

In the Matter of:

LabMD, Inc.

May 20, 2014
Trial - Public Record
Volume 1

Condensed Transcript with Word Index



For The Record, Inc.
(301) 870-8025 - www.ftrinc.net - (800) 921-5555

1

1 FEDERAL TRADE COMMISSION
 2 I N D E X
 3 IN RE LABMD, INC.
 4 TRIAL VOLUME 1
 5 PUBLIC RECORD
 6 MAY 20, 2014
 7
 8 WITNESS: DIRECT CROSS REDIRECT RECROSS VOIR
 9 HILL 81
 10
 11
 12 EXHIBITS FOR ID IN EVID IN CAMERA STRICKEN/REJECTED
 13 CX
 14 (none)
 15
 16 RX
 17 (none)
 18
 19 JX
 20 Number2 6
 21
 22
 23
 24
 25

3

1 APPEARANCES:
 2
 3 ON BEHALF OF THE FEDERAL TRADE COMMISSION:
 4 LAURA RIPOSO VANDRUFF, ESQ.
 5 ALAIN SHEER, ESQ.
 6 MARGARET LASSACK, ESQ.
 7 Federal Trade Commission
 8 Bureau of Consumer Protection
 9 Division of Privacy and Identity Protection
 10 600 Pennsylvania Avenue, N.W.
 11 Washington, D.C. 20580
 12 (202) 326-2999
 13 lvandruff@ftc.gov
 14
 15 ON BEHALF OF THE RESPONDENT:
 16 WILLIAM A. SHERMAN, II, ESQ.
 17 REED D. RUBINSTEIN, ESQ.
 18 Dinsmore & Shohl LLP
 19 801 Pennsylvania Avenue, N.W.
 20 Suite 610
 21 Washington, D.C. 20004
 22 (202) 372-9100
 23 william.sherman@dinsmore.com
 24
 25

2

1 UNITED STATES OF AMERICA
 2 FEDERAL TRADE COMMISSION
 3
 4 In the Matter of)
 5 LabMD, Inc., a corporation,) Docket No. 9357
 6 Respondent.)
 7 -----)
 8
 9 May 20, 2014
 10 10:11 a.m.
 11 TRIAL VOLUME 1
 12 PUBLIC RECORD
 13
 14 BEFORE THE HONORABLE D. MICHAEL CHAPPELL
 15 Chief Administrative Law Judge
 16 Federal Trade Commission
 17 600 Pennsylvania Avenue, N.W.
 18 Washington, D.C.
 19
 20 Reported by: Josett F. Whalen, Court Reporter
 21
 22
 23
 24
 25

4

1 APPEARANCES: (continued)
 2
 3 ON BEHALF OF THE RESPONDENT:
 4 KENT G. HUNTINGTON, ESQ.
 5 MICHAEL PEPSON, ESQ.
 6 Cause of Action
 7 1919 Pennsylvania Avenue, N.W.
 8 Suite 650
 9 Washington, D.C. 20006
 10 (202) 499-2426
 11 kent.huntington@causeofaction.org
 12
 13
 14
 15
 16
 17
 18
 19
 20
 21
 22
 23
 24
 25

5

1 PROCEEDINGS
 2 - - - - -
 3 JUDGE CHAPPELL: Call to order Docket 9357,
 4 In Re LabMD, Inc.
 5 I'm going to start with the appearances of the
 6 parties, government first.
 7 MS. VANDRUFF: Good morning, Your Honor.
 8 Laura VanDruff for complaint counsel.
 9 With me at counsel table is Alain Sheer and
 10 Maggie Lassack and Jon Owens.
 11 JUDGE CHAPPELL: And for respondent?
 12 MR. SHERMAN: Good morning, Your Honor.
 13 William Sherman on behalf of LabMD.
 14 Seated next to me on my left is
 15 Mr. Michael Daugherty, who is the owner and CEO of
 16 LabMD.
 17 Next to him is Kent Huntington, who you met last
 18 week, counsel from Cause of Action.
 19 Next to him is my law partner, Reed Rubinstein.
 20 And next to him is co-counsel Mike Pepson, also
 21 from Cause of Action.
 22 JUDGE CHAPPELL: All right. Thank you.
 23 Before I hear your opening statements, I'm going
 24 to admit -- I understand there's a JX 2, and we have
 25 copies of it?

6

1 MS. VANDRUFF: Your Honor, this morning we
 2 served copies -- complaint counsel served copies on
 3 Your Honor's office. I have copies for the court today
 4 as well if that would be helpful.
 5 JUDGE CHAPPELL: Right. Let's have the
 6 original. If you want to approach the bench.
 7 MS. VANDRUFF: Certainly, Your Honor.
 8 (Pause in the proceedings.)
 9 JUDGE CHAPPELL: This is the same JX 2 that was
 10 e-mailed to my office?
 11 MS. VANDRUFF: That was e-mailed this morning,
 12 that's correct, Your Honor.
 13 JUDGE CHAPPELL: All right. I've reviewed this
 14 exhibit and JX 2 is admitted.
 15 (Joint Exhibit Number 2 was admitted into
 16 evidence.)
 17 JUDGE CHAPPELL: Any other evidentiary or
 18 procedural issues to raise at this time?
 19 MS. VANDRUFF: Two, Your Honor, if I may.
 20 JUDGE CHAPPELL: All right.
 21 MS. VANDRUFF: The first is that the parties
 22 had jointly submitted a prior stipulation, and I don't
 23 know, because it wasn't filed with the Office of the
 24 Secretary, whether there is any process we must
 25 dispense with in order to withdraw that stipulation.

7

1 JUDGE CHAPPELL: Was it part of a motion?
 2 MS. VANDRUFF: No, Your Honor. It was
 3 submitted prior to the preliminary -- sorry -- the
 4 pretrial hearing and Your Honor rejected it, and in its
 5 stead is JX 2 which you've just admitted.
 6 JUDGE CHAPPELL: So it was filed as a joint
 7 stipulation with the Office of the Secretary.
 8 MS. VANDRUFF: It was submitted to Your Honor.
 9 It was not filed with the Office of the Secretary.
 10 JUDGE CHAPPELL: If it was not filed, then don't
 11 worry about it.
 12 MS. VANDRUFF: All right. Terrific.
 13 JUDGE CHAPPELL: And anything that has been
 14 filed, you can always do a joint motion to withdraw, but
 15 since it was not, it's of no concern. I handled it on
 16 the record last week.
 17 MS. VANDRUFF: That was my understanding,
 18 Your Honor, but I wanted to make sure that there wasn't
 19 something more that the parties needed to do.
 20 On a second issue, Your Honor, it is the
 21 parties' understanding that consistent with
 22 rule 3.41(b)(6) that Your Honor typically reserves
 23 closing argument until after the parties have submitted
 24 their posttrial findings of fact and conclusions of
 25 law.

8

1 Is that Your Honor's intent with respect to
 2 this proceeding?
 3 JUDGE CHAPPELL: Yes.
 4 MS. VANDRUFF: Thank you, Your Honor.
 5 JUDGE CHAPPELL: Is that what you would desire?
 6 Is there an objection to that?
 7 MS. VANDRUFF: There's no objection to that,
 8 Your Honor.
 9 JUDGE CHAPPELL: It's always been suggested by
 10 the parties. That's why I do it.
 11 MS. VANDRUFF: There's no objection, Your Honor.
 12 Just in terms of planning, that was the reason for our
 13 inquiry.
 14 JUDGE CHAPPELL: Okay.
 15 MS. VANDRUFF: Thank you, Your Honor.
 16 JUDGE CHAPPELL: Is she speaking for you,
 17 Mr. Sherman?
 18 MR. SHERMAN: We discussed that briefly, prior
 19 to Your Honor coming on the bench. Again, just a little
 20 foreign to me, but I think that as long as we know ahead
 21 of time, we can accommodate it.
 22 JUDGE CHAPPELL: Things flow better logically
 23 that way. All the briefing is done, and then I hear the
 24 closing at that time when it's all in front of me.
 25 MR. SHERMAN: Very well.

9

1 JUDGE CHAPPELL: All right. Let's have opening
 2 statements. I'll start with the government.
 3 And I remind you that you're not to reveal
 4 information that's been granted in camera treatment
 5 during your opening statements.
 6 Are we going to need a timer or are you going to
 7 be well under the two hours?
 8 MR. SHEER: Your Honor, we'll be well under two
 9 hours.
 10 JUDGE CHAPPELL: All right.
 11 MR. SHEER: Good morning.
 12 May it please the court.
 13 I'm Alain Sheer, complaint counsel.
 14 This case is about a medical testing laboratory
 15 that failed to use reasonable measures to protect
 16 sensitive information entrusted to it.
 17 By failing to take reasonable security
 18 measures, LabMD exposed information about hundreds of
 19 thousands of consumers, including their names,
 20 Social Security numbers and medical testing information,
 21 to people who never should have had it.
 22 The evidence will show that in two documented
 23 incidents, one involving a popular peer-to-peer
 24 file-sharing program and the other involving identity
 25 thieves in Sacramento, sensitive personal information

10

1 for nearly 10,000 consumers was disclosed without
 2 authorization.
 3 The company's security practices --
 4 JUDGE CHAPPELL: Is it your position that the
 5 information that was on the peer-to-peer file-sharing
 6 program, LimeWire, that was a violation of the law,
 7 merely posting it on that? Is that your position?
 8 MR. SHEER: That is a consequence of the
 9 company's unreasonable security practices and is
 10 indicative of the way the practices failed to protect
 11 sensitive information.
 12 JUDGE CHAPPELL: But if I heard you correctly,
 13 mere posting of the information is not a violation.
 14 MR. SHEER: The posting of the information
 15 makes the information available to anyone who searches
 16 on the P2P network to find it. It is there for the
 17 world to see. And by simply disclosing that
 18 information and making it available, the company has
 19 demonstrated that its practices were not reasonable and
 20 appropriate.
 21 JUDGE CHAPPELL: So that's a yes or a no to my
 22 question? I asked you twice.
 23 MR. SHEER: A breach itself may not by itself be
 24 a law violation, but it is indicative that security
 25 practices are not reasonable and appropriate, and that's

11

1 the circumstances here.
 2 JUDGE CHAPPELL: All right. Go ahead.
 3 MR. SHEER: As I was saying, the company's
 4 information security practices put at risk very
 5 sensitive information of as many as 750,000 people
 6 whose information is maintained on the company's
 7 network.
 8 The evidence will show that LabMD's security
 9 practices were unfair under section 5 of the FTC Act
 10 because they were not reasonable.
 11 Reasonableness is a flexible concept that takes
 12 into account all of the circumstances, including actual
 13 and potential harm from unauthorized disclosure of
 14 consumer information and the costs of preventing the
 15 harm.
 16 Specifically, the evidence will show that
 17 LabMD's security practices caused or are likely to cause
 18 identity theft, medical identity theft and other
 19 substantial harms.
 20 The evidence will show that consumers had no way
 21 of knowing about LabMD's security practices and thus
 22 could not reasonably avoid those harms.
 23 And because the failures could have been
 24 corrected at low cost, there are no countervailing
 25 benefits to consumers or competition.

12

1 The court will hear from LabMD about extraneous
 2 issues, but the evidence will show that the company's
 3 failure to provide reasonable and appropriate security
 4 for the very sensitive information it maintains about
 5 hundreds of thousands of consumers was an unfair act or
 6 practice.
 7 LabMD collected and maintained the most
 8 sensitive kinds of information for 750,000 consumers,
 9 including information about approximately a hundred
 10 thousand consumers for whom it never provided any
 11 services at all. In addition to names, addresses, dates
 12 of birth and Social Security numbers, LabMD also
 13 maintains their sensitive health and financial
 14 information.
 15 The evidence will show that if this information
 16 is disclosed, it can be used to perpetrate identity
 17 theft, medical identity theft and other significant
 18 harms.
 19 Complaint counsel's expert witnesses, Rick Kam
 20 and Jim Van Dyke, will explain that LabMD's failure to
 21 provide reasonable and appropriate security for
 22 sensitive information is likely to result in concrete
 23 and substantial harms to consumers.
 24 In the two documented incidents of unauthorized
 25 disclosure of sensitive information involving the

13

1 information of approximately 10,000 consumers, Mr. Kam
 2 and Mr. Van Dyke will describe, based on their
 3 experience and research, the likelihood that consumers
 4 will suffer identity theft, medical identity theft and
 5 other substantial harms.
 6 JUDGE CHAPPELL: Do you plan to offer any
 7 evidence of actual harm in this case?
 8 MR. SHEER: Complaint counsel will not be
 9 putting up identity theft victims, but that does not
 10 mean that actual harm did not occur. And that is
 11 because, in many cases, identity theft victims are
 12 unable to connect up the dots. They're unable to
 13 identify the source of the information that was used to
 14 harm them.
 15 And that's particularly the case here because
 16 LabMD did not provide notice to the 9300 consumers whose
 17 information was found on the P2P network. And that's
 18 especially true for the hundred thousand people whose
 19 information -- who did not even know that LabMD had its
 20 information, their information.
 21 The evidence will show that these risks are
 22 particularly acute for the 9300 consumers --
 23 JUDGE CHAPPELL: Hang on a second.
 24 So if I understood your answer, you don't plan
 25 to introduce evidence of harm, but your position is

14

1 that doesn't mean no harm occurred? Is that what you
 2 said?
 3 MR. SHEER: That's correct.
 4 JUDGE CHAPPELL: Okay.
 5 MR. SHEER: And I'm also saying, though, that
 6 the legal standard is that we -- the legal standard is
 7 caused harm or is likely to cause harm.
 8 JUDGE CHAPPELL: I'm aware of the standard,
 9 sir.
 10 MR. SHEER: The evidence will show that
 11 consumers cannot avoid these harms. Physicians, rather
 12 than consumers, decide to use LabMD. Consumers do not
 13 have information about LabMD's security practices and
 14 cannot evaluate whether the practices are reasonable.
 15 LabMD's security failures were not close to
 16 being reasonable. As a preview, consider three obvious,
 17 longstanding security issues at LabMD.
 18 First, the evidence will show that LabMD failed
 19 to adequately assess risks, with the result that very
 20 serious, well-known and easily fixed vulnerabilities
 21 went unpatched for years on the company's servers that
 22 handled sensitive information.
 23 For example, it did not conduct external
 24 vulnerability scans to find commonly known or reasonably
 25 foreseeable risks until 2010.

15

1 Second, despite it being common knowledge that
 2 easily guessed passwords are a security no-no, LabMD
 3 allowed employees with access to sensitive information
 4 to log into their computers using, quote-unquote,
 5 "LabMD" as their password. One such employee used this
 6 password for years without being required to change it.
 7 LabMD did not use the password management function
 8 already built into the Windows operating systems it was
 9 using to ensure that passwords were strong.
 10 Third, IT employees and non-IT employees were
 11 inadequately trained. IT employees did not receive
 12 periodic security training to keep up with evolving
 13 threats and how to address them. Some non-IT employees
 14 could install unauthorized programs and disable security
 15 settings on their computers without approval, but they
 16 weren't trained that doing so could compromise the
 17 security of LabMD's networks.
 18 These and other security failures increased the
 19 risk of unauthorized disclosure of sensitive information
 20 on LabMD's network.
 21 One result was that an employee installed a
 22 peer-to-peer file-sharing program called LimeWire on a
 23 computer used by LabMD's billing manager. LimeWire
 24 allows users to designate files that they will share
 25 from their own computers, search for files on other

16

1 computers and download them.
 2 An insurance billing file that was designated
 3 for sharing from the billing manager's computer was
 4 found at IP addresses in Arizona, San Diego,
 5 Costa Rica, and London. The file, which we call the
 6 1718 File, contained information about more than
 7 9300 consumers.
 8 JUDGE CHAPPELL: Excuse me. You say this
 9 information was found in these various places. How was
 10 it found?
 11 MR. SHEER: It was found by a third party who
 12 was searching the P2P networks.
 13 JUDGE CHAPPELL: And what was their motivation
 14 to be searching?
 15 MR. SHEER: The motivation of the search is
 16 that the third party is in the business of trying to
 17 protect the information of its clients, and it does so
 18 by searching P2P networks, looking for information
 19 about the clients. In doing that, it came across these
 20 files.
 21 JUDGE CHAPPELL: Is this a
 22 non-government-affiliated entity?
 23 MR. SHEER: It is.
 24 JUDGE CHAPPELL: Not funded by taxpayer money in
 25 any way?

