risk," and if I
18 was just to remove that and have that be my only
19 information on the diagram, would that be --

20 A Wait. I'm sorry. The only information
21 would be the "Risk" column or without the "Risk"
22 column?

1 Q With the "Risk" column.

2 A And that was the only information. So we
3 got rid of the "Name" column and the "Labels"
4 column?

5 Q Yes.

6 A Okay.

7 Q Would that sort of diagram or column be
8 helpful to you in performing a risk analysis?

9 A It wouldn't be helpful, but it also
10 wouldn't be helpful with the information that we
11 have here. This is -- this is not a -- when you
12 have a risk associated with buffer overflow,
13 they've associated it with a threat, but there's
14 no context. That's -- there's nothing useful
15 about that either.

16 Q Well, wouldn't one useful thing -- so you
17 would need to know what the threat is related to
18 or the source of that threat in order for it to be
19 useful -- right? -- in order to mitigate it?

20 A Well, no. I think what I'm saying is, so,
21 first of all, these would be put into the model,
22 right? So these -- this is a description of

1 threat that can be identified in the model.

2 But in terms of doing a risk analysis, the
3 information that you would need in order to do a
4 risk assessment would also include things like the
5 data that's at risk so you have some concept of
6 impact.

7 Q Can we look at claim 1 of the '366 patent?

8 A Sure.

9 I have it.

10 Q And then so column 43 --

11 A Yes.

12 Q -- that's claim 1.

13 And then we'll go down to line 50. I just
14 want to look at that claim limitation. And this
15 limitation --

16 A Yes, I see it.

17 Q This limitation reads, "Displaying on the
18 one or more user interfaces a relational diagram
19 of one of a system and application and/or process
20 using visual representations of the threat model
21 components correlated with a subset of third-party
22 diagram components, the relational diagram

1 defining a threat model."

2 So in claim 1, the relational diagram
3 that's defined describes the threat model; is that
4 right?

5 MR. JACKSON: Objection.

6 BY THE WITNESS:

7 A It defines a threat model.

8 BY MR. MIDDLETON:

9 Q If we look at Figure 10 of the '366
10 patent.

11 A Figure 10?

12 Q Yes.

13 A Yes, I have it.

14 Q Does Figure 10 show a threat model as
15 defined by the '366 patent?

16 MR. JACKSON: Objection.

17 BY THE WITNESS:

18 A Are you asking if it shows the A threat
19 model from claim 1?

20 BY MR. MIDDLETON:

21 Q Yes.

22 A I don't think I have done that analysis.

1 I have not -- well, let me double-check and make
2 sure. I don't believe I have that analysis in my
3 report.

4 Q Well, let's step back a little bit. We
5 talked about Figure 10 previously, and we talked
6 about the various components in Figure 10; is that
7 right?

8 A Figure 10 does include threat model
9 components, yes.

10 Q And one example that we talked about
11 earlier was the BT port, and depending on
12 perspective, it could be the laptop or the office
13 network, depending on the context?

14 A The laptop with a Bluetooth port could be
15 a component for bluejacking, for example. And you
16 could have an office network with a laptop with a
17 Bluetooth port that would be a source of
18 bluejacking -- office network I think. Making
19 sure I said office network and not office.

20 Q And another component in the laptop
21 section is Wi-Fi port, right?

22 A Wi-Fi port is a component if there's a

1 threat identified associated with that -- with
2 this as a source.

3 Q And what is the -- so does this diagram in
4 Figure 10, does this diagram identify any specific
5 threats?

6 A The '366 patent explains it this way. And
7 I'm starting at the bottom of column 16. This is
8 the last line.

9 "From interface 1000, the user may select
10 a desired component and drag it to the desired
11 location on the canvas, and by dragging multiple
12 items, the user may begin to add the components of
13 a system, application, or process to be modeled.

14 "By non-limiting example, Figure 10 shows
15 interface 10 with a relational diagram (diagram
16 1004) already fully created by the user. As can
17 be seen, the user has dragged multiple components
18 onto the canvas 1002 and has defined various
19 relationships between them.

20 "The user dragging components to the
21 canvas is one way in which the user selects
22 relevant components or relevant sources as

1 described with respect to Figure 2, and it is from
2 these relevant components (relevant sources) that
3 the system identifies relevant threats by
4 identifying the threats that are associated
5 through the database with those components."

6 Q But the threats aren't displayed on
7 Figure 10, right?

8 A Well, there is a representation of this
9 relational diagram in Figure 10.

10 Q Is that a yes, that the threats aren't
11 displayed?

12 A The system is displaying components that
13 include identified threats. So, again, I'm not
14 entirely sure what you would be looking for for it
15 to say bluejacking happening, but the threat
16 bluejacking is associated with the Bluetooth port
17 component that is displayed there.

18 Q And what are some other threats that could
19 be associated with the Wi-Fi port component?

20 A Well, I mean, I'm sure there are a number,
21 just like there are multiple that could be
22 associated with the Bluetooth port. Would you

1 like me to look through the patent for ones they
2 may have identified?

3 Q No, just ones that you would understand
4 may or may not exist.

5 A Well, I mean, that depends on the
6 database, right? Like, the database is what
7 associates the threats with the threat sources.
8 So that depends on what's configured.

9 Q So Figure 10 also shows relationship
10 between the -- relationships between the
11 components, right?

12 A It shows some relationships between
13 components, yes.

14 Q And, for example, one relationship is
15 represented between Wi-Fi port and Wi-Fi access
16 point by an arrow?

17 A Yes.

18 Q Can we go to claim 1 again, column 43.

19 A Sure.

20 I have it.

21 Q Line 30 -- 31 where it says, "The one or
22 more mapping files correlating the threat model

1 components with visual diagram components of a
2 third-party software application."

3 And what is your definition of
4 "correlating" here?

5 MR. JACKSON: Object to the form.

6 BY THE WITNESS:

7 A So while I did not provide a definition
8 that covers all possible meanings of "correlated,"
9 one example of what correlation is would be what's
10 described, for example, in dependent claim 5. It
11 says, "Wherein, determining for the subset of
12 third-party diagram components correlated threat
13 model components comprises."

14 So this is determining correlated
15 components, or, in my mind, that would be the same
16 thing as correlating, and that involves doing a
17 lookup and finding a match.

18 There are some other requirements there,
19 but certainly the correlating is finding that
20 there is a relationship defined between the one
21 and the other. I think that would be a fair
22 example of correlating, but obviously I'm not

1 suggesting that that's somehow the -- you know,
2 all correlating means that.

3 BY MR. MIDDLETON:

4 Q So is it fair to say one example of
5 correlating is associating one component with
6 another component? And in the case of claim 5, it
7 would be associating a threat model component with
8 a third-party diagram component.

9 A Just trying to say that in the forward
10 direction. What we have in column 43 in claim 1
11 is that the mapping file has to correlate a threat
12 model component with a third-party diagram
13 component.

14 And as I explained in my report,
15 third-party components are independent -- are
16 components from independent third-party software
17 applications while the threat model components are
18 elements of the native software. I'm reading from
19 Paragraph 95 of my report, of which there are then
20 visual representations.

21 So what we have in column 43 in claim 1 is
22 a mapping file that is correlating threat model

1 components, which are from the native application,
2 with visual diagram components of the third-party
3 or non-native application and associating them
4 together if the mapping file would provide the
5 correlation.

6 MR. MIDDLETON: Can we look at
7 Exhibit 1004.

8 THE TECHNICIAN: One second.

9 (WHEREUPON, Nielson Exhibit No. 1004 was
10 presented to the witness.)

11 BY THE WITNESS:

12 A Okay. I have Exhibit 1004 open.

13 BY MR. MIDDLETON:

14 Q And this is the Keenan reference, right?

15 A Yes, it is.

16 Q And did you review this reference in
17 advance of your deposition?

18 A I did.

19 Q Could we go to column 16, line 45 to 48.

20 A Yes, I have it.

21 Q And do you see where it says, "A technical
22 risk measurement view 708 uses color to represent

1 different types of risks (e.g. cyber,
2 environmental, accidental, et cetera)"?

3 A I see that, yes.

4 Q This is saying that Keenan's system
5 discloses color-coding its diagram views based on
6 the types of risks such as cyber, environmental,
7 and accidental; is that right?

8 A It states it uses color for different
9 types of risks, for the different types that you
10 read off.

11 Q And what are types of risks?

12 A They're just categories. So, you know,
13 cyber risks and environmental risks relate to
14 risks from different types of problems, whether
15 you're having cyber losses or whether you're
16 having environmental losses.

17 Q And how would you determine the type of
18 risk?

19 A I mean, some of that is a little
20 subjective. You could define computers as causing
21 environmental risk -- right? -- from the amount of
22 electricity used. But obviously there are some

1 more bright-line distinctions. If I have
2 electronically stored data that is somehow stolen,
3 you know, that's data that's stored in cyberspace
4 and the loss is from cyberspace.

5 BY MR. MIDDLETON:

6 Q So one thing insurance companies do is
7 provide life insurance, right?

8 A Well, I am not an expert in insurance. I
9 myself have some life insurance, so I reasonably
10 conclude that life insurance is a product provided
11 in the marketplace.

12 Q And with life insurance, the insurance
13 company's required to pay out the policy when
14 someone dies, right?

15 A I do not know all the legal limitations,
16 but typically there is an expectation that
17 policies will be paid out when somebody dies.

18 Q So in this scenario, the risk to the
19 insurance company is the risk of -- risk of loss
20 that occurs when someone dies, right?

21 A Well, I'm not an insurance expert, but
22 that's not even my amateur understanding.

1 Q So what would be your understanding?

2 A Again, I am speaking as a non-expert, so
3 you would need to speak to an insurance expert if
4 you wanted a more detailed insider's view, but my
5 understanding of insurance is that the risk is
6 that the insurance company pays out more than they
7 take in above thresholds they define.

8 Q And that risk occurs when someone dies,
9 right?

10 A Well, no, everybody is going to die. So
11 especially if you're talking about whole life
12 policies like I have, they absolutely know they're
13 going to pay out someday; that's not a risk.

14 Q So if the risk is that the insurance
15 company pays out more than they take in above
16 thresholds they define, then the event that causes
17 that is somebody dying at a certain time?

18 A I'm not sure at this point. You're
19 reaching the end of my understanding as an
20 insurance expert, as I'm not one.

21 I don't know how they model their threats
22 or if they call them threats or if they consider

1 that threat modeling that they then use to
2 determine risk. I suspect that they are not
3 treating it like a threat-model-based analysis for
4 the reasons we've discussed earlier, that there
5 isn't really a threat actor and a human operating
6 against them.

7 So while I suspect that there's not any
8 kind of threat model involved, I'm not an expert
9 enough to know how they develop all of their
10 systems.

11 Coincidentally, I have helped insurance
12 companies, but related to cyber threats. So,
13 that, I can talk about.

14 Q What kind of cyber threats have you helped
15 insurance companies with?

16 A Well, they deal with financial systems,
17 and so they deal with the sort of cybersecurity
18 threats you'd expect.

19 It's actually -- so I worked with one
20 very, very large insurance company. I guess this
21 was tangential to their business. They had
22 financial components for their employees. Like,

1 their employees had financial systems, retirement,
2 et cetera. And I was evaluating the adequacy of
3 their security -- the vendor's security to the
4 insurance company for providing tech components of
5 the retirement and other financial offerings they
6 had for their employees.

7 MR. MIDDLETON: Can we look at
8 Exhibit 1005.

9 THE TECHNICIAN: One second, please.

10 (WHEREUPON, Nielson Exhibit No. 1005 was
11 presented to the witness.)

12 BY THE WITNESS:

13 A I have 1005.

14 BY MR. MIDDLETON:

15 Q Can we look at column 4, line 31.

16 A Yes, I have that.

17 Q Do you see where it says, "In some
18 embodiments, the visualization model 116 generates
19 and renders the base layer 202 to visualize a
20 company's application architecture (e.g., suites
21 of software applications and relationships among
22 the software applications) as components in a

1 map"?

2 A Yes, I see that.

3 Q So this says, for Zheng's system,
4 visualize a company's application or architecture
5 as components in a map.

6 Application architecture can include
7 suites of software applications and the
8 relationships among those applications, right?

9 A The application architecture according to
10 Exhibit 1005 says that that could be suites of
11 software applications and relationships among the
12 software applications.

13 Q So an application architecture could just
14 mean the various suites of applications that a
15 company has?

16 A I mean, obviously some part of it is the
17 company's, but there are suites of software
18 applications and relationships among the software
19 applications that it listed as an example of the
20 architecture.

21 Q So could Microsoft Office be an example of
22 a suite of application architecture -- in the

1 application architecture -- a suite of software
2 applications in the application architecture?

3 A Did you say "and" or "in"?

4 Q Let me rephrase the question.

5 Could Microsoft Office be an example of
6 one such suite of software applications in the
7 application architecture?

8 A Yes, Outlook could be -- I'm sorry, did
9 you say Outlook? You said Microsoft which?

10 Q I said Microsoft Office.

11 A Okay. Well, Microsoft Office is a suite
12 of applications, and certainly those applications
13 could be the types of applications that are in
14 here. So yes.

15 Q And you mentioned Outlook. So Outlook
16 could be another example?

17 A That's part of Microsoft Office suite.

18 Q Can we look at column 4, line 52.

19 A Yes, I have it.

20 Q And do you see where it says, "Based on
21 the received information, the visualization module
22 116 can render, on a computer display, the base

1 layer 202 by graphically depicting components of
2 one or more application suites as components in a
3 map"?

4 A Yes.

5 Q So this is saying, you know, the
6 visualizations of the application architecture are
7 displayed on a display using graphical depictions;
8 is that right?

9 MR. JACKSON: Object to the form.

10 BY THE WITNESS:

11 A This sentence says that you can depict
12 what is essentially that application architecture
13 as a visual physical map.

14 BY MR. MIDDLETON:

15 Q And specifically you can graphically
16 depict the components of one or more application
17 suites as components in that map, right?

18 A In the visualized map, right? So this is
19 describing taking those components and laying them
20 out in a visualization, and it's describing that
21 visualization as a map.

22 I want to distinguish that from the

1 mapping files that we have in the '366 patent.
2 The word "map" does not mean the same thing in
3 these two uses.

4 Q I understand that. I think my question is
5 almost literally reading from the sentence. I
6 mean, I'm asking if the system can graphically
7 depict components of one or more application
8 suites as components in a map.

9 A Of course you're reading the sentence
10 correctly. I'm just making sure the word "map" is
11 correctly understood.

12 Q And graphical depictions of those
13 components can include, you know, various shapes
14 and symbols that represent those components,
15 right?

16 A Yes, a visualization includes shapes and
17 symbols.

18 Q So there are shapes and symbols in Zheng
19 on a display that represent the application
20 architecture?

21 A The application architecture is depicted
22 graphically that would involve using shapes and

1 symbols for the depiction.

2 Q And how does Zheng's system know which
3 shapes are associated with which software
4 applications in the application architecture?

5 MR. JACKSON: Object to the form.

6 BY THE WITNESS:

7 A The way Zheng describes this -- and we can
8 see this in the same column just a paragraph up --
9 is it says -- this is starting on line -- well,
10 let's just start in line 28.

11 "To generate and render the different
12 types of the multi-layered structure 200, the
13 visualization module 116 can receive and process
14 data from a variety of sources as illustrated in
15 Figure 1. In some embodiments, visualization
16 module 116 generates and renders the base layer
17 202 to visualize a company's application
18 architecture (e.g. suites of software applications
19 and relationships among the software applications)
20 as components in the map.

21 "Thus, the base layer 202 can be defined
22 by application architecture and graphically

1 constructed" -- graphically constructed -- "as a
2 map to mirror the application landscape. The data
3 used to construct the base layer 202 can be
4 gathered and provided to the visualization module
5 116 from sources related to application
6 architecture. For example, characteristics of
7 each software application (e.g. interaction with
8 other applications relative size, et cetera) can
9 be used to generate features of the base layer 202
10 in a map-like environment."

11 Q So to generate the visualization, Zheng's
12 system receives and processes data from a variety
13 of sources; is that what this is saying?

14 A Well, the visualization module receives
15 and processes data from a variety of sources, as I
16 read, so it uses that data to generate the shapes
17 that Zheng represent the suites of software
18 applications. In this paragraph I didn't read
19 anything about specific types of shapes.

20 What it did say is it could look at
21 features and then generate visual features based
22 on those. So if it was a large application, it

1 could have that be an attribute, and then it could
2 generate a large shape. If it has a lot of
3 connections between software, then the visualized
4 representation would show that software having
5 a lot of -- in the next paragraph, like roads,
6 like it's got a lot of roads to other pieces of
7 software.

8 Q So you mentioned that, like, if you had a
9 large application, then the Zheng system could
10 generate a large shape. How would it do that
11 exactly?

12 A Well, I'm just reading what Zheng says.
13 "For example" -- this is quoting from Zheng,
14 line 40 here in column 4. "For example,
15 characteristics of each software application (e.g.
16 interaction with other applications, relative
17 size, et cetera) can be used to generate features
18 of the base layer 202 in a map-like environment."

19 Q And how does Zheng's system know which
20 features relate to which shapes?

21 MR. JACKSON: Object to the form.

22

1 BY THE WITNESS:

2 A I don't see any explanation, at least in
3 this paragraph, from Zheng of how it does that. I
4 don't think Zheng explains anything other than it
5 just says it doesn't.

6 BY MR. MIDDLETON:

7 Q And what is your understanding of how a
8 system like Zheng's might associate shapes with
9 specific features?

10 MR. JACKSON: Objection.

11 BY THE WITNESS:

12 A I mean, somewhere there would be
13 instructions that would tell the program how to
14 draw the graphical display. You know, obviously
15 that could be done in a lot of different
16 programming language or a lot of different
17 algorithms.

18 BY MR. MIDDLETON:

19 Q Could it be done with a database table?

20 MR. JACKSON: Objection.

21 BY THE WITNESS:

22 A Well, I'm not sure. If we're going to do

1 something like a relative size, that sounds more
2 like it's a dynamic calculation and not something
3 that would be in a database.

4 (WHEREUPON, discussion was had off the
5 stenographic record.)

6 BY MR. MIDDLETON:

7 Q Can we look at column 4, line 64.

8 A Yes, I have it.

9 Q So column 4 line 64 says, "Figure 2 shows
10 an exemplary multi-layered structure 200 that can
11 be rendered in a computer display by the
12 visualization model 116 of the system architecture
13 in Figure 1"; is that right?

14 A I think we must be in the wrong spot. I'm
15 in column 4, line 64. It says, "In some
16 embodiments, to gain further levels of
17 abstraction, a map can have..."

18 MR. JACKSON: Which exhibit are you
19 referring to?

20 MR. MIDDLETON: Zheng, 1005.

21 BY THE WITNESS:

22 A Column 4, line 64 is in the middle of a

1 sentence. It starts with, "Embodiments, to gain
2 further levels of abstraction, a map..."

3 BY MR. MIDDLETON:

4 Q Let's try column 3, line 64.

5 A Yes.

6 Q So here this says, "Figure 2 shows an
7 exemplary multi-layered structure 200 that can be
8 rendered in a computer display by the
9 visualization module 116 of the system
10 architecture of Figure 1," right?

11 A Yes.

12 Q And if you keep going, this bleeds onto
13 column 4, which is probably where I got column 4
14 from. "As shown, the multi-layered structure 200
15 includes four different overlaying layers, with
16 the base layer 202 representing at least a portion
17 of the company's application architecture."

18 A Yes.

19 Q So this is saying Zheng discloses a
20 multi-layered visualization structure, right?

21 A Yes, Zheng has multiple layers that are
22 visualization.

1 Q And then one of those layers is the base
2 layer?

3 A One of those layers is the base layer 202.

4 Q And if you keep reading column 4 -- you
5 can read it to yourself if you like -- you would
6 agree that one of those other layers is the
7 threat-modeling layer?

8 A There is layers including threat modeling
9 of perceived threats, a layer representing
10 security controls, and a layer representing
11 realtime or near realtime actual threats, and a
12 layer representing simulated data flow throughout
13 the application ecosystem.

14 Q And these layers can overlay the
15 foundational map layer, right?

16 A That is how I understand Zheng, yes.

17 Q And then can we go to column 5, line 12.

18 A Yes, I have it.

19 Q And this says, "Generally, data in the
20 threat modeling layer 204 can be organized into
21 threat agents, vectors, and targets. The threats
22 can also be categorized into different types."

1 You see that, right?

2 A Yes.

3 Q What are types of threats in Zheng?

4 A I don't see Zheng defining the types.

5 Q So what is your understanding of different
6 types of threats?

7 A Well, Zheng does say that the threats can
8 also be categorized into different types. So it's
9 not uncommon to create taxonomies; like, I'm going
10 to group these types of threats together and I'll
11 group these types of threats together.

12 Q Could cyber threats be one type of
13 taxonomy?

14 A For Zheng, I don't think so because in
15 Zheng, I would have to guess that all of the
16 threats they're dealing with would be cyber
17 threats in one way or another.

18 Q So their categorizations would get more
19 granular?

20 A Well, again, Zheng doesn't define it. But
21 it's not uncommon -- so taxonomies are to whatever
22 extent they're useful, right? The attack does

1 what the attack does.

2 But if it's helpful, the defenders or the
3 owners of the assets to be able to group certain
4 types together, Zheng talks about being able to
5 turn off certain types and be able to process
6 based on type, but that's a label. Like, I'm
7 labeling this type of attack and this, you know,
8 type of threat and then that's for the benefit of
9 the defender or the asset owner.

10 Q If we continue down the same column, the
11 next sentence says, "Each threat can be visually
12 associated with at least one of a threat actor
13 application, a threat target application, and a
14 displayable vector connecting the two to represent
15 and visualize a particular attack modeling."

16 A I see that.

17 Q So the threat-modeling layer associates
18 threats with threat target applications; is that
19 correct?

20 A Well, in this case, the threat actor would
21 be where the attack is coming from, and then the
22 target would be what's being tasked, and then the

1 displayable vector would connect the two.

2 Q And the threat target applications, are
3 those just applications in the application
4 architect?

5 A Could be. That would be a legitimate
6 threat target application.

7 Q So when you overlay the threat-modeling
8 layer on top of the -- so let me step back.

9 The application architecture is found in
10 the base layer, right?

11 A Correct.

12 Q And when you overlay the threat-modeling
13 layer, that's when you see the threats and the --
14 which applications are associated with those
15 threats, right?

16 A That seems to be some of the description.
17 There was a description earlier that, using this
18 map analogy, it was suggesting that you would
19 overlay, for example, the analogy it uses is an
20 accident. Like, you could overlay an accident on
21 a road, you could overlay an attack on a route,
22 and the visualization would combine the two.