17

1 MR. SHEER: It is not.
 2 As I was saying, the file, which we call the
 3 1718 File, has very sensitive information about
 4 9300 consumers, including their names and
 5 Social Security numbers and medical test codes. Their
 6 test codes reveal the nature of the tests performed,
 7 such as for prostate cancer or sexually transmitted
 8 diseases or hepatitis.
 9 The evidence will show that unauthorized
 10 disclosure of this kind of information causes or is
 11 likely to cause substantial injury in the form of
 12 identity theft, medical identity theft and other harms.
 13 Complaint counsel's information security expert,
 14 Indiana University computer science professor
 15 Raquel Hill, will explain that the 1718 File incident
 16 was only the tip of LabMD's security iceberg. This case
 17 is not about a single, isolated failure. It's about
 18 systemic, easily addressed security failures that
 19 persisted for years.
 20 The evidence will show that LabMD
 21 systematically failed to practice what IT practitioners
 22 call defense in depth. Although it will sound
 23 technical, some points, the main point is simple. LabMD
 24 failed to implement the basic, simple, effective
 25 security measures to protect the information in its

18

1 care.
 2 So what's defense in depth on a computer
 3 network? A bricks-and-mortar analogy is a castle
 4 defended with a moat and sturdy inside and outside
 5 walls. These multiple defenses are effective, because
 6 if one defense fails, there will be another one to back
 7 it up.
 8 As Professor Hill will explain, defense in depth
 9 on a computer network is the same concept. Use a
 10 variety of security measures at the network perimeter
 11 and inside the network. That way, if one measure fails,
 12 other measures will protect the network.
 13 Professor Hill will explain that the particular
 14 security measures that accomplish reasonable defense in
 15 depth for a network start with understanding the network
 16 and its vulnerabilities and weaknesses.
 17 JUDGE CHAPPELL: This defense in depth you're
 18 talking about, is this a law, regulation or guideline
 19 that's out there for everybody to see?
 20 MR. SHEER: This is the practice that
 21 information security professionals use and have used for
 22 many, many years. It is available in many forms,
 23 including in standards that have been produced by the
 24 government, the National Institute of Science and
 25 Technology, as well as many other private organizations

19

1 that supply information to --
 2 JUDGE CHAPPELL: I'm talking about government
 3 only. My question goes to the government only.
 4 MR. SHEER: Yes.
 5 JUDGE CHAPPELL: Law, regulation or guideline
 6 published by the government.
 7 MR. SHEER: There are guidelines that have been
 8 published, for example, having to do with the security
 9 of health information that have these same basic
 10 concepts built into them. They're not always called
 11 defense in depth, but there are a series of standard
 12 steps, which we're going to talk about, that will
 13 illustrate what "defense in depth" means.
 14 JUDGE CHAPPELL: These guidelines have been
 15 published. Can you cite me to them right now?
 16 MR. SHEER: I can point you to the -- I can
 17 point you to pieces of it right now. I can point you to
 18 the HIPAA security rule which has -- which lays out in
 19 some detail what defense in depth requires.
 20 JUDGE CHAPPELL: Did you say HIPAA?
 21 MR. SHEER: I did.
 22 JUDGE CHAPPELL: Okay.
 23 MR. SHEER: And I can point you, if you will
 24 give me a few moments, to other sources at the
 25 National Institute of Standards and Technology.

20

1 JUDGE CHAPPELL: That's fine. I don't expect
 2 you to in your opening. I'm just wondering if you're
 3 going to do it here in the trial.
 4 Is it part of your case?
 5 MR. SHEER: References have been made to those
 6 things by our experts.
 7 As I was saying, Professor Hill will explain
 8 the particular security measures that constitute
 9 reasonable defense in depth for a network start with
 10 the network and its vulnerabilities and weaknesses.
 11 Defense in depth counters these threats by putting in
 12 place a series of roadblocks to close the
 13 vulnerabilities and weaknesses at different layers of
 14 the network.
 15 Reasonable defense in depth is proactive, not
 16 static. This is because threats and attack methods
 17 change quickly, and security has to keep pace to be
 18 effective. That, for example, is the point of regularly
 19 updating antivirus programs.
 20 At least for networks that connect to the
 21 Internet, like LabMD's, defense in depth is not a
 22 "set it up and forget it" endeavor.
 23 Can we have slide 1, please.
 24 I'd like to turn to LabMD's security failures.
 25 The evidence -- the evidence will show that there were a

21

1 number of them.
 2 First up is risk assessment.
 3 The evidence will show that LabMD failed to
 4 conduct adequate risk assessments.
 5 Professor Hill will explain that risk
 6 assessment is an essential part to reasonable security.
 7 Risk assessment is just like it sounds. It's
 8 tools to spot commonly known or reasonably foreseeable
 9 vulnerabilities on a network so that they can be closed
 10 before they're exploited.
 11 Companies can't fix vulnerabilities they don't
 12 know about. And because no one tool can find all the
 13 different types of vulnerabilities that may be present
 14 on a network, a variety of tools are needed to evaluate
 15 exposure to the different types of risks.
 16 The evidence will show that LabMD did not use an
 17 appropriate set of risk assessment tools.
 18 For example, it did not perform external
 19 vulnerability scans, which are also called penetration
 20 tests. Penetration tests help companies find
 21 vulnerabilities and close them before intruders can
 22 exploit them.
 23 LabMD performed no penetration tests of its
 24 network until at least 2010, after the commission
 25 investigation began. The 2010 test results show why

22

1 this failure was unreasonable.
 2 First, the tests found urgent the most -- or
 3 the most serious vulnerabilities in two of LabMD's
 4 servers.
 5 Second, the servers with these urgent
 6 vulnerabilities handled sensitive information which
 7 identity thieves use to conduct identity theft.
 8 Using a file transfer protocol or FTP program,
 9 this server had received information about hundreds of
 10 thousands of consumers from physicians, including their
 11 names and addresses and Social Security numbers and
 12 medical information.
 13 The other server had this information plus
 14 laboratory tests and also was used to keep a backup copy
 15 of the information -- of this information and the other
 16 information on LabMD's systems.
 17 Third, the vulnerabilities could be exploited to
 18 access sensitive consumer information handled by the
 19 servers.
 20 Fourth, the vulnerabilities identified in
 21 2010 penetration tests were publicly identified and
 22 commonly known to IT practitioners years before.
 23 And finally, the vulnerabilities could have
 24 been found at very low cost and then fixed at low cost.
 25 But to use these low-cost fixes, LabMD first had to know

23

1 the vulnerabilities were there. That's the point of
 2 risk assessment.
 3 To illustrate these points, let's turn to the
 4 penetration tests run on the server that --
 5 JUDGE CHAPPELL: Hold on a second. I'm trying
 6 to follow you here.
 7 Are you saying that respondent didn't even have
 8 some type of spyware or virus program on their system?
 9 Is that what you're saying?
 10 MR. SHEER: No, it isn't.
 11 What I am saying is that there are a variety of
 12 risk assessment tools, of which antivirus programs and
 13 spyware programs are one type. The distinction is that
 14 no one program, no one tool can identify all of the
 15 vulnerabilities that may be present on a system.
 16 So, for example, an antivirus program can find
 17 viruses, but it can't tell whether there's an
 18 unauthorized program on a computer, and so it goes, and
 19 so it isn't generally enough to be able to say, I have
 20 an antivirus program and I have an antispysware program.
 21 And the reason for that is because those programs are
 22 not capable of identifying other very significant risks
 23 that may confront a network.
 24 This is an example of that. The vulnerabilities
 25 that we are talking about cannot be identified using an

24

1 antivirus program or a spyware program.
 2 JUDGE CHAPPELL: So if I understand your
 3 position, any company out there today, in the
 4 United States of America, operating with customer
 5 information, who only has, let's say, McAfee or Norton
 6 spyware, adware, malware, virus protection, they're in
 7 violation of the FTC Act section 5?
 8 MR. SHEER: We're not saying that.
 9 Reasonable security, reasonable defense in
 10 depth depends on the circumstances. It takes into
 11 account all of the circumstances, including the size
 12 and complexity of the network, the kinds of information
 13 it has, the amount of information it has, the harm that
 14 could be done with that information, and the
 15 available -- and the cost of measures to address -- to
 16 address the risks and vulnerabilities.
 17 And so it is based on the totality of the
 18 circumstances rather than a laundry list of things that
 19 you check off and say yes, I have or don't have.
 20 JUDGE CHAPPELL: Go ahead.
 21 MR. SHEER: Turning to the penetration test that
 22 was run on the server that received sensitive
 23 information about hundreds of thousands of consumers, it
 24 is Exhibit CX 070.
 25 The test found that the server's overall

25

1 security posture was poor, partly because of the urgent
 2 risk to the FTP program used to receive the
 3 information.
 4 This vulnerability allows anonymous log-in to
 5 the FTP program. What that means is that anyone -- it
 6 was set up so that anyone could log in without having a
 7 user name and password.
 8 In conducting the test, the penetration tester
 9 passed through LabMD's firewall, found the FTP program,
 10 and tested it and found the vulnerability. An intruder
 11 could do exactly the same.
 12 The urgent risk identified in Exhibit CX 070 was
 13 well-known years before the 2010 pen test was conducted.
 14 It shows that the vulnerability was identified in 1999,
 15 if not earlier, in free national databases of
 16 vulnerabilities and exposures, along with an easy fix.
 17 The fix is to change the settings in the FTP
 18 program to disable anonymous log-in.
 19 JUDGE CHAPPELL: You said this Exhibit CX 70 was
 20 some type of penetration test? Who generated this
 21 document?
 22 MR. SHEER: This test was prepared by a company
 23 named ProviDyn. It is an outside information security
 24 firm. LabMD engaged it, well after the commission's
 25 investigation began, to test -- to conduct penetration

26

1 tests on nine IP addresses. It did so.
 2 JUDGE CHAPPELL: So this was a company that was
 3 retained by respondent.
 4 MR. SHEER: It was.
 5 JUDGE CHAPPELL: All right.
 6 MR. SHEER: The cost to LabMD of finding this
 7 vulnerability and other vulnerabilities was low. The
 8 company performing the penetration tests charged
 9 \$450 for nine tests, including the test in
 10 Exhibit CX 070.
 11 This cost is well within LabMD's reach given
 12 that it is a very profitable company that since 2005 had
 13 revenues of between 35 and 40 million dollars.
 14 The penetration tester found --
 15 JUDGE CHAPPELL: Is that million or billion, M
 16 or B?
 17 MR. SHEER: M, millions.
 18 The penetration tester found the FTP
 19 vulnerability using a free program called Nessus, which
 20 is often used by penetration testers and IP
 21 practitioners to spot a variety of network
 22 vulnerabilities. LabMD did not run Nessus on its own.
 23 Additional evidence will show that LabMD failed
 24 to use other appropriate risk assessment tools or did
 25 not use them properly. It did not use an intrusion

27

1 detection program to warn of attacks. Its antivirus
 2 program at times provided little or no protection.
 3 For example, the antivirus program on a server
 4 would not run a scan for about a year and did not have
 5 up-to-date antivirus definitions to warn of newly
 6 discovered attacks.
 7 Untrained employees were expected to respond to
 8 warnings on their computers from the antivirus programs
 9 on the computers.
 10 LabMD's answer to its risk assessment failures
 11 is that it had a firewall and manually inspected
 12 computers for vulnerabilities.
 13 The evidence will show, however, that the
 14 firewall does not have or does not eliminate the need
 15 for risk assessment. The firewall let some traffic
 16 through, opening doors through which vulnerabilities and
 17 intruders could enter the network.
 18 And although the firewall logged a limited
 19 amount of information that might have given some
 20 insight into risks, the information was overwritten
 21 every few days and was not systematically reviewed.
 22 LabMD actually only reviewed the firewall logs when
 23 users complained that their computers were not
 24 performing as they wished.
 25 As for manual inspections, which are also known

28

1 as walk-around inspections here, through at least
 2 mid-2008, these inspections were not systematic. LabMD
 3 conducted manual inspections only when a user
 4 complained that their computer was not working
 5 correctly.
 6 In addition, the inspections were cursory,
 7 seeking only to resolve the complaint.
 8 JUDGE CHAPPELL: You're talking about computer
 9 users. Are you talking about employees of LabMD?
 10 MR. SHEER: Yes.
 11 The manual inspections were not thorough.
 12 As Professor Hill will explain, even though
 13 systematic manual inspections are a poor substitute for
 14 automated -- she will explain that systematic manual
 15 inspections are a poor substitute for automated risk
 16 assessment tools.
 17 As the 1718 File incident shows, the evidence
 18 shows or will show that the 1718 File was disclosed
 19 without authorization to a public P2P network through
 20 LimeWire. It was a program for which LabMD had no
 21 business need.
 22 File-sharing programs, like LimeWire, present
 23 well-known risks.
 24 Georgetown University computer science
 25 professor Clay Shields, complaint counsel's expert on

29

1 P2P file-sharing programs, will explain that by 2005,
 2 IT practitioners were well aware of the risk that P2P
 3 programs and their users would inadvertently share
 4 files they did not intend to share, such as business
 5 files containing sensitive information. Inadvertent
 6 file sharing occurs because users mistakenly designate
 7 files for sharing.
 8 The evidence will show that LimeWire was
 9 installed on the LabMD computer in 2006. The billing
 10 manager used LimeWire to share music.
 11 Also designated for sharing from the computer
 12 was every file in the Windows My Documents folder, which
 13 is the default folder for a user's files.
 14 In all, more than 900 files were designated for
 15 sharing from the computer, including, most likely
 16 inadvertently, the 1718 File and other LimeWire LabMD
 17 business files.
 18 Would you bring up slide 6, please.
 19 Slide 6 is a screen shot of LimeWire taken from
 20 the computer used by LabMD's billing manager.
 21 And now can we have slide 7, please.
 22 Slide 7 has two highlighted lines. One shows a
 23 file -- it's the lower one I believe --
 24 JUDGE CHAPPELL: Is that my glasses or is that
 25 blurred?

30

1 MR. SHEER: It is blurry. And I apologize for
 2 that. This is the best that we can do with what we
 3 received.
 4 But if you look at the lower box, you will see
 5 three files. One of them is being highlighted now in
 6 yellow. It's called the Insurance Aging_6.05.071.pdf,
 7 and it's available for sharing. This is the 1718 File's
 8 true name.
 9 The upper bullet or the upper box has a
 10 highlighted line, and it shows that there were 950 files
 11 available for sharing from this computer.
 12 The evidence will show that LabMD's ordinary
 13 inspections did not find the LimeWire program.
 14 JUDGE CHAPPELL: Was this employee authorized to
 15 use LimeWire?
 16 MR. SHEER: LabMD is going to tell you no. And
 17 what the evidence is going to show, however, is that
 18 there were inadequate controls, as we will get to,
 19 inadequate controls to prevent this employee from
 20 downloading -- from installing -- downloading and
 21 installing LimeWire on the computer and using it.
 22 JUDGE CHAPPELL: Was that a no?
 23 MR. SHEER: That was a no.
 24 The evidence will show that LabMD's ordinary
 25 manual inspections did not find the LimeWire program.

31

1 LabMD found it on the computer two years after the
 2 program was installed and then only because it was
 3 informed by a third party that the 1718 File was
 4 available on a public P2P network.
 5 I'm going to turn now to the next of the
 6 security failures at LabMD, so we'll go back to slide 1,
 7 and this is authentication.
 8 The evidence will show that LabMD did not
 9 require employees and others to use appropriate
 10 authentication -- authentication-related security
 11 measures.
 12 Professor Hill will explain that LabMD did not
 13 have a strong password policy and did not use measures
 14 to ensure that employees use strong passwords.
 15 Could you pull up slide 8 now, please.
 16 Slide 8 is a 2010 table of user names and
 17 passwords.
 18 JUDGE CHAPPELL: Let's back up the truck here.
 19 This LimeWire program you're talking about, if
 20 that had never been downloaded by an employee, would we
 21 not be here today?
 22 MR. SHEER: It is likely that we would not know
 23 about the defects in LabMD's security practices had we
 24 not known that LimeWire was out on the -- that --
 25 rather, that the 1718 File was on the P2P network.

32

1 JUDGE CHAPPELL: So whatever information got out
 2 there in cyberspace was a result of LimeWire?
 3 MR. SHEER: It was a result of the company's
 4 security failures that allowed LimeWire to be used by an
 5 employee to --
 6 JUDGE CHAPPELL: But directly, was it a result
 7 of LimeWire directly? Is that how it got on the
 8 Internet?
 9 MR. SHEER: Yes, it is.
 10 JUDGE CHAPPELL: Thank you.
 11 MR. SHEER: Going back to this exhibit, it is a
 12 2010 table of user names and passwords at LabMD. It
 13 shows that a number of employees were able to use or
 14 allowed to use, quote-unquote, "LabMD" as their
 15 password. The vertical line in yellow identifies all
 16 of the instances in which that password "LabMD" was
 17 used.
 18 The evidence will show that reasonable
 19 security -- password security practices would have
 20 prevented employees from using "LabMD" or other easily
 21 guessed passwords.
 22 The last entry in the billing department's
 23 section on this exhibit -- it's the horizontal line --
 24 identifies "sbrown" as a user name and "labmd" as the
 25 corresponding password.

33

1 Sandra Brown was LabMD's billing manager in
 2 2005 and thereafter its insurance claim processor. She
 3 did most of the insurance claim processing work from her
 4 home computer and had access to very sensitive
 5 information, including files like the 1718 File. She
 6 used these same credentials -- "sbrown" plus "labmd" --
 7 without changing them between 2006 and 2013.
 8 The evidence will show that LabMD also provided
 9 computers to physician offices for them to use to
 10 transmit information to LabMD, including names,
 11 Social Security numbers and medical information. It did
 12 not set these computers up with strong passwords.
 13 JUDGE CHAPPELL: What's the operator password of
 14 the employee who downloaded LimeWire?
 15 MR. SHEER: I do not know. The employee who
 16 downloaded LimeWire is named Ros -- I'm sorry. Let me
 17 backtrack.
 18 We do not know, LabMD does not know, the name of
 19 the employee who installed LimeWire on the billing
 20 manager's computer.
 21 What we do know is that that computer was used
 22 by Ros Woodson, who was LabMD's billing manager. Her
 23 credentials, her user name and password are not included
 24 on this table.
 25 JUDGE CHAPPELL: Why is that?

34

1 MR. SHEER: Because she was dismissed from the
 2 company before this table was created.
 3 JUDGE CHAPPELL: So did you tell me this
 4 S. Brown is also a billing manager?
 5 MR. SHEER: For a time, for one year in 2005,
 6 Ms. Brown, Mrs. Brown, was the billing manager, and
 7 thereafter she was the insurance claim processor,
 8 working from home mainly.
 9 JUDGE CHAPPELL: All right. Thank you.
 10 MR. SHEER: Going back to the computers and the
 11 passwords for them set up in the physicians' offices,
 12 LabMD did not set these computers up with strong
 13 passwords, and the evidence will show that passwords --
 14 that the passwords were easy to guess.
 15 LabMD did not effectively secure these
 16 computers, exposing them to vulnerabilities that could
 17 be used to reach into LabMD's network and access
 18 sensitive consumer information there.
 19 Professor Hill will explain that the dangers of
 20 weak passwords are well-known. They can be exploited
 21 to obtain unauthorized access to networks and the
 22 computers and the information on them.
 23 The weak passwords used at LabMD on the
 24 computers in the company and the computers that the
 25 company provided to physician offices could be misused

35

1 to obtain unauthorized access to sensitive consumer
 2 information. This is the kind of information that
 3 identity thieves want and use to conduct identity
 4 theft.
 5 JUDGE CHAPPELL: These computers you're talking
 6 about provided to physician offices?
 7 MR. SHEER: Yes.
 8 JUDGE CHAPPELL: Am I mistaken or does the
 9 document here say they were not networked?
 10 MR. SHEER: They were networked. I don't think
 11 that's what the document says. The way --
 12 JUDGE CHAPPELL: In the column that says
 13 "Notes or Changes"?
 14 MR. SHEER: I understand.
 15 That is referring to the inside physicians at
 16 LabMD who are actually reading the tests and conducting
 17 them.
 18 What I'm talking about, however, is LabMD's
 19 business model, which was to put computers into the
 20 doctors' offices so that they could use them to place
 21 orders with LabMD.
 22 JUDGE CHAPPELL: And those computers are not on
 23 this document?
 24 MR. SHEER: Those computers are not on this
 25 document.

36

1 JUDGE CHAPPELL: But they were part of the
 2 network.
 3 MR. SHEER: They were part of the network.
 4 In fact, as we'll talk in a few moments, the
 5 FTP program vulnerability that we were talking about
 6 earlier and the risk assessment as part of CX 070, that
 7 FTP program is one of the principal ways in which
 8 doctors' offices transmitted sensitive consumer
 9 information to LabMD using these computers.
 10 The evidence will show that LabMD's Windows
 11 operating system had built-in functionality to manage
 12 passwords and that LabMD could have used this
 13 functionality at low cost. The company didn't do so,
 14 and it didn't use other methods to test password
 15 strength.
 16 I'd like to go back now to slide 1 and to the
 17 third of the security failures, which is detection and
 18 prevention.
 19 The evidence will show that LabMD did not use
 20 readily available security measures to prevent and
 21 detect unauthorized access to its network.
 22 The 2010 penetration tests identified urgent
 23 vulnerabilities that could have been used to obtain
 24 unauthorized access to LabMD's network, such as through
 25 the anonymous FTP log-in.

37

1 Professor Hill will explain that LabMD easily
 2 could have configured the FTP program to prohibit
 3 anonymous log-in and prevent unauthorized access into
 4 its system in that way.
 5 In addition, the evidence will show that some
 6 employees were given administrative controls over their
 7 computers, and some had Internet -- unrestricted
 8 Internet access as well, creating unnecessary security
 9 risks that could lead to unauthorized access and
 10 disclosure of sensitive information.
 11 Administrative control is the highest category
 12 of control available on Windows computers, and it
 13 allows users to install unauthorized programs without
 14 prior approval. Without administrative control, an
 15 employee could not have installed LimeWire on the
 16 billing manager's computer.
 17 Administrative control also means that
 18 employees could change security settings on their
 19 computers, such as by turning off built-in Windows
 20 security settings, without getting approval from
 21 anyone.
 22 Professor Hill will explain that LabMD could
 23 have avoided these risks at low cost using
 24 functionality already built into the Windows operating
 25 system on its computers. By doing so, it could have

38

1 prevented employees from installing unauthorized
 2 programs and changing security settings. The evidence
 3 will show it did not do that.
 4 Finally, LabMD required sensitive -- required
 5 sensitive consumer information, such as the information
 6 contained in the 1718 File, to be backed up on
 7 computers used by certain employees, including the
 8 billing manager. The need to back up information is
 9 obvious, but the evidence will show that LabMD easily
 10 could have backed up the information to a more secure
 11 location on its network.
 12 I'd like to turn now to the fourth of the
 13 security failures, its training.
 14 The evidence will show that LabMD failed to
 15 adequately train employees about information security.
 16 IT employees did not receive periodic security
 17 training.
 18 Professor Hill will explain that such training
 19 is intended to keep IT employees up-to-date about
 20 evolving threats and how to address them. IT training
 21 helps the employees stay ahead in the computer security
 22 arms race.
 23 The evidence will show that IT training
 24 appropriate for LabMD's employees was available from a
 25 number of sources at little or no cost.

39

1 JUDGE CHAPPELL: Regarding the training and the
 2 step above that where you said that employees could
 3 change security settings, et cetera, do you plan to
 4 introduce evidence of actual penetration of the
 5 network?
 6 MR. SHEER: We are not going to introduce
 7 evidence of that sort. And the reason for that is that
 8 we are unable to determine whether it happened. And
 9 the reason for that is that among LabMD's security
 10 failures is that it did not keep records and logs of
 11 activity on its network, which would allow one to go
 12 backwards and look and see what had actually happened.
 13 In addition, because it did not use an
 14 intrusion detection program, there were no warnings and
 15 records that would be created by that program to say
 16 something is happening here, there may be a breach, and
 17 there would be records to look back at. It is a
 18 fundamental security failure not to keep records that
 19 allow the company to look backwards and see what's
 20 happening on its network.
 21 JUDGE CHAPPELL: So if I understand your
 22 position as the United States government, because,
 23 first of all, you don't have evidence of penetration of
 24 the network, but because they don't have records
 25 showing it didn't happen, I'm to assume it did happen?

40

1 MR. SHEER: No. What we are saying here is
 2 that these vulnerabilities, these security failures,
 3 created an unreasonable risk of an intrusion or, if you
 4 will, as happened in this case, the exfiltration of
 5 information by an insider.
 6 Either way, the security vulnerabilities were
 7 such that it put the information at risk.
 8 JUDGE CHAPPELL: So you're not suggesting an
 9 inference that something happened just because records
 10 don't exist.
 11 MR. SHEER: No. We are saying simply that there
 12 is no way to determine whether something happened
 13 because the records don't exist.
 14 As I mentioned, LabMD had given non-IT
 15 employees administrative control over their computers.
 16 The evidence will show that the company did not
 17 adequately train non-IT employees about the security
 18 measures the company used or about the security risks to
 19 the company's networks if employees used administrative
 20 control to install unauthorized programs or change the
 21 security settings on their computers.
 22 The next of the security failures is updates.
 23 The evidence will show that LabMD failed to
 24 maintain and update operating systems and other devices
 25 on its network.

41

1 JUDGE CHAPPELL: Can you hold on a second?
 2 (Pause in the proceedings.)
 3 Go ahead.
 4 MR. SHEER: Back to updates.
 5 Professor Hill will explain that the
 6 penetration tests LabMD performed after the
 7 commission's investigation began identified an urgent
 8 default password vulnerability in the backup program
 9 that the company used. The vulnerability could be used
 10 to obtain unauthorized access to sensitive information
 11 on LabMD's network.
 12 The company easily could have updated the
 13 program and closed the vulnerability using a free
 14 update the program vendor provided in 2005. It didn't
 15 do that.
 16 Besides not updating the backup program, the
 17 evidence also will show that LabMD continued to run a
 18 Windows NT 4.0 operating system on a server for two
 19 years after Microsoft had stopped supporting it and had
 20 recommended using a more secure product.
 21 Turning to the sixth of the security failures,
 22 this is access controls.
 23 The evidence will show that LabMD failed to use
 24 adequate controls to limit employee access to just the
 25 sensitive information they needed to perform their

42

1 jobs.
 2 LabMD maintained very sensitive information
 3 about approximately 750,000 consumers in databases on
 4 its network, including their names, addresses,
 5 Social Security numbers, and medical information. The
 6 databases were accessible to managers and laboratory, IT
 7 and billing employees.
 8 LabMD did not use access control functionality
 9 built into its operating systems to limit the
 10 information employees could access. Because these
 11 access controls have to be programmed to actually work,
 12 the measures themselves can identify the types of
 13 information that employees were authorized to view.
 14 The evidence will show, however, that LabMD
 15 cannot identify the types of information employees were
 16 able to access. It could have used these access
 17 controls at low cost, but it didn't.
 18 In addition, included in the database employees
 19 could access was information about approximately a
 20 hundred thousand consumers to whom LabMD never provided
 21 any service at all. These consumers had no reason to
 22 know that the company had their information.
 23 The company collected the information to
 24 facilitate test ordering, but it didn't use it. And
 25 instead of deleting it, the company permanently retained

43

1 the information in databases where it was accessible to
 2 many company employees. Doing so put the information at
 3 risk of misuse through identity theft.
 4 And now we turn to number 7, the last of the
 5 security failures that we'll talk about. It is a
 6 written comprehensive information security program
 7 failure.
 8 Professor Hill will explain that the specific
 9 security measures that provide reasonable defense in
 10 depth on a particular computer network are the result
 11 of a security strategy. This strategy applies equally
 12 to large and small networks, and it takes into account
 13 the size and complexity of the network, the flow of
 14 information into and within the network, and the amount
 15 and sensitivity of the information on the network. The
 16 result is called a written comprehensive information
 17 security program.
 18 A written program is the road map the company
 19 follows to protect the network. At the core are
 20 specific goals, security goals, policies to achieve
 21 those goals, and procedures and tools to implement the
 22 policies.
 23 Comprehensive programs cover all rather than
 24 just some of the security issues that a company faces.
 25 The program tells IT employees what the security goals

44

1 are, as well as the policies, procedures and tools to
 2 use to achieve those goals. It also provides a basis
 3 for training non-IT employees about risks and their
 4 responsibilities in addressing them.
 5 The evidence will show that LabMD's security was
 6 ad hoc. The company did not have written security
 7 policies and procedures until 2010.
 8 As a result, until at least 2010, there was no
 9 written road map for LabMD's employees to follow to know
 10 how to secure the network. A road map was necessary for
 11 LabMD's employees.
 12 Would you please put up slide 9.
 13 This is an employment timeline for LabMD's IT
 14 employees. What it shows is there's an awful lot of
 15 turnover in the IT department and there's no long-term
 16 IT employee to pass on institutional knowledge about the
 17 company's security practices and experiences.
 18 The evidence will show that LabMD replaced
 19 outside IT contractors with the company's own IT
 20 employees, who are not network security specialists.
 21 The evidence will also show that LabMD's
 22 security practices were not comprehensive.
 23 For example, there was no policy about whether
 24 information was to be encrypted while it was stored on
 25 the network.

45

1 And some of the practices simply were not
 2 effective.
 3 For example, although the company had a policy
 4 recommending that employees encrypt sensitive
 5 information in e-mails, it provided no means for them to
 6 do that. There were no tools.
 7 Similarly, LabMD says it had a policy to
 8 identify and remove unauthorized programs from
 9 computers. The method for doing that was the manual or
 10 walk-around inspections we've talked about.
 11 The evidence will show, however, that for more
 12 than two years these walk-around inspections did not
 13 discover that LimeWire was installed on a LabMD computer
 14 used by the billing manager.
 15 LabMD could have created a written
 16 comprehensive information security program at low cost
 17 using model programs from national experts that had
 18 been available at no charge for years. The model
 19 programs provide a menu of security policies and
 20 procedures that companies can consider in developing
 21 their own information security programs that are
 22 appropriate for their circumstances.
 23 Turning now to relief, the order proposed by
 24 complaint counsel is not intended to punish LabMD. It
 25 is to ensure that the company protects the very

46

1 sensitive information it maintains about approximately
 2 750,000 consumers.
 3 It requires LabMD to implement a written
 4 comprehensive information security program that is
 5 appropriate to its circumstances.
 6 The proposed order also requires the company to
 7 obtain periodic third-party audits to verify that the
 8 program is providing reasonable and appropriate
 9 security. The company can choose its own assessor.
 10 Finally, the proposed order requires LabMD to
 11 provide notice to consumers whose information may have
 12 been disclosed without authorization, such as the
 13 9300 consumers whose information was in the 1718 File.
 14 An order is necessary, even though LabMD is no
 15 longer providing testing services, for several reasons.
 16 First, LabMD has no intention of dissolving and
 17 may in the future start anew. Were it to do so, an
 18 order could ensure that it practices reasonable defense
 19 in depth going forward.
 20 Second, the evidence will show that LabMD
 21 maintains sensitive information about approximately
 22 750,000 consumers on a computer network that can be
 23 accessed over the Internet. The information includes
 24 names, Social Security numbers, and medical
 25 information.

47

1 JUDGE CHAPPELL: If I understood you properly,
 2 you're saying that should LabMD completely dissolve and
 3 go out of business, that's irrelevant?
 4 MR. SHEER: They are telling us that they are
 5 not planning on dissolving, and the issue still would
 6 be, if they were dissolving, what happens to the
 7 information about 750,000 consumers.
 8 So it's got this information on a network that
 9 has access to the Internet and can be accessed through
 10 the Internet. The company operates the network, but
 11 it's dismissed all of its IT employees, so there are no
 12 IT personnel to manage the network security.
 13 There are no plans to conduct penetration tests,
 14 for example.
 15 LabMD's security is static in the face of
 16 evolving and growing threats. An appropriate order
 17 would ensure that the company protected the very
 18 sensitive information about 750,000 consumers that it
 19 maintains on this network.
 20 To sum up, the evidence will show that LabMD
 21 engaged in a number of practices that taken together
 22 fail to provide reasonable security for the most
 23 sensitive information of as many as 750,000 consumers.
 24 It did not practice defense in depth and its security
 25 was not proactive.

48

1 In particular, going back to slide 1, LabMD
 2 failed to adequately identify risks.
 3 It failed to adequately authenticate users.
 4 It failed to adequately use reasonable measures
 5 to detect and prevent unauthorized access to its
 6 networks.
 7 It failed to adequately train employees about
 8 security.
 9 It did not appropriately update its systems, and
 10 it didn't use access controls that were appropriate to
 11 prevent employees from using or accessing information
 12 that they did not need to do their jobs.
 13 And finally, it did not establish and implement
 14 a comprehensive information security program.
 15 Although the company may point to walk-around
 16 inspections and routers and firewalls, its security was
 17 equivalent to a castle with half a moat and with holes
 18 in the inner and outer walls.
 19 LabMD's failure to practice defense in depth is
 20 an unfair practice under section 5 of the FTC Act. It
 21 caused or is likely to cause identity theft, medical
 22 identity theft and other substantial harms.
 23 Consumers had no way of knowing about LabMD's
 24 security practices and thus could not reasonably avoid
 25 those harms.

1 And because the failures could have been
 2 corrected at low cost, there are no countervailing
 3 benefits to consumers or competition.
 4 Thank you.
 5 JUDGE CHAPPELL: Thank you.
 6 Who will speak for LabMD?
 7 MR. SHERMAN: I will, Your Honor.
 8 JUDGE CHAPPELL: Are you prepared?
 9 MR. SHERMAN: I had anticipated, as they
 10 represented last week, that their opening would be two
 11 hours. And in doing so, I can't say that I'm fully
 12 prepared, but if the court wants, we can proceed.
 13 JUDGE CHAPPELL: Are you requesting a short
 14 break?
 15 MR. SHERMAN: Yes, sir.
 16 JUDGE CHAPPELL: Subtly, though, but requesting
 17 a short break.
 18 I feel really accommodating this morning, so
 19 we'll take a break and we'll return at 11:30.
 20 We're in recess.
 21 (Recess)
 22 JUDGE CHAPPELL: We're back on the record.
 23 Is everyone ready?
 24 MR. SHERMAN: We are, Your Honor.
 25 JUDGE CHAPPELL: Proceed.