1 Q And just so I understand, in this
2 scenario, the road is the application?

3 A Well, it describes it as a route, so a
4 connection between applications. What I was
5 trying to illustrate here is what Zheng says is
6 you have a set of icons that represent the base
7 layer. So, for example, it's got some kind of
8 icon that looks like a road in this example.

9 And then it says here -- this is in
10 column 4, line 24 -- "In general, the warning
11 signs and icons displayed in each layer can
12 represent the type of threat or control use to
13 mitigate the threat for the visualization."

14 So if you've got some application, which
15 it was mapping in this visualization to a city,
16 then if that's a target, there would be some kind
17 of icon representing that that's a target.

18 Q And so the icon representing that the
19 city's a target would be found in the
20 threat-modeling layer, right?

21 A It would be visualized in the
22 threat-modeling layer. It would be overlaid --

1 you'd get a composite view.

2 Q Can we go to column 8, line 25.

3 A Yes, I have it.

4 Q And this reads, "In some embodiments, at
5 least one database table is used to store data for
6 each layer and for each possible
7 combination/interaction of the layers"; is that
8 right?

9 A Yes.

10 Q So this is saying that Zheng's system uses
11 a database table to store data for each layer and
12 for the various combinations/interactions between
13 the layers, right?

14 A In at least some embodiments, database
15 tables are used for storing data about each layer
16 and the possible combinations or interactions of
17 the layers.

18 Q So when the threat-modeling layer
19 interacts with other layers, that combination of
20 layers and the interaction of those layers it
21 would be stored in the database table, right?

22 MR. JACKSON: Objection.

1 BY THE WITNESS:

2 A Data about that would be stored.

3 BY MR. MIDDLETON:

4 Q And what type of data is Zheng's system
5 referring to?

6 A Well, if it's displaying that there's a
7 threat under attack, that would be stored in the
8 database. So here's an active threat would be
9 something I imagine would be stored in the
10 database.

11 Q I'm sorry, in your testimony you said
12 "there's a threat under attack." Did you mean a
13 threat target application under attack?

14 A I meant to say a threat that was actually
15 being actualized, right? A threat could be a
16 potential event but if there's -- it talks about
17 realtime in Zheng -- right? -- where this is
18 something that's actually occurring right now.
19 The fact that something is occurring right now
20 could be stored in the database.

21 Q And would it also store in the database
22 tables which applications in the base layer are

1 threat target applications?

2 MR. JACKSON: Objection.

3 BY THE WITNESS:

4 A Well, so if you look down at the same
5 paragraph we're talking about -- right? -- in
6 column 8, this is starting on line 33, it
7 discusses having three active layers. One is the
8 base layer -- well, let's see. No, that's the
9 threat-modeling layer, the security controls
10 layer, and the threat update layer. It discusses
11 creating a database tables that represent
12 interactions between them.

13 So, for example, it lists each of those
14 layers as an individual database table, which
15 would be data for each of those layers
16 individually, and then it lists all possible
17 combinations, so AB, AC, BC, and ABC. So
18 presumably data related to their interactions
19 would be stored in the appropriate tables.

20 BY MR. MIDDLETON:

21 Q Can we go to Zheng column 3, line 28.

22 A Yes, I have it.

1 Q This says, "Specifically, by utilizing a
2 visualization approach like cartography,
3 application architecture can be represented in a
4 comprehensible view that enhances security and
5 risk analysis."

6 A Yes, there's a misspelling of
7 "comprehensible" but, other than that, that is
8 correctly read.

9 Actually, that might not be a misprint.
10 Hold on a second.

11 Q It might have been a misread on my part.

12 A I think it is actual "compressible." So
13 it's spelled c-o-m-p-r-e-s-s-i-b-l-e. So when you
14 first read it off, I'm like maybe that's just a
15 misprint for "comprehensible," but I think it is
16 "compressible."

17 Q And compressible would just mean you could
18 minimize the view?

19 A I mean, based on what it's describing with
20 these different layers, I imagine that it's
21 suggesting that you can reduce the information
22 that you need to look at to something that's

1 manageable --

2 Q Yeah, and --

3 A -- look through and see.

4 Q And Zheng discloses that you could
5 visualize any combination of layers at a time,
6 right?

7 A It suggests that you can layer -- that you
8 can visualize based on whichever set of layers you
9 would like to view.

10 Q And when it talks about its visualization
11 approach, it says approaches like cartography,
12 right? So cartography is just being used as one
13 example here, right?

14 MR. JACKSON: Objection.

15 BY THE WITNESS:

16 A That is the example that it uses
17 throughout. All of the descriptions, all of the
18 explanations, all of the way it's described are
19 described within that example. So if there are
20 other ways of doing it, I don't know what they are
21 without those descriptions.

22

1 BY MR. MIDDLETON:

2 Q So cartography is the practice of drawing
3 maps, right?

4 A That's my understanding of the word.

5 Q And cartography uses symbols or shapes on
6 the map to represent different objects?

7 A Yes, symbols and shapes are used in
8 cartography to represent things in the real world.

9 Q And with cartography, you know, maps,
10 especially like a world map or a map of the land,
11 might include a legend, you know, that tells you
12 specifically, you know, what symbols are
13 associated with what; is that right?

14 Like, you could have a --

15 A I see --

16 Q Sorry. Go ahead.

17 A I was going to say I have seen legends in
18 maps before, yes.

19 Q And it's just one example, like, you could
20 have a triangle that represents a mountain?

21 A You could.

22 Q And you could include "triangle equals

1 mountain" in your legend, right?

2 A You could.

3 Q Can we go to column 4, line 13.

4 A Yes, I have it.

5 Q This says these, "Additional layers 204
6 through 210 can overlay the foundational map layer
7 202 similar to how traffic and other information
8 in addition to basic cartographical details is
9 represented on maps"; is that right?

10 A Yes, you read that correctly.

11 Q Now, it says "information in addition to
12 basic cartographical details"; is that right?

13 A That's what the text says.

14 Q So doesn't that mean it's adding more than
15 basic cartographical details?

16 A It identifies traffic, for example, as
17 something beyond basic cartographical details.
18 And, I mean, if we're going back to what we talked
19 about a few minutes ago, this is just the analogy
20 of overlaying the active attacks on top of the
21 system architecture.

22 Q So the overlay is in addition to the basic

1 cartographical details?

2 A That is how Zheng is describing it in this
3 sentence.

4 MR. MIDDLETON: We've been going for
5 a while, and I have a bit more to go, so I think
6 we should take another ten-minute break here.

7 MR. JACKSON: Okay.

8 (WHEREUPON, a recess was had.)

9 MR. MIDDLETON: Can we please look at
10 Exhibit 1006.

11 THE TECHNICIAN: Please stand by.

12 (WHEREUPON, Nielson Exhibit No. 1006 was
13 presented to the witness.)

14 BY THE WITNESS:

15 A All right. I have Exhibit 1006.

16 BY MR. MIDDLETON:

17 Q And can we look at Paragraph 25 --
18 actually, to start, this is the Baker reference,
19 right?

20 A That is correct.

21 Q And did you review this in advance of your
22 deposition?

1 A I did.

2 Q Let's turn to Baker Paragraph 25.

3 A I have it.

4 Q And the third sentence there, "As
5 understood by persons involved in risk management
6 processes, a risk management flow chart utilizes
7 symbols of various shapes to indicate actions,
8 determinations, or other elements of an activity
9 or evaluation so that respective personnel of an
10 organization can understand actions to be taken to
11 successfully manage an activity or avoid a
12 negative outcome."

13 Is that right?

14 A You read that correctly, yes.

15 Q So Baker's system utilizes shapes or other
16 symbols to represent its diagrams, right?

17 A It uses shapes and other symbols in its
18 diagrams.

19 Q And these shapes represent actions,
20 determinations, or other elements of an activity
21 or evaluation?

22 A Some of the shapes or symbols are used to

1 indicate actions, determinations, or other
2 elements of an activity or evaluations so that the
3 respective personnel in organizations can
4 understand actions to be taken to successfully
5 manage an activity or avoid a negative outcome.

6 Q And what is an activity or evaluation?

7 A I mean, those seem like fairly generic
8 terms. Do you have a more specific question?

9 Q Just how Baker uses the term "activity" or
10 "evaluation," like, what do you understand those
11 terms to mean?

12 A I mean, "activity" seems pretty broad.
13 "Evaluation" also seems pretty broad.

14 Q And then the next sentence, it says,
15 "Importantly, risk management or control flow
16 charts may be imported at step 104 from
17 third-party software such as that marketed as
18 Microsoft Office Visio. The process 100 then
19 proceeds to step 106. The text and shape of each
20 element of the flow chart are stored in the
21 process database 30 and memory 26. At step 106
22 the processor 20 acts to automatically assign or

1 associate predetermined objectives or controls
2 according to the shapes of the imported flow
3 charts."

4 Is that right?

5 A You read that correctly, yes.

6 Q So this is saying that the risk management
7 or control flow charts, or at least the shapes
8 representing the risk management or control flow
9 charts, can be imported from Visio into Baker's
10 system, right?

11 A That's what you read, yes.

12 Q And then the processor automatically
13 assigns or associates predetermined objectives or
14 controls to the shapes of the imported flow
15 charts, right?

16 A That's also what's written here.

17 Q And Baker's inventors didn't invent Visio,
18 right?

19 A They did not.

20 Q And Visio was created by Microsoft?

21 A Yes. That's correct.

22 Q And Baker isn't assigned to Microsoft,

1 correct?

2 A I didn't see it on the face of the patent.

3 Q And we can look at the face of the patent
4 now if you'd like.

5 A Yeah, no, I'm agreeing; I did not see it
6 assigned to Microsoft on the face of the patent.

7 Q So is it fair to say that Baker's system
8 is different from Microsoft Visio?

9 MR. JACKSON: Objection.

10 BY THE WITNESS:

11 A The software that is described by Baker is
12 not the same thing as Visio.

13 BY MR. MIDDLETON:

14 Q It's going to have different code, right?

15 A I would presume so, yes.

16 Q So the codes of the shape -- the code that
17 makes up the shapes of Baker's system is going to
18 be different than the code that makes up the
19 shapes of Visio, right?

20 A Yeah, presumably.

21 Q And in order to import Visio shapes into
22 Baker's system, Baker's system would need to do

1 something to associate Visio shapes with the
2 predetermined shapes in Baker's system, right?

3 A I mean, clearly it's assigning them. It
4 says automatically assigns them.

5 Q And how would it automatically assign
6 them?

7 MR. JACKSON: Objection.

8 BY THE WITNESS:

9 A It says here -- let's see. This is the
10 next sentence I think. "It is understood that the
11 predetermined data" -- that's the predetermined
12 objectives for controls. "It is understood that
13 the predetermined data may have been stored
14 previously in the process database 30 of the
15 memory 26. This process data may later be
16 retrieved for use in initiating process searches
17 over the internet 12 as will be described later."

18 There is some follow-ups that go on to
19 describe how this searching works. It can even
20 search for examples of, like, online known issues
21 or known concerns and then associate those with
22 the shapes.

1 BY MR. MIDDLETON:

2 Q So there's a set of predetermined data
3 that associates specific shapes to Visio shapes?

4 MR. JACKSON: Objection.

5 BY THE WITNESS:

6 A That associates what with Visio shapes?

7 BY MR. MIDDLETON:

8 Q Specific shapes of Baker's system to Visio
9 shapes that are imported into Baker's system.

10 MR. JACKSON: Objection.

11 BY THE WITNESS:

12 A I mean, certainly nothing we read suggests
13 that. It just says that it imports the shapes and
14 assigns or associates objectives or controls with
15 them.

16 BY MR. MIDDLETON:

17 Q So the part that you just read to me
18 previously, though, is that "It is understood that
19 predetermined data may have been stored previously
20 in the process database 30 of the memory 26 and
21 this process data may later be retrieved in
22 initiating process searches over the internet"; is

1 that right?

2 A Correct.

3 Q And so it uses this data to associate the
4 Visio shapes with the shapes in Baker's system?

5 MR. JACKSON: Objection.

6 BY THE WITNESS:

7 A I didn't say that.

8 BY MR. MIDDLETON:

9 Q How is Baker's system able to recognize
10 the Visio shapes?

11 A Well, it doesn't provide a description
12 here. It simply says that once you import a
13 shape, it assigns or associates predetermined
14 objectives or controls according to the shapes of
15 the imported flow charts.

16 Q So there's predetermined data stored in a
17 database that assigns or associates objectives or
18 controls according to the shapes of the imported
19 flow charts; is that right?

20 MR. JACKSON: Objection.

21 BY THE WITNESS:

22 A So it says -- what Baker says is that the

1 processor acts to automatically assign or
2 associate predetermined objectives or controls
3 according to the shapes of the imported flow
4 charts. That predetermined data may have been
5 stored previously.

6 BY MR. MIDDLETON:

7 Q And that predetermined data may have been
8 stored previously in a database, right?

9 A That's what it says, yes.

10 Q Can we go to your declaration again,
11 Exhibit 2009.

12 A Yes, I have it.

13 Q And can we look at your table of contents.

14 A Yes, I'm at the table of contents.

15 Q And on the second page of your table of
16 contents, you have a section labeled "Opinions
17 Concerning the Challenged Claims," right?

18 A Yes.

19 Q And you opine that Keenan does not
20 disclose the claimed threats; is that right?

21 A Yes.

22 Q And you also opine that Keenan does not

1 disclose the other threat terms of the '366 patent
2 including threat model, threat model components,
3 visual representations of the threat model
4 components, or threat report, right?

5 A Yes.

6 Q And when you dispute the other threat
7 terms in this section, you're saying that you
8 dispute these terms because they include the word
9 "threat," right?

10 A I have a section that's about a page long
11 that walks through that that explains where I
12 think Mr. Hurlbut and the petitioner have
13 conflated risk and threat and that that impacts
14 these other claimed elements.

15 Q And you don't provide any independent
16 reason as to why these terms aren't met, right --
17 any other independent reason as to why these terms
18 aren't met, right? So, for example, you don't say
19 that Keenan doesn't provide a report, right?

20 A Well, the claim requires the threat
21 report, and Keenan doesn't disclose a threat
22 report.

1 Q So Keenan might disclose a report, just
2 not a threat report.

3 And you're welcome to review. It's
4 Paragraph 119 through 122 of your report.

5 A Yes, I'm reading it.

6 I do not have any analysis here that there
7 are no reports of any kind in Keenan.

8 Q So your analysis in this section,
9 Paragraphs 119 through 122, is based on your
10 opinion that Keenan does not disclose threats,
11 right?

12 A I do provide some rebuttal to specific
13 statements of Mr. Hurlbut related to, for example,
14 threat model components. Yes, it is related to
15 there not being -- that risk and threat are not
16 the same, but I -- I mean, what I have written
17 here is what I have written, and I'm not saying
18 that it's not there.

19 Q And I'm not asking you to say if it's not
20 there; I'm just asking in general if your opinion
21 is based on -- so your opinion in, you know, that
22 section, where you opine that Keenan does not

1 disclose the other threat terms of the '366
2 patent, just generally follows the same reasoning
3 as the previous section where Keenan doesn't
4 disclose threats so it also doesn't disclose, you
5 know, a threat model?

6 A What I'm saying is that what I've written
7 there is my analysis. So, I mean, I can read
8 through out loud my analysis if you'd like, and
9 that is my complete analysis for this section.
10 I'm not summarizing it or reducing it in some way.

11 Q And just jumping back to your table of
12 contents.

13 A Sure. I have it.

14 Q You also opine that Keenan does not
15 disclose dependent claims 2, 3, 9, 10, 17, or 18,
16 right?

17 A Correct.

18 Q And then you also opine that Keenan does
19 not disclose dependent claim 5, right?

20 A Yes.

21 Q And you also opine that Keenan does not
22 disclose dependent claim 6, right?

1 A Yes.

2 Q Are these all your opinions regarding the
3 Keenan reference?

4 MR. JACKSON: Object to the form.

5 BY MR. MIDDLETON:

6 Q Let me rephrase the question, actually.

7 Are these all your opinions related to
8 Keenan related to whether or not Keenan meets a
9 claimed limitation?

10 A Well, I mean, Keenan is used again in
11 ground 4. So I have opinions in Paragraph 142 and
12 143 that relate to Keenan in combination.

13 Q Okay. Can we jump to Appendix A.

14 A Sure.

15 Q And this is a listing of the challenged
16 claims, right?

17 A Yes.

18 Q And just going limitation by limitation,
19 you don't dispute that Keenan discloses providing
20 one or more databases, right?

21 A I have no analysis related to that
22 limitation.

1 Q And you don't dispute that Keenan
2 discloses providing one or more mapping files
3 communicatively coupled with the one or more
4 databases, correct?

5 A I don't have any analysis related to that
6 in this report.

7 Q And you don't dispute that Keenan
8 discloses visual diagram components of a
9 third-party software application, right?

10 A Would you say your question again, please?

11 Q Sure. You don't dispute that Keenan
12 discloses visual diagram components of a
13 third-party software application, right?

14 A I do not have any analysis about that in
15 my report -- that it doesn't -- that it doesn't
16 disclose that.

17 Q And you don't dispute that Keenan
18 discloses using one or more user interfaces
19 displayed on one or more computing devices
20 communicatively coupled with one or more
21 databases, right?

22 A That's also not something for which I have

1 any analysis in this declaration.

2 Q And you don't dispute that Keenan
3 discloses the one or more computing devices
4 reading a data file generated by the third-party
5 software application, the data file comprising a
6 subset of the third-party diagram components, the
7 data file defining one or more relationships
8 between the subset of third-party diagram
9 components; is that correct?

10 A I have not disputed that in this report.

11 Q And you don't dispute that Keenan
12 discloses displaying on the one or more user
13 interfaces a relational diagram of one of a system
14 and application and process?

15 MR. JACKSON: Object to the form.

16 BY THE WITNESS:

17 A Well, to the extent that relational
18 diagram defines a threat model, I guess I would be
19 disputing the relational diagram.

20 BY MR. MIDDLETON:

21 Q And you don't dispute that Keenan
22 discloses displaying on the one or more user

1 interfaces a relational diagram -- sorry. I
2 reread my own sentence again -- scratch that.

3 And you don't dispute that Keenan
4 discloses claim 4, right?

5 MR. JACKSON: Object to the form.

6 BY THE WITNESS:

7 A I do not have any disputes about that here
8 in my declaration.

9 BY MR. MIDDLETON:

10 Q I'll rephrase the question.

11 You don't dispute that Keenan discloses
12 claim 4 except to the extent you also dispute that
13 the independent claim -- the underlying
14 independent claim meets the challenged claims; is
15 that right?

16 A That's fair. I do dispute that claim 1 is
17 obviously not met by Keenan, so -- but, beyond
18 that, I don't have any additional analysis
19 disputing the additional requirements of claim 4.

20 Q And same question for claim 7.

21 A Well, I mean, I've already said there
22 aren't threat model components, so I've disputed

1 that threat model components are disclosed.

2 Q Your declaration doesn't include any
3 analysis specific to claim 7, right?

4 A I do not have any additional analysis in
5 my declaration related to the additional
6 requirements of claim 7.

7 Q And I understand that you dispute that
8 Keenan discloses a threat model, but you don't
9 dispute that Keenan discloses a model, right?

10 A That's correct. I have stated in my
11 declaration that I believe Keenan is working with
12 a risk model.

13 Q And you don't dispute -- you dispute that
14 Keenan discloses threat model components, but you
15 don't dispute that Keenan discloses components,
16 right?

17 MR. JACKSON: Objection.

18 BY THE WITNESS:

19 A I'm not even entirely sure what components
20 would be here because the term is used in such a
21 specific way in the '366. So I'm not sure how you
22 would divide up threat model components.

1 BY MR. MIDDLETON:

2 Q Do you include any specific analysis in
3 your report related to the components?

4 A Well, the components have to be a source
5 of a threat. I'm not sure how you would subdivide
6 that out. I don't know what a component would be
7 if you took out threat in the context of the '366.

8 Q And you don't dispute that Keenan
9 discloses visual representations, right?

10 A I do not have any disputations here in my
11 declaration that Keenan has visual -- I'm sorry,
12 what was the -- I lost your question. Would you
13 mind repeating it?

14 Q Sure. You just don't dispute that Keenan
15 has visual representations, right?

16 A I don't have any disputes about that in my
17 declaration.

18 Q And we might have covered this already,
19 but you dispute that Keenan discloses a threat
20 report, but you don't dispute that Keenan
21 discloses reports, right?

22 A I do not have any separate analysis about

1 reports in Keenan separate from threat reports.

2 Q And moving to claim 8, you don't dispute
3 that Keenan has an import interface as described
4 in claim 8, right?

5 MR. JACKSON: Object to the form.

6 BY MR. MIDDLETON:

7 Q I'll rephrase the question.

8 You don't dispute that Keenan discloses
9 the ability to import Visio diagrams, correct?

10 A I do not have anything disputing that in
11 my report.

12 Q And can we look at Paragraph 135 of your
13 report?

14 A Yes, I have it.

15 Q And this section you opine on the alleged
16 obviousness of claims 1 through 4, 7 through 11,
17 and 15 through 18 over Zheng in view of Baker and
18 Jones; is that right?

19 A Correct.

20 Q And you argue in Paragraph 136 that the
21 combination of Zheng, Baker, and Jones doesn't
22 disclose the claimed mapping file; is that right?

1 A Yes. I mean, 136 is specifically about
2 Zheng, but I go on in the subsequent paragraphs to
3 deal with the other references.

4 Q So then Paragraph 137, you argue that the
5 combination of Zheng, Baker, and Jones doesn't
6 disclose the one or more mapping files correlating
7 the threat model components with visual diagram
8 components of a third-party software application?

9 MR. JACKSON: Objection.

10 BY THE WITNESS:

11 A So in the subsequent paragraphs, I talk
12 about Zheng and Baker specifically, as those were
13 the ones identified by petitioner and Mr. Hurlbut
14 for this limitation, but that's within the context
15 of ground 2, which is Zheng in view of Baker and
16 Jones.

17 BY MR. MIDDLETON:

18 Q So let's go back to Appendix A again and
19 some of the same questions.

20 A Sure.

21 I'm there.

22 Q So you don't dispute that the combination

1 of Zheng -- and, you know what? I'm going to
2 refer to Zheng, Baker, and Jones together as just
3 "the combination" to save myself a little bit of
4 grief.

5 So how about the combination in
6 ground 2 --

7 A Fine. I was going to suggest that. That
8 works for me.

9 Q So you don't dispute that the combination
10 in ground 2 discloses a threat modeling method,
11 right?

12 MR. JACKSON: Object to the form.

13 BY THE WITNESS:

14 A I mean, we can walk through each of these
15 if you'd like. I think the only analysis I have
16 is the analysis we walked over. It says what it
17 says, but, I mean, if you want to walk through
18 each one, we can.