1 MR. SHERMAN: Good morning, Your Honor.
 2 May it please the court.
 3 Complaint counsel.
 4 Your Honor, I apologize for the delay and
 5 appreciate the court's indulgence.
 6 JUDGE CHAPPELL: This is a laptop that will be
 7 available from now on; correct?
 8 MR. SHERMAN: Yes, sir.
 9 JUDGE CHAPPELL: Okay.
 10 MR. SHERMAN: The evidence in this case will
 11 show that the FTC initiated its investigation of LabMD
 12 for unfair trade practices back in January of 2010.
 13 And the law is section 5 of the
 14 Federal Trade Commission Act. In pertinent part, it
 15 reads that "The Commission shall have no authority under
 16 this section or section 57a of this title to declare
 17 unlawful an act or practice on the grounds that such act
 18 or practice is unfair unless the act or practice causes
 19 or is likely to cause substantial injury to consumers
 20 which is not reasonably avoidable by consumers
 21 themselves and not outweighed by countervailing benefits
 22 to consumers or to competition."
 23 And I submit to the court that that is what the
 24 government must prove and that is what the government
 25 cannot prove.

1 And what portion of it is there that the
 2 government cannot prove, Your Honor? Well, let me start
 3 by saying this.
 4 As I mentioned before that this forum is a bit
 5 foreign to me, that being the case, this case fits
 6 within that foreign aspect that we're dealing with here
 7 because it appears that this case is more about what
 8 could have happened, it's more about what might happen,
 9 what might have happened, but it's certainly not about
 10 what happened.
 11 And the evidence will show that the government
 12 is unable to establish the link between what they allege
 13 are LabMD's data security practices and any harm to any
 14 consumer.
 15 JUDGE CHAPPELL: What about the likelihood of
 16 harm?
 17 MR. SHERMAN: I submit to the court that the
 18 evidence will be deficient in connecting LabMD's alleged
 19 data security practices and the likelihood of harm. And
 20 I submit to the court that that is precisely what they
 21 will be unable to prove.
 22 What the evidence will show -- and counsel did a
 23 very thorough and succinct job in terms of presenting to
 24 the court what their expert witness, Professor Hill, has
 25 laid out as LabMD's alleged inadequacies. But as the

1 court has lasered in on, what about the likelihood of
 2 this harm?
 3 Well, the problem with the evidence is,
 4 Dr. Hill says LabMD's data security practices are
 5 inadequate because they didn't do A, B, C, D, E, F and
 6 G.
 7 The evidence will show that Mr. Van Dyke will
 8 come in and say, Well, I was asked to assume that the
 9 practices were inadequate, and oh, by the way, if the
 10 information gets out and if it's in the hands of
 11 unauthorized third parties, the rate of injury is
 12 30.5 percent, not the likelihood of injury but the rate
 13 of injury.
 14 Dr. Kam or Professor Kam makes the same type of
 15 leap.
 16 Now, it's up to the government to bridge that
 17 chasm. They won't. They can't.
 18 In fact, the evidence will show that they don't
 19 know how the 1718 File escaped the possession of LabMD.
 20 The evidence will show that they don't know how
 21 the day sheets that were found in Sacramento escaped the
 22 possession of LabMD.
 23 So there's no causal connection between the
 24 alleged data security inadequacies and the appearance of
 25 these documents.

53

1 And what the evidence will show, Your Honor, is
 2 that there are a number of ways that these documents
 3 could have escaped the possession of LabMD even if
 4 LabMD's data security practices were perfect.
 5 And we've joked over and over again, thank God
 6 for Eric (sic) Snowden, because if documents can escape
 7 the NSA, then there is no perfect security. And every
 8 data security witness that appears on the stand will
 9 confirm that there is no perfect security.
 10 And so without this causal connection between
 11 this alleged inadequacy and the appearance of these
 12 documents outside of LabMD's possession, how does the
 13 government establish likelihood?
 14 JUDGE CHAPPELL: So you're saying, if I'm
 15 following you correctly, if there's no such thing as a
 16 perfect system, logic would dictate that harm would
 17 always be likely.
 18 MR. SHERMAN: It's not quite that simple,
 19 Judge.
 20 If I juggle knives for a living, there's a
 21 likelihood I will get my fingers cut. There's a
 22 likelihood. But I don't because I'm really, really good
 23 at juggling knives. Or I'm good enough at juggling
 24 knives that I don't get my finger cut.
 25 Now, if some expert comes in and says, Hey, for

54

1 the most part, you know, we did a survey of knife
 2 jugglers and 30.5 percent of people who juggle knives
 3 cut their fingers, that doesn't mean I'm going to cut
 4 mine. And if after I juggle knives there is no blood,
 5 there are no cuts.
 6 The government has submitted --
 7 JUDGE CHAPPELL: But in your analogy, in your
 8 analogy, though, the government's position from what I
 9 take it would be that you wouldn't be that knife
 10 juggler who's well-trained, you would be the knife
 11 juggler who's not as prepared, just following their
 12 opening statement.
 13 MR. SHERMAN: Even so, Your Honor, I'm prepared
 14 enough.
 15 JUDGE CHAPPELL: You're saying that the
 16 predictability analysis is flawed.
 17 MR. SHERMAN: Absolutely.
 18 I'm prepared enough that my fingers did not get
 19 cut. But they want this court to make the quantum leap
 20 that, Oh, Mr. Sherman, if you keep juggling those
 21 knives, you're likely to cut your fingers. Well, that's
 22 true. But I haven't. And is that enough?
 23 JUDGE CHAPPELL: But again, following their
 24 case, you've already cut yourself.
 25 MR. SHERMAN: That's where their case fails,

55

1 Your Honor. Because in order to -- if you cut, you
 2 bleed. There's no blood here. There's no harm.
 3 There's even a question as to whether or not
 4 they can prove that this file was found on a
 5 peer-to-peer network.
 6 But what the evidence will show, Judge, on top
 7 of this, is that even if it were found on a
 8 peer-to-peer network, it was found by a company by the
 9 name of Tiversa. And the evidence will show that
 10 Tiversa has issued press releases comparing its search
 11 capabilities and its search capacities to that of
 12 Google, that Tiversa has indicated even to the Congress
 13 of the United States that it has patented technology
 14 which allows it to search peer-to-peer networks in an
 15 unprecedented breadth and volume.
 16 JUDGE CHAPPELL: And Tiversa was the company not
 17 named by the government trolling for breaches in
 18 security?
 19 MR. SHERMAN: That's correct.
 20 JUDGE CHAPPELL: Do you concur that that company
 21 has no taxpayer funding?
 22 MR. SHERMAN: I do not.
 23 JUDGE CHAPPELL: Are you saying they were under
 24 government contract when they were trolling and
 25 identified your company, your client?

56

1 MR. SHERMAN: I don't know who they were
 2 providing services for or if they were providing
 3 services for anybody or if they just trolled. Because
 4 they collect information, and when somebody asks them if
 5 my information is out there, they have a huge database
 6 where they can search what they've already trolled and
 7 downloaded and tell someone whether or not their
 8 information is out there.
 9 But I will suggest that the evidence will show
 10 that they have government contracts.
 11 And so to say that they're not funded in any
 12 way by taxpayer dollars, Your Honor, I think is
 13 incorrect.
 14 JUDGE CHAPPELL: And what you're telling me
 15 you're going to provide in the record in this trial.
 16 You have evidence.
 17 MR. SHERMAN: Mr. Boback has been
 18 testified (sic) to show up here, and if he tells the
 19 truth, he must admit that they have government
 20 contracts.
 21 JUDGE CHAPPELL: That's the gentleman who moved
 22 to quash the subpoena?
 23 MR. SHERMAN: Yes, sir. That is the CEO, owner,
 24 president, man in charge of Tiversa, Inc.
 25 What the evidence will show here, Your Honor, is

57

1 that Tiversa was a research partner with
 2 Dartmouth College.
 3 You can put that exhibit up now.
 4 Dartmouth College in fact, in the 2004, '5, '6
 5 time frame, had a contract with Homeland Security.
 6 It's not that contract; it's the other one.
 7 JUDGE CHAPPELL: Who are you talking to?
 8 MR. SHERMAN: I'm talking to my technical
 9 people.
 10 JUDGE CHAPPELL: I can't --
 11 MR. SHERMAN: It's actually my attorneys
 12 actually. They've just --
 13 JUDGE CHAPPELL: Nothing I can do about that
 14 screen.
 15 MR. SHERMAN: This contract concerns itself with
 16 cyber sharing, cyber security collaboration and
 17 information sharing. It's RX 404.
 18 And Dartmouth College conducted research, with
 19 the help of Tiversa, on this very subject matter for the
 20 financial industry and for the medical industry.
 21 And here's where the 1718 File comes into play.
 22 But what's interesting about what the evidence
 23 will show with regard to this research, Tiversa's
 24 involvement as a research partner with
 25 Dartmouth College, is that neither Dartmouth College

58

1 professor Eric Johnson, who also filed a motion to
 2 quash his subpoena but will be here on Friday, nor
 3 Mr. Gormley, who was the operations officer at Tiversa
 4 during this time, neither of them could tell me during
 5 their depositions how the 1718 File was found.
 6 Mr. Johnson couldn't directly tie it to his
 7 research methodology in his data hemorrhaging in the
 8 health sector report that he put out.
 9 Tiversa could not tell me whether or not they
 10 found it as a result of work they were doing on the
 11 data hemorrhaging article, whether they were doing it
 12 for one of their other clients, or whether they just
 13 fed Mr. Johnson this document to, as he says in an
 14 e-mail to his research partner at Tiversa, to spice up
 15 my report.
 16 JUDGE CHAPPELL: So you're saying the company
 17 that allegedly found the document, 1718 File, can't
 18 tell you or tell us how it came to be, how they found
 19 it?
 20 MR. SHERMAN: Not from anyone we've talked to
 21 thus far.
 22 Now, let me say this, Judge.
 23 If Mr. Boback testifies consistent with his
 24 deposition testimony, he will say that the 1718 File
 25 was found at an IP address in San Diego, California.

59

1 He will also say that prior to his deposition, which
 2 was taken in November of 2013, that it was also found
 3 on three separate IP addresses. I believe complaint
 4 counsel mentioned that.
 5 JUDGE CHAPPELL: Since it's your client, for the
 6 benefit of all these people here that don't know what
 7 we're talking about, what is the 1718 File and a day
 8 sheet?
 9 MR. SHERMAN: The 1718 File is an insurance
 10 aging report that LabMD's billing manager created. And
 11 what LabMD did with these insurance aging reports is
 12 they collected money from those people who owed them
 13 money for tests that they had performed.
 14 On the 1718 File, the insurance aging report,
 15 name, address, Social Security number for most people,
 16 and so they created the file. And there is testimony in
 17 the deposition designations that once these files were
 18 created, they were destroyed. They were shredded at the
 19 end of the day because they would be handed out to
 20 billing department, and they would then make calls to
 21 collect the money owed to LabMD.
 22 A day sheet, on the other hand, is a sheet which
 23 again contains --
 24 JUDGE CHAPPELL: Let me back up there.
 25 The 1718 File then was maintained as a

60

1 reconciliation document, so after your insurance paid,
 2 this is what the client owed or the customer owed in the
 3 end?
 4 I'm just trying to figure out the purpose for
 5 maintaining the file.
 6 MR. SHERMAN: See, that's just it, Your Honor.
 7 In the normal course of LabMD's business, files like
 8 the 1718 File were not maintained. They were actually
 9 created using a database which the billing manager will
 10 put in parameters, okay, let's see who still owes us
 11 from June to July, print off a file similar to the
 12 1718 File.
 13 JUDGE CHAPPELL: Is it a 1718 File like
 14 1718 File, for example, they do them all the time or was
 15 it --
 16 MR. SHERMAN: Daily.
 17 JUDGE CHAPPELL: -- one, one file?
 18 MR. SHERMAN: Daily.
 19 JUDGE CHAPPELL: Okay.
 20 MR. SHERMAN: Or every other day or until the
 21 pages that were created that day to collect were
 22 actually called upon by the people in the billing
 23 department. People in the billing department shredded
 24 them on a daily basis.
 25 The anomaly of the existence of the 1718 File is

61

1 still boggling because, even with all the resources of
 2 the federal government, no one has been able to find
 3 Ros Woodson, the very person who was using LimeWire on
 4 her computer, the very person who created the 1718 File.
 5 And there's testimony that she didn't know what
 6 she was doing when she was using LimeWire. And in fact,
 7 the article that's on the screen assumes inadvertent
 8 file sharing.
 9 And so if you take all of the evidence that's
 10 presented about how this LimeWire works and how people
 11 use it to download music and inadvertently share other
 12 information that they didn't intend to share, the story
 13 makes a little more sense.
 14 JUDGE CHAPPELL: And what's a day sheet?
 15 MR. SHERMAN: A day sheet is a sheet again
 16 that's used for collection purposes. I think what it
 17 shows -- it's kind of like a back end of the 1718 File
 18 that shows who paid, what payments were received.
 19 And so the day sheets, the evidence will show,
 20 Your Honor, are not electronically maintained. In fact,
 21 it's the type of document that you open up, you populate
 22 it with the information, but you cannot save the
 23 information electronically, and so LabMD would print the
 24 day sheets and store them in their paper form on LabMD
 25 premises.

62

1 So part of what the evidence will show is that
 2 the day sheets could not have escaped LabMD's possession
 3 as a result of a data -- an electronic data
 4 security-type breach or inadequacy.
 5 But back to the background of the story, and
 6 I'll -- I have to move along a little quicker than I am,
 7 Judge.
 8 Dartmouth and Tiversa are research partners.
 9 Dartmouth has the grant. The testimony is that Tiversa,
 10 in exchange for Dartmouth evaluating its search
 11 capabilities, agreed to be Dartmouth's research partner
 12 and therefore receive no remuneration for their
 13 participation with Dartmouth College.
 14 But again, it was from Tiversa that
 15 Dartmouth College received the 1718 File and made
 16 representations in this report that they received this
 17 1718 File as a result of their research methodology,
 18 their digital footprint, and therefore gave the public
 19 this idea, including the government, this idea that this
 20 file was easily downloadable by anybody using LimeWire
 21 or a peer-to-peer network.
 22 The fact of the matter is, the evidence will
 23 show that upon immediately learning that this file had
 24 allegedly escaped LabMD's possession, LabMD had one of
 25 its IT personnel go home, download LimeWire and use

63

1 precisely -- precisely -- the file name and search for
 2 the file. They didn't find it.
 3 A few years later, LabMD had another of its IT
 4 persons search using a peer-to-peer network using the
 5 precise file name. He didn't find it.
 6 I think it's significant, Your Honor, that the
 7 evidence will show that the only entity able to find
 8 this file has patented technology.
 9 Likely to cause substantial harm I think not.
 10 JUDGE CHAPPELL: If that's the case, how do you
 11 explain the allegation -- I don't know if it's
 12 disputed -- of the documents turning up in a flophouse
 13 in California?
 14 MR. SHERMAN: We don't. The government doesn't
 15 explain it either.
 16 The government, again, wants this court to say,
 17 Well, the documents showed up in a house in Sacramento.
 18 Somebody must be harmed.
 19 Who is it? When? How did the documents
 20 escape? I submit to you, there's no -- there will be
 21 no evidence of how the document escaped. And what they
 22 must prove is that the practice was unfair and that
 23 unfair practice is likely to cause harm.
 24 But again, this case is not about what actually
 25 happens but what might happen, what could have

64

1 happened.
 2 LabMD had firewalls in place. LabMD had spyware
 3 and antivirusware in place and they had routers and they
 4 had all these things in place, but it just wasn't good
 5 enough. Yeah, they had it, but it wasn't good enough
 6 for Dr. Hill.
 7 It wasn't good enough for Professor Shields, I
 8 believe it is. It just wasn't good enough.
 9 But the evidence will show that it was good
 10 enough to keep someone from likely being harmed, because
 11 nobody has been harmed.
 12 The evidence will further show that --
 13 JUDGE CHAPPELL: Wait a second.
 14 So your position is, if it did not happen, it is
 15 not likely?
 16 MR. SHERMAN: My position is that the federal
 17 government should not be able to come in and say that we
 18 find, through our expert, based on a three-year
 19 investigation and all of the information that you've
 20 given us about what you were doing, that what you were
 21 doing was unfair and not have to prove how likely it is
 22 that substantial harm is going to occur in face of no
 23 harm occurring.
 24 I think that their job would be a lot easier if
 25 they could show some harm. But without it, they have

65

1 to prove "likely," and I don't know that they will
 2 present -- all the evidence that I've seen, Judge,
 3 "likely" is missing.
 4 The rate at which people will be injured if
 5 certain factors exist is documented by Van Dyke and
 6 Kam, but the evidence will show that when Van Dyke and
 7 Kam are questioned about the facts in this case, "Well,
 8 I wasn't asked to consider that" is their answer. When
 9 Van Dyke and Kam are asked, Well, did the government
 10 tell you that no one had been harmed? Well, why no.
 11 And so if the government is going to take the
 12 position, which they have, that the data security
 13 standards which the regulated business community should
 14 be aware of will be applied on a case-by-case basis, it
 15 seems to me that the evidence should show that their
 16 experts considered the facts in this case. And I submit
 17 to the court that the evidence is not going to show
 18 that.
 19 What the evidence will show is that when the
 20 LabMD employees were questioned about what was in
 21 place, for example, who had access to information
 22 necessary to do their jobs, employee after employee
 23 after IT person basically said, Well, it was my
 24 understanding that the workstations were configured
 25 such that people only had access to what they needed

66

1 for their job. Billing did not have access to financial
 2 information. The people in the lab didn't have access
 3 to billing information, but billing did have access to
 4 people in the lab because they needed the codes, so they
 5 had.
 6 JUDGE CHAPPELL: What about his slide that
 7 showed people didn't change passwords for over five
 8 years?
 9 MR. SHERMAN: People didn't change passwords for
 10 over five years.
 11 JUDGE CHAPPELL: But does that mean anybody can
 12 sit there and access whatever they need to?
 13 MR. SHERMAN: It doesn't mean they didn't log
 14 off, Judge. I mean, I can keep my password for five
 15 years and you'll never know what it is. That doesn't
 16 mean because my password is five years old that somehow
 17 you're going to have access to the information on my
 18 desktop.
 19 JUDGE CHAPPELL: Well, I have no idea what kind
 20 of operation LabMD was running. I don't know if it was
 21 a 15-story building full of people, one room with three
 22 cubicles, so when you said billing didn't know what the
 23 other department was doing, it's hard for me to put that
 24 in context. I mean, were there a hundred employees? I
 25 have no idea.