19 BY MR. MIDDLETON:

20 Q Yeah, why don't we.

21 A All right. Go ahead. Ask the question
22 again.

1 Q So you don't dispute that the combination
2 in ground 2 discloses a threat modeling method,
3 right?

4 MR. JACKSON: Objection. Form.

5 BY THE WITNESS:

6 A Well, to the extent that the method
7 includes steps that I have indicated aren't
8 disclosed and to the extent the combination
9 requires a motivation to combine, which I have
10 identified as not being adequate or actually I
11 disagree with motivation to combine, then I
12 disagree with the combination for ground 2 on the
13 motivation to combine, and I disagree with
14 ground 2 on a method that includes the steps that
15 I've identified as not being satisfied.

16 BY MR. MIDDLETON:

17 Q Sure. Let me rephrase the question.

18 You don't dispute that the combination in
19 ground 2 discloses threat modeling, right?

20 MR. JACKSON: Objection. Form.

21 BY THE WITNESS:

22 A Well, again, I have kind of, I guess, a

1 general objection to the combination because there
2 has to be a motivation to combine for the
3 combination.

4 Separate from the combination -- excuse
5 me. Separate from the motivation to combine, the
6 combination for ground 2, I do not have any
7 analysis stating that there's no threat model.

8 BY MR. MIDDLETON:

9 Q And all my future questions going forward
10 can be with the understanding that you have
11 analysis related to the motivation to combine, and
12 we'll just go element by element; is that fair?

13 A Sure.

14 Q You don't dispute that the combination in
15 ground 2 discloses providing one or more
16 databases, right?

17 MR. JACKSON: Objection. Form.

18 BY THE WITNESS:

19 A With all the caveats and leaving out the
20 other parts of the claim limitation that you're
21 not asking about, then I don't have any disputes
22 about there being databases in this declaration.

1 BY MR. MIDDLETON:

2 Q And you don't dispute that the combination
3 in ground 2 with those same caveats discloses the
4 databases comprising threat model components
5 stored therein, right?

6 MR. JACKSON: Object to the form.

7 MR. MIDDLETON: And, Don, I'm not sure I
8 understand the objection, but if you want a
9 standing objection going forward just to make this
10 less painful for us.

11 MR. JACKSON: Sure. I'm going to object
12 to any question that involves the combination
13 because it assumes that it's a proper combination.
14 So I'll take the standing objection.

15 BY THE WITNESS:

16 A All I want to put in my answer here is
17 that even though I'm specifically addressing the
18 mapping file, there's elements about that analysis
19 that relate to threat model components and visual
20 diagram components of third-party software
21 applications.

22 So I have not specifically put in a

1 dispute about this limitation of plurality of
2 threat model components stored therein, but what I
3 have in my analysis section is what I have. And
4 to the extent that it is commenting on threat
5 model components, then it's -- you know, it's an
6 analysis related to threat model components.

7 BY MR. MIDDLETON:

8 Q And you don't dispute that the combination
9 in ground 2 discloses a plurality of threats
10 stored therein where each of the threats is
11 associated with at least one threat model
12 component through the one or more databases?

13 A Subject to the caveat I've stated, I don't
14 have any additional analysis about this limitation
15 in this declaration.

16 Q And you don't dispute that the combination
17 in ground 2 discloses one or more user interfaces
18 displayed on one or more computing devices
19 communicatively coupled with the one or more
20 databases; is that right?

21 A I do not have any analysis about that in
22 this declaration.

1 Q And you don't dispute that the combination
2 of ground 2 discloses using the one or more
3 computing devices reading a data file generated by
4 the third-party software application, the data
5 file comprising a subset of the third-party
6 diagram components, the data file defining one or
7 more relationships between the subset of
8 third-party diagram components; is that right?

9 A Subject to my same caveats about analysis
10 that I do have that may discuss some of these same
11 terms or be related, I don't have any additional
12 analysis that is specific to this specific
13 limitation.

14 Q And you don't dispute that the combination
15 of ground 2 discloses determining using the one or
16 more computing devices for the subset of
17 third-party diagram components correlated threat
18 model components as defined in the one or more
19 mapping files; is that right?

20 MR. JACKSON: Object to the form.

21 BY THE WITNESS:

22 A I mean, I clearly dispute --

1 THE WITNESS: Sorry. Did you have another
2 objection?

3 MR. JACKSON: Yeah, I just objected to the
4 form.

5 You can answer.

6 BY THE WITNESS:

7 A So I do object to mapping files. Again,
8 to the extent I didn't add any additional analysis
9 about this limitation, that I don't have it, but I
10 disputed the existence of the mapping files.

11 BY MR. MIDDLETON:

12 Q And you don't dispute generating -- you
13 don't dispute that the combination of ground 2
14 discloses generating using the one or more
15 computing devices and displaying on the one or
16 more user interfaces a threat report displaying
17 each threat that is associated through the one or
18 more databases with one of the threat model
19 components included in the threat model; is that
20 right?

21 A Subject to my caveats that I've stated
22 previously, I don't have any additional analysis

1 about this limitation in my declaration.

2 Q And you don't dispute whether the
3 combination meets claim 2 except to the extent you
4 dispute claim 1; is that correct?

5 A We're talking about ground 2?

6 Q Ground 2, claim 2.

7 A Yes. So the analysis that I have for the
8 combination identified in ground 2 beyond the
9 motivation to combine, the rest of the analysis is
10 about claim 1 and not -- nothing additional about
11 the dependent claims.

12 Q And that would include also dependent
13 claims 3, 4, 5, 6, and 7?

14 A Claims 2, 3, 4, 7, 8, 9, 10, 11, and 15,
15 16, 18 are the ones identified here in my
16 declaration.

17 MR. MIDDLETON: I have no further
18 questions.

19 MR. JACKSON: Can we take a short break
20 and let me think about whether I have any
21 questions? We'll go off the record.

22 (WHEREUPON, a recess was had.)

1 MR. JACKSON: No questions.

2 MS. REPORTER: Anything else on the
3 record?

4 MR. MIDDLETON: No.

5 MR. JACKSON: Nothing further.

6 (WHEREUPON, the deposition was concluded
7 at 2:54 p.m. CST)

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22

ACKNOWLEDGMENT OF DEPONENT

I, SETH JAMES NIELSON, Ph.D., do hereby
acknowledge that I have read and examined the
foregoing testimony and the same is a true,
correct, and complete transcription of the
testimony given by me and any corrections appear
on the attached errata sheet signed by me.

(SIGNATURE) (DATE)

1 C E R T I F I C A T E O F R E P O R T E R

2

3 I, MICHELLE M. YOHLER, a Certified
4 Shorthand Reporter within and for the County of
5 Will, State of Illinois, do hereby certify:

6 That previous to the commencement of the
7 examination of the witness, the witness was duly
8 sworn to testify the whole truth concerning the
9 matters herein;

10 That the foregoing deposition transcript
11 was reported stenographically by me, was
12 thereafter reduced to typewriting under my
13 personal direction and constitutes a true record
14 of the testimony given and the proceedings had;

15 That the said deposition was taken
16 remotely before me at the time and place
17 specified;

18 That I am not a relative or employee or
19 attorney or counsel, nor a relative or employee of
20 such attorney or counsel for any of the parties
21 hereto, nor interested directly or indirectly in
22 the outcome of this action.

1 IN WITNESS WHEREOF, I do hereunto set my
2 hand and affix my seal of office at Chicago,
3 Illinois, this 13th day of March, 2024.

4
5
6
7 *Michelle M. Yohler*
8 _____

9 Michelle M. Yohler, CSR, RMR, CRR
10 Certified Shorthand Reporter
11 CSR No.: 84-4531

A			
ab	138:10, 142:14,	acknowledgment	123:18, 125:9,
124:17	144:7, 146:16,	158:1	129:18, 141:6,
abc	146:22, 148:1,	acronym	150:10
124:17	148:12, 149:5,	13:10	actuarial
ability	151:21, 151:22,	across	63:21, 73:19,
147:9	152:18, 153:1,	67:6	74:16
able	153:14, 153:21,	act	adam
12:7, 33:8,	154:9, 155:9,	58:9, 80:2,	14:12
119:3, 119:4,	156:1, 156:5,	80:3	add
119:5, 136:9	156:10, 156:20	action	35:20, 37:12,
about	above	159:22	37:14, 96:12,
12:6, 15:14,	27:3, 104:7,	actions	155:8
15:18, 15:19,	104:15	130:7, 130:10,	added
17:2, 17:10,	absolute	130:19, 131:1,	29:6
17:21, 19:19,	29:12, 34:21,	131:4	adding
23:17, 26:13,	34:22	active	38:3, 128:14
29:8, 31:4,	absolutely	58:5, 123:8,	addition
32:6, 36:14,	25:22, 37:3,	124:7, 128:20	21:14, 128:8,
37:20, 38:11,	104:12	activity	128:11, 128:22
38:20, 39:5,	abstraction	130:8, 130:11,	additional
42:7, 42:15,	115:17, 116:2	130:20, 131:2,	28:3, 128:5,
43:18, 45:16,	ac	131:5, 131:6,	144:18, 144:19,
47:6, 49:8,	124:17	131:9, 131:12	145:4, 145:5,
50:11, 54:8,	accept	actor	153:14, 154:11,
54:20, 56:17,	46:19, 71:20,	51:19, 105:5,	155:8, 155:22,
57:19, 59:11,	72:10	119:12, 119:20	156:10
61:2, 63:2,	accepted	actors	address
64:13, 65:17,	36:4	52:5	72:3
66:3, 68:14,	access	acts	addressing
69:4, 69:9,	98:15	131:22, 137:1	152:17
71:22, 72:18,	accessed	actual	adequacy
72:19, 79:3,	91:7	6:18, 60:2,	106:2
79:22, 80:2,	accident	65:20, 66:1,	adequate
81:1, 81:3,	51:12, 51:15,	66:18, 68:16,	150:10
81:4, 84:14,	120:20	76:2, 82:3,	adjusting
84:15, 87:13,	accidental	82:11, 117:11,	47:6
88:3, 88:18,	102:2, 102:7	125:12	advance
89:3, 89:16,	according	actualized	31:6, 101:17,
89:17, 89:19,	80:11, 107:9,	123:15	129:21
92:15, 95:5,	132:2, 136:14,	actually	adversaries
95:6, 95:10,	136:18, 137:3	6:9, 10:20,	52:8
104:11, 105:13,	accordingly	12:4, 19:12,	adversary
112:19, 119:4,	27:3	22:7, 25:19,	78:1, 78:2,
122:15, 123:2,	accounting	26:22, 58:5,	82:14
123:16, 124:5,	57:8	58:15, 65:19,	adverse
126:10, 128:19,	accurate	78:11, 79:6,	19:22, 20:8,
	35:4	89:22, 90:11,	20:10, 39:14,
	acknowledge	105:19, 123:14,	40:2, 48:11,
	158:3		

48:12, 48:19, 52:18, 52:20, 53:4, 53:8, 54:22, 59:9, 60:18, 65:19, 74:22, 75:21, 75:22, 82:7, 82:12, 82:13, 82:21, 83:5, 83:11, 83:13, 83:15 affix 160:2 again 10:1, 21:1, 24:16, 32:11, 33:17, 36:6, 48:4, 57:16, 58:2, 62:11, 63:1, 73:5, 82:10, 88:10, 89:15, 97:13, 98:18, 104:2, 118:20, 137:10, 141:10, 142:10, 144:2, 148:18, 149:22, 150:22, 155:7 against 17:19, 52:5, 105:6 agarwal 14:5, 14:8 agencies 11:8, 13:4 agency 13:7, 56:9 agents 117:21 aggressively 68:8, 68:22 ago 128:19 agree 29:15, 37:5, 37:7, 39:19, 45:7, 53:9, 61:19, 117:6	agreed 36:2, 86:18, 86:20, 88:19 agreeing 133:5 ahead 50:7, 58:13, 127:16, 149:21 algorithms 114:17 all 7:10, 7:20, 7:22, 10:10, 10:11, 11:19, 24:17, 25:4, 25:7, 25:8, 29:7, 31:3, 31:16, 32:19, 35:3, 38:17, 43:13, 47:3, 47:11, 52:1, 59:9, 59:11, 59:16, 60:13, 67:20, 70:7, 70:13, 71:11, 71:12, 73:7, 74:5, 80:6, 81:7, 83:4, 84:18, 92:21, 99:8, 100:2, 103:15, 105:9, 118:15, 124:16, 126:17, 126:18, 129:15, 141:2, 141:7, 149:21, 151:9, 151:19, 152:16 alleged 147:15 allows 55:10 almost 23:13, 23:14, 23:19, 25:20, 53:19, 110:5 alone 13:19 along 6:20, 23:15,	59:6, 91:1 already 28:21, 38:9, 38:15, 47:15, 48:7, 79:4, 96:16, 144:21, 146:18 also 3:18, 9:8, 13:6, 14:8, 17:6, 20:15, 21:9, 21:16, 22:22, 24:5, 25:1, 27:16, 35:21, 40:17, 42:19, 48:19, 50:4, 55:5, 55:7, 59:13, 66:3, 66:5, 71:18, 80:22, 83:8, 83:9, 92:9, 93:4, 98:9, 117:22, 118:8, 123:21, 131:13, 132:16, 137:22, 140:4, 140:14, 140:18, 140:21, 142:22, 144:12, 156:12 although 77:13 alto 13:1 always 23:13, 23:14, 23:19, 66:11, 81:13 amateur 103:22 among 42:3, 106:21, 107:8, 107:11, 107:18, 111:19 amount 23:2, 80:18, 81:13, 81:17, 102:21 analogy 120:18, 120:19,	128:19 analyses 9:8, 9:10 analysis 9:11, 9:22, 10:2, 10:3, 10:4, 10:14, 10:20, 11:4, 17:8, 18:4, 18:12, 21:14, 23:9, 24:10, 24:12, 24:13, 24:17, 24:20, 25:1, 28:5, 29:15, 30:17, 32:12, 32:16, 38:4, 38:8, 38:15, 39:4, 39:22, 44:10, 51:18, 63:2, 66:5, 71:13, 71:17, 92:8, 93:2, 94:22, 95:2, 105:3, 125:5, 139:6, 139:8, 140:7, 140:8, 140:9, 141:21, 142:5, 142:14, 143:1, 144:18, 145:3, 145:4, 146:2, 146:22, 149:15, 149:16, 151:7, 151:11, 152:18, 153:3, 153:6, 153:14, 153:21, 154:9, 154:12, 155:8, 155:22, 156:7, 156:9 analyze 55:10, 55:16, 79:19 analyzed 40:6, 44:12, 44:17, 72:16 anderson 18:22 annualized 67:8, 67:18
--	--	--	---

another 10:12, 11:17, 15:22, 22:1, 23:1, 23:4, 33:7, 33:15, 34:3, 34:6, 35:1, 35:20, 37:15, 42:20, 51:19, 54:9, 57:22, 58:8, 60:15, 68:9, 68:12, 72:7, 74:14, 76:8, 84:3, 87:16, 95:20, 100:6, 108:16, 118:17, 129:6, 155:1 answer 36:7, 43:2, 56:20, 56:22, 79:9, 152:16, 155:5 answer's 56:12 anurag 14:5 any 5:15, 5:19, 8:2, 8:4, 8:10, 11:8, 12:19, 15:15, 24:6, 38:22, 40:13, 41:18, 42:5, 96:4, 105:7, 114:2, 126:5, 138:15, 138:17, 139:6, 139:7, 142:5, 142:14, 143:1, 144:7, 144:18, 145:2, 145:4, 146:2, 146:10, 146:16, 146:22, 151:6, 151:21, 152:12, 153:14, 153:21, 154:11, 155:8, 155:22, 156:20, 158:6, 159:20	anyone 14:19 anything 5:22, 23:19, 49:9, 112:19, 114:4, 147:10, 157:2 anywhere 59:6 appeal 1:3 appear 158:6 appendix 141:13, 148:18 application 17:5, 40:7, 40:9, 41:18, 42:5, 57:8, 93:19, 96:13, 99:2, 101:1, 101:3, 106:20, 107:4, 107:6, 107:9, 107:13, 107:22, 108:1, 108:2, 108:7, 109:2, 109:6, 109:12, 109:16, 110:7, 110:19, 110:21, 111:4, 111:17, 111:22, 112:2, 112:5, 112:7, 112:22, 113:9, 113:15, 116:17, 117:13, 119:13, 120:3, 120:6, 120:9, 121:2, 121:14, 123:13, 125:3, 142:9, 142:13, 143:5, 143:14, 148:8, 154:4 application-to-a- pplication 57:9 applications 100:17, 106:21, 106:22, 107:7,	107:8, 107:11, 107:12, 107:14, 107:18, 107:19, 108:2, 108:6, 108:12, 108:13, 111:4, 111:18, 111:19, 112:8, 112:18, 113:16, 119:18, 120:2, 120:3, 120:14, 121:4, 123:22, 124:1, 152:21 applied 39:17, 62:2 applies 35:3, 35:6 apply 40:13, 62:12 approach 18:15, 56:9, 125:2, 126:11 approached 22:14 approaches 18:13, 80:1, 126:11 appropriate 22:10, 124:19 arbitrarily 84:9 archie 14:8 architect 120:4 architecture 15:20, 31:15, 106:20, 107:4, 107:6, 107:9, 107:13, 107:20, 107:22, 108:1, 108:2, 108:7, 109:6, 109:12, 110:20, 110:21, 111:4, 111:18, 111:22, 112:6, 115:12, 116:10, 116:17, 120:9, 125:3, 128:21	area 9:13, 11:8 aren't 97:6, 97:10, 138:16, 138:18, 144:22, 150:7 argue 147:20, 148:4 argument 29:22 around 29:5, 84:10, 86:1 arp 76:15 arriving 58:14 arrow 98:16 art 31:7, 65:1 ascending 90:22 aside 77:11 asked 49:22 asking 23:22, 38:7, 79:11, 87:2, 87:3, 94:18, 110:6, 139:19, 139:20, 151:21 aspects 12:8 assess 10:4 assessing 57:6, 57:13 assessment 10:7, 93:4 asset 119:9 assets 119:3 assign 131:22, 134:5, 137:1
---	---	---	--

assigned 132:22, 133:6 assigning 134:3 assigns 132:13, 134:4, 135:14, 136:13, 136:17 associate 114:8, 132:1, 134:1, 134:21, 136:3, 137:2 associated 20:14, 34:9, 62:8, 63:5, 64:16, 70:17, 89:20, 90:6, 90:7, 90:12, 90:14, 91:12, 91:15, 92:12, 92:13, 96:1, 97:4, 97:16, 97:19, 97:22, 111:3, 119:12, 120:14, 127:13, 153:11, 155:17 associates 98:7, 119:17, 132:13, 135:3, 135:6, 135:14, 136:13, 136:17 associating 100:5, 100:7, 101:3 assume 29:21, 35:5, 47:3 assumes 152:13 assuming 24:16, 71:5, 87:12 assumption 38:8 assumptions 28:21, 38:13 atlantic 84:4, 85:1,	85:6, 85:7 atm 21:7, 21:8 attached 91:11, 158:7 attaching 38:2 attack 19:4, 19:5, 51:7, 55:11, 55:17, 58:19, 60:15, 70:16, 76:18, 77:3, 77:7, 78:19, 118:22, 119:1, 119:7, 119:15, 119:21, 120:21, 123:7, 123:12, 123:13 attacker 56:8, 78:22 attackers 50:1 attacks 50:3, 50:11, 76:7, 128:20 attempting 85:11 attempts 76:5, 85:15 attorney 159:19, 159:20 attribute 113:1 audit 82:1 austin 6:6 auth 20:11 automated 12:8, 25:1, 32:1 automatically 131:22, 132:12, 134:4, 134:5, 137:1 automation 40:11	available 42:3, 68:17 avoid 130:11, 131:5 aware 8:11, 51:1 B back 27:13, 28:4, 30:2, 36:1, 36:14, 39:6, 44:9, 48:10, 48:14, 49:2, 49:10, 62:5, 65:22, 66:17, 72:20, 85:10, 88:9, 95:4, 120:8, 128:18, 140:11, 148:18 background 41:22 bad 59:18, 66:11, 66:14, 79:2 baker 4:13, 129:18, 130:2, 131:9, 132:22, 133:11, 136:22, 147:17, 147:21, 148:5, 148:12, 148:15, 149:2 baker's 130:15, 132:9, 132:17, 133:7, 133:17, 133:22, 134:2, 135:8, 135:9, 136:4, 136:9 base 66:5, 106:19, 108:22, 111:16, 111:21, 112:3, 112:9, 113:18, 116:16, 117:1, 117:3, 120:10, 121:6, 123:22,	124:8 based 10:4, 10:7, 22:11, 22:16, 28:10, 30:11, 46:9, 47:6, 49:10, 51:15, 52:7, 64:14, 65:16, 70:12, 71:17, 75:8, 80:22, 81:3, 81:11, 102:5, 108:20, 112:21, 119:6, 125:19, 126:8, 139:9, 139:21 basic 78:8, 78:9, 128:8, 128:12, 128:15, 128:17, 128:22 basically 57:17 basis 67:9 bc 124:17 became 44:13 because 9:13, 17:21, 21:21, 23:1, 27:16, 28:17, 29:22, 34:20, 38:11, 47:9, 52:12, 54:4, 54:11, 54:16, 55:3, 55:5, 59:9, 60:2, 60:6, 64:12, 66:14, 73:15, 118:14, 138:8, 145:20, 151:1, 152:13 become 52:11 becomes 69:12
--	--	--	---