67

1 MR. SHERMAN: There were anywhere between 25 to
 2 35 employees, 15 to 20 desktops.
 3 JUDGE CHAPPELL: Now, you had at some point I
 4 guess technicians or medical personnel doing medical
 5 tests.
 6 MR. SHERMAN: That's correct.
 7 JUDGE CHAPPELL: Are they part of this net that
 8 had access to the computer system and didn't change
 9 passwords?
 10 MR. SHERMAN: The medical personnel were not --
 11 the medical personnel looked at the actual slides,
 12 tissue, urine, blood samples, and they made their
 13 diagnosis of cancer.
 14 What the evidence will show is that the
 15 countervailing benefit to doing it this way, to having
 16 physician clients transfer information from their office
 17 to LabMD, was consistent with what the federal
 18 government was asking the medical community to do
 19 anyway, which was to go to electronic medical data.
 20 And the benefit is, you cut down on paper.
 21 That's obvious.
 22 Secondly, you cut down on data entry mistakes.
 23 Once it's there, it's there.
 24 JUDGE CHAPPELL: These 15 or 20 personnel who
 25 had desktops, does that include the outside companies?

68

1 MR. SHERMAN: No, it does not.
 2 And the evidence will show that the -- this
 3 concept about all physician clients having LabMD
 4 computers installed is something that may have occurred
 5 on a more regular basis in 2005, '6 and '7, but the
 6 evidence will show that as medical doctors' offices
 7 became more technologically savvy, you know, they were
 8 able to transfer this information using their own
 9 information technology through a secure FTP. And that's
 10 how it was done.
 11 And the speed with which a doctor could order a
 12 test was simply by identifying the patient
 13 identification number and the test that that patient
 14 needed. That information was already on LabMD's
 15 database -- the evidence will show and Mr. Daugherty
 16 will testify to it -- that information was already on
 17 LabMD's database.
 18 It's transferred electronically. No one has to
 19 go in and read someone's sloppy handwriting about,
 20 you know, what test is performed and what is the
 21 identification number for the client. It's already
 22 there. It's in electronic form. You know what test you
 23 want to perform. The sample arrives. The doctor does
 24 the test. And guess what? The physician has access to
 25 the test results electronically. He doesn't have to

69

1 wait.

2 And so there is countervailing benefit to the

3 consumer, to someone who wants to know whether or not

4 they've got cancer, which, as we know, is an

5 exigent-type disease. The sooner you find out, the

6 better.

7 And so when Dr. Hill and the federal government

8 says, Well, you know, yeah, you had a firewall, but you

9 didn't block access to every port coming in, well, yeah,

10 maybe LabMD didn't, but they're playing with knives and

11 they're not bleeding.

12 And so --

13 JUDGE CHAPPELL: What's the operating status of

14 your client? Are they in business?

15 MR. SHERMAN: They are in business to the extent

16 that if doctors call and say, "What was the result of

17 that test back in 2006 or back in 2010?" LabMD has the

18 ability to give them that result. Their database is

19 not, the evidence will show, is not connected to the

20 Internet, so these dangers that would exist don't

21 currently exist.

22 JUDGE CHAPPELL: At what point did LabMD cease

23 testing new samples?

24 MR. SHERMAN: In January of this year,

25 Your Honor.

70

1 JUDGE CHAPPELL: So this database of hundreds of

2 thousands of consumers, what's the purpose of

3 maintaining that?

4 MR. SHERMAN: I believe HIPAA requires that that

5 information be retained for a period of years.

6 And the evidence will show, Your Honor, that

7 LabMD, if it succeeds here, will attempt to restart its

8 business.

9 The evidence will show that LabMD, if it's

10 successful here, will attempt to get the necessary

11 insurance that it's unable to get currently to operate

12 its business.

13 JUDGE CHAPPELL: So the scientific or technical

14 and medical personnel have been laid off or fired or --

15 MR. SHERMAN: Absolutely.

16 Judge, if I might move forward, what you will

17 find from the evidence is that only --

18 JUDGE CHAPPELL: Let me finish my line of

19 questioning.

20 MR. SHERMAN: Yes, sir.

21 JUDGE CHAPPELL: And what's going to be your

22 position of the reason why LabMD ceased operating in

23 January of 2014?

24 MR. SHERMAN: It's my understanding that LabMD

25 was losing money every month as a result of physicians

71

1 being very wary of the fact that LabMD is being

2 investigated by the FTC for data security inadequacy.

3 And clearly, if a physician then continues to

4 send protected health information to a place where there

5 is some doubt as to whether or not it's adequately

6 protected, then that physician is putting itself in

7 liability's way.

8 JUDGE CHAPPELL: So your position is, caused by

9 the government case, not by the business model?

10 MR. SHERMAN: Your Honor, the business model was

11 cutting edge at its time. The business model was

12 applauded by the physicians. The business model enabled

13 LabMD to compete with labs ten times its size.

14 JUDGE CHAPPELL: LabCorp? Like LabCorp?

15 MR. SHERMAN: To name one. Absolutely.

16 LabMD had clients in six or seven states across

17 the south. Why? Because they were doing things

18 electronically, Judge.

19 And the evidence will show that they had no

20 complaints from doctors concerning the loss of patient

21 information.

22 They didn't have the Cadillac of systems. They

23 didn't meet Dr. Hill's standard. They didn't. But they

24 didn't cut their fingers.

25 They took the appropriate precautions, and

72

1 because they did so, the government will not be able to

2 establish "likely," because everything points against

3 "likely."

4 But I do understand that this case is not about

5 what actually happened but what might and what could

6 have and what might have and those types of things, so

7 we have to deal with the forum in which we find ourself,

8 but what you will get from the IT managers and from the

9 employees of LabMD is that, well, only the managers had

10 access to the Internet, and the purpose for that was so

11 that they could access the insurance companies'

12 Web sites so that they could follow the regulations set

13 out by the insurance companies and use the appropriate

14 codes for the appropriate tests and services that they

15 provided so that they could get paid.

16 LabMD was a small business in the business of

17 doing business, cancer detection. They were not in the

18 business of creating the best data security system out

19 there. It's simply just not how it works in the real

20 world.

21 What the employees will say is that even the

22 managers who had access to the Internet, in order to

23 download programs from the Internet, were supposed to

24 get permission from the IT department. That was a

25 policy. It was known across the board at LabMD. If

73

1 you're going to download something, you need to get
 2 permission from IT to do it.
 3 JUDGE CHAPPELL: The government's position is
 4 those employees had admin privileges, which means they
 5 didn't have to get permission.
 6 MR. SHERMAN: That's correct. That's correct.
 7 But they knew that they should have gotten permission.
 8 And what you find, Your Honor, is after the
 9 peer -- after LimeWire was found on one computer, it
 10 wasn't found on any other. They checked every computer.
 11 There were no peer-to-peer programs on any other
 12 computer. The policy was being followed. But you
 13 always have an Eric Snowden in your midst. And you
 14 can't protect against a rogue employee.
 15 JUDGE CHAPPELL: So who is Eric Snowden in this
 16 scenario?
 17 MR. SHERMAN: Eric Snowden is Ros Woodson,
 18 potentially.
 19 JUDGE CHAPPELL: And no one has been able to
 20 depose Ros?
 21 MR. SHERMAN: Your Honor, it's the strangest
 22 thing. The federal government cannot find Ros Woodson.
 23 Found Osama bin Laden. We can't find Ros Woodson.
 24 JUDGE CHAPPELL: Well, that took a while.
 25 But let's talk about Ros Woodson. If no one has

74

1 found her, how do we know -- and I don't know if I heard
 2 it today or I read it in pleadings -- how do we know her
 3 motivation for LimeWire?
 4 MR. SHERMAN: We don't.
 5 JUDGE CHAPPELL: So we don't know if it was just
 6 to download music.
 7 MR. SHERMAN: We have testimony from Ms. Garrett
 8 I believe that Ros Woodson didn't have a computer at
 9 home and she just wanted to download music and she was
 10 burning music files, and that's why she downloaded
 11 LimeWire and -- that's what we heard.
 12 It would have been nice to know from Ms. Woodson
 13 why she did what she did, but apparently she's -- she's
 14 pretty good at concealing her whereabouts.
 15 JUDGE CHAPPELL: I don't believe she's on any
 16 witness list, is she, on either side?
 17 MR. SHERMAN: I don't think she is. We may
 18 have put her on our witness list, you know, with our
 19 fingers crossed that she would somehow -- but I don't
 20 expect that Ms. Woodson will show up and testify. She
 21 has not been subpoenaed.
 22 JUDGE CHAPPELL: So as far as you know, she has
 23 taken off to some country without an expedition treaty
 24 to the United States? Off the grid?
 25 MR. SHERMAN: She could be in Costa Rica.

75

1 What you will see from the deposition --
 2 JUDGE CHAPPELL: Regarding her, I just want to
 3 make sure, was she fired over this incident? Is that
 4 the company's position?
 5 MR. SHERMAN: There's testimony from the
 6 person --
 7 JUDGE CHAPPELL: Do you want to consult with the
 8 guy shaking his head?
 9 MR. SHERMAN: It depends on which way he was
 10 shaking his head because -- there's testimony that she
 11 was fired for not performing her duties up to the level
 12 of a manager.
 13 Now, maybe that's some employment law CYA, but
 14 she was fired because, in not performing her duties up
 15 to the level of a manager, she had LimeWire on her
 16 computer.
 17 JUDGE CHAPPELL: Okay. But it happened to be
 18 right after LimeWire was discovered.
 19 MR. SHERMAN: Yes, it was.
 20 JUDGE CHAPPELL: All right.
 21 MR. SHERMAN: What the IT employees at LabMD
 22 will say --
 23 JUDGE CHAPPELL: And I know there's members of
 24 the press out there. They're not saying she was fired
 25 just for LimeWire, just so we're clear.

76

1 MR. SHERMAN: Thank you, Your Honor.
 2 The IT employees will say over and over again
 3 that they received on-the-job training. They received
 4 on-the-job training to do what they were hired to do.
 5 Many of them were just lab technicians -- I'm sorry --
 6 computer technicians, who would go around and set up new
 7 computers, download the necessary software, so that
 8 LabMD could do business.
 9 What the IT employees will say is that they
 10 believed that LabMD's security was adequate. Was it
 11 perfect? I don't think any of them can say that. But
 12 they will say that it was adequate. They will testify
 13 that they themselves know of no security breach.
 14 As I said before, they will testify concerning
 15 LabMD having multiple firewalls in place, that LabMD's
 16 firewalls prevented unauthorized intruders into their
 17 system.
 18 JUDGE CHAPPELL: Does your client have an IT
 19 manager? A webmaster? Anything like that?
 20 MR. SHERMAN: In the early years, 2005, 2006,
 21 2007, I would describe LabMD's IT department as flat.
 22 JUDGE CHAPPELL: Meaning?
 23 MR. SHERMAN: Meaning there was no manager.
 24 There were three people who did what they had to do on a
 25 daily basis, and the more complex areas of IT were

77

1 handled by third-party providers, such as -- APT? Is
 2 that what it was called? Truett's company -- such as
 3 APT. The evidence will show this.
 4 In or about 2007, John Boyle was hired as the
 5 chief operating officer. And John Boyle has extensive
 6 experience in terms of information technology and
 7 network security, and he was in charge from 2007 all the
 8 way up until I believe 2011.
 9 JUDGE CHAPPELL: And when was the LimeWire
 10 incident?
 11 MR. SHERMAN: The LimeWire incident -- LimeWire
 12 was discovered in May of 2008. There will be evidence
 13 to show that, Your Honor.
 14 But again, there will be testimony from those
 15 who were there that will describe the technological
 16 processes and efforts that were put in place by LabMD to
 17 protect the protected health information, which they
 18 knew was key to gaining the trust of their physician
 19 clients and building a business that would operate.
 20 And so to suggest, as the government has, that
 21 LabMD willy-nilly did as little as possible to protect
 22 the very life's blood of their business is I think a
 23 far-reaching, ludicrous --
 24 JUDGE CHAPPELL: And let's remember, this is
 25 opening statement, not argument.

78

1 MR. SHERMAN: I understand.
 2 And so with that, Judge, I believe that I've
 3 given you a pretty good overview of what the
 4 respondent's position is with regard to really what the
 5 evidence will show and mainly what evidence will not be
 6 shown.
 7 Thank you, Your Honor.
 8 JUDGE CHAPPELL: Thank you.
 9 All right. We're going to take a lunch break.
 10 When we come back, I expect the government to be
 11 prepared to call their first witness. We're going to
 12 get after this.
 13 We're going to return at 1:45.
 14 We're in recess.
 15 (Whereupon, at 12:37 p.m., a lunch recess was
 16 taken.)
 17
 18
 19
 20
 21
 22
 23
 24
 25

79

1 AFTERNOON SESSION
 2 (1:51 p.m.)
 3 JUDGE CHAPPELL: Back on the record.
 4 We have a few scheduling issues to deal with.
 5 Some general information if you're -- I think
 6 this was in our e-mail to the parties.
 7 We're generally going to be here from 9:30 a.m.
 8 to 5:30 p.m. starting tomorrow, we're at 9:30.
 9 We'll take a one-hour lunch break sometime in
 10 the afternoon, a ten-minute break in the morning and
 11 afternoon as appropriate.
 12 There will be days when we have a witness from
 13 out of town or out of the country, and with prior
 14 approval, we can go late. The "prior approval" means
 15 you let me know no later than the day before. And
 16 that's simply because there's a lot more people involved
 17 in making this happen than who you see up here. We've
 18 got building personnel and others involved to go late in
 19 this building.
 20 Generally, the morning break will be between
 21 11:00 and 11:30, lunch sometime between 1:00 and 2:00,
 22 afternoon break sometime between 3:30 and 4:00.
 23 And make a note, this Thursday, the 22nd, we
 24 will end court no later than 5:00 p.m. on that day.
 25 Any questions on that?

80

1 MS. VANDRUFF: No, Your Honor.
 2 MR. SHERMAN: No, sir.
 3 JUDGE CHAPPELL: All right. Call your first
 4 witness.
 5 MS. LASSACK: Good afternoon, Your Honor.
 6 Maggie Lassack for complaint counsel.
 7 We'd like to call to the stand Dr. Raquel Hill.
 8 JUDGE CHAPPELL: All right. Step up here, and
 9 the court reporter will swear you in.
 10 - - - - -
 11 Whereupon --
 12 RAQUEL HILL, Ph.D.
 13 a witness, called for examination, having been first
 14 duly sworn, was examined and testified as follows:
 15 JUDGE CHAPPELL: All right. Go ahead.
 16 MS. LASSACK: Your Honor, one preliminary
 17 matter. We have binders of documents for the witness
 18 and opposing counsel that we may use today. May I
 19 approach to provide one to Your Honor and to your
 20 clerks?
 21 JUDGE CHAPPELL: If I need a document, I'll ask
 22 for it. And it's okay to provide binders to the witness
 23 if the documents are in evidence and the opposing party
 24 is aware or has a copy of it.
 25 MR. SHERMAN: I do have a copy, Your Honor.

81

1 - - - - -
2 DIRECT EXAMINATION
3 BY MS. LASSACK:
4 **Q. Good afternoon, Dr. Hill.**
5 A. Good afternoon.
6 **Q. Would you please introduce yourself to the**
7 **court.**
8 A. My name is Dr. Raquel Hill. I'm an associate
9 professor of computer science at Indiana University.
10 **Q. Dr. Hill, how much experience do you have in**
11 **computing?**
12 A. I have over 25 years in computing.
13 **Q. What are your areas of expertise?**
14 A. My areas of expertise are data security, system
15 security and data privacy.
16 **Q. How long have you been a professor of computer**
17 **science at Indiana University?**
18 A. I've been a professor at Indiana University for
19 nine years.
20 **Q. When did you earn tenure?**
21 A. I earned tenure in 2012.
22 **Q. Professor Hill, would you please describe for**
23 **the court your education that you received to become a**
24 **professor in computer science.**
25 A. I received my bachelor's degree in computer

82

1 science with honors from Georgia Institute of Technology
2 in Atlanta, Georgia; my master's degree in computer
3 science from Georgia Tech; and my Ph.D. in computer
4 science from Harvard University.
5 **Q. When did you earn your Ph.D. in computer**
6 **science?**
7 A. In 2002.
8 **Q. Professor Hill, would you describe for the court**
9 **your dissertation research.**
10 A. My dissertation research, I designed and
11 implemented a lightweight reservation protocol that
12 would allocate bandwidth for audio and video
13 applications so that they could run over the Internet.
14 **Q. Professor Hill, was there any security component**
15 **to your dissertation research?**
16 A. Yes. I did an evaluation of the -- of the
17 protocol and -- a security evaluation of the protocol,
18 and I designed mechanisms to address the vulnerabilities
19 in the protocol.
20 **Q. Describe for the court how the protocol worked.**
21 A. The way that the protocol worked is that it was
22 an end-to-end protocol, so you had a client user on one
23 side of the communications channel and then maybe there
24 was a server on the other side that it wanted to
25 retrieve the video or audio data from, and so instead of

83

1 using more heavyweight signaling protocols that would
2 require you to use additional bandwidth, my protocol
3 actually embedded the request in the headers of the data
4 packets that flow between the two endpoints of the
5 communications channel.
6 And so by doing that embedding of information in
7 the headers, routers along the path can make a decision
8 about whether they could support the traffic, and so as
9 that data was propagated from one router in the Internet
10 to the next, each router made a decision about whether
11 it would support that data.
12 **Q. Would you describe the security mechanisms that**
13 **you designed in connection with that work.**
14 A. So one of the security mechanisms was to
15 prevent --
16 JUDGE CHAPPELL: Excuse me. Are we still
17 talking about the dissertation?
18 MS. LASSACK: Yes, Your Honor.
19 JUDGE CHAPPELL: And before we get too far down
20 the rabbit hole, are you going to connect what she's
21 saying now to her opinions in this case?
22 MS. LASSACK: This is to qualify her as an
23 expert, Your Honor.
24 JUDGE CHAPPELL: Is there an objection to her
25 qualification?

84

1 MR. SHERMAN: No, sir, Your Honor.
2 JUDGE CHAPPELL: Why don't we just get to the
3 heart of the matter here.
4 MS. LASSACK: Okay.
5 BY MS. LASSACK:
6 **Q. Professor Hill, I'd like to direct your**
7 **attention to CX 740.**
8 **It also appears on the screen as well.**
9 **Professor Hill, what is CX 740?**
10 A. CX 740 is my expert report.
11 JUDGE CHAPPELL: And just so we're clear, I'm
12 not stepping on your ability to examine your expert
13 witness, but I assume her CV is somewhere in the record,
14 so I don't think we need to hear it unless there's an
15 objection to her qualification.
16 MS. LASSACK: Okay, Your Honor. We'll move on.
17 JUDGE CHAPPELL: And that goes for any expert
18 that comes in here.
19 BY MS. LASSACK:
20 **Q. Professor Hill, did complaint counsel ask you to**
21 **assess whether LabMD provides reasonable and appropriate**
22 **security for personal information within its computer**
23 **network?**
24 A. Yes.
25 **Q. What did you conclude?**

1 A. I concluded that they did not provide reasonable
 2 and appropriate security.
 3 **Q. What time period does your conclusion cover?**
 4 A. January 2005 until July of 2010.
 5 **Q. Professor Hill, I'd like you to look at**
 6 **paragraph 48 of your expert report.**
 7 **Will you please read aloud the second sentence**
 8 **of that paragraph.**
 9 A. "From my review of the record, there are not
 10 sufficiently diverse types of information available
 11 after the relevant time period for me to offer opinions
 12 about that period."
 13 **Q. Please explain to the court what that means.**
 14 A. That means that during the relevant time
 15 period, there were a variety of types of information,
 16 including antivirus scans, deposition testimony, risk
 17 assessment scans, and all of this information wasn't
 18 available after the relevant time period.
 19 **Q. Can you give the court an example of something**
 20 **that was not available?**
 21 A. One of the things that was not available was
 22 the antivirus scans. There were -- another thing that
 23 was very helpful were the vendor reports, like the APT
 24 documents that discussed the specific things that had
 25 been done, so those types of things were not available.

1 **Q. When you say "the APT documents," what are**
 2 **those?**
 3 A. The ATP -- APT was a vendor that provided
 4 services, computer maintenance services for LabMD early
 5 in the relevant time period, and that there were
 6 descriptions of the vulnerabilities that they addressed
 7 or other problems that they addressed on the LabMD
 8 network, and so that provided specific details.
 9 JUDGE CHAPPELL: Is that an acronym for the
 10 company or is that the actual name of the company?
 11 THE WITNESS: I don't recall, sir, if that was
 12 the actual -- if that's the actual name or it is an
 13 acronym.
 14 MR. SHERMAN: If it would help the court, it's
 15 an acronym.
 16 MS. LASSACK: It's Automated PC Technologies.
 17 BY MS. LASSACK:
 18 **Q. Professor Hill, what material did you consider**
 19 **in reaching your conclusion?**
 20 A. I considered the record evidence that was
 21 provided to me.
 22 I also considered government standards and
 23 guidelines and industry standards.
 24 I also considered my own knowledge about the
 25 subject matter.

1 **Q. When you say "government standards," what do you**
 2 **mean by that?**
 3 A. When I say "government standards," I mean
 4 documents that have been provided by government agencies
 5 as guidelines for securing computing infrastructure,
 6 also national vulnerability databases and those types of
 7 things that are managed by government entities and
 8 industry and academia.
 9 **Q. You considered industry standards as well;**
 10 **correct?**
 11 A. Yes, I did.
 12 **Q. Have you read the expert report submitted by**
 13 **LabMD's expert?**
 14 A. Yes, I have.
 15 **Q. I'd like to draw your attention to CX 737.**
 16 **It's up on the screen as well.**
 17 **What is CX 737?**
 18 A. CX 737 is my rebuttal of the expert report.
 19 **Q. Now, Professor Hill, I'd like to direct you back**
 20 **to your expert report at CX 740, in particular**
 21 **paragraph 49.**
 22 JUDGE CHAPPELL: Before you do that, I want to
 23 mention something for the record because I saw a lot of
 24 blank faces on the left side of the room when you were
 25 trying to qualify your expert.

1 I'm going to accept someone as an expert unless
 2 there's an objection, but what I'm saying is that to the
 3 extent any opinions offered meet the proper legal
 4 standards, those opinions will be considered.
 5 Any questions on that?
 6 MR. SHERMAN: No questions, Your Honor.
 7 JUDGE CHAPPELL: Go ahead.
 8 BY MS. LASSACK:
 9 **Q. Professor Hill, will you read the last two**
 10 **sentences of that paragraph starting with "Record**
 11 **evidence."**
 12 A. "Record evidence shows that LabMD maintains
 13 personal information about more than 750,000 consumers.
 14 For purposes of this report, I have assumed that these
 15 types of information can be used to harm consumers,
 16 through identity theft, medical identity theft, and
 17 disclosing private information."
 18 **Q. Why did you make that assumption?**
 19 A. I made that assumption -- the assumption of harm
 20 was provided to me by complaint counsel.
 21 **Q. Professor Hill, before we discuss in detail how**
 22 **you reached your opinions, I'd like to ask you some**
 23 **background questions about networks and network**
 24 **security.**
 25 A. Okay.

89

1 **Q. What is a network?**
 2 A. A network is a composition of computers,
 3 servers, workstations that are connected via some type
 4 of communications channel.
 5 **Q. Professor Hill, will you turn to paragraph 17 of**
 6 **your expert report. And I'm also showing on the screen**
 7 **what's been marked as CXD 2.**
 8 **Professor Hill, what is CXD 2?**
 9 A. CXD 2 is an image that illustrates a very simple
 10 map.
 11 **Q. How does CXD 2 compare to figure 17 in your**
 12 **report?**
 13 A. It's the exact same figure.
 14 **Q. Will CXD 2 help you give background testimony**
 15 **about networks and network security?**
 16 A. Yes, it will.
 17 **Q. What is a local area network?**
 18 A. A local area network, if you look -- I'm sorry.
 19 I'm trying to get it on the -- it's kind of
 20 hard (indicating).
 21 But if you look in the square box, that
 22 illustrates a local area network. The computers on the
 23 network are connected to the network via a network
 24 interface card.
 25 **Q. What is a network interface card?**

90

1 A. A network interface card is an adapter that's
 2 placed in a computer to communicate on the computer's
 3 behalf, an example of which would be like an Ethernet
 4 card.
 5 And each card has a unique address called a MAC
 6 address, a medium access control address. And that
 7 address uniquely identifies that computer on the local
 8 area network.
 9 MS. LASSACK: Your Honor, may co-counsel
 10 approach Professor Hill with a laser pointer to use in
 11 connection with CXD 2?
 12 JUDGE CHAPPELL: You mean to hand it to her?
 13 MS. LASSACK: Yes.
 14 JUDGE CHAPPELL: Sure. I didn't want him to
 15 just blink it in her eyes or anything.
 16 MS. LASSACK: I'm sure she appreciates that.
 17 JUDGE CHAPPELL: Did you try this out?
 18 MS. LASSACK: We weren't able to try it out
 19 here beforehand with the laser pointer exactly,
 20 Your Honor.
 21 BY MS. LASSACK:
 22 **Q. Professor Hill, how is data transferred between**
 23 **computers with a local area network?**
 24 A. Data is transferred via the use of this
 25 switch (indicating). And a switch is a medium access

91

1 control device. The switch is the box here, this blue
 2 box. And the switch basically --
 3 JUDGE CHAPPELL: Does anyone see the laser
 4 pointer?
 5 UNIDENTIFIED SPEAKER: Yes.
 6 JUDGE CHAPPELL: It must be the angle here.
 7 MS. VANDRUFF: May I turn the monitor,
 8 Your Honor?
 9 JUDGE CHAPPELL: Try turning it toward the
 10 crowd.
 11 UNIDENTIFIED SPEAKER: It's green, not red. A
 12 red laser would be like normal.
 13 THE WITNESS: It's kind of hard because it's
 14 green.
 15 JUDGE CHAPPELL: Is it on the one at the right?
 16 MS. LASSACK: No. It's only on the one on the
 17 left.
 18 JUDGE CHAPPELL: If this is very important, she
 19 can step down and point to the exhibit, because the
 20 screen is being pointed toward the crowd. That's what
 21 it's for. I've got my own screen here.
 22 MS. LASSACK: And I think we can continue
 23 without the laser pointer.
 24 JUDGE CHAPPELL: All of that for nothing.
 25 THE WITNESS: Would you like for me to step

92

1 down?
 2 JUDGE CHAPPELL: It's her rodeo.
 3 MS. LASSACK: Your Honor, if it would be helpful
 4 to you, may the witness step down?
 5 JUDGE CHAPPELL: It's your show. I'm allowing
 6 her if you need her to. But we do need to turn that
 7 screen back towards the audience.
 8 THE WITNESS: So this is the local area network
 9 here that's enclosed in the box (indicating). And this
 10 device here, the blue box with the arrows on top, is a
 11 switch.
 12 And a switch is a medium access control device,
 13 and it works at that layer of the networking stack.
 14 And as data is forwarded to the switch, the switch will
 15 look at the data and it will look at the IP address,
 16 the Internet protocol address, that's contained within
 17 this device, and then it will ask the computers that
 18 are connected to this switch which computer has the
 19 MAC address that uniquely identifies that computer that
 20 corresponds to that particular IP address.
 21 So the switch is responsible for forwarding any
 22 data to the computers on this network based on the
 23 MAC address.
 24 And the MAC address for these computers that are
 25 on this local area network are not known outside of that

1 local area network, so it's only known within this
 2 network. And the switch uses the MAC address in order
 3 to forward data.

4 BY MS. LASSACK:

5 **Q. Thank you, Professor Hill. I think you can**
 6 **return to the witness stand now.**

7 **Once the data arrives at the destination**
 8 **computer, what happens?**

9 A. Once the data arrives at the destination
 10 computer, the destination computer uses what is known
 11 as a port number to forward the data to the
 12 corresponding application for which the data is
 13 destined.

14 **Q. What is an application?**

15 A. An application is a piece of software that is
 16 executed on a computer that is providing some function.

17 An example of an application would be a Web
 18 server, an e-mail client, an FTP server, file transfer
 19 protocol server. All of those are examples of
 20 applications.

21 **Q. Using the device you have at the witness stand,**
 22 **can you illustrate on CXD 2 an application?**

23 A. So as you see, there's an FTP box that has
 24 popped up on one of the monitors, and that illustrates
 25 an application.

1 **Q. Can you explain what an FTP application does?**

2 A. "FTP" stands for file transfer protocol, and it
 3 is an application. An FTP server basically manages the
 4 distribution of data. An FTP client can connect to the
 5 FTP server to either transfer data to the server or
 6 retrieve data from the server.

7 So an FTP, file transfer protocol, basically
 8 defines the process for transferring that data.

9 JUDGE CHAPPELL: Ma'am, earlier you were saying
 10 "MAC address." Is that M-A-C?

11 THE WITNESS: M-A-C.

12 JUDGE CHAPPELL: Does that stand for something?

13 THE WITNESS: Yes. Medium access control
 14 address.

15 JUDGE CHAPPELL: Thank you.

16 BY MS. LASSACK:

17 **Q. Professor Hill, you mentioned ports.**

18 A. Yeah.

19 **Q. What is a port?**

20 A. A port is basically a doorway into your
 21 network. The port maps to an application, and it
 22 provides access to your computing system.

23 The -- one main security goal is to close all
 24 unused ports within your system because an open port is
 25 just like an open door at your house. If you leave the

1 house, the door open, anyone can walk into your house.
 2 And the same thing, if there's an open port on a
 3 computer, then that presents an opportunity for someone
 4 outside of your network to gain access to your network.

5 **Q. How does a destination computer use the port**
 6 **number to send data to an application?**

7 A. The destination computer, once it receives the
 8 data, it extracts the port number from that data, and
 9 then it sends that data to the application that is
 10 listening on that particular port.

11 **Q. You mentioned the importance of closing unused**
 12 **ports.**

13 **How is a port closed?**

14 A. A port closed is closed by the use of a device
 15 or piece of software called a firewall.

16 **Q. What is a firewall?**

17 A. A firewall is a barrier protection mechanism,
 18 and it's a proactive security mechanism that allows you
 19 to limit access and restrict access of data into your
 20 network.

21 **Q. Professor Hill, what is the most effective way**
 22 **to provide reasonable security for a network?**

23 A. The most effective way to provide reasonable
 24 security for your network is to first identify the
 25 resources that need to be protected. And once you

1 identify the resources that need to be protected, you
 2 need to then specify the goals that you would like to
 3 have achieved with that protection.

4 The second step would be to define policies for
 5 satisfying those security goals.

6 The third step is to identify mechanisms for
 7 enforcing those goals. It's an overall -- it's a
 8 process of evaluating, you know, the things that need to
 9 be protected in your system.

10 And once the security mechanisms have been
 11 identified, the best strategy to use for deploying those
 12 mechanisms is defense in depth.