been 5:5, 5:10, 11:11, 23:3, 23:17, 33:11, 37:21, 38:9, 38:15, 61:21, 64:17, 125:11, 129:4, 134:13, 135:19, 137:4, 137:7 before 1:3, 2:2, 5:10, 9:9, 13:21, 14:3, 14:6, 14:11, 14:13, 14:21, 15:1, 15:2, 15:4, 15:8, 15:12, 15:15, 16:21, 18:6, 21:20, 22:19, 27:13, 31:8, 42:13, 50:9, 56:17, 68:15, 70:18, 79:9, 127:18, 159:16 begin 17:8, 96:12 begins 23:2 behalf 3:2, 3:10 behaving 51:9 being 12:7, 28:20, 30:20, 31:2, 31:3, 34:18, 35:4, 40:5, 43:6, 43:7, 43:9, 46:3, 54:9, 58:5, 68:5, 70:13, 71:11, 74:11, 75:4, 75:13, 84:8, 119:4, 119:22, 123:15, 126:12, 139:15,	150:10, 150:15, 151:22 believe 8:2, 14:9, 14:10, 16:16, 41:7, 95:2, 145:11 below 19:20, 88:20 benefit 119:8 best 5:16, 9:15 better 44:11, 81:14 between 23:4, 24:9, 30:16, 32:8, 51:22, 96:19, 98:10, 98:12, 98:15, 99:20, 113:3, 121:4, 122:12, 124:12, 143:8, 154:7 beyond 56:14, 128:17, 144:17, 156:8 big 23:11, 43:21 bigger 44:2, 72:7, 73:8 bit 9:12, 30:19, 41:21, 46:18, 55:6, 59:5, 64:5, 67:19, 72:14, 95:4, 129:5, 149:3 bleeds 116:12 bluejacking 25:17, 27:5, 27:9, 27:20, 29:9, 30:1, 30:3, 30:5, 30:11, 30:13, 38:12, 38:20,	39:2, 41:9, 42:18, 45:17, 45:19, 46:1, 46:22, 47:13, 47:16, 47:19, 95:15, 95:18, 97:15, 97:16 bluetooth 25:15, 25:16, 25:18, 27:4, 27:9, 27:18, 27:20, 28:14, 28:17, 29:2, 29:9, 30:7, 30:11, 30:15, 38:12, 42:12, 42:19, 45:4, 45:5, 45:19, 46:2, 46:3, 46:20, 47:3, 47:5, 47:12, 47:15, 47:18, 95:14, 95:17, 97:16, 97:22 board 1:3, 23:7, 23:12, 30:12, 30:14, 33:3, 36:3, 36:8, 37:1, 37:4, 37:6, 37:8, 37:14, 37:17, 37:19, 39:2 boarding 32:7 book 18:20, 18:22, 19:1 books 22:4 both 6:22, 7:5, 7:8, 11:3, 21:12, 24:19, 61:22, 64:20, 67:2 bottom 41:14, 96:7 bounds 77:18, 78:3	box 43:15, 44:1, 44:2, 45:2, 45:12, 45:21, 78:18 boxes 44:1 break 60:21, 84:16, 84:18, 84:21, 87:16, 87:17, 129:6, 156:19 bright-line 103:1 bring 24:22 broad 9:13, 11:5, 12:5, 12:13, 13:15, 131:12, 131:13 broader 40:9, 56:1 broken 84:17 bt 45:2, 45:11, 95:11 buffer 17:21, 76:17, 76:19, 77:6, 77:7, 78:21, 92:12 bug 21:7, 21:9 build 23:6, 24:6, 25:11, 25:13, 30:10, 62:6, 62:9, 84:10 building 24:9, 27:14, 54:21, 63:1 built 53:14, 53:18, 54:21, 55:1, 86:1 built-in 25:2
--	---	--	--

bunch 25:6, 44:1, 66:2 business 105:21 buy 47:5 bytes 77:20, 77:21 C c-i-s-a 13:10 c-o-m-p-r-e-s-s-- i-b-l-e 125:13 calculate 63:20, 64:2, 66:12, 67:4, 67:14, 80:16, 81:7 calculated 54:1, 67:8, 73:19, 74:16 calculating 54:6, 69:4, 69:7, 71:4, 75:7 calculation 62:15, 62:16, 62:18, 63:4, 67:14, 69:10, 115:2 calculations 68:14 california 53:13, 53:14 call 42:12, 104:22 called 5:5, 8:16, 19:5, 40:19, 77:18, 78:11 can't 5:15, 45:22, 55:13, 60:10, 66:11, 72:7, 79:3 cancer 52:6	canvas 96:11, 96:18, 96:21 capable 37:18 capitalized 11:19 card 20:13 career 10:11, 23:5, 61:22 cartographical 128:8, 128:12, 128:15, 128:17, 129:1 cartography 125:2, 126:11, 126:12, 127:2, 127:5, 127:8, 127:9 cascade 20:4 case 13:22, 14:3, 14:6, 14:11, 14:13, 14:21, 15:4, 15:12, 28:16, 33:13, 41:12, 75:22, 83:19, 85:3, 89:3, 89:5, 100:6, 119:20 categories 102:12 categorizations 118:18 categorized 117:22, 118:8 category 18:8, 18:10, 57:16, 57:20 cause 19:22, 20:10, 39:13, 40:2, 52:18, 53:4, 60:18 caused 82:8, 82:22, 83:17, 84:2	83:17, 84:2 causes 84:1, 85:16, 104:16 causing 75:14, 75:16, 75:19, 102:20 caveat 36:7, 153:13 caveats 78:8, 151:19, 152:3, 154:9, 155:21 center 44:22 ceo 70:8 certain 11:13, 12:8, 13:16, 34:21, 34:22, 60:11, 78:10, 90:6, 104:17, 119:3, 119:5 certainly 85:9, 99:19, 108:12, 135:12 certified 2:3, 159:3, 160:10 certify 159:5 cetera 76:2, 102:2, 106:2, 112:8, 113:17 chain 58:19, 59:10 challenged 137:17, 141:15, 144:14 challenges 73:11 chance 51:10, 51:16 change 17:13, 47:1 changes 46:9, 52:3	changing 38:5 characteristics 112:6, 113:15 characters 78:4 charge 81:11 chart 33:15, 130:6, 131:20 charting 33:14 charts 131:16, 132:3, 132:7, 132:9, 132:15, 136:15, 136:19, 137:4 chat 7:1, 26:7 checking 77:18, 78:3 chicago 160:2 choose 30:18, 46:17, 59:13, 59:14, 60:13, 74:2, 74:3, 74:13 chose 75:9 circle 30:12, 32:7, 35:18 circumstance 28:19, 42:11, 53:9 cisa 13:8, 13:9, 13:10, 13:13, 13:15 citing 90:16 city 121:15 city's 121:19 claim 93:7, 93:12,
--	---	---	---

93:14, 94:2, 94:19, 98:18, 99:10, 100:6, 100:10, 100:21, 138:20, 140:19, 140:22, 144:4, 144:12, 144:13, 144:14, 144:16, 144:19, 144:20, 145:3, 145:6, 147:2, 147:4, 151:20, 156:3, 156:4, 156:6, 156:10 claimed 137:20, 138:14, 141:9, 147:22 claims 137:17, 140:15, 141:16, 144:14, 147:16, 156:11, 156:13, 156:14 clarify 12:4, 75:18 clear 24:8 clearly 6:4, 25:8, 134:3, 154:22 click 67:9, 69:8, 70:6 clicking 59:12, 68:4, 68:20, 69:21, 70:8, 72:22 clicks 59:2, 59:15, 66:19 client 9:14, 16:15, 22:11, 28:8 client's 22:17 clients 16:9, 16:14, 16:17 code 9:4, 10:14,	10:15, 78:12, 133:14, 133:16, 133:18 codes 133:16 coffee 29:8, 29:15 coincidentally 105:11 collect 12:11 collecting 12:10 collision 50:19, 51:6, 51:12 color 101:22, 102:8 color-coding 102:5 column 26:15, 26:16, 27:2, 33:19, 33:20, 41:14, 42:1, 50:12, 50:16, 55:9, 57:2, 64:10, 90:9, 90:19, 91:3, 91:17, 91:21, 91:22, 92:1, 92:3, 92:4, 92:7, 93:10, 96:7, 98:18, 100:10, 100:21, 101:19, 106:15, 108:18, 111:8, 113:14, 115:7, 115:9, 115:15, 115:22, 116:4, 116:13, 117:4, 117:17, 119:10, 121:10, 122:2, 124:6, 124:21, 128:3 columns 91:10 combination 122:7, 122:19,	126:5, 141:12, 147:21, 148:5, 148:22, 149:3, 149:5, 149:9, 150:1, 150:8, 150:12, 150:18, 151:1, 151:3, 151:4, 151:6, 151:14, 152:2, 152:12, 152:13, 153:8, 153:16, 154:1, 154:14, 155:13, 156:3, 156:8 combinations 122:12, 122:16, 124:17 combine 120:22, 150:9, 150:11, 150:13, 151:2, 151:5, 151:11, 156:9 come 36:12, 49:1, 69:11, 73:16 comes 22:8 coming 67:21, 70:17, 119:21 commencement 159:6 commenting 153:4 common 9:3, 9:7, 24:3, 31:16 commonly 31:13, 31:19 communicatively 142:3, 142:20, 153:19 community 86:10, 87:10 commuting 50:15, 50:18 companies 12:18, 53:14,	103:6, 105:12, 105:15 company 9:1, 103:19, 104:6, 104:15, 105:20, 106:4, 107:15 company's 103:13, 106:20, 107:4, 107:17, 111:17, 116:17 compared 73:8 comparison 73:6 compatible 61:17 complete 140:9, 158:5 component 13:16, 21:3, 27:10, 30:8, 42:9, 42:14, 42:19, 42:20, 43:16, 44:5, 44:14, 44:19, 44:21, 45:7, 45:9, 45:14, 45:18, 46:1, 46:4, 46:6, 46:9, 46:16, 50:19, 90:14, 91:2, 95:15, 95:20, 95:22, 96:10, 97:17, 97:19, 100:5, 100:6, 100:7, 100:8, 100:12, 100:13, 146:6, 153:12 components 20:16, 20:19, 21:13, 24:22, 32:16, 38:14, 40:20, 41:2, 42:4, 42:7, 43:6, 44:11, 44:18, 46:10,
---	--	--	--

46:15, 64:14, 93:21, 93:22, 95:6, 95:9, 96:12, 96:17, 96:20, 96:22, 97:2, 97:5, 97:12, 98:11, 98:13, 99:1, 99:12, 99:13, 99:15, 100:15, 100:16, 100:17, 101:1, 101:2, 105:22, 106:4, 106:22, 107:5, 109:1, 109:2, 109:16, 109:17, 109:19, 110:7, 110:8, 110:13, 110:14, 111:20, 138:2, 138:4, 139:14, 142:8, 142:12, 143:6, 143:9, 144:22, 145:1, 145:14, 145:15, 145:19, 145:22, 146:3, 146:4, 148:7, 148:8, 152:4, 152:19, 152:20, 153:2, 153:5, 153:6, 154:6, 154:8, 154:17, 154:18, 155:19 composite 122:1 comprehensible 125:4, 125:7, 125:15 compressible 125:12, 125:16, 125:17 comprises 99:13 comprising 143:5, 152:4, 154:5 computer 5:22, 8:22,	24:1, 24:5, 56:12, 56:14, 56:22, 57:20, 77:8, 108:22, 115:11, 116:8 computer-based 50:10 computers 57:19, 102:20 computing 55:21, 57:5, 142:19, 143:3, 153:18, 154:3, 154:16, 155:15 conceive 42:11 concept 86:16, 87:1, 93:5 concepts 86:3 concerned 63:3 concerning 137:17, 159:8 concerns 134:21 conclude 103:10 concluded 157:6 conclusion 36:12 concrete 17:3, 17:20, 29:14 conduct 82:1 conference 15:15, 15:17, 15:22 configured 98:8 confirm 34:12, 88:10 conflated 138:13 connect 15:11, 15:12,	25:16, 27:18, 120:1 connected 35:19 connecting 119:14 connection 121:4 connections 113:3 connotation 85:12 conscious 52:4 consequences 81:7 consider 19:3, 29:16, 33:6, 84:9, 104:22 consideration 28:1, 28:22, 41:19 considered 22:13 constitutes 159:13 construct 80:20, 112:3 constructed 112:1 construed 19:21, 39:12 consulting 9:4 contents 137:13, 137:14, 137:16, 140:12 context 19:14, 20:22, 25:11, 28:1, 28:3, 29:4, 38:18, 38:21, 40:1, 42:22, 43:4, 45:17, 46:7, 46:9, 47:7, 47:21, 48:4, 48:6,	49:6, 69:3, 69:4, 79:9, 79:10, 79:13, 92:14, 95:13, 146:7, 148:14 context-dependent 48:20 context-specific 9:12, 10:2 continue 119:10 contractor 21:9 control 78:7, 78:11, 78:12, 78:14, 78:18, 121:12, 131:15, 132:7, 132:8 controls 117:10, 124:9, 132:1, 132:14, 134:12, 135:14, 136:14, 136:18, 137:2 controversial 86:16, 86:22 convert 34:5, 34:14, 34:22 converting 33:14, 34:2 copy 7:10, 7:13 correct 5:11, 5:12, 7:11, 7:14, 8:13, 8:18, 9:3, 9:9, 13:12, 14:10, 16:10, 16:11, 25:18, 27:6, 27:11, 30:9, 34:11, 39:15, 45:13, 55:15, 56:4, 61:13, 65:10, 71:14, 88:12, 89:1, 119:19,
---	---	--	--

120:11, 129:20, 132:21, 133:1, 136:2, 140:17, 142:4, 143:9, 145:10, 147:9, 147:19, 156:4, 158:5 corrections 8:10, 158:6 correctly 57:11, 57:12, 110:10, 110:11, 125:8, 128:10, 130:14, 132:5 correlate 100:11 correlated 50:20, 93:21, 99:8, 99:12, 99:14, 154:17 correlating 98:22, 99:4, 99:16, 99:19, 99:22, 100:2, 100:5, 100:22, 148:6 correlation 99:9, 101:5 costs 63:5 could 19:9, 20:9, 23:6, 23:12, 24:5, 24:13, 25:8, 25:17, 27:19, 27:22, 29:14, 30:12, 30:18, 31:1, 32:5, 32:7, 32:9, 32:21, 33:4, 37:1, 37:3, 37:5, 37:7, 42:9, 42:11, 46:5, 46:19, 47:18, 47:21, 48:1, 48:5, 51:8, 53:1, 53:3,	53:4, 53:10, 58:15, 59:8, 59:13, 59:14, 59:16, 62:21, 63:13, 63:19, 64:2, 64:21, 67:13, 75:9, 75:11, 75:15, 76:4, 76:7, 76:9, 76:16, 76:18, 82:11, 84:3, 84:6, 84:8, 95:12, 95:14, 95:16, 97:18, 97:21, 101:19, 102:20, 107:10, 107:13, 107:21, 108:5, 108:8, 108:13, 108:16, 112:20, 113:1, 113:9, 114:15, 114:19, 118:12, 120:5, 120:20, 120:21, 123:15, 123:20, 125:17, 126:4, 127:14, 127:19, 127:21, 127:22, 128:2 couldn't 42:19, 75:3 counsel 159:19, 159:20 counsel's 6:7 count 22:20 county 159:4 couple 62:20 coupled 61:10, 88:22, 142:3, 142:20, 153:19 course 22:3, 37:20, 59:1, 66:16,	110:9 courses 18:21 court 11:18, 13:11 covered 146:18 covers 99:8 create 65:4, 118:9 created 96:16, 132:20 creating 11:3, 18:13, 31:4, 34:9, 124:11 credentials 66:20, 70:14, 70:16, 71:8, 71:10, 73:21, 74:5, 74:18, 74:19, 74:22, 75:2, 75:12, 75:17, 76:1, 76:4, 76:17 crimson 8:17, 8:21 crowdstrike 12:21 crr 1:22, 2:3, 160:9 cryptanalysis 20:8 cryptography 10:17 csr 1:22, 2:3, 2:4, 160:9, 160:11 cst 1:18, 157:7 cto 70:8 cuff 67:19 current 7:21	currently 8:1 cut 43:17, 56:16 cyber 18:5, 18:7, 57:7, 57:14, 57:21, 58:1, 60:16, 102:1, 102:6, 102:13, 102:15, 105:12, 105:14, 118:12, 118:16 cybersecurity 8:12, 8:14, 9:16, 9:17, 10:11, 11:6, 12:17, 12:19, 13:3, 13:7, 13:13, 13:19, 15:18, 16:8, 70:4, 71:13, 71:15, 86:6, 86:9, 86:13, 87:4, 87:10, 105:17 cyberspace 103:3, 103:4 D d-e-s 20:9 damage 54:1, 62:22, 66:7, 67:16, 71:6, 84:4, 84:15, 85:5 data 12:10, 12:11, 15:20, 15:22, 22:1, 28:9, 29:14, 53:14, 66:2, 68:10, 68:11, 68:13, 68:16, 73:20, 74:17, 78:15, 78:16, 83:9, 83:10, 83:13,
--	---	---	---

83:15, 83:17, 93:5, 103:2, 103:3, 111:14, 112:2, 112:12, 112:15, 112:16, 117:12, 117:19, 122:5, 122:11, 122:15, 123:2, 123:4, 124:15, 124:18, 134:11, 134:13, 134:15, 135:2, 135:19, 135:21, 136:3, 136:16, 137:4, 137:7, 143:4, 143:5, 143:7, 154:3, 154:4, 154:6 database 46:12, 46:15, 46:22, 50:21, 97:5, 98:6, 114:19, 115:3, 122:5, 122:11, 122:14, 122:21, 123:8, 123:10, 123:20, 123:21, 124:11, 124:14, 131:21, 134:14, 135:20, 136:17, 137:8 databases 141:20, 142:4, 142:21, 151:16, 151:22, 152:4, 153:12, 153:20, 155:18 date 158:10 day 160:3 deal 47:10, 49:21, 52:1, 68:7, 68:21, 70:1, 72:1, 73:2, 74:12, 74:13, 105:16, 105:17,	148:3 dealing 17:18, 50:3, 52:4, 52:8, 54:4, 56:18, 71:7, 72:13, 89:10, 118:16 deals 54:3 decide 17:9, 72:9, 74:3, 81:10, 81:12 decision 72:18 decisions 51:20, 71:22 declaration 4:14, 4:16, 7:11, 7:12, 7:14, 8:9, 16:3, 18:17, 20:20, 39:7, 88:15, 137:10, 143:1, 144:8, 145:2, 145:5, 145:11, 146:11, 146:17, 151:22, 153:15, 153:22, 156:1, 156:16 declarations 7:16, 7:19, 8:5 deeper 75:9 defender 119:9 defenders 119:2 defense 70:21 define 102:20, 104:7, 104:16, 118:20 defined 27:4, 29:3, 41:2, 52:22, 94:3, 94:15, 96:18, 99:20,	111:21, 154:18 defines 94:7, 143:18 defining 65:12, 94:1, 118:4, 143:7, 154:6 definitely 13:16, 34:14 definition 19:13, 39:16, 39:19, 48:10, 48:12, 48:14, 48:16, 49:6, 52:16, 58:2, 59:22, 61:14, 61:17, 61:19, 61:20, 62:2, 62:11, 86:18, 86:19, 88:10, 88:11, 88:20, 99:3, 99:7 degree 54:3 deleting 66:2 delivered 70:19, 71:5 delivery 66:22, 67:13, 68:2, 69:5, 70:18, 71:2 denial-of-service 60:15, 76:20, 77:2 department 31:19 depend 41:11, 46:18, 59:5, 62:20, 79:5, 79:14 dependent 99:10, 140:15, 140:19, 140:22, 156:11, 156:12 depending 23:10, 23:11, 47:21, 48:4,	48:6, 58:16, 76:18, 95:11, 95:13 depends 44:15, 46:6, 48:20, 53:17, 60:12, 79:12, 98:5, 98:8 depict 109:11, 109:16, 110:7 depicted 110:21 depicting 109:1 depiction 111:1 depictions 109:7, 110:12 deponent 158:1 deposed 5:10 deposition 1:16, 2:1, 5:19, 7:17, 101:17, 129:22, 157:6, 159:10, 159:15 derivation 32:17 derive 32:2, 64:21 des 20:8 descending 90:22 describe 10:8, 30:5, 134:19 described 28:20, 30:3, 30:8, 30:20, 32:12, 33:3, 36:13, 97:1, 99:10, 126:18, 126:19, 133:11, 134:17, 147:3
---	--	--	---

describes 21:2, 38:13, 94:3, 111:7, 121:3 describing 31:6, 55:7, 83:4, 109:19, 109:20, 125:19, 129:2 description 9:2, 92:22, 120:16, 120:17, 136:11 descriptions 126:17, 126:21 designed 31:8, 58:7 desired 96:10 detailed 23:10, 104:4 details 17:20, 23:16, 128:8, 128:15, 128:17, 129:1 details" 128:12 determinations 71:19, 130:8, 130:20, 131:1 determine 22:16, 42:22, 53:21, 68:1, 79:20, 80:21, 82:3, 89:7, 102:17, 105:2 determined 10:16 determining 99:11, 99:14, 154:15 develop 16:9, 16:12, 22:5, 22:7, 105:9 developed 16:18, 22:19, 23:2	developing 18:11 device 16:15 devices 25:16, 27:19, 142:19, 143:3, 153:18, 154:3, 154:16, 155:15 diagram 19:8, 34:2, 34:3, 34:8, 34:16, 35:11, 43:20, 91:19, 92:7, 93:18, 93:22, 94:2, 96:3, 96:4, 96:15, 97:9, 99:1, 99:12, 100:8, 100:12, 101:2, 102:5, 142:8, 142:12, 143:6, 143:8, 143:13, 143:18, 143:19, 144:1, 148:7, 152:20, 154:6, 154:8, 154:17 diagramed 18:16 diagramming 24:6, 24:14, 24:15, 30:22 diagrams 25:6, 32:21, 33:1, 33:9, 34:13, 130:16, 130:18, 147:9 die 104:10 dies 103:14, 103:17, 103:20, 104:8 difference 9:21, 51:22 different 16:22, 17:11, 18:3, 23:9,	28:6, 30:18, 30:20, 32:4, 43:9, 52:3, 58:15, 67:1, 72:12, 76:8, 76:10, 78:1, 84:17, 86:3, 87:1, 87:3, 90:18, 102:1, 102:8, 102:9, 102:14, 111:11, 114:15, 114:16, 116:15, 117:22, 118:5, 118:8, 125:20, 127:6, 133:8, 133:14, 133:18 differently 43:8, 50:2 difficult 22:22, 72:2 dig 75:9 direction 100:10, 159:13 directly 159:21 disagree 150:11, 150:12, 150:13 disaster 49:4, 51:11, 53:1, 53:4, 53:7, 54:12 disasters 55:14 disclose 137:20, 138:1, 138:21, 139:1, 139:10, 140:1, 140:4, 140:15, 140:19, 140:22, 142:16, 147:22, 148:6 disclosed 145:1, 150:8 discloses 102:5, 116:19,	126:4, 141:19, 142:2, 142:8, 142:12, 142:18, 143:3, 143:12, 143:22, 144:4, 144:11, 145:8, 145:9, 145:14, 145:15, 146:9, 146:19, 146:21, 147:8, 149:10, 150:2, 150:19, 151:15, 152:3, 153:9, 153:17, 154:2, 154:15, 155:14 disclosing 79:16 discuss 38:10, 43:10, 79:15, 154:10 discussed 35:18, 55:8, 64:9, 105:4 discusses 124:7, 124:10 discussing 61:5 discussion 88:3, 115:4 display 108:22, 109:7, 110:19, 114:14, 115:11, 116:8 displayable 119:14, 120:1 displayed 97:6, 97:11, 97:17, 109:7, 121:11, 142:19, 153:18 displaying 93:17, 97:12, 123:6, 143:12, 143:22, 155:15, 155:16 disputations 146:10 dispute 138:6, 138:8,
--	---	--	--

141:19, 142:1, 142:7, 142:11, 142:17, 143:2, 143:11, 143:21, 144:3, 144:11, 144:12, 144:16, 145:7, 145:9, 145:13, 145:15, 146:8, 146:14, 146:19, 146:20, 147:2, 147:8, 148:22, 149:9, 150:1, 150:18, 151:14, 152:2, 153:1, 153:8, 153:16, 154:1, 154:14, 154:22, 155:12, 155:13, 156:2, 156:4 disputed 143:10, 144:22, 155:10 disputes 144:7, 146:16, 151:21 disputing 143:19, 144:19, 147:10 distinct 86:11 distinction 24:9 distinctions 103:1 distinguish 109:22 distinguishing 37:22 distributed 60:14, 76:19, 77:2 divide 40:14, 145:22 dla 3:4 dns 76:14 document 24:2, 24:5,	25:6, 25:9, 30:19, 30:21, 31:1, 31:10, 31:12, 31:15, 31:18, 32:5, 32:9, 33:2, 33:4, 35:16, 37:8, 38:5 documentation 25:2, 32:13, 32:15 documenting 24:10, 24:20, 32:10 documents 5:19, 5:20, 31:12 doing 58:5, 60:5, 67:2, 67:19, 93:2, 99:16, 126:20 dollar 64:3 dollars 64:1 don 88:1, 152:7 donald 3:11 done 10:15, 10:19, 10:20, 11:3, 11:11, 23:4, 23:18, 24:17, 30:17, 31:2, 31:3, 31:13, 31:19, 32:11, 32:12, 39:4, 50:2, 50:8, 76:14, 87:8, 94:22, 114:15, 114:19 doru 3:19 double-check 33:12, 95:1 down 17:19, 20:4,	25:7, 54:15, 55:2, 58:22, 59:10, 59:11, 65:5, 84:6, 84:7, 84:16, 84:17, 84:19, 84:21, 85:20, 90:13, 93:13, 119:10, 124:4 download 76:11 dr 5:9, 7:5, 61:2, 88:9 drag 96:10 dragged 96:17 dragging 96:11, 96:20 draw 30:12, 30:14, 30:16, 32:8, 32:21, 33:1, 37:1, 37:3, 37:5, 37:7, 37:15, 39:1, 114:14 drawing 25:6, 38:2, 38:5, 127:2 drawn 36:3 drew 37:13 drive 3:13 drive-by 76:11 driver 51:8 dropped 6:22 drunk 51:8 due 61:10, 63:8, 63:13, 84:4,	85:5, 88:21, 89:12, 89:14 duly 5:3, 5:5, 159:7 dying 104:17 dynamic 115:2 E e 102:1, 106:20, 111:18, 112:7, 113:15 each 21:2, 49:21, 64:16, 91:1, 91:10, 112:7, 113:15, 119:11, 121:11, 122:6, 122:11, 122:15, 124:13, 124:15, 131:19, 149:14, 149:18, 153:10, 155:17 earlier 10:22, 28:5, 39:11, 41:1, 47:20, 55:6, 56:4, 56:11, 63:1, 65:8, 69:13, 88:19, 90:20, 95:11, 105:4, 120:17 earthquake 53:6, 62:6, 63:9, 63:13 earthquakes 54:17 ecosystem 117:13 edraw 34:5, 35:7, 35:10 effect 50:4, 53:8, 54:22, 82:13, 82:21
--	--	---	---

effects 20:1, 20:4, 20:8, 20:10, 39:14, 40:3, 48:11, 48:13, 48:19, 52:18, 52:20, 53:5, 59:9, 60:18 either 10:5, 15:3, 92:15 electricity 102:22 electronic 24:14, 31:12 electronically 103:2 element 131:20, 151:12 elements 34:7, 34:16, 35:10, 100:18, 130:8, 130:20, 131:2, 138:14, 152:18 else 23:19, 30:14, 30:22, 66:12, 157:2 email 58:10, 58:14, 59:3, 66:19, 66:22, 67:12, 68:1 emails 67:10, 71:5 embodiments 106:18, 111:15, 115:16, 116:1, 122:4, 122:14 emphasize 73:15, 74:9 emphasizes 40:8, 40:10 employee 159:18, 159:19 employee's 58:11	employees 67:7, 67:9, 72:21, 105:22, 106:1, 106:6 encompasses 56:1 encompassing 56:14 end 43:19, 46:3, 66:13, 68:5, 104:19 ends 23:1 engineer 16:8 engineering 8:22, 19:2, 76:11 enhances 125:4 enough 77:22, 105:9 enterprise 15:20 entirely 97:14, 145:19 environment 112:10, 113:18 environmental 102:2, 102:6, 102:13, 102:16, 102:21 equal 70:14, 71:11 equals 127:22 erase 45:20 errata 158:7 especially 62:10, 104:11, 127:10 essentially 109:12 establish 17:7	estimating 69:17 et 76:2, 102:2, 106:2, 112:8, 113:17 evaluating 69:18, 106:2 evaluation 130:9, 130:21, 131:6, 131:10, 131:13 evaluations 131:2 even 10:14, 28:15, 28:22, 51:4, 53:18, 58:20, 58:21, 58:22, 59:2, 60:6, 68:15, 70:21, 76:17, 77:17, 78:15, 83:3, 85:19, 86:17, 103:22, 134:19, 145:19, 152:17 event 20:9, 20:14, 54:7, 58:4, 59:7, 59:8, 59:17, 60:1, 60:2, 60:12, 60:17, 75:14, 75:18, 75:20, 82:8, 82:11, 82:16, 82:22, 83:4, 83:7, 83:19, 104:16, 123:16 events 19:22, 20:13, 39:13, 40:2, 52:17, 53:2, 65:18, 75:15, 76:1, 83:20, 83:21, 84:1 ever 13:21, 14:2,	14:5, 14:12, 14:17, 15:5, 15:10, 15:14, 18:5, 31:8, 36:2, 47:4 every 47:4, 72:21, 81:17 everybody 104:10 everyday 25:14 everything 45:21, 47:8 exactly 16:12, 68:12, 70:3, 84:2, 89:18, 113:11 examination 5:7, 159:7 examine 78:14 examined 5:6, 158:3 example 10:13, 10:15, 10:17, 11:17, 13:5, 17:5, 17:9, 20:9, 27:4, 28:14, 29:4, 31:14, 33:7, 34:4, 34:7, 34:15, 35:2, 35:6, 36:20, 36:21, 36:22, 37:9, 40:4, 41:16, 42:12, 42:13, 43:1, 43:7, 45:20, 46:11, 46:13, 46:14, 48:3, 49:2, 50:14, 50:17, 53:7, 54:12, 54:20, 56:13, 57:22, 58:9, 59:19, 60:15, 62:6, 62:8,
---	---	---	--

63:7, 63:10, 63:14, 63:17, 65:22, 66:17, 68:9, 72:13, 72:20, 74:14, 74:15, 79:15, 79:17, 79:21, 80:5, 84:3, 84:13, 85:15, 91:6, 95:10, 95:15, 96:14, 98:14, 99:9, 99:10, 99:22, 100:4, 107:19, 107:21, 108:5, 108:16, 112:6, 113:13, 113:14, 120:19, 121:7, 121:8, 124:13, 126:13, 126:16, 126:19, 127:19, 128:16, 138:18, 139:13 examples 42:21, 62:21, 134:20 except 144:12, 156:3 excuse 151:4 executives 71:19, 81:11 exemplary 38:16, 115:10, 116:7 exhibit 6:12, 6:15, 6:17, 7:2, 7:10, 7:13, 16:3, 18:18, 19:16, 20:17, 21:1, 26:2, 26:4, 26:6, 36:15, 36:16, 36:18, 39:6, 48:17, 61:3, 88:16, 101:7, 101:9, 101:12, 106:8,	106:10, 107:10, 115:18, 129:10, 129:12, 129:15, 137:11 exhibits 4:9, 6:22, 7:5, 7:8 exist 57:6, 57:13, 98:4 existence 155:10 exists 34:1 expect 105:18 expectation 103:16 expected 66:4, 66:10, 67:15, 67:16, 74:11 experience 10:9, 22:9, 22:16, 67:6 experienced 67:17, 74:11 experiencing 75:7 experiments 82:2 expert 8:15, 86:18, 103:8, 103:21, 104:3, 104:20, 105:8 expertise 8:12, 22:8 explain 51:21 explained 19:20, 100:14 explains 96:6, 114:4, 138:11 explanation 23:20, 114:2 explanations 126:18	explanatory 23:20 explicit 39:5 exploit 18:2, 54:10, 79:1 extension 57:18 extent 118:22, 143:17, 144:12, 150:6, 150:8, 153:4, 155:8, 156:3 external 17:12, 28:13 F face 133:2, 133:3, 133:6 facing 73:12 fact 24:2, 42:14, 51:19, 65:3, 75:5, 123:19 factored 10:18, 12:12 failure 20:11 fair 8:21, 9:2, 27:12, 29:6, 35:5, 68:22, 84:5, 99:21, 100:4, 133:7, 144:16, 151:12 fairly 28:14, 54:2, 72:8, 131:7 fake 76:13 false 20:11 familiar 11:6, 12:2, 12:10, 12:20,	13:3, 13:6, 14:15, 14:16, 32:19 far 11:15, 12:1 fashion 12:8, 32:1 fault 53:15, 53:18, 53:22, 54:13, 54:21, 55:2, 62:7 feature 54:14, 55:1, 62:7, 63:8, 63:13 features 34:8, 34:17, 35:11, 63:6, 112:9, 112:21, 113:17, 113:20, 114:9 feel 38:17 felt 56:5 few 5:18, 61:2, 128:19 field 77:10 figure 20:6, 41:15, 43:11, 43:13, 44:9, 45:1, 81:22, 90:1, 90:5, 90:17, 90:19, 91:6, 91:14, 94:9, 94:11, 94:14, 95:5, 95:6, 95:8, 96:4, 96:14, 97:1, 97:7, 97:9, 98:9, 111:15, 115:9, 115:13, 116:6, 116:10 figures 78:22
---	---	--	--

file 34:2, 34:3, 34:6, 34:9, 35:1, 35:12, 76:8, 100:11, 100:22, 101:4, 143:4, 143:5, 143:7, 147:22, 152:18, 154:3, 154:5, 154:6 files 98:22, 110:1, 142:2, 148:6, 154:19, 155:7, 155:10 financial 62:21, 62:22, 105:16, 105:22, 106:1, 106:5 find 68:16 finding 99:17, 99:19 finds 78:2 fine 6:10, 56:18, 87:19, 149:7 firm 8:16 first 5:5, 28:7, 31:3, 48:11, 50:8, 50:11, 56:6, 79:6, 92:21, 125:14 first-level 20:3 flow 76:19, 78:11, 117:12, 130:6, 131:15, 131:20, 132:2, 132:7, 132:8, 132:14, 136:15, 136:19, 137:3 follow-ups 134:18	follows 5:6, 140:2 foothold 78:19 foregoing 158:4, 159:10 forever 11:11 forgery 20:14 form 10:3, 10:12, 33:15, 49:14, 49:18, 60:9, 76:19, 82:19, 99:5, 109:9, 111:5, 113:21, 141:4, 143:15, 144:5, 147:5, 149:12, 150:4, 150:20, 151:17, 152:6, 154:20, 155:4 forth 64:19 forward 100:9, 151:9, 152:9 found 120:9, 121:19 foundational 117:15, 128:6 founded 8:19 founder 8:16 four 116:15 frame 11:16 framework 21:16, 22:6, 72:14 frameworks 11:14, 11:15, 11:21, 21:19, 22:2, 22:12 freeway 50:19, 50:21,	51:5, 51:12 frequency 80:21, 80:22 front 7:6, 7:8 fully 57:8, 96:16 further 84:16, 84:18, 115:16, 116:2, 156:17, 157:5 future 151:9 G gain 115:16, 116:1 gathered 112:4 gave 56:20, 74:14, 74:15 general 55:22, 84:19, 121:10, 139:20, 151:1 generally 11:6, 117:19, 140:2 generate 111:11, 112:9, 112:11, 112:16, 112:21, 113:2, 113:10, 113:17 generated 143:4, 154:3 generates 106:18, 111:16 generating 41:17, 155:12, 155:14 generic 131:7 generically 42:16, 84:11 germany 80:9 getting 7:7, 11:9,	32:4, 64:5 give 5:15, 26:9, 29:12, 80:5 given 42:5, 42:21, 62:10, 158:6, 159:14 gives 65:5 giving 78:8 go 6:20, 11:15, 11:22, 12:1, 16:5, 19:11, 23:9, 23:15, 26:12, 26:22, 30:2, 33:19, 39:6, 48:10, 49:2, 50:7, 50:9, 50:12, 56:14, 58:13, 59:9, 65:22, 66:17, 71:16, 72:20, 73:14, 74:4, 83:10, 83:14, 83:17, 88:3, 88:5, 88:6, 88:9, 88:14, 90:18, 91:3, 93:13, 98:18, 101:19, 117:17, 122:2, 124:21, 127:16, 128:3, 129:5, 134:18, 137:10, 148:2, 148:18, 149:21, 151:12, 156:21 go-to 21:21 goal 78:13 goes 11:4, 13:9, 14:8, 28:4, 38:11, 54:14,
--	---	--	--

55:2 going 6:16, 6:18, 6:19, 25:5, 27:13, 28:19, 36:14, 41:20, 44:8, 44:10, 46:18, 46:20, 46:21, 47:2, 47:4, 47:5, 47:12, 48:14, 50:16, 54:10, 58:2, 62:5, 64:12, 71:20, 72:9, 72:18, 77:21, 81:10, 81:13, 81:14, 84:9, 85:10, 85:16, 90:18, 104:10, 104:13, 114:22, 116:12, 118:9, 127:17, 128:18, 129:4, 133:14, 133:17, 141:18, 149:1, 149:7, 151:9, 152:9, 152:11 good 29:19, 87:15 government 11:8, 13:4, 13:14, 13:20 granular 118:19 granularity 44:11, 44:20, 44:21, 47:2 graphical 109:7, 110:12, 114:14 graphically 109:1, 109:15, 110:6, 110:22, 111:22, 112:1 grasp 72:7 greensboro 3:13	grief 149:4 ground 141:11, 148:15, 149:6, 149:10, 150:2, 150:12, 150:14, 150:19, 151:6, 151:15, 152:3, 153:9, 153:17, 154:2, 154:15, 155:13, 156:5, 156:6, 156:8 group 118:10, 118:11, 119:3 guess 44:15, 48:7, 60:3, 83:19, 85:9, 105:20, 118:15, 143:18, 150:22 guidance 22:12 H hackers 49:8, 49:13 half 56:10 halip 3:19 hand 160:2 handle 13:19 handles 13:13, 13:15 happen 54:11, 65:2, 66:12, 76:9 happened 52:12, 66:15, 77:4, 80:10, 80:12, 80:13, 81:6, 81:14, 81:22, 83:12 happening 59:18, 59:19,	59:20, 66:8, 69:17, 69:18, 81:2, 81:3, 97:15 happens 58:17 happy 43:9 hard 73:20, 74:17 head 12:18 heading 43:19 heard 13:21, 14:2, 14:5, 14:12, 14:17, 14:22, 15:7, 15:10 held 2:2 help 23:20, 28:17 helped 105:11, 105:14 helpful 92:8, 92:9, 92:10, 119:2 hence 47:16 here 12:6, 16:7, 17:2, 19:13, 19:14, 20:6, 20:21, 21:13, 28:20, 29:20, 32:12, 34:19, 39:11, 41:20, 43:16, 53:12, 55:7, 55:14, 58:3, 61:5, 64:8, 64:12, 67:20, 69:9, 90:15, 91:5, 91:12, 92:11, 99:4, 108:14, 113:14, 116:6, 121:5, 121:9,	126:13, 129:6, 132:16, 134:9, 136:12, 139:6, 139:17, 144:7, 145:20, 146:10, 152:16, 156:15 here's 123:8 hereby 158:2, 159:5 herein 5:5, 159:9 hereto 159:21 hereunto 160:1 hesitant 29:12 hi 5:9 high 8:14, 17:16, 17:17, 63:9, 63:13, 64:18, 64:19, 65:6, 73:1 high-risk 64:6 higher 17:7, 54:3, 68:6, 68:7, 68:12, 68:21, 71:9 hits 59:14 hold 125:10 hope 29:20 house 48:4, 49:2, 49:5 houses 84:4, 84:15, 85:5 however 31:1, 35:16, 35:22, 52:21,
--	--	---	--

66:6, 67:16, 74:7 http 47:9 https 47:8 huge 70:9, 80:8 human 51:19, 54:9, 56:9, 105:5 humans 40:6, 54:5, 54:18 hurlbut 86:18, 138:12, 139:13, 148:13 hurricanes 84:5, 84:19, 85:1, 85:6, 85:7 hyper 34:18, 35:4 hypothetical 27:14, 27:16, 29:7, 29:13, 36:5, 36:10, 53:12, 62:11, 70:7, 70:10	148:13, 150:10, 150:15, 156:8, 156:15 identifies 46:16, 97:3, 128:16 identify 11:1, 28:11, 40:15, 73:17, 74:7, 85:11, 85:12, 86:13, 96:4 identifying 22:22, 59:4, 72:15, 75:10, 85:2, 85:7, 97:4 illinois 159:5, 160:3 illuminate 23:16 illustrate 121:5 illustrated 111:14 illustration 18:19, 18:20, 19:9, 20:16, 36:15, 37:10 illustrative 51:3 imagine 123:9, 125:20 impact 61:9, 61:21, 62:17, 62:18, 63:4, 64:1, 65:2, 65:14, 65:15, 65:16, 65:19, 65:20, 66:3, 66:4, 66:7, 66:9, 67:4, 67:5, 68:6, 69:11, 69:12, 69:16, 70:12, 74:6, 74:22, 75:8, 75:21, 75:22, 81:5, 81:6,	82:7, 82:12, 82:18, 83:11, 83:13, 83:15, 84:11, 85:22, 86:20, 88:12, 88:21, 89:2, 93:6 impacts 138:13 implementations 42:2, 90:21 implies 21:10 imply 83:6 import 33:9, 34:13, 35:10, 133:21, 136:12, 147:3, 147:9 important 13:16, 17:8 importantly 131:15 imported 131:16, 132:2, 132:9, 132:14, 135:9, 136:15, 136:18, 137:3 importing 34:7, 34:15 imports 135:13 inbox 58:22, 59:14 inc 1:5, 1:8, 3:10 include 40:6, 50:1, 52:9, 52:13, 55:13, 59:16, 60:2, 93:4, 95:8, 97:13, 107:6, 110:13, 127:11, 127:22, 138:8, 145:2, 146:2, 156:12 included 16:21, 18:5,	45:11, 155:19 includes 25:2, 41:17, 42:3, 50:4, 110:16, 116:15, 150:7, 150:14 including 65:14, 65:15, 65:16, 117:8, 138:2 independent 100:15, 100:16, 138:15, 138:17, 144:13, 144:14 indicate 130:7, 131:1 indicated 150:7 indication 74:10 indirectly 159:21 individual 57:7, 69:8, 124:14 individually 124:16 industries 11:8 industry 21:22, 86:6, 86:13, 87:4 information 10:18, 25:7, 25:8, 32:1, 32:18, 62:13, 72:17, 74:13, 80:15, 80:17, 82:6, 82:7, 82:9, 82:14, 82:15, 82:16, 82:17, 82:21, 83:18, 83:21, 83:22, 89:21, 91:19, 91:20, 92:2, 92:10, 93:3, 108:21, 125:21, 128:7,
I			
icon 121:8, 121:17, 121:18 icons 121:6, 121:11 idea 67:21 identifiable 83:4 identification 13:17, 85:17 identified 21:6, 21:13, 46:12, 47:15, 72:16, 73:13, 75:10, 84:8, 93:1, 96:1, 97:13, 98:2,			