13 **Q. What is defense in depth?**

14 A. Defense in depth is a strategy by which
 15 mechanisms and policies, security mechanisms and
 16 security policies, are deployed in a layered fashion
 17 throughout your network. And --

18 **Q. Why are they deployed in a layered fashion?**

19 A. They are deployed in a layered fashion to
 20 reduce the probability that an attack will be
 21 successful.

22 **Q. Is defense in depth a common practice in the**
 23 **IT industry?**

24 A. Yes.

25 **Q. Please explain for the court how defense in**

97

1 **depth reduces the likelihood of an attack.**
 2 A. Defense in depth reduces the likelihood of an
 3 attack -- let's just assume that an attacker has a
 4 probability of -- a 50 percent chance of being
 5 successful in exploiting a vulnerability, and so at each
 6 layer of a mechanism -- at each layer of your system,
 7 the attacker has a 50 percent chance.
 8 So if, for an example, you know, let's just
 9 assume that we have a scenario where there is an
 10 unauthorized application downloading on one of the
 11 computers that's on your local area network, and so if
 12 I want to have -- an example of a possible defense in
 13 depth strategy would be one where I want to deploy
 14 mechanisms throughout in order to address that problem.
 15 **Q. Why is downloading an unauthorized application a**
 16 **risk?**
 17 A. Downloading an unauthorized application is a
 18 risk because it introduces a vulnerability in the
 19 network. That application could have a malicious
 20 software embedded within it. The individual downloading
 21 it may not understand the consequences of the download.
 22 It may not -- the individual may not also understand how
 23 the application works.
 24 So it just introduces a risk. If it's not
 25 needed for -- if there's no business need for the

98

1 application, then it introduces a risk.
 2 **Q. In the example you're describing,**
 3 **Professor Hill, will you use CXD 2 to describe the first**
 4 **step of defense in depth.**
 5 A. Okay.
 6 So with this example, I'm going to present some
 7 parts of what would be a defense in depth strategy to
 8 protect against an unauthorized download.
 9 So the first part that we see here is the
 10 firewall that is at -- that's right between the
 11 Internet cloud and the router. That router there is a
 12 gateway router. And routers are devices that are used
 13 to connect networks together.
 14 And so what a firewall does, it's a barrier
 15 protection mechanism, as I've previously stated, and it
 16 can be used to block traffic from entering the network.
 17 Traffic that is initiated outside of the network can be
 18 blocked by the firewall based on the Internet protocol
 19 address and port number, so you can use the firewall to
 20 block those ports.
 21 So in here I call that the Internet connection
 22 layer.
 23 **Q. Are there any other types of mechanisms that**
 24 **could be deployed at the Internet connection layer as**
 25 **part of a defense in depth strategy?**

99

1 A. Another type of mechanism would be an intrusion
 2 detection system.
 3 **Q. What is an intrusion detection system?**
 4 A. An intrusion detection system is like a sensor
 5 in your network, and its purpose is to detect malicious
 6 activity.
 7 **Q. Professor Hill, what is the next step in your**
 8 **example of a defense in depth strategy?**
 9 A. The next step would be to deploy security
 10 mechanisms at what I've designated as the workstation
 11 layer. And here, I'm designating the use of a --
 12 another firewall. And this would be a software firewall
 13 that would be executed on individual workstations and
 14 servers.
 15 **Q. How would you describe the workstation server**
 16 **layer?**
 17 A. Can you clarify?
 18 **Q. What types of devices are located at the**
 19 **workstation server layer?**
 20 A. Security devices?
 21 **Q. More computer hardware devices.**
 22 A. Oh, okay.
 23 At the workstation and server layer we
 24 basically have our computers. We have -- and these are
 25 workstations that are used by individual -- by

100

1 individuals within an organization.
 2 There are servers at the workstation and server
 3 layer, and they are used to run like your server
 4 applications, like e-mail servers, database servers,
 5 and those types of things. You can have laptops at this
 6 workstation and server layer.
 7 And so those are some of the different devices
 8 that are at the workstation and server layer.
 9 **Q. In the example you have up here at CXD 2, will**
 10 **you explain how the software firewall enhances the**
 11 **security with the hardware firewall at the router.**
 12 A. Okay. One thing that we should all know is
 13 that there's no such thing as perfect security,
 14 especially whenever there are humans involved in the
 15 configuration of the software. There can always be
 16 mistakes, and that's one of the reasons why we want to
 17 do defense in depth.
 18 So if there's been a misconfiguration, for
 19 example, of the firewall at the Internet connection
 20 layer, this mistake could hopefully be addressed by
 21 having a software firewall at the workstation layer.
 22 Another reason for having a firewall at the
 23 workstation layer is that there is some traffic that
 24 you want to allow into your network, but you don't
 25 want -- that traffic should be destined for a specific

101

1 machine, and maybe you want to have a simple
 2 coarse-grained firewall rule at the Internet connection
 3 layer, and you can have a more stringent fine-grained
 4 rule at the workstation layer, so this allows you to do
 5 that.
 6 **Q. Will you continue on in your example at
 7 CXD 2 and show the next step in the defense in depth
 8 strategy.**
 9 A. The next step in the defense in depth strategy
 10 is the user account layer.
 11 And so at the user account layer, what you want
 12 to deploy are mechanisms that can be used to
 13 authenticate a user, limit access to data and
 14 resources, and those can be done at the user account
 15 layer.
 16 And also you would want to limit the
 17 functionality that the user has within that particular
 18 workstation.
 19 **Q. What do you mean by "limit the functionality
 20 that the user has"?**
 21 A. So, for example, it's a common practice in the
 22 IT profession to not give regular users of a system
 23 administrative access to their computer.
 24 What administrative access does, it gives you
 25 full control over that machine. And one of the

102

1 functionalities that comes with administrative access is
 2 the ability to download software onto the computer.
 3 **Q. Professor Hill, does an appropriate defense in
 4 depth strategy take into account the size of a company's
 5 network?**
 6 A. Yes, it does.
 7 **Q. How does it do that?**
 8 A. It takes it -- it takes -- as I said before,
 9 the -- a defense in depth strategy -- and when you're
 10 defining a comprehensive information security plan,
 11 it's a process.
 12 It takes into consideration the size of the
 13 network by looking at the number of machines that the
 14 network may contain, the amount of data that would be
 15 flowing into the network, the amount of information
 16 that the system will maintain and store, so all of
 17 those things are taken into consideration because the
 18 larger the network, the -- probably the more costly the
 19 mechanisms that you would need to use to secure that
 20 network.
 21 **Q. Professor Hill, does an appropriate defense in
 22 depth strategy take into account the volume and
 23 sensitivity of the types of information stored on the
 24 network?**
 25 A. Yes.

103

1 Go ahead.
 2 **Q. How so?**
 3 A. If the -- if there are large amounts of
 4 information that's stored on the system, you need to
 5 think about how to limit an individual's access to that
 6 information. It is not a good practice to give an
 7 individual access to all information. And the reason
 8 for that is the insider threat.
 9 So you could have a malicious insider. If given
 10 access, full access to all information, then that one
 11 individual could expose all of that information.
 12 **Q. How does the sensitivity of the information
 13 affect an appropriate defense in depth strategy?**
 14 A. If the information is highly sensitive, then it
 15 is imperative that you protect that information.
 16 So you would need to think more about how do I
 17 protect that information when it's stored.
 18 If the information is being backed up and it's
 19 highly sensitive, and I'm not -- there is no need to
 20 access that information throughout the day, you may want
 21 to consider encrypting that backup.
 22 You would not want to store this information,
 23 this sensitive information, on an individual's
 24 multiple-use computer.
 25 So those are some of the things that you would

104

1 need to take into consideration when you have sensitive
 2 information.
 3 In addition, you want to think about how do I
 4 transmit this sensitive information in a secure manner.
 5 **Q. Professor Hill, do technical security measures
 6 alone provide reasonable security?**
 7 A. No, technical security measures alone do not
 8 provide reasonable security.
 9 You can attempt to just deploy mechanisms even
 10 in a layered fashion, but if you don't first understand
 11 the goals that are to be achieved, if you don't
 12 understand the policies that need to be specified and
 13 defined in order to satisfy those goals, then simply
 14 deploying mechanisms, even in a layered fashion, will
 15 not result in reasonable and appropriate security for
 16 your system.
 17 **Q. Professor Hill, I'd like to direct your
 18 attention to paragraph 31 of your expert report.
 19 Will you read the first sentence of that
 20 paragraph, please.**
 21 A. "There are seven principles that help to specify
 22 the policies and identify the mechanisms that are to be
 23 deployed at each layer of a defense in depth security
 24 strategy."
 25 **Q. Please explain to the court the first of those**

105

1 **seven principles.**
 2 A. The first of the seven principles is don't keep
 3 what you don't need.
 4 **Q. Why is that important?**
 5 A. That's important because if you keep
 6 information that is not required for your business
 7 practices, then that introduces an additional burden on
 8 the individual to secure that information, and it could
 9 also, if there is a compromise, increase the scope of
 10 harm.
 11 **Q. Please explain the second of the seven**
 12 **principles.**
 13 A. The second principle is to patch. And what
 14 that means is that software is -- will have
 15 vulnerabilities. Applications. Operating systems.
 16 Researchers have found that for every ten lines of
 17 computer code, there is on average one coding mistake or
 18 flaw.
 19 And so if we look at something like the
 20 operating system Windows 2003, that operating system
 21 has 50 million lines of code, and so you would expect
 22 on average there to be five million flaws, coding
 23 mistakes, in that operating system software. And so all
 24 of those mistakes will not be identified before that
 25 software is deployed, and so vendors, like Microsoft,

106

1 will issue updates and patches to coding mistakes that
 2 are found in their software.
 3 **Q. What is the third of the seven principles?**
 4 A. This third is ports.
 5 And so we've talked about ports and the fact
 6 that a port is an open door to your network, and so this
 7 principle is basically saying close all used and
 8 unneeded ports.
 9 **Q. All right. That was unused?**
 10 A. Unused.
 11 **Q. What's the next of the seven principles?**
 12 A. The next of the seven principles is policies.
 13 And the overall process for defining a
 14 comprehensive information security plan, you know, is
 15 composed of a step where you are to define the policies
 16 that will satisfy your security goal.
 17 So specifying policies is an important part of
 18 creating a comprehensive security plan.
 19 **Q. What is a comprehensive information security**
 20 **plan?**
 21 A. A comprehensive information security plan is
 22 one in which you have identified the sensitive
 23 resources that need to be protected, you've specified
 24 your goals, you have also defined policies for
 25 enforcing and satisfying those goals and you have

107

1 identified the mechanisms and the way they would be
 2 deployed.
 3 It also includes training of individuals who
 4 will be using the systems and the ones that will be
 5 maintaining and securing the system.
 6 **Q. Should a comprehensive information security**
 7 **program be in writing?**
 8 A. Yes, it should.
 9 **Q. Why is that?**
 10 A. It should be in writing for several reasons.
 11 One of the first is because it documents the
 12 current practices and it provides a guide for the IT
 13 professionals on how to secure the system.
 14 Another reason that it should be in writing is
 15 because it serves as a training tool also for
 16 individuals who are going to use the system and also
 17 maintain it.
 18 Another reason that it should be in writing is
 19 because oftentimes in an organization there's turnover,
 20 and so if there is little or no overlap with regards to
 21 the people who are managing the system, then that
 22 comprehensive -- that written comprehensive information
 23 security plan provides the guidance for the new IT
 24 professionals who are assuming the responsibility for
 25 maintaining and securing the network.

108

1 **Q. We'll be talking about a comprehensive**
 2 **information security plan shortly.**
 3 **I'd like to turn back to the next of the seven**
 4 **principles, which is protect.**
 5 **What does that mean?**
 6 A. "Protect" basically means that you should
 7 deploy mechanisms that will protect your system. And
 8 we've talked about some of those mechanisms, for
 9 example, a firewall, which is a proactive mechanism and
 10 because it proactively tries to prevent unauthorized
 11 traffic from entering the network.
 12 We also have reactive mechanisms, like antivirus
 13 software, that whose goal is to detect the presence of
 14 malicious software.
 15 And so protect is very important because it
 16 talks about the mechanisms that you are actually
 17 deploying in order to protect your system.
 18 **Q. What is the next of the seven principles?**
 19 A. The next of the seven principles is probe.
 20 And probe is all about assessing the risk and
 21 the vulnerabilities within your system and through
 22 things like penetration testing, reviewing of security
 23 logs, monitoring traffic that comes into your network,
 24 intrusion detection, those types of things.
 25 **Q. What is the last of the seven principles**

109

1 **identified in paragraph 31 of your report?**
 2 A. The last is physical.
 3 So with physical protection, you want to ensure
 4 that your computer infrastructure is physically
 5 protected. You have a server room and the server room
 6 is locked. Your computer rooms are locked and you limit
 7 the physical access to these resources.
 8 **Q. Does limiting the physical access to the**
 9 **resources prevent electronic attack?**
 10 A. No, it does not.
 11 **Q. Professor Hill, how did you identify the seven**
 12 **principles listed in paragraph 31 of your report?**
 13 A. These seven principles are known. And through
 14 my training and experience, that's how I've come to
 15 understand and know these seven principles.
 16 But these seven principles are also provided in
 17 guidelines that have been defined by various government,
 18 industry, and academic organizations for protecting and
 19 securing a network.
 20 **Q. I believe earlier you testified that there's no**
 21 **such thing as perfect security.**
 22 A. Yes.
 23 **Q. Why is that?**
 24 A. There's no such thing as perfect security
 25 because threats are always evolving. And as we define

110

1 mechanisms to protect or protect against or prevent or
 2 mitigate a risk, there's a new risk, and so it's an
 3 arms race. And even if I've addressed a particular
 4 risk and vulnerability, that vulnerability could evolve
 5 to evade the techniques that I'm using to mitigate that
 6 risk.
 7 **Q. If there's no such thing as perfect security,**
 8 **what is the result of an appropriate defense in depth**
 9 **strategy based on the seven principles?**
 10 A. The result is is that you want to limit the
 11 likelihood of an attack. And as I was previously
 12 stating, if an attacker has a 50 percent chance of
 13 attacking your system, if you have a layered approach of
 14 deploying your mechanisms, then in the example that I
 15 gave where we had three layers, you reduce your chance
 16 of success from one-half to one-eighth, given that
 17 particular example scenario.
 18 JUDGE CHAPPELL: You say there's no such thing
 19 as perfect security; is that correct?
 20 THE WITNESS: Yes, sir.
 21 JUDGE CHAPPELL: Isn't that also saying then
 22 that in every system there always is a likelihood of a
 23 problem?
 24 THE WITNESS: Yes, sir.
 25 And if I could respond --

111

1 JUDGE CHAPPELL: Go ahead.
 2 THE WITNESS: -- to that point.
 3 And that is why you would want to use a defense
 4 in depth and you want to use a set of heterogeneous
 5 mechanisms deployed throughout, because there's a
 6 chance of a vulnerability, there's a chance of human
 7 error.
 8 And so if, for example, one of those mechanisms
 9 are penetrated, the hope is by deploying multiple
 10 mechanisms throughout your network, you could reduce the
 11 overall likelihood.
 12 JUDGE CHAPPELL: But with all that, even a
 13 system you designed, if an employee managed to download
 14 LimeWire, you'd still have a problem.
 15 THE WITNESS: If an employee manages to
 16 download LimeWire, you would have a problem. But you
 17 would also have to go back and look at your policy
 18 regarding user accounts and whether employees need the
 19 ability -- need to be able to download software in order
 20 to do the work that they are required to do.
 21 MS. LASSACK: Do you have any additional
 22 questions, Your Honor?
 23 JUDGE CHAPPELL: No.
 24 BY MS. LASSACK:
 25 **Q. Professor Hill, I'd like to turn to the next**

112

1 **topic, which is LabMD's network.**
 2 **Please describe for the court LabMD's network**
 3 **during the relevant time period for your conclusions.**
 4 A. LabMD's network, I consider it to be a small
 5 network, maybe no more than 50 workstations on the
 6 network.
 7 There were I don't think no more than ten
 8 servers throughout the lifetime of the network during
 9 the relevant period, time period.
 10 There were laptops of the salespeople that
 11 weren't directly connected to the network but could
 12 connect remotely to the network.
 13 And another part about the network is that it
 14 did store large amounts of sensitive data.
 15 And another interesting part about LabMD's
 16 network is the manner in which data flowed into the
 17 network from the doctors' offices, and so doctors'
 18 offices were allowed to basically push data into LabMD's
 19 network.
 20 So what I mean by "push" is to write data into
 21 the network, and so that creates an interesting
 22 scenario and interesting in the fact that you have to
 23 be extremely careful when you allow an external entity
 24 write privileges within your network, especially an
 25 external entity for which you have no control over the

113

1 device from which the writing is occurring.
 2 **Q. I'd like to back up for a second.**
 3 **What does it mean to write to a network?**
 4 A. So what it means is, to write is to place files
 5 that are stored on your -- on the remote machine, to
 6 actually place those files within LabMD's network on one
 7 of their servers, so it means to basically change, make
 8 changes to the hard disks that are stored within LabMD's
 9 network.
 10 **Q. Will you explain how doctors' offices did that.**
 11 A. Doctors' offices did that in a couple of
 12 different ways. One was -- one way was through a Web
 13 portal application. They entered patient information
 14 manually and that data was saved on through -- saved on
 15 the LabMD machines via the Web application.
 16 Another way was through bulk file transfer of
 17 multiple patient files at a time. And if -- if the
 18 doctor's office had their own electronic health record
 19 system, those files would be taken from that doctor's
 20 office server, copied to the machine that LabMD had
 21 provided to the doctor's office, and then written to
 22 LabMD's server within LabMD's network. And this was
 23 done via an anonymous file transfer protocol.
 24 **Q. We'll talk about that in more detail later.**
 25 **What types of information did the doctors'**

114

1 **offices transmit to LabMD?**
 2 A. They transmitted things like the patient's name,
 3 the address, Social Security number, insurance
 4 information, the types of tests that were to be
 5 performed, and those are some of the -- date of birth.
 6 **Q. What happened when that information got to**
 7 **LabMD's network?**
 8 A. Once the -- the information was written into
 9 LabMD's mapper server, and then it was combined with
 10 information on their demographic server and stored for
 11 the use of their laboratory information system that --
 12 the physicians and the individuals who were responsible
 13 for evaluating tests actually used that information, and
 14 the information was also used for LabMD's billing
 15 system.
 16 **Q. What was LabMD's billing system called?**
 17 A. LabMD's billing system was called Lytec.
 18 **Q. What did the mapper server do?**
 19 A. The mapper server basically collected this
 20 information and maintained that information and then
 21 transferred that information to the different servers
 22 within LabMD's network.
 23 **Q. Professor Hill, I'd like to direct you to**
 24 **paragraph 38 of your report.**
 25 **Will you please read that aloud.**

115

1 A. "Physician clients typically retrieved the
 2 results of the services they ordered from LabMD through
 3 LabMD's Web portal. In doing so, they accessed personal
 4 information stored on LabMD's network."
 5 **Q. How did the physician clients do that?**
 6 A. Through their Web application.
 7 **Q. How did the Web application work?**
 8 A. Web applications, the way they work, typically
 9 there's a Web server that's responsible for managing and
 10 serving the data, and then there is a client application
 11 that enables a client to access that data.
 12 And so a client would initiate a request to the
 13 Web server in order to retrieve information.
 14 **Q. You mentioned LabMD employee computers earlier.**
 15 JUDGE CHAPPELL: Hold on a second.
 16 In your paragraph 38, you're saying they, I
 17 guess as the physicians, access personal information.
 18 Are you saying everyone's personal information
 19 or just that information which they had business to
 20 access regarding their own patients?
 21 THE WITNESS: Your Honor, I'm not exactly sure.
 22 I would think that they were accessing the patient
 23 information --
 24 JUDGE CHAPPELL: I don't want you to think. I
 25 want to know what you know based on your analysis.