128:11 informed 71:22, 72:18 infrastructure 13:7, 53:15 inherent 32:13 initial 7:12 initiating 134:16, 135:22 input 22:11, 32:18, 33:7, 77:9 inputs 77:12 insecure 52:11 inside 44:2 insider 17:10, 17:11, 17:13, 28:13 insider's 104:4 instance 9:14 instead 31:9 instructions 114:13 insurance 74:2, 79:20, 103:6, 103:7, 103:8, 103:9, 103:10, 103:12, 103:19, 103:21, 104:3, 104:5, 104:6, 104:14, 104:20, 105:11, 105:15, 105:20, 106:4 intelligence 80:8 interaction 112:7, 113:16, 122:7, 122:20 interactions 57:9, 122:12,	122:16, 124:12, 124:18 interacts 122:19 interchangeably 86:8, 87:6 interested 28:8, 159:21 interface 90:21, 91:6, 96:9, 96:15, 147:3 interfaces 93:18, 142:18, 143:13, 144:1, 153:17, 155:16 internet 134:17 internet" 135:22 interpreted 51:2 interrupt 50:6 invent 132:17 inventors 132:17 invest 9:15 investigate 73:14 investigation 74:4, 81:21 investing 9:17 involve 10:13, 49:8, 49:17, 56:1, 56:7, 56:8, 110:22 involved 50:15, 51:20, 105:8, 130:5 involves 8:12, 10:13, 55:21, 99:16, 152:12	involving 50:17 ipr 1:11, 7:22, 8:3, 8:5, 8:9, 12:7, 17:2, 73:16 iriusrisk 1:5, 3:2, 13:21, 15:1 iriusrisk's 86:17 issue 68:7, 68:21, 70:1, 73:9 issues 47:9, 52:2, 52:9, 52:13, 55:14, 81:19, 134:20 item 91:7 items 96:12 itself 32:10, 38:3, 67:5, 74:10	150:20, 151:17, 152:6, 152:11, 154:20, 155:3, 156:19, 157:1, 157:5 james 1:16, 2:1, 4:3, 4:14, 4:17, 5:4, 158:2 job 1:20 john 14:17 jones 147:18, 147:21, 148:5, 148:16, 149:2 jump 141:13 jumping 140:11
			K
			keenan 4:11, 79:16, 79:17, 101:14, 137:19, 137:22, 138:19, 138:21, 139:1, 139:7, 139:10, 139:22, 140:3, 140:14, 140:18, 140:21, 141:3, 141:8, 141:10, 141:12, 141:19, 142:1, 142:7, 142:11, 142:17, 143:2, 143:11, 143:21, 144:3, 144:11, 144:17, 145:8, 145:9, 145:11, 145:14, 145:15, 146:8, 146:11, 146:14, 146:19, 146:20, 147:1, 147:3, 147:8 keenan's 102:4

keep 116:12, 117:4 key 37:20, 54:14, 55:1, 62:6, 85:10 kind 10:20, 11:5, 12:3, 12:6, 14:14, 17:7, 17:22, 18:1, 20:3, 24:1, 24:8, 27:14, 28:4, 28:21, 32:14, 32:15, 38:4, 38:10, 46:19, 54:14, 56:7, 56:8, 57:17, 58:19, 64:12, 64:13, 65:4, 67:19, 70:21, 72:16, 105:8, 105:14, 121:7, 121:16, 139:7, 150:22 knew 46:2, 75:3 knowledge 22:16 known 134:20, 134:21 knows 74:12, 78:1 L label 119:6 labeled 43:15, 44:2, 45:12, 137:16 labeling 119:7 labels 91:11, 92:3 land 68:2, 127:10 lands 70:20	landscape 112:2 language 50:4, 55:7, 77:14, 77:16, 114:16 languages 77:17 laptop 25:14, 25:15, 25:17, 27:17, 27:19, 28:10, 28:11, 29:10, 41:12, 42:20, 45:14, 45:18, 45:21, 45:22, 46:5, 47:4, 47:13, 47:14, 47:17, 47:21, 48:1, 95:12, 95:14, 95:16, 95:20 laptop" 45:12 laptops 47:3, 47:12 large 13:5, 43:14, 81:17, 105:20, 112:22, 113:2, 113:9, 113:10 larger 44:2, 44:13, 44:18, 45:11 last 15:21, 54:20, 80:19, 96:8 later 69:18, 134:15, 134:17, 135:21 law 29:17 layer 106:19, 109:1, 111:16, 111:21, 112:3, 112:9, 113:18, 116:16, 117:2, 117:3,	117:7, 117:9, 117:10, 117:12, 117:15, 117:20, 119:17, 120:8, 120:10, 120:13, 121:7, 121:11, 121:20, 121:22, 122:6, 122:11, 122:15, 122:18, 123:22, 124:8, 124:9, 124:10, 126:7, 128:6 layers 116:15, 116:21, 117:1, 117:3, 117:6, 117:8, 117:14, 122:13, 122:17, 122:19, 122:20, 124:7, 124:14, 124:15, 125:20, 126:5, 126:8, 128:5 layers" 122:7 laying 109:19 lead 20:13, 59:9 leak 80:8, 82:6, 82:9, 82:15, 82:16, 82:22, 83:6, 83:9, 83:18 leaked 80:9, 80:17, 80:18, 81:17 leaks 80:15, 81:13, 81:21 least 29:20, 35:6, 35:9, 42:17, 80:10, 84:1, 114:2, 116:16, 119:12, 122:5, 122:14, 132:7, 153:11	leaving 151:19 legal 103:15 legend 127:11, 128:1 legends 127:17 legitimate 120:5 less 12:1, 152:10 let's 25:13, 26:22, 29:21, 33:19, 35:17, 35:19, 37:9, 37:12, 37:13, 48:10, 49:3, 49:10, 50:12, 53:12, 60:20, 66:21, 67:4, 68:9, 77:19, 80:21, 81:1, 88:5, 88:6, 88:14, 95:4, 111:10, 116:4, 124:8, 130:2, 134:9, 148:18 letter 15:21 letting 56:19, 68:1 level 8:14, 17:7, 17:16, 17:17, 44:20, 44:21, 57:8, 64:15, 64:20, 69:10, 91:1, 91:10 levels 16:22, 18:3, 28:6, 58:15, 59:6, 65:6, 115:16, 116:2 libraries 77:17 life 25:14, 103:7,
--	--	---	---

103:9, 103:10, 103:12, 104:11 likelihood 54:6, 54:7, 61:11, 61:21, 62:16, 63:8, 63:11, 63:12, 63:16, 63:20, 64:21, 65:9, 66:7, 67:3, 67:22, 69:11, 70:20, 71:2, 74:6, 75:8, 84:12, 85:22, 86:20, 88:11, 88:22, 89:4, 89:8, 89:12, 89:13 likely 28:12, 29:11, 29:12, 89:5, 89:21 limit 84:12 limitation 93:14, 93:15, 93:17, 141:9, 141:18, 141:22, 148:14, 151:20, 153:1, 153:14, 154:13, 155:9, 156:1 limitations 103:15 limited 9:19, 28:15, 49:12, 49:16, 84:20 line 24:4, 26:17, 30:16, 32:8, 33:19, 33:21, 41:14, 42:2, 50:12, 53:15, 53:18, 53:22, 54:13, 54:22, 55:2, 55:9, 57:4, 62:7,	64:11, 90:20, 91:3, 91:5, 93:13, 96:8, 98:21, 101:19, 106:15, 108:18, 111:9, 111:10, 113:14, 115:7, 115:9, 115:15, 115:22, 116:4, 117:17, 121:10, 122:2, 124:6, 124:21, 128:3 lines 35:19 link 59:3, 66:19 links 69:21, 72:22 list 64:13, 90:22, 91:9 listed 91:1, 107:19 listing 141:15 lists 124:13, 124:16 literal 51:4 literally 110:5 literature 22:4 litigation 87:14 little 9:12, 30:19, 41:20, 44:1, 45:2, 46:18, 55:6, 59:5, 64:5, 67:19, 95:4, 102:19, 149:3 llp 3:4 local 58:20, 66:22, 70:18, 71:1	located 6:5, 6:8 location 69:7, 96:11 long 64:13, 138:10 longer 87:17, 88:1 look 16:2, 17:14, 24:18, 31:5, 43:10, 43:11, 47:2, 49:5, 61:3, 64:7, 64:10, 65:20, 66:4, 66:6, 69:13, 69:22, 70:17, 72:1, 73:10, 80:14, 81:5, 81:9, 84:11, 85:14, 90:1, 90:13, 93:7, 93:14, 94:9, 98:1, 101:6, 106:7, 106:15, 108:18, 112:20, 115:7, 124:4, 125:22, 126:3, 129:9, 129:17, 133:3, 137:13, 147:12 looked 52:10 looking 11:1, 19:8, 43:13, 55:8, 55:9, 65:2, 65:20, 66:9, 66:21, 69:19, 71:6, 72:4, 73:3, 97:14 looks 76:13, 121:8 lookup 99:17 loses 66:20 losing 70:14, 70:15,	71:8, 71:10, 73:21, 74:5, 74:18, 74:19, 74:21, 75:1, 75:22 loss 20:5, 20:14, 54:1, 54:7, 63:5, 63:8, 63:12, 65:3, 65:16, 65:18, 65:21, 66:1, 66:4, 66:10, 66:18, 67:15, 67:16, 68:15, 74:10, 74:11, 75:7, 75:14, 75:16, 75:19, 76:3, 76:4, 82:13, 82:17, 89:2, 89:3, 89:5, 89:12, 89:14, 89:22, 103:4, 103:19 losses 102:15, 102:16 lost 75:4, 75:13, 76:16, 146:12 lot 8:6, 16:22, 17:15, 30:18, 31:9, 33:14, 52:10, 53:13, 66:13, 78:13, 113:2, 113:5, 113:6, 114:15, 114:16 loud 140:8 low 64:7 lower-value 68:13 lucidchart 32:19, 32:21, 33:1, 33:4, 33:10, 34:4,
--	---	--	---

34:13, 35:7, 35:9 lunch 87:17, 87:21	132:8 manifold 78:14 manner 54:2 manual 78:3 manufacturer 16:16 many 16:17, 22:18, 70:5, 73:21, 74:18, 80:19, 81:1, 81:2, 81:3 map 107:1, 107:5, 109:3, 109:13, 109:17, 109:18, 109:21, 110:2, 110:8, 110:10, 111:20, 112:2, 115:17, 116:2, 117:15, 120:18, 127:6, 127:10, 128:6 map-like 112:10, 113:18 mapping 98:22, 100:11, 100:22, 101:4, 110:1, 121:15, 142:2, 147:22, 148:6, 152:18, 154:19, 155:7, 155:10 maps 127:3, 127:9, 127:18 maps" 128:9 march 1:17, 8:20, 160:3 mark 6:11 marker 6:18 market 3:5	marketed 131:17 marketplace 103:11 massive 81:6 match 99:17 matter 7:20, 12:3, 12:15, 44:6, 75:12 matters 159:9 matthew 3:3 maybe 13:1, 28:15, 36:21, 46:3, 47:4, 59:18, 60:11, 63:21, 64:4, 70:9, 71:21, 77:21, 84:16, 84:18, 85:4, 85:12, 87:11, 87:17, 125:14 mclean 3:15 mean 8:6, 8:7, 19:21, 23:21, 27:22, 28:2, 30:17, 36:18, 38:6, 39:12, 39:21, 40:5, 40:17, 48:12, 50:6, 51:7, 51:8, 51:15, 53:1, 56:16, 57:17, 58:13, 60:11, 65:11, 66:9, 67:18, 72:4, 76:17, 77:1, 80:3, 81:18, 82:15, 86:14, 86:15, 86:17, 97:20,	98:5, 102:19, 107:14, 107:16, 110:2, 110:6, 114:12, 123:12, 125:17, 125:19, 128:14, 128:18, 131:7, 131:11, 131:12, 134:3, 135:12, 139:16, 140:7, 141:10, 144:21, 148:1, 149:14, 149:17, 154:22 meaning 45:18 meaningless 72:9 meanings 99:8 means 100:2 meant 38:20, 87:9, 123:14 measure 28:16 measured 64:1 measurement 101:22 medical 16:15 medium 64:19, 65:7 meets 141:8, 144:14, 156:3 memory 76:18, 77:11, 78:5, 78:6, 78:10, 78:15, 78:17, 131:21, 134:15, 135:20 mentioned 10:21, 56:5, 88:19, 90:20, 108:15, 113:8 mentions 34:19, 47:8
--	--	---	---

merging 50:21 met 138:16, 138:18, 144:17 method 41:17, 149:10, 150:2, 150:6, 150:14 methods 57:6, 57:13, 74:8, 79:18 michelle 1:22, 2:3, 159:3, 160:9 microsoft 15:5, 15:7, 34:6, 34:22, 107:21, 108:5, 108:9, 108:10, 108:11, 108:17, 131:18, 132:20, 132:22, 133:6, 133:8 middle 19:19, 90:9, 91:16, 115:22 middleton 3:3, 4:4, 5:8, 6:11, 6:16, 7:4, 12:16, 26:2, 26:14, 49:15, 50:5, 60:20, 61:1, 83:1, 87:15, 87:22, 88:6, 88:8, 94:8, 94:20, 100:3, 101:6, 101:13, 103:5, 106:7, 106:14, 109:14, 114:6, 114:18, 115:6, 115:20, 116:3, 123:3, 124:20, 127:1, 129:4, 129:9, 129:16, 133:13, 135:1, 135:7, 135:16,	136:8, 137:6, 141:5, 143:20, 144:9, 146:1, 147:6, 148:17, 149:19, 150:16, 151:8, 152:1, 152:7, 153:7, 155:11, 156:17, 157:4 might 17:4, 20:5, 31:14, 38:5, 41:12, 42:12, 55:2, 65:1, 66:5, 66:18, 81:18, 81:20, 86:13, 114:8, 125:9, 125:11, 127:11, 139:1, 146:18 mind 26:20, 52:20, 79:11, 99:15, 146:13 minimize 125:18 minutes 87:17, 128:19 mirror 112:2 miscalculating 57:10 misprint 125:9, 125:15 misread 125:11 misspeaking 87:11 misspelling 125:6 misspoke 90:11, 90:12 mitigate 54:17, 54:18, 72:10, 74:2, 74:3, 75:1, 75:9, 75:11, 80:3, 82:4,	92:19, 121:13 mitigating 71:16 mitigation 81:20 modeled 96:13 modeler 46:18, 47:1 modeling 10:9, 10:12, 10:13, 10:19, 10:22, 11:7, 11:10, 15:6, 15:8, 15:10, 15:12, 15:14, 23:4, 41:16, 48:2, 50:1, 50:2, 50:3, 50:15, 50:17, 51:6, 54:3, 55:10, 55:16, 55:21, 55:22, 56:2, 57:5, 57:6, 59:5, 60:13, 79:16, 80:6, 85:14, 85:15, 105:1, 117:8, 117:20, 119:15, 149:10, 150:2, 150:19 models 11:3, 11:4, 15:19, 16:9, 16:13, 16:18, 16:21, 17:1, 17:6, 18:12, 18:13, 22:5, 22:8, 22:18, 23:3, 31:8, 31:11, 31:13, 47:6, 52:14, 84:11, 84:19, 85:19 module 108:21, 111:13, 111:16, 112:4, 112:14, 116:9	moment 19:14 more 11:9, 12:10, 17:2, 17:20, 18:7, 19:21, 21:4, 21:22, 22:21, 29:11, 29:16, 39:12, 43:4, 52:17, 53:2, 53:19, 62:13, 63:3, 68:7, 68:22, 75:15, 77:22, 78:4, 93:18, 98:22, 103:1, 104:4, 104:6, 104:15, 109:2, 109:16, 110:7, 115:1, 118:18, 128:14, 129:5, 131:8, 141:20, 142:2, 142:3, 142:18, 142:19, 142:20, 143:3, 143:7, 143:12, 143:22, 148:6, 151:15, 153:12, 153:17, 153:18, 153:19, 154:2, 154:7, 154:16, 154:18, 155:14, 155:16, 155:18 most 9:21, 10:10, 17:8, 24:3, 28:12, 77:14, 90:22 mostly 22:6 motivation 150:9, 150:11, 150:13, 151:2, 151:5, 151:11, 156:9 mountain 127:20, 128:1 moving 147:2
--	--	--	--

much 27:16, 35:15, 35:21, 59:19, 67:16, 68:6, 68:16, 68:21, 71:5 multi-layered 111:12, 115:10, 116:7, 116:14, 116:20 multiple 34:19, 74:8, 83:20, 96:11, 96:17, 97:21, 116:21 multiplication 65:4 multiply 66:14, 67:17, 69:16 must 29:1, 115:14 myself 103:9, 149:3 N name 14:14, 14:15, 85:13, 91:10, 92:3 naming 85:9 narrative 23:15, 90:18 narrow 84:6 narrowed 85:19 native 32:15, 100:18, 101:1 natural 49:4, 51:10, 53:1, 53:4, 53:7, 54:12, 55:14 nature 72:8, 85:17	near 91:8, 117:11 necessarily 49:7, 51:7, 60:6, 73:18, 84:12 need 17:17, 17:18, 23:15, 23:18, 28:3, 40:9, 42:22, 43:4, 43:5, 44:17, 47:10, 48:22, 62:14, 62:15, 62:16, 63:4, 68:7, 68:21, 71:15, 72:17, 73:14, 89:8, 89:11, 89:13, 89:20, 92:17, 93:3, 104:3, 125:22, 133:22 needed 9:14, 49:22 needs 22:17, 23:22, 77:8, 77:10 negative 20:12, 130:12, 131:5 network 17:4, 31:15, 43:15, 43:16, 44:5, 44:10, 44:13, 44:16, 44:19, 44:20, 45:8, 45:15, 47:14, 47:17, 78:20, 95:13, 95:16, 95:18, 95:19 network" 44:3 networks 13:1, 55:22, 57:5, 57:20 never 14:22, 15:2,	77:4 new 37:12, 37:14 newspapers 80:7, 80:11 next 45:5, 50:16, 55:19, 113:5, 119:11, 131:14, 134:10 niche 11:9 nielson 1:16, 2:1, 4:3, 4:15, 4:17, 5:4, 5:9, 7:2, 7:5, 26:4, 61:2, 88:9, 101:9, 106:10, 129:12, 158:2 nist 11:16, 13:5, 21:16, 21:21, 22:6, 72:14 nobody 31:7 non-computer-rel- ated 56:2 non-expert 104:2 non-limiting 96:14 non-native 101:3 normal 77:4 normally 77:2, 77:3, 77:5 nos 7:2 note 86:17 notes 23:20 nothing 25:3, 66:14,	92:14, 135:12, 156:10, 157:5 notice 2:2 noun 83:8 number 8:8, 9:19, 22:22, 23:5, 67:1, 69:12, 72:12, 76:6, 76:8, 78:8, 80:15, 97:20 numbering 6:17, 6:19 numbers 62:9, 67:18, 69:12, 69:16, 70:11 O o-w-a-s-p 11:19 oath 5:13 object 40:15, 49:14, 49:18, 82:19, 99:5, 109:9, 111:5, 113:21, 141:4, 143:15, 144:5, 147:5, 149:12, 152:6, 152:11, 154:20, 155:7 objected 155:3 objection 94:5, 94:16, 114:10, 114:20, 122:22, 124:2, 126:14, 133:9, 134:7, 135:4, 135:10, 136:5, 136:20, 145:17, 148:9, 150:4, 150:20, 151:1, 151:17, 152:8,
---	---	---	--

152:9, 152:14, 155:2 objectives 132:1, 132:13, 134:12, 135:14, 136:14, 136:17, 137:2 objects 127:6 obtained 83:21 obviously 8:6, 12:5, 12:9, 37:18, 46:17, 60:1, 70:6, 99:22, 102:22, 107:16, 114:14, 144:17 obviousness 147:16 occur 19:22, 39:13, 52:18, 76:4, 76:6, 89:1, 89:6 occur" 61:11 occurred 60:18, 89:4 occurring 123:18, 123:19 occurs 61:10, 65:19, 68:15, 88:22, 103:20, 104:8 odds 52:6 offering 8:2 offerings 106:5 office 1:1, 29:17, 29:18, 43:15, 43:16, 44:3, 44:5, 44:9, 44:13, 44:16, 44:19, 44:20, 45:8, 45:15,	47:14, 47:17, 95:12, 95:16, 95:18, 95:19, 107:21, 108:5, 108:10, 108:11, 108:17, 131:18, 160:2 okay 6:13, 6:21, 25:10, 29:21, 43:14, 49:7, 58:8, 60:20, 68:5, 69:6, 73:12, 80:16, 80:20, 87:18, 87:20, 90:5, 92:6, 101:12, 108:11, 129:7, 141:13 once 30:17, 32:11, 72:15, 75:10, 78:14, 136:12 one-thousandths 67:17 one-to-one 86:21 ones 12:14, 17:9, 98:1, 98:3, 148:13, 156:15 online 134:20 only 34:18, 44:10, 45:18, 56:6, 60:10, 65:18, 70:4, 73:5, 77:21, 84:7, 84:9, 91:18, 91:20, 92:2, 149:15 open 5:22, 25:21, 26:11, 101:12 operate 60:10 operating 105:5	opine 137:19, 137:22, 139:22, 140:14, 140:18, 140:21, 147:15 opinion 139:10, 139:20, 139:21 opinions 7:20, 7:21, 7:22, 8:3, 8:4, 8:7, 8:8, 137:16, 141:2, 141:7, 141:11 order 66:12, 79:18, 79:19, 79:20, 80:1, 82:3, 91:1, 92:18, 92:19, 93:3, 133:21 organization 16:1, 68:3, 68:19, 69:20, 70:5, 70:15, 71:8, 71:10, 73:12, 74:12, 130:10 organizational 57:10 organizations 131:3 organized 91:9, 117:20 original 34:8, 35:11 other 6:3, 8:2, 8:4, 21:19, 29:4, 55:14, 60:7, 66:5, 71:11, 71:19, 73:7, 73:20, 74:16, 76:10, 76:16, 77:17, 78:5, 78:6, 78:19, 97:18, 99:18, 99:21, 106:5,	112:8, 113:6, 113:16, 114:4, 117:6, 122:19, 125:7, 126:20, 128:7, 130:8, 130:15, 130:17, 130:20, 131:1, 138:1, 138:6, 138:14, 138:17, 140:1, 148:3, 151:20 otherwise 75:20 out 12:13, 19:10, 20:15, 25:20, 38:18, 43:17, 53:11, 55:6, 60:5, 67:20, 68:3, 68:19, 69:20, 70:6, 70:7, 70:13, 70:15, 72:21, 73:8, 78:2, 78:17, 78:22, 80:8, 81:22, 82:1, 87:7, 90:17, 103:13, 103:17, 104:6, 104:13, 104:15, 109:20, 140:8, 146:6, 146:7, 151:19 outcome 130:12, 131:5, 159:22 outcomes 83:5 outlook 58:11, 108:8, 108:9, 108:15 output 25:4 outside 56:22 over 25:5, 26:22, 31:6, 57:2,
--	---	---	---

64:8, 80:14, 80:19, 134:17, 135:22, 147:17, 149:16 overflow 76:17, 77:6, 77:7, 92:12 overflows 17:21, 78:21 overlaid 121:22 overlap 23:3 overlay 117:14, 120:7, 120:12, 120:19, 120:20, 120:21, 128:6, 128:22 overlaying 116:15, 128:20 overview 78:9 overwrite 78:5, 78:9 overwriting 78:6 owasp 11:16, 11:18, 21:16, 21:22 own 30:22, 32:14, 78:12, 144:2 owner 1:9, 119:9 owners 119:3	palo 13:1 paper 37:16, 37:19 papers 22:4 paragraph 16:5, 18:17, 19:9, 19:15, 20:17, 21:2, 36:16, 36:19, 37:10, 38:19, 39:9, 48:16, 55:20, 61:3, 61:8, 88:14, 100:19, 111:8, 112:18, 113:5, 114:3, 124:5, 129:17, 130:2, 139:4, 141:11, 147:12, 147:20, 148:4 paragraphs 43:6, 139:9, 148:2, 148:11 part 10:19, 11:10, 18:11, 26:12, 26:18, 40:21, 41:21, 43:10, 43:17, 43:20, 51:1, 51:18, 53:10, 78:10, 79:7, 83:22, 107:16, 108:17, 125:11, 135:17 particular 9:13, 16:15, 28:19, 31:14, 40:8, 71:3, 119:15 particularly 86:16 parties 71:20, 159:20 parts 49:20, 78:5, 78:6, 151:20	password 76:7, 77:10 past 70:21 patent 1:1, 1:3, 1:9, 1:12, 4:10, 4:11, 4:12, 20:22, 21:2, 25:12, 27:1, 27:8, 30:1, 30:4, 30:6, 30:8, 30:21, 31:2, 31:4, 32:10, 33:17, 38:11, 38:18, 38:21, 38:22, 39:4, 40:20, 41:8, 41:13, 43:12, 47:6, 49:12, 49:16, 50:4, 51:2, 58:3, 61:6, 61:15, 61:16, 62:1, 64:4, 64:9, 88:19, 90:2, 93:7, 94:10, 94:15, 96:6, 98:1, 110:1, 133:2, 133:3, 133:6, 138:1, 140:2 pay 103:13, 104:13 payload 58:6 pays 104:6, 104:15 pennsylvania 3:7 people 11:11, 11:12, 11:13, 68:4, 68:19, 69:20, 70:13, 86:6, 86:9, 87:4 perceived 117:9	percent 60:3 percentage 63:20, 63:22 perfect 53:20 perfectly 53:20 perform 9:22, 29:14 performed 9:8, 9:10, 38:9, 38:15, 39:22 performing 92:8 perhaps 64:22 person 64:22 personal 159:13 personnel 130:9, 131:3 persons 130:5 perspective 44:6, 45:8, 45:15, 47:14, 47:17, 51:6, 52:11, 95:12 petitioner 1:6, 138:12, 148:13 ph 1:16, 2:1, 4:3, 4:15, 4:17, 5:4, 158:2 philadelphia 3:7 phishing 58:9, 58:10, 59:3, 66:18, 66:22, 67:9, 67:12, 68:1, 70:16, 76:5, 76:7 phrasing 83:3
P			
page 4:2, 4:9, 76:13, 76:14, 137:15, 138:10 pages 1:21 paid 103:17 painful 152:10			

physical 5:20, 109:13 physically 37:18 piece 37:15, 37:16, 37:19 pieces 113:6 piper 3:4 place 43:8, 64:8, 71:4, 77:11, 159:16 places 9:15, 40:10 players 11:7 please 6:11, 6:13, 10:8, 16:5, 19:9, 20:15, 26:1, 106:9, 129:9, 129:11, 142:10 plurality 153:1, 153:9 point 19:10, 20:15, 22:1, 34:19, 40:21, 43:2, 43:19, 46:3, 55:6, 71:12, 85:21, 98:16, 104:18 pointing 12:13 points 31:18 poisoning 76:15 policies 103:17, 104:12 policy 103:13 port 25:16, 25:18,	27:4, 27:10, 27:18, 27:20, 29:2, 29:9, 30:7, 30:11, 30:15, 38:12, 42:13, 42:19, 45:2, 45:4, 45:11, 45:19, 46:2, 46:4, 46:21, 47:5, 47:15, 47:18, 95:11, 95:14, 95:17, 95:21, 95:22, 97:16, 97:19, 97:22, 98:15 portion 116:16 ports 47:4, 47:12 possible 47:16, 55:4, 68:17, 80:12, 99:8, 122:6, 122:16, 124:16 potential 19:21, 21:3, 21:7, 21:8, 21:10, 38:13, 39:13, 45:10, 49:3, 52:17, 53:2, 53:6, 55:11, 55:17, 57:7, 57:14, 59:20, 60:1, 60:3, 60:6, 60:14, 60:17, 61:9, 65:18, 71:4, 75:20, 76:1, 76:2, 82:10, 84:7, 88:21, 123:16 potentially 28:2, 46:6, 67:13, 78:3, 78:5 practice 127:2	precise 34:18 predetermined 132:1, 132:13, 134:2, 134:11, 134:13, 135:2, 135:19, 136:13, 136:16, 137:2, 137:4, 137:7 prefer 68:16 preference 12:3, 12:15, 68:16 preferences 11:12, 11:13 premiums 79:21 preparation 7:17 present 3:18 presented 7:3, 26:5, 101:10, 106:11, 129:13 presumably 124:18, 133:20 presume 133:15 pretty 29:19, 35:15, 35:21, 39:5, 81:6, 131:12, 131:13 previous 140:3, 159:6 previously 95:5, 134:14, 135:18, 135:19, 137:5, 137:8, 155:22 primarily 22:2 primary 21:21, 55:16 prior 31:7	prioritize 10:6, 11:1, 55:11, 55:17, 70:2, 70:3, 71:13, 71:15 priority 73:1 probabilities 54:5 probability 69:14, 71:1 probably 35:3, 63:3, 73:1, 116:13 problem 70:9, 72:7 problems 13:17, 102:14 proceeding 6:20 proceedings 159:14 proceeds 131:19 process 41:17, 41:18, 42:2, 42:5, 69:13, 93:19, 96:13, 111:13, 119:5, 131:18, 131:21, 134:14, 134:15, 134:16, 135:20, 135:21, 135:22, 143:14 processer 131:22 processes 56:3, 112:12, 112:15, 130:6 processor 132:12, 137:1 produce 31:11 product 103:10 professional 16:8 profile 52:7
---	--	--	---

program 77:19, 78:16, 114:13 programming 17:22, 77:16, 114:16 programs 34:5 proper 152:13 properties 48:21 protect 28:10, 48:21 protecting 17:19 protections 29:19 protocol 20:10 provide 9:4, 9:6, 22:12, 61:16, 63:17, 99:7, 101:4, 103:7, 136:11, 138:15, 138:19, 139:12 provided 103:10, 112:4 providers 12:3 provides 24:19, 24:22, 54:13 providing 36:10, 70:10, 79:18, 106:4, 141:19, 142:2, 151:15 publication 13:17 publications 86:12 pull 19:12, 20:21, 33:8, 33:16, 78:16, 90:14 purpose 55:16	purposes 38:16 pursuant 2:2 put 6:18, 9:20, 22:9, 42:20, 46:11, 46:15, 59:18, 77:20, 78:4, 78:11, 81:8, 92:21, 152:16, 152:22 putting 29:4 Q qualify 71:21 qualitative 10:6 quantify 73:11 quantitative 10:5 quantize 65:5 quantized 64:6, 64:17, 65:11 question 11:5, 26:21, 27:13, 32:4, 36:6, 37:20, 48:7, 50:9, 56:10, 56:20, 56:21, 57:18, 79:6, 85:4, 108:4, 110:4, 131:8, 141:6, 142:10, 144:10, 144:20, 146:12, 147:7, 149:21, 150:17, 152:12 questions 5:18, 28:7, 38:7, 56:5, 61:2, 148:19, 151:9, 156:18,	156:21, 157:1 quickly 87:12 quite 72:14 quoting 25:20, 113:13 R random 51:10, 51:16 range 12:13, 28:15, 28:16 reaching 66:22, 104:19 read 34:1, 41:15, 43:7, 55:15, 57:11, 57:12, 64:11, 77:8, 80:7, 90:17, 102:10, 112:16, 112:18, 117:5, 125:8, 125:14, 128:10, 130:14, 132:5, 132:11, 135:12, 135:17, 140:7, 158:3 read-on 5:2 reading 19:15, 21:1, 27:12, 100:18, 110:5, 110:9, 113:12, 117:4, 139:5, 143:4, 154:3 reads 93:17, 122:4 real 48:3, 49:2, 53:11, 59:19, 76:14, 127:8 really 38:7, 56:6, 66:2, 68:11, 77:13, 86:14,	105:5 realtime 117:11, 123:17 reason 5:15, 53:17, 60:4, 69:21, 138:16, 138:17 reasonable 28:2, 29:16, 44:14 reasonably 103:9 reasoning 140:2 reasons 52:3, 84:17, 105:4 rebuttal 139:12 recall 14:14, 16:17, 56:4, 56:11, 79:3 receive 67:12, 111:13 received 59:8, 108:21 receives 66:19, 112:12, 112:14 receiving 60:11 recess 60:22, 88:7, 129:8, 156:22 recognize 67:10, 136:9 recommendations 13:18 record 24:11, 24:13, 88:3, 115:5, 156:21, 157:3, 159:13 redirected 76:12 redirection 76:15
--	---	--	--

reduce 125:21 reduced 159:12 reducing 140:10 refer 19:16, 64:18, 72:14, 79:8, 149:2 reference 4:13, 101:14, 101:16, 129:18, 141:3 referenced 55:5 references 148:3 referring 18:9, 40:22, 41:15, 79:9, 115:19, 123:5 refers 41:13 regarding 141:2 regards 57:4 relate 9:18, 102:13, 113:20, 141:12, 152:19 related 10:11, 10:16, 17:3, 47:9, 55:21, 89:16, 92:17, 105:12, 112:5, 124:18, 139:13, 139:14, 141:7, 141:8, 141:21, 142:5, 145:5, 146:3, 151:11, 153:6, 154:11 relational 93:18, 93:22, 94:2, 96:15, 97:9, 143:13,	143:17, 143:19, 144:1 relationship 86:21, 98:9, 98:14, 99:20 relationships 96:19, 98:10, 98:12, 106:21, 107:8, 107:11, 107:18, 111:19, 143:7, 154:7 relative 112:8, 113:16, 115:1, 159:18, 159:19 relevant 21:3, 27:5, 29:3, 41:2, 41:5, 42:4, 52:21, 96:22, 97:2, 97:3 rely 11:15 remark 6:14 remember 15:21, 33:11, 63:15, 65:17 remote 1:16 remotely 2:2, 5:19, 159:16 remove 47:9, 91:18 render 108:22, 111:11 rendered 115:11, 116:8 renders 106:19, 111:16 repeating 26:20, 146:13 rephrase 85:4, 108:4, 141:6, 144:10, 147:7, 150:17 report 19:13, 20:7,	24:11, 24:13, 39:7, 39:17, 62:3, 79:7, 79:16, 79:20, 86:2, 86:17, 88:14, 95:3, 100:14, 100:19, 138:4, 138:19, 138:21, 138:22, 139:1, 139:2, 139:4, 142:6, 142:15, 143:10, 146:3, 146:20, 147:11, 147:13, 155:16 reported 1:22, 159:11 reporter 2:4, 11:19, 13:11, 157:2, 159:4, 160:10 reports 8:10, 139:7, 146:21, 147:1 represent 7:19, 7:21, 101:22, 110:14, 110:19, 112:17, 119:14, 121:6, 121:12, 124:11, 127:6, 127:8, 130:16, 130:19 representation 38:1, 97:8, 113:4 representations 93:20, 100:20, 138:3, 146:9, 146:15 representative 41:16 represented 53:20, 98:15, 125:3, 128:9 representing 116:16, 117:9, 117:10, 117:12, 121:17, 121:18,	132:8 represents 127:20 reproduced 20:7 require 81:20 required 103:13 requirements 85:20, 99:18, 144:19, 145:6 requires 10:3, 138:20, 150:9 reread 144:2 research 8:22 resources 9:16, 9:18, 9:20, 70:4, 71:14, 71:16 respect 97:1 respected 21:22 respective 130:9, 131:3 response 20:11, 49:11 responses 13:18 responsible 71:20 rest 59:10, 156:9 result 54:16, 55:3, 76:16, 82:11, 89:22 resulted 65:3 resulting 54:1, 76:3 results 66:1, 75:21, 82:11
---	--	---	---

retaining 34:8, 34:16, 35:11 retirement 106:1, 106:5 retrieved 134:16, 135:21 reverse 10:21 review 7:16, 9:5, 10:15, 101:16, 129:21, 139:3 reviews 10:15 rid 92:3 rimon 3:12 risks 10:6, 57:10, 64:18, 64:19, 72:1, 72:4, 73:7, 84:15, 86:3, 87:5, 89:16, 89:17, 89:19, 90:5, 102:1, 102:6, 102:9, 102:11, 102:13, 102:14 rmr 1:22, 2:3, 160:9 road 120:21, 121:2, 121:8 roads 113:5, 113:6 ross 18:22 route 120:21, 121:3 routers 31:17 rows 91:9 run 15:22, 82:1	running 78:16 russia 80:9, 82:17 s safe 15:1 safely 50:18 safety 50:2, 51:22, 52:2, 52:4, 52:9, 52:12, 52:13, 55:14 said 29:7, 44:12, 48:6, 63:1, 65:8, 95:19, 108:9, 108:10, 123:11, 144:21, 159:15 sake 29:22 same 6:17, 6:19, 15:22, 19:4, 24:4, 33:2, 33:4, 42:10, 55:20, 68:12, 99:15, 110:2, 111:8, 119:10, 124:4, 133:12, 139:16, 140:2, 144:20, 148:19, 152:3, 154:9, 154:10, 158:4 satisfied 150:15 save 149:3 say 8:21, 10:10, 13:19, 15:2, 19:17, 22:7, 23:13, 25:13, 29:1, 34:15, 35:17, 35:19, 36:20, 36:22, 37:12, 37:13, 41:11, 42:16, 42:22, 45:21, 46:20, 47:2, 49:3, 53:12, 53:17, 58:4, 64:22, 66:21, 68:9, 70:19, 73:19, 73:20, 74:17, 74:21, 77:19, 79:19, 85:3, 97:15, 100:4, 100:9, 108:3, 108:9, 112:20, 118:7, 123:14, 127:17, 133:7, 136:7, 138:18, 139:19, 142:10 saying 27:9, 28:5, 31:9, 34:20, 36:12, 46:13, 51:17, 55:13, 73:6, 73:7, 77:3, 92:20, 102:4, 109:5, 112:13, 116:19, 122:10, 132:6, 138:7, 139:17, 140:6 says 27:1, 27:2, 29:1, 29:2, 31:5, 31:22, 34:1, 34:21, 42:1, 45:1, 45:2, 46:14, 50:14, 55:20, 56:13, 57:4, 57:13, 90:10, 90:13, 91:5, 91:14, 91:17, 98:21, 99:11, 101:21, 106:17, 107:3, 107:10, 108:20, 109:11, 111:9, 113:12, 114:5, 115:9, 115:15, 116:6, 117:19, 119:11, 121:5, 121:9, 125:1, 126:11, 128:5, 128:11, 128:13, 131:14, 134:4, 134:9, 135:13, 136:12, 136:22, 137:9, 149:16, 149:17 scenario 48:8, 49:1, 54:19, 63:18, 72:22, 74:19, 82:5, 103:18, 121:2 schedule 88:4 scope 56:1 scratch 40:18, 144:2 seal 160:2 search 134:20 searches 134:16, 135:22 searching 134:19 second 7:7, 26:3, 26:10, 43:17, 56:10, 101:8, 106:9, 125:10, 137:15 secrets 80:18, 81:17 section 95:21, 137:16, 138:7, 138:10, 139:8, 139:22, 140:3, 140:9, 147:15, 153:3 security 8:22, 11:11,
--	---

13:7, 17:14, 19:2, 43:20, 51:22, 52:1, 52:3, 52:4, 52:21, 53:8, 54:14, 54:15, 55:1, 55:2, 62:6, 63:3, 63:6, 63:8, 63:12, 106:3, 117:10, 124:9, 125:4 see 17:4, 20:6, 21:5, 26:9, 27:2, 43:5, 43:14, 44:22, 45:1, 46:5, 48:8, 50:13, 51:5, 79:8, 80:17, 90:18, 93:16, 101:21, 102:3, 106:17, 107:2, 108:20, 111:8, 114:2, 118:1, 118:4, 119:16, 120:13, 124:8, 126:3, 127:15, 133:2, 133:5, 134:9 seem 131:7 seems 29:11, 43:15, 120:16, 131:12, 131:13 seen 96:17, 127:17 sees 59:1 select 96:9 selecting 42:3, 91:7 selects 96:21 sending 58:10	sense 17:3, 53:21 sentence 55:15, 55:19, 109:11, 110:5, 110:9, 116:1, 119:11, 129:3, 130:4, 131:14, 134:10, 144:2 separate 64:15, 146:22, 147:1, 151:4, 151:5 separately 49:21 server 58:18, 58:21, 59:7, 67:1, 67:13, 68:2, 68:10, 68:12, 69:5, 70:18, 70:20, 70:22, 71:2 service 9:4 services 9:6 session 6:3 set 12:5, 20:3, 46:17, 46:19, 46:20, 77:11, 77:19, 121:6, 126:8, 135:2, 160:1 seth 1:16, 2:1, 4:3, 4:14, 4:16, 5:4, 87:18, 158:2 shape 113:2, 113:10, 131:19, 133:16, 136:13 shapes 110:13, 110:16, 110:18, 110:22, 111:3, 112:16,	112:19, 113:20, 114:8, 127:5, 127:7, 130:7, 130:15, 130:17, 130:19, 130:22, 132:2, 132:7, 132:14, 133:17, 133:19, 133:21, 134:1, 134:2, 134:22, 135:3, 135:6, 135:8, 135:9, 135:13, 136:4, 136:10, 136:14, 136:18, 137:3 sheet 158:7 shop 29:8, 29:15 short 156:19 shorthand 2:4, 159:4, 160:10 shostack 14:12 should 11:1, 12:4, 19:21, 22:13, 71:21, 83:10, 83:14, 85:4, 129:6 shoulder 21:10 shouldn't 58:20, 83:16, 83:18 show 20:12, 70:11, 94:14, 113:4 showing 90:5, 91:10 shown 91:8, 116:14 shows 20:4, 91:6, 94:18, 96:14, 98:9, 98:12,	115:9, 116:6 sign 64:3 signature 158:10 signature-b7fzp 160:6 signed 158:7 significant 23:2, 28:18, 58:16, 75:5 signs 121:11 similar 128:7 similarly 47:11 simple 35:17 simply 85:22, 136:12 simulated 117:12 since 5:18, 14:22, 33:12 single 85:20 sitting 29:17, 54:13 situation 74:21, 89:15 situations 60:7, 76:16, 89:19 size 112:8, 113:17, 115:1 skeletal 36:21 skeleton 23:14 skill 65:1 skip 41:20, 57:2 slice 60:13
--	---	--	---

slightly 87:16 smartdraw 34:4, 35:7, 35:9 social 76:11 soft 34:5, 35:7, 35:10 software 1:8, 3:10, 24:6, 24:19, 34:1, 99:2, 100:16, 100:18, 106:21, 106:22, 107:7, 107:11, 107:12, 107:17, 107:18, 108:1, 108:6, 111:3, 111:18, 111:19, 112:7, 112:17, 113:3, 113:4, 113:7, 113:15, 131:17, 133:11, 142:9, 142:13, 143:5, 148:8, 152:20, 154:4 solutions 72:12 some 10:3, 11:12, 11:13, 12:7, 12:17, 21:6, 22:12, 23:15, 23:20, 24:1, 24:20, 25:2, 28:1, 28:21, 29:4, 29:19, 34:8, 35:11, 38:4, 38:13, 40:1, 54:13, 55:20, 56:7, 56:8, 64:18, 65:4, 70:21, 71:1, 76:10, 76:15, 77:8, 78:21, 79:18,	81:13, 81:18, 93:5, 97:18, 98:12, 99:18, 102:19, 102:22, 103:9, 106:17, 107:16, 111:15, 115:15, 120:16, 121:7, 121:14, 121:16, 122:4, 122:14, 130:22, 134:18, 139:12, 140:10, 148:19, 154:10 somebody 51:9, 77:20, 87:8, 87:11, 103:17, 104:17 someday 104:13 somehow 100:1, 103:2 someone 30:14, 86:12, 103:14, 103:20, 104:8 something 18:9, 25:20, 40:14, 60:5, 63:21, 115:1, 115:2, 123:9, 123:18, 123:19, 125:22, 128:17, 134:1, 142:22 sometimes 14:8, 18:21, 19:5, 67:8, 78:17, 86:7, 86:12, 87:5 somewhat 10:1, 32:13 somewhere 87:7, 87:8, 114:12 sorry 26:20, 35:14, 36:18, 40:18, 48:14, 56:17, 58:13, 62:13,	83:6, 88:15, 91:20, 108:8, 123:11, 127:16, 144:1, 146:11, 155:1 sort 12:5, 12:7, 44:22, 84:22, 92:7, 105:17 sorted 64:14 sound 77:13 sounds 14:15, 14:16, 115:1 source 9:4, 10:14, 10:15, 21:4, 21:7, 21:8, 21:10, 21:11, 27:5, 29:3, 41:6, 45:9, 45:18, 45:22, 46:12, 46:22, 47:13, 47:18, 92:18, 95:17, 96:2, 146:4 sources 20:20, 22:3, 41:3, 42:8, 42:15, 42:16, 75:10, 75:11, 84:13, 96:22, 97:2, 98:7, 111:14, 112:5, 112:13, 112:15 speak 104:3 speaking 87:12, 104:2 specific 18:8, 18:9, 18:10, 43:1, 45:17, 58:9, 59:17, 79:7, 79:9, 79:10, 83:7, 96:4,	112:19, 114:9, 131:8, 135:3, 135:8, 139:12, 145:3, 145:21, 146:2, 154:12 specifically 90:16, 109:15, 125:1, 127:12, 148:1, 148:12, 152:17, 152:22 specification 26:12, 26:19, 40:22 specified 159:17 spelled 125:13 spoken 15:14, 15:19 spot 115:14 square 30:15, 32:8, 35:18 stage 71:3 stand 6:13, 26:1, 129:11 standard 46:19, 46:20, 46:21 standing 152:9, 152:14 start 5:9, 17:16, 20:7, 30:12, 62:22, 70:19, 72:15, 111:10, 129:18 starting 19:19, 41:13, 41:14, 55:9, 64:10, 96:7, 111:9, 124:6 starts 20:3, 26:17, 90:20, 116:1
---	---	--	--

state 159:5 stated 145:10, 153:13, 155:21 statement 68:22 statements 139:13 states 1:1, 84:5, 85:1, 85:6, 102:8 stating 151:7 statistics 53:20 stenographic 115:5 stenographically 159:11 step 22:14, 22:15, 69:13, 69:15, 69:18, 95:4, 120:8, 131:16, 131:19, 131:21 steps 150:7, 150:14 steven 14:17 stick 37:9 sticking 24:4 still 42:14, 51:5, 54:5, 60:4, 60:12, 65:12, 70:9, 77:16 stolen 76:7, 103:2 stop 25:3 store 77:11, 122:5, 122:11, 123:21 stored 103:2, 103:3,	122:21, 123:2, 123:7, 123:9, 123:20, 124:19, 131:20, 134:13, 135:19, 136:16, 137:5, 137:8, 152:5, 153:2, 153:10 storing 122:15 straightforward 54:2 strange 77:14 street 3:5 strictly 64:2 stronger 85:12 structure 111:12, 115:10, 116:7, 116:14, 116:20 students 51:21 sub-menu 91:7 subdivide 146:5 subject 153:13, 154:9, 155:21 subjective 102:20 subsequent 20:12, 148:2, 148:11 subset 93:21, 99:11, 143:6, 143:8, 154:5, 154:7, 154:16 successful 20:13 successfully 130:11, 131:4 suggest 149:7	suggesting 31:7, 39:1, 100:1, 120:18, 125:21 suggests 126:7, 135:12 suite 3:6, 3:14, 107:22, 108:1, 108:6, 108:11, 108:17 suites 106:20, 107:7, 107:10, 107:14, 107:17, 109:2, 109:17, 110:8, 111:18, 112:17 summarize 64:12 summarizing 140:10 supplemental 4:16, 7:14, 16:2, 18:17 supplementary 20:7 suppose 77:1 supposed 70:22 sure 8:7, 10:10, 12:20, 16:4, 16:6, 19:11, 20:18, 23:3, 26:15, 26:18, 26:22, 27:12, 33:16, 34:14, 36:1, 50:12, 52:9, 55:4, 63:17, 69:2, 82:16, 87:2, 87:7, 90:3, 93:8, 95:2, 95:19, 97:14, 97:20, 98:19, 104:18, 110:10, 114:22, 140:13,	141:14, 142:11, 145:19, 145:21, 146:5, 146:14, 148:20, 150:17, 151:13, 152:7, 152:11 surfing 21:10 surprise 33:13 suspect 105:2, 105:7 suspicious 72:22 sworn 5:3, 5:6, 159:8 symbol 45:5 symbols 110:14, 110:17, 110:18, 111:1, 127:5, 127:7, 127:12, 130:7, 130:16, 130:17, 130:22 system 20:1, 20:10, 23:10, 23:12, 24:11, 25:1, 32:14, 39:14, 39:21, 40:1, 40:2, 40:3, 40:4, 40:5, 40:13, 40:17, 41:5, 41:10, 41:19, 42:5, 42:6, 42:9, 42:13, 43:5, 44:13, 44:16, 44:19, 47:22, 48:1, 48:5, 52:11, 52:19, 52:21, 53:8, 54:10, 54:12, 54:21, 60:19, 61:9, 77:8, 77:10, 78:7, 78:12, 78:18,
--	---	--	--

79:17, 79:19, 82:12, 88:21, 90:21, 93:19, 96:13, 97:3, 97:12, 102:4, 107:3, 110:6, 111:2, 112:12, 113:9, 113:19, 114:8, 115:12, 116:9, 122:10, 123:4, 128:21, 130:15, 132:10, 133:7, 133:17, 133:22, 134:2, 135:8, 135:9, 136:4, 136:9, 143:13 systemic 81:18 systems 40:19, 42:16, 55:22, 56:2, 56:12, 56:15, 56:22, 57:6, 78:19, 79:18, 105:10, 105:16, 106:1	78:12, 87:16, 87:22, 91:16, 104:7, 104:15, 129:6, 152:14, 156:19 taken 18:20, 130:10, 131:4, 159:15 takes 38:17 taking 5:18, 25:4, 28:21, 51:4, 60:5, 68:10, 78:17, 84:13, 109:19 talk 17:10, 43:18, 45:16, 50:10, 65:17, 66:3, 79:22, 80:2, 84:13, 84:14, 105:13, 148:11 talked 32:6, 42:21, 89:17, 95:5, 95:10, 128:18 talking 12:6, 17:2, 23:17, 26:13, 38:11, 38:20, 42:6, 42:15, 49:7, 54:19, 57:18, 59:11, 63:2, 69:4, 69:9, 87:13, 89:3, 89:16, 89:19, 104:11, 124:5, 156:5 talks 47:6, 64:13, 119:4, 123:16, 126:10 tangential 105:21 tape 37:16 taping 37:19	target 20:1, 39:14, 39:21, 40:4, 40:17, 40:19, 41:5, 41:10, 42:9, 44:15, 44:16, 44:18, 47:21, 48:5, 52:18, 54:20, 60:19, 82:12, 119:13, 119:18, 119:22, 120:2, 120:6, 121:16, 121:17, 121:19, 123:13, 124:1 targets 117:21 tasked 119:22 taxonomies 118:9, 118:21 taxonomy 118:13 teach 15:18, 15:19 tech 53:13, 106:4 technical 101:21 technician 3:19, 5:2, 6:13, 6:22, 26:1, 26:3, 26:6, 101:8, 106:9, 129:11 technology 12:18, 12:19, 49:8, 49:13, 49:17 tell 45:22, 69:17, 73:13, 114:13 telling 65:13 tells 127:11 ten-minute 60:21, 129:6	tend 17:2, 17:16 term 13:15, 19:20, 39:12, 43:5, 48:11, 83:6, 131:9, 145:20 terms 23:21, 31:5, 40:12, 41:8, 44:17, 66:4, 66:10, 67:3, 78:22, 86:10, 93:2, 131:8, 131:11, 138:1, 138:7, 138:8, 138:16, 138:17, 140:1, 154:11 testified 5:6, 14:22, 21:15, 35:14, 35:15, 36:16, 39:11, 41:1, 47:20, 65:8, 68:18, 69:1, 69:3, 79:3, 86:2, 88:18 testify 16:7, 159:8 testimony 5:16, 123:11, 158:4, 158:6, 159:14 texas 6:6 text 90:13, 128:13, 131:19 th 160:3 thank 7:9 thereafter 159:12 thereby 57:9 therefore 66:15
T			
table 114:19, 122:5, 122:11, 122:21, 124:14, 137:13, 137:14, 137:15, 140:11 tables 63:21, 73:19, 74:16, 122:15, 123:22, 124:11, 124:19 take 16:2, 24:17, 24:21, 28:1, 30:12, 31:22, 37:16, 48:3, 60:20, 67:4, 67:16, 69:11, 77:21, 78:7,			

therein 152:5, 153:2, 153:10 thing 19:4, 36:3, 42:10, 52:12, 54:8, 66:12, 80:14, 83:17, 85:10, 92:16, 99:16, 103:6, 110:2, 133:12 things 19:11, 23:9, 24:18, 31:10, 31:12, 34:19, 37:21, 38:2, 38:3, 46:11, 47:9, 64:6, 68:4, 68:20, 70:8, 70:13, 71:11, 82:1, 93:4, 127:8 think 22:10, 25:19, 30:19, 32:3, 33:6, 38:6, 38:22, 51:5, 51:17, 81:2, 86:9, 86:15, 86:22, 87:15, 92:20, 94:22, 95:18, 99:21, 110:4, 114:4, 115:14, 118:14, 125:12, 125:15, 129:5, 134:10, 138:12, 149:15, 156:20 thinking 9:14, 38:8 third 130:4 third-party 24:21, 93:21, 99:2, 99:12, 100:8, 100:12, 100:15, 100:16, 101:2, 131:17,	142:9, 142:13, 143:4, 143:6, 143:8, 148:8, 152:20, 154:4, 154:5, 154:8, 154:17 thought 48:9 threat" 27:5 threat's 91:10 threat-model-bas- ed 105:3 threat-modeling 117:7, 119:17, 120:7, 120:12, 121:20, 121:22, 122:18, 124:9 threatmodeler 1:8, 3:10, 14:2, 14:20, 15:1, 24:19, 25:5 threats 10:7, 16:20, 17:18, 18:1, 18:5, 18:7, 19:10, 19:11, 21:4, 21:6, 21:12, 28:12, 28:13, 38:14, 40:15, 41:3, 42:8, 42:17, 44:7, 44:8, 44:9, 49:8, 49:16, 50:11, 50:15, 50:17, 55:21, 56:2, 56:14, 57:7, 57:14, 57:15, 57:19, 57:21, 59:4, 68:13, 71:16, 82:3, 82:4, 84:14, 86:3, 86:7, 86:14, 87:3,	87:5, 89:16, 89:20, 90:6, 91:7, 91:8, 91:9, 96:5, 97:3, 97:4, 97:6, 97:10, 97:13, 97:18, 98:7, 104:21, 104:22, 105:12, 105:14, 105:18, 117:9, 117:11, 117:21, 118:3, 118:6, 118:7, 118:10, 118:11, 118:12, 118:16, 118:17, 119:18, 120:13, 120:15, 137:20, 139:10, 140:4, 153:9, 153:10 three 22:15, 35:3, 124:7 thresholds 104:7, 104:16 through 19:20, 25:10, 25:18, 27:20, 31:19, 42:22, 48:9, 50:20, 76:5, 97:5, 98:1, 126:3, 128:6, 138:11, 139:4, 139:9, 140:8, 147:16, 147:17, 149:14, 149:17, 153:12, 155:17 throughout 23:5, 117:12, 126:17 throw 53:11 time 56:19, 80:14, 87:16, 87:21, 104:17, 126:5, 159:16	times 17:15, 52:10, 54:7, 61:21, 69:11, 74:6, 75:8, 78:13, 80:19, 85:22, 86:20 tinier 44:1 title 91:8 today 5:13, 5:16, 5:20, 6:5, 7:17, 8:10 together 22:9, 81:8, 101:4, 118:10, 118:11, 119:4, 149:2 told 56:18 took 146:7 tool 15:6, 15:8, 24:6, 24:14, 24:15, 25:5 tools 11:12, 12:1, 12:2, 12:4, 12:5, 12:6, 12:9, 12:10, 12:14, 15:2, 31:10, 33:14 top 12:18, 91:8, 120:8, 128:20 total 16:19 trace 82:1 trademark 1:1 traditional 57:5 traffic 128:7, 128:16
---	---	--	---

transcript 159:10 transcription 158:5 transfer 25:8, 72:10 transmitted 83:22 treated 43:7, 43:9 treating 105:3 tree 18:12, 18:16, 18:19, 19:3, 19:4, 19:5, 19:6, 20:2, 20:3, 21:5, 21:14, 23:17, 37:13, 58:19 trial 1:3 triangle 127:20, 127:22 tricked 67:11 troubleshoot 31:20 true 27:16, 52:1, 60:8, 71:18, 158:4, 159:13 truth 159:8 try 49:21, 74:4, 116:4 trying 15:21, 28:9, 33:11, 36:11, 44:7, 44:8, 48:21, 54:9, 70:11, 79:13, 89:7, 100:9, 121:5 turn 64:8, 78:18, 119:5, 130:2	two 7:16, 7:19, 22:1, 22:15, 30:16, 32:8, 49:20, 56:5, 56:19, 56:21, 84:1, 110:3, 119:14, 120:1, 120:22 type 12:19, 17:11, 28:5, 28:9, 33:7, 34:2, 34:3, 34:6, 35:1, 40:1, 102:17, 118:12, 119:6, 119:7, 119:8, 121:12, 123:4 types 11:21, 16:20, 17:17, 28:12, 102:1, 102:6, 102:9, 102:11, 102:14, 108:13, 111:12, 112:19, 117:22, 118:3, 118:4, 118:6, 118:8, 118:10, 118:11, 119:4, 119:5 typewriting 159:12 typically 10:2, 11:15, 11:22, 22:9, 103:16 U uncommon 118:9, 118:21 under 5:13, 41:19, 43:19, 123:7, 123:12, 123:13, 159:12 underlies 77:16	underlying 70:1, 144:13 understand 5:10, 5:13, 8:1, 9:15, 13:10, 17:17, 23:21, 28:18, 32:3, 38:6, 54:9, 73:3, 74:4, 79:13, 85:15, 86:10, 98:3, 110:4, 117:16, 121:1, 130:10, 131:4, 131:10, 145:7, 152:8 understandable 53:19 understanding 40:12, 69:2, 72:2, 72:5, 79:11, 85:17, 85:21, 103:22, 104:1, 104:5, 104:19, 114:7, 118:5, 127:4, 151:10 understood 38:21, 56:16, 69:19, 75:4, 110:11, 130:5, 134:10, 134:12, 135:18 unfamiliar 14:11 united 1:1, 84:5, 85:1, 85:6 unknown 83:12 unless 18:8, 46:2, 60:5, 60:7, 75:3 unpredictability 54:4 unsafe 51:9 until 66:18	update 124:10 use 6:15, 6:16, 6:19, 12:14, 18:12, 18:15, 18:21, 23:16, 24:5, 28:10, 28:11, 41:8, 54:5, 54:6, 58:8, 59:22, 62:19, 78:19, 80:21, 86:7, 87:5, 105:1, 121:12, 134:16 useful 44:10, 92:14, 92:16, 92:19, 118:22 user 42:3, 55:10, 59:1, 59:2, 59:12, 59:15, 66:19, 77:9, 77:11, 93:18, 96:9, 96:12, 96:16, 96:17, 96:20, 96:21, 142:18, 143:12, 143:22, 153:17, 155:16 user's 58:22, 59:14 username 77:9, 77:20 uses 61:15, 101:22, 102:8, 110:3, 112:16, 120:19, 122:10, 126:16, 127:5, 130:17, 131:9, 136:3 using 20:19, 25:14, 27:3, 27:15, 27:17, 30:22, 42:13, 46:7, 58:3, 61:22,
--	---	---	--

67:22, 80:1, 93:20, 109:7, 110:22, 120:17, 142:18, 154:2, 154:15, 155:14 usually 50:1, 50:3, 77:21, 79:1 utilizes 130:6, 130:15 utilizing 125:1	148:15 views 102:5 virginia 3:15 visio 33:9, 34:6, 34:9, 34:13, 34:22, 35:12, 131:18, 132:9, 132:17, 132:20, 133:8, 133:12, 133:19, 133:21, 134:1, 135:3, 135:6, 135:8, 136:4, 136:10, 147:9 vista 8:17, 8:21 visual 34:7, 34:16, 35:10, 93:20, 99:1, 100:20, 101:2, 109:13, 112:21, 138:3, 142:8, 142:12, 146:9, 146:11, 146:15, 148:7, 152:19 visualization 106:18, 108:21, 109:20, 109:21, 110:16, 111:13, 111:15, 112:4, 112:11, 112:14, 115:12, 116:9, 116:20, 116:22, 120:22, 121:13, 121:15, 125:2, 126:10 visualizations 109:6 visualize 106:19, 107:4, 111:17, 119:15, 126:5, 126:8 visualized 109:18, 113:3,	121:21 visually 119:11 vulnerabilities 10:16, 11:2, 17:4, 18:1, 54:15, 55:3, 55:12, 55:18 vulnerability 10:14, 10:21, 12:11, 64:15, 64:20, 73:17 vulnerable 90:22	47:1, 55:6, 104:4 warning 121:10 way 10:22, 17:13, 19:19, 20:2, 24:11, 28:10, 32:7, 32:9, 33:2, 33:3, 33:4, 39:1, 41:12, 43:9, 51:9, 59:7, 59:10, 59:11, 59:18, 61:21, 63:19, 65:20, 66:16, 67:3, 73:11, 75:3, 78:4, 83:3, 84:18, 96:6, 96:21, 111:7, 118:17, 126:18, 140:10, 145:21 ways 30:18, 32:4, 33:14, 67:2, 76:6, 76:9, 76:10, 78:2, 126:20 we'll 47:13, 93:13, 151:12, 156:21 we're 5:18, 6:17, 12:6, 17:1, 17:18, 17:21, 42:15, 44:8, 46:7, 46:19, 47:2, 51:4, 63:2, 66:21, 68:10, 73:21, 74:5, 80:1, 81:14, 81:16, 83:4, 89:3, 114:22, 124:5, 128:18, 156:5 we've 23:17, 80:7,
v		w	
valuable 40:11, 66:2, 68:11 value 64:16, 65:5, 74:10 values 74:7 variety 111:14, 112:12, 112:15 various 95:6, 96:18, 107:14, 110:13, 122:12, 130:7 vary 28:15, 70:12 vector 119:14, 120:1 vectors 55:11, 55:17, 117:21 vendor's 106:3 versus 24:1, 24:5, 37:22 vice-versa 87:9 view 87:11, 101:22, 104:4, 122:1, 125:4, 125:18, 126:9, 147:17,		wait 66:11, 91:20 walk 25:10, 149:14, 149:17 walked 149:16 walks 138:11 want 6:14, 9:20, 19:12, 23:11, 24:8, 25:10, 25:13, 28:16, 30:21, 31:1, 31:16, 31:17, 35:19, 36:1, 36:4, 36:6, 36:7, 37:14, 40:14, 42:12, 43:2, 43:11, 49:1, 49:3, 49:4, 50:9, 53:16, 53:21, 59:6, 61:20, 69:21, 73:15, 74:9, 79:8, 87:22, 88:3, 93:14, 109:22, 149:17, 152:8, 152:16 wanted 30:10, 37:12,	

105:4, 129:4 web 76:13, 76:14 wednesday 1:17 welcome 139:3 well-documented 86:11 went 83:15 whatever 30:22, 40:1, 40:5, 40:15, 58:6, 59:2, 67:11, 118:21 whereas 61:9 wherein 99:11 whereof 160:1 whereupon 5:3, 7:2, 26:4, 60:22, 88:7, 101:9, 106:10, 115:4, 129:8, 129:12, 156:22, 157:6 wherever 40:14 whether 17:9, 22:4, 49:22, 50:9, 72:9, 76:2, 87:2, 87:4, 102:14, 102:15, 141:8, 156:2, 156:20 whichever 126:8 white 23:7, 23:12, 30:12, 30:14, 32:6, 33:3, 36:3, 36:8, 37:1, 37:3, 37:6, 37:8,	37:14, 37:17, 37:19, 39:2 whole 38:18, 38:21, 104:11, 159:8 wi-fi 31:17, 95:21, 95:22, 97:19, 98:15 within 38:19, 39:22, 46:10, 126:19, 148:14, 159:4 without 34:9, 57:8, 67:20, 72:2, 72:5, 91:21, 126:21 witness 4:2, 5:3, 5:5, 7:3, 11:18, 11:20, 26:5, 26:8, 49:19, 82:20, 87:19, 88:2, 94:6, 94:17, 99:6, 101:10, 101:11, 106:11, 106:12, 109:10, 111:6, 114:1, 114:11, 114:21, 115:21, 123:1, 124:3, 126:15, 129:13, 129:14, 133:10, 134:8, 135:5, 135:11, 136:6, 136:21, 143:16, 144:6, 145:18, 148:10, 149:13, 150:5, 150:21, 151:18, 152:15, 154:21, 155:1, 155:6, 159:7, 160:1 word 25:5, 30:13, 30:15, 76:12, 87:8, 110:2,	110:10, 127:4, 138:8 words 86:7, 87:5, 87:12 work 16:7, 17:19, 18:11, 19:14, 25:15, 27:17, 29:7, 36:11, 50:16, 50:18, 66:16 worked 16:8, 24:3, 34:20, 105:19 working 52:5, 145:11 works 14:19, 20:2, 77:3, 77:5, 134:19, 149:8 world 15:20, 27:15, 48:3, 49:2, 53:11, 127:8, 127:10 worried 17:21 worse 58:21, 58:22, 59:2 worst 78:22 wouldn't 18:10, 23:16, 33:13, 53:15, 82:13, 85:3, 92:9, 92:10, 92:16 wow 81:16 write 61:8 writing 17:22, 25:6, 67:20 written 132:16, 139:16,	139:17, 140:6 wrong 19:12, 23:9, 115:14 Y yeah 6:16, 13:9, 18:22, 24:4, 25:19, 25:22, 29:19, 30:21, 34:18, 126:2, 133:5, 133:20, 149:20, 155:3 year 67:8, 67:9, 72:21, 73:21, 74:18, 80:19, 81:18 years 77:15, 80:19 yohler 1:22, 2:3, 159:3, 160:9 yourself 117:5 Z zero 66:13, 66:14, 66:15 zheng 4:12, 110:18, 111:7, 112:17, 113:9, 113:12, 113:13, 114:3, 114:4, 115:20, 116:19, 116:21, 117:16, 118:3, 118:4, 118:7, 118:14, 118:15, 118:20, 119:4, 121:5, 123:17, 124:21, 126:4, 129:2, 147:17, 147:21, 148:2, 148:5, 148:12, 148:15, 149:1,
--	--	--	--

149:2 zheng's 107:3, 111:2, 112:11, 113:19, 114:8, 122:10, 123:4 zoom 6:3 .3300 3:8 .7700 3:16 0 00656 1:11 01 1:18 1 1 156:4 1" 115:13 1,000 22:21, 67:7, 68:4, 68:19, 69:20, 70:6, 70:8, 70:13, 70:15, 72:21, 73:8 10 26:15, 26:16, 27:2, 43:11, 43:13, 45:1, 94:9, 94:11, 94:14, 95:5, 95:6, 95:8, 96:4, 96:14, 96:15, 97:7, 97:9, 98:9, 140:15, 156:14 10,713,366 1:12 100 60:3, 131:18	1000 96:9 1001 4:10, 26:2, 26:4 1002 96:18 1004 4:11, 96:16, 101:7, 101:9, 101:12 1005 4:12, 106:8, 106:10, 106:13, 107:10, 115:20 1006 4:13, 129:10, 129:12, 129:15 101 4:11 104 131:16 106 4:12, 131:19, 131:21 11 147:16, 156:14 116 106:18, 108:22, 111:13, 111:16, 112:5, 115:12, 116:9 119 139:4, 139:9 12 26:17, 117:17, 134:17 122 139:4, 139:9 129 4:13 13 26:17, 128:3, 160:3 135 147:12 136 147:20, 148:1	137 148:4 14 91:3 142 141:11 143 141:12 15 147:17, 156:14 16 77:21, 96:7, 101:19, 156:15 160 1:21 1650 3:5 17 42:2, 140:15 18 140:15, 147:17, 156:15 19103 3:7 1st 8:20 2 2 157:7 2,000 77:20, 77:22, 78:4 20 77:22, 80:19, 87:17, 131:22 200 41:17, 42:2, 111:12, 115:10, 116:7, 116:14 2009 4:14, 6:12, 7:2, 7:10, 19:16, 21:1, 36:15, 36:16, 39:6, 48:17, 61:3, 88:16, 137:11	2010 4:16, 6:12, 7:3, 7:13, 16:3, 18:18, 20:17, 36:19 2015 16:16 2016 8:20 202 106:19, 109:1, 111:17, 111:21, 112:3, 112:9, 113:18, 116:16, 117:3, 128:7 2023 1:11 2024 1:17, 160:3 204 117:20, 128:5 208 41:18 210 128:6 215.656 3:8 22102 3:15 228 4:11 24 121:10 25 64:10, 87:17, 90:19, 122:2, 129:17, 130:2 26 4:10, 131:21, 134:15, 135:20 28 111:10, 124:21 3 30 98:21, 131:21, 134:14, 135:20 31 98:21, 106:15
--	---	--	--

33 124:6 366 4:10, 20:22, 21:2, 25:11, 25:20, 27:1, 27:8, 28:20, 30:1, 30:4, 30:6, 30:8, 30:20, 31:2, 31:4, 31:5, 31:22, 32:9, 32:11, 33:6, 33:16, 38:10, 38:12, 38:22, 39:4, 40:8, 40:20, 41:7, 41:13, 42:6, 42:17, 43:2, 43:12, 46:10, 47:5, 49:12, 49:16, 50:4, 55:8, 56:13, 61:5, 61:15, 61:16, 64:4, 64:9, 88:18, 90:1, 93:7, 94:9, 94:15, 96:6, 110:1, 138:1, 140:1, 145:21, 146:7 4 40 113:14 43 93:10, 98:18, 100:10, 100:21 45 101:19 4531 2:4, 160:11 47 33:19, 33:21 48 101:19 5 50 93:13	500 3:14, 68:3, 68:19, 69:20, 70:15, 71:8, 72:21 5000 3:6 52 108:18 527767 1:20 54 157:7 571.765 3:16 6 60 55:9 64 115:7, 115:9, 115:15, 115:22, 116:4 65 41:14 66 50:12 7 708 101:22 78 19:15, 39:9, 48:16 8 80 61:3, 61:8, 88:14 800 91:6 8300 3:13 84 2:4, 160:11 9 9 1:18	90 21:2 907 4:12 95 100:19	
--	--	--	--