116

1 THE WITNESS: Based on my analysis, I didn't
 2 have information to determine whether they were able to
 3 access other patient information that were not their
 4 patients. I didn't have that information, so I can't
 5 answer definitively whether they -- whether or not they
 6 had access to patients that were not their patients.
 7 JUDGE CHAPPELL: So that paragraph 38, you're
 8 not saying that's a bad thing necessarily.
 9 THE WITNESS: No, I'm not saying that's a bad
 10 thing. It's just a description of how they accessed the
 11 information remotely.
 12 JUDGE CHAPPELL: It could be a bad thing, but
 13 you don't know.
 14 THE WITNESS: It could be a bad thing, but I
 15 don't know.
 16 JUDGE CHAPPELL: Okay.
 17 MS. LASSACK: Did you have any additional
 18 questions, Your Honor?
 19 JUDGE CHAPPELL: No. I'll ask them if I have
 20 them. Go ahead.
 21 BY MS. LASSACK:
 22 **Q. Did LabMD employees use their computers to**
 23 **access personal information stored on LabMD's servers?**
 24 A. Yes.
 25 **Q. Did any LabMD employees access the LabMD network**

117

1 remotely?
 2 A. Yes.
 3 **Q. Was any personal information maintained on LabMD**
 4 **employee computers?**
 5 A. Yes.
 6 **Q. Can you give the court an example, please.**
 7 A. One example was the billings manager's
 8 computer. There was a specific backup policy which
 9 stated that there would be backups to the billings
 10 manager's computer of I think it was billings-related
 11 information, but it was -- that billings-related
 12 information was sensitive information.
 13 **Q. Professor Hill, I'd like to direct you to**
 14 **CX 6 page 10.**
 15 **What is CX 6 page 10?**
 16 A. CX 6 page 10 is a data backup policy.
 17 **Q. Is this the policy that you were referring to?**
 18 A. Yes.
 19 **Q. Did LabMD contend that this policy was in effect**
 20 **during the relevant time period?**
 21 A. Yes.
 22 **Q. Were these backups encrypted?**
 23 A. No.
 24 **Q. What is encryption?**
 25 A. Encryption is a process for taking plain text

118

1 data and making it unreadable by individuals who don't
 2 have access to the encryption key.
 3 **Q. What is an encryption key?**
 4 A. An encryption key is a numeric value that's used
 5 as a part of the algorithm to transform the data into
 6 something that is not humanly readable.
 7 **Q. Was any other data on LabMD's network**
 8 **encrypted?**
 9 A. No.
 10 **Q. Were there any applications installed on any**
 11 **LabMD computers that were not necessary for business**
 12 **purpose?**
 13 A. Yes.
 14 **Q. What are those?**
 15 A. One was the LimeWire file-sharing application.
 16 **Q. Where was that application installed?**
 17 A. On the billings manager's computer.
 18 **Q. When was that application installed on the**
 19 **billing manager's computer?**
 20 A. That application was installed at some time
 21 between 2005 and 2006.
 22 **Q. Can you explain what the LimeWire application**
 23 **does briefly?**
 24 A. The LimeWire application allows individuals who
 25 are part of the network and using the application to

119

1 search and retrieve files from individual machines and
 2 not from a central server.
 3 **Q. What are those applications called generally?**
 4 A. Peer-to-peer file-sharing applications.
 5 **Q. How does a peer-to-peer file-sharing application**
 6 **work to share files?**
 7 A. A request is actually made by one application
 8 to retrieve for a specific file, and that file is then
 9 returned by the owner of the file, so then there's a
 10 search -- there could be a search of a particular host
 11 for all files that are available for sharing on that
 12 particular file, and then the requester makes a request
 13 for that file if it sees something that it is interested
 14 in retrieving.
 15 **Q. What is a host?**
 16 A. A host is just a computer. And a host in a
 17 peer-to-peer file-sharing network is just a computer
 18 that's using the file-sharing application.
 19 **Q. How do users of a peer-to-peer file-sharing**
 20 **application make files available to share?**
 21 A. They make them available for sharing by
 22 designating them as sharing. But there's some -- there
 23 are opportunities for them to inadvertently share
 24 without them knowing.
 25 **Q. How does a user designate a file for sharing?**

120

1 A. They would actually have to select this file and
 2 say that it is to be shared.
 3 So the application provides mechanisms that will
 4 allow them to designate the file as a shared file.
 5 **Q. How long have peer-to-peer programs been**
 6 **available?**
 7 A. Peer-to-peer programs have been available since
 8 1999.
 9 **Q. How widely were they used?**
 10 A. They've been widely used since their
 11 introduction. One of the major reasons for this is
 12 that they were -- they made the sharing of music and
 13 video files readily available to peers on the network.
 14 **Q. Are there any types of risks associated with**
 15 **peer-to-peer file-sharing programs?**
 16 A. Yes. The one I've already mentioned is the
 17 inadvertent file sharing.
 18 Another is that if you download files from a
 19 peer-to-peer file-sharing network, you have no idea of
 20 whether malicious components are embedded within the
 21 file that you've downloaded. And research has shown
 22 that many of the files on peer-to-peer sharing networks
 23 actually have malicious components.
 24 **Q. Has anyone provided warnings about these risks?**
 25 A. Yes.

121

1 **Q. Who?**
 2 A. Security experts have been providing warnings
 3 about these as early as 2005.
 4 **Q. If a file is inadvertently shared using a**
 5 **peer-to-peer file-sharing program, how easy or difficult**
 6 **is it to get the file back?**
 7 A. Very difficult.
 8 **Q. Why?**
 9 A. One of the reasons why is that you may not know
 10 all of the nodes or computers on the file-sharing
 11 network that may have that file and are making it
 12 available for sharing, because there's no guarantee that
 13 a computer will actually be on at the time that you're
 14 trying to search and find all of the computers that
 15 actually contain that file.
 16 Another reason is that once you have digital
 17 content and it leaves your control, it's impossible to
 18 identify all the places that this file is now present,
 19 because a file can also be shared in a nonelectronic
 20 manner outside of the scope of the peer-to-peer
 21 file-sharing network.
 22 **Q. Professor Hill, I'd like to turn to paragraph 49**
 23 **of your report.**
 24 JUDGE CHAPPELL: Let me ask you a question about
 25 peer-to-peer.

122

1 What about, for example, you have Firefox
 2 browser and you see there's an update and you connect
 3 and get the download or the update. Isn't that similar
 4 to a peer-to-peer?
 5 THE WITNESS: That is -- you are not getting
 6 that update from a peer. You're getting that update
 7 from a trusted server.
 8 So with Firefox and other applications that you
 9 purchase from vendors where you're getting an update,
 10 that process of updating is typically authenticated, so
 11 you verify the identity of the server that you're
 12 retrieving the update from, and so there's this trusted
 13 relationship between your computer and the computer from
 14 which you are downloading that information.
 15 JUDGE CHAPPELL: But if someone had hacked onto
 16 that other computer, hacked into that system, you could
 17 still be exposed.
 18 THE WITNESS: If someone had hacked into the
 19 server that from which you're retrieving the update,
 20 there's a compromise there and you could -- you could be
 21 exposed. You could download then a compromised piece of
 22 software.
 23 JUDGE CHAPPELL: And as far as your definition
 24 of "peer-to-peer," is it always, for example, my
 25 computer at home to your computer at home, or does it

123

1 also encompass a system where there might be an
 2 intermediary server involved?
 3 THE WITNESS: In peer-to-peer, that was the
 4 value of peer-to-peer. You don't have to interact
 5 through an intermediate server. You could have direct
 6 interaction between two computers, so there's no need
 7 for the intermediate server.
 8 JUDGE CHAPPELL: So anything untoward or
 9 malicious would have to come from the other peer or
 10 computer.
 11 THE WITNESS: Yes, it's coming from the other
 12 peer computer.
 13 And you don't know anything about a peer
 14 computer. There's no authentication process. And it's
 15 like doing business with someone you don't know, and so
 16 there's no trust that has been established between the
 17 two peers, because you're separated by the Internet, and
 18 so there's really no way to establish trust.
 19 JUDGE CHAPPELL: Are we talking about digital
 20 trust?
 21 THE WITNESS: Yes, I'm talking about digital
 22 trust.
 23 JUDGE CHAPPELL: All right. Thank you.
 24 MS. LASSACK: And Your Honor, complaint
 25 counsel's expert, Dr. Clay Shields, will be here later

124

1 in the week to talk more about peer-to-peer software as
 2 well.
 3 BY MS. LASSACK:
 4 **Q. Professor Hill, I'd like to direct you to**
 5 **section 7 of your report which begins on paragraph 49.**
 6 **Now that you've provided the court the relevant**
 7 **background, I'd like to turn back to your overall**
 8 **conclusion that you've reached about the reasonableness**
 9 **of LabMD's data security.**
 10 **What did you conclude?**
 11 A. I concluded that LabMD did not provide
 12 reasonable and appropriate security for their systems
 13 and the data that they stored within their system.
 14 **Q. How much personal information did LabMD store on**
 15 **its system?**
 16 A. Approximately 750,000 consumer records.
 17 **Q. What types of information did that include?**
 18 A. That included the name of consumers, their
 19 Social Security number, credit card information, banking
 20 information, insurance information, types of tests that
 21 had been requested. That's some of the information that
 22 was stored.
 23 **Q. Could LabMD have corrected its security failures**
 24 **at relatively low cost?**
 25 A. Yes.

125

1 **Q. So in addition to asking you about your overall**
 2 **conclusions about LabMD's data security practices, did**
 3 **complaint counsel also ask you to provide opinions about**
 4 **specific data security practices at LabMD?**
 5 A. Yes.
 6 **Q. I'd like to ask you about some of those specific**
 7 **opinions now, actually all of them.**
 8 **So first, did complaint counsel ask you to**
 9 **provide an opinion on whether LabMD developed,**
 10 **implemented and maintained a comprehensive information**
 11 **security program?**
 12 A. Yes.
 13 **Q. What did you conclude?**
 14 A. I concluded that they did not develop and
 15 maintain a comprehensive information security program.
 16 **Q. And you testified earlier about what a**
 17 **comprehensive information security program is. Can you**
 18 **summarize that for the court again?**
 19 A. A comprehensive information security program is
 20 one that is developed by a process, and it's a
 21 balancing process of balancing what your security goals
 22 are with the types of information that you're trying to
 23 protect. And once you specify those goals, you then
 24 also define mechanisms that will satisfy -- define
 25 policies that will satisfy those goals and mechanisms to

126

1 enforce those goals.
 2 **Q. What are some examples of the types of goals a**
 3 **comprehensive information security program should**
 4 **address?**
 5 A. Some examples include confidentiality, integrity
 6 and availability.
 7 **Q. What is a confidentiality goal?**
 8 A. A confidentiality goal is a goal in which you
 9 ensure that there will be no unauthorized access to a
 10 sensitive resource, like a data resource.
 11 **Q. What is an integrity goal?**
 12 A. An integrity goal is one in which you ensure
 13 that if there is a change, an unauthorized change to the
 14 system or to data or to files stored within the system,
 15 that you will be able to detect that change.
 16 **Q. What is an availability goal?**
 17 A. An availability goal is one in which you ensure
 18 that your system and data are accessible when they are
 19 needed.
 20 **Q. Why did you conclude that LabMD did not have a**
 21 **comprehensive information security program?**
 22 A. I concluded that they did not have a
 23 comprehensive information security program because
 24 there was no evidence, first and foremost, that a
 25 process for developing one had been put in place.

127

1 There were no written security policies until 2010.
 2 Then the policies themselves were not sufficient in
 3 some areas. And then there were policies that were not
 4 enforced.
 5 **Q. Let's start with the issue of whether LabMD had**
 6 **written information security policies.**
 7 **How do you know that LabMD did not have**
 8 **information -- written information security policies**
 9 **until 2010?**
 10 A. This fact was provided in the record evidence.
 11 MS. LASSACK: Your Honor, I'd like to show the
 12 witness CXD 1, which Mr. Sheer showed during his opening
 13 today, but in poster form.
 14 JUDGE CHAPPELL: A demonstrative?
 15 MS. LASSACK: Yes.
 16 JUDGE CHAPPELL: Go ahead.
 17 MS. LASSACK: And can we show it on the screen
 18 as well.
 19 BY MS. LASSACK:
 20 **Q. Professor Hill, what is CXD 1?**
 21 A. CXD 1 is a LabMD IT employee timeline.
 22 **Q. Have you reviewed the testimony of the**
 23 **individuals listed in CXD 1?**
 24 A. Yes, I have.
 25 **Q. Did they testify about the dates when they were**

128

1 **employed at LabMD?**
 2 A. Yes.
 3 **Q. Does CXD 1 accurately reflect their testimony?**
 4 A. Yes, it does.
 5 **Q. What does CXD 1 show about the importance of**
 6 **having written information security policies?**
 7 A. What CXD 1 shows is that there's a lot of
 8 transition of the -- and turnover of the IT employees.
 9 Sometimes there's very little overlap in the previous
 10 IT employees and the ones that were -- that would
 11 assume those positions.
 12 And as I previously stated, that one of the
 13 reasons for providing written information security
 14 programs is so that they can be a guide when there is
 15 this turnover, and there's very little overlap between
 16 employees.
 17 MS. LASSACK: Your Honor, may the witness
 18 approach the exhibit and may I approach the witness to
 19 continue our testimony to --
 20 JUDGE CHAPPELL: Yes and yes.
 21 MS. LASSACK: Thank you.
 22 BY MS. LASSACK:
 23 **Q. Professor Hill, will you please indicate on**
 24 **CXD 1 when LabMD put its information security plans in**
 25 **writing.**

129

1 A. They put their plans in writing in 2010,
 2 so -- (indicating).
 3 **Q. Will you indicate that, please.**
 4 JUDGE CHAPPELL: Go ahead and deface that
 5 thing.
 6 She's reticent about marking up your document.
 7 (Pause in the proceedings.)
 8 MS. LASSACK: Thank you, Your Honor. May the
 9 witness return to the witness stand?
 10 JUDGE CHAPPELL: That's all?
 11 MS. LASSACK: For now.
 12 JUDGE CHAPPELL: Go ahead.
 13 BY MS. LASSACK:
 14 **Q. Professor Hill, did LabMD have an employee**
 15 **handbook in writing?**
 16 A. Yes.
 17 **Q. Why did you conclude that the employee handbook**
 18 **was not a comprehensive information security plan?**
 19 A. The employee handbook did not contain specific
 20 policies about protecting data resources and the
 21 infrastructure.
 22 **Q. Professor Hill, earlier you testified that there**
 23 **were other reasons why you concluded that LabMD's**
 24 **information security program was not sufficiently**
 25 **comprehensive other than not being in writing?**

130

1 A. Yes.
 2 **Q. Was one of those that some of its policies were**
 3 **not being enforced, E-N-F-O-R-C-E-D?**
 4 A. Yes.
 5 **Q. Can you give the court an example, please.**
 6 A. One example of the policies not being enforced
 7 was one that regarded the transmission of sensitive
 8 data electronically via e-mail, and it said that -- the
 9 policy stated that encryption tools would be used in
 10 order to transmit sensitive data via e-mail, but record
 11 evidence shows that data was transmitted via personal
 12 e-mail in an unencrypted form.
 13 **Q. I'd like to direct you to page 6 of CX 6, and it**
 14 **will be up on the screen as well.**
 15 **And in particular, the fourth policy down.**
 16 **What is that policy?**
 17 A. That's the e-mail security and encryption
 18 policy.
 19 **Q. What does that policy say should be done?**
 20 A. It says that corporate e-mail -- LabMD's
 21 corporate e-mail system has security settings, and it's
 22 recommended that information of a sensitive nature and
 23 containing sensitive data should not be sent via e-mail
 24 unless messages and attachments are encrypted.
 25 **Q. Did LabMD provide mechanisms to encrypt**

131

1 **messages?**
 2 A. No.
 3 **Q. You said that LabMD had no written information**
 4 **security policies until 2010; is that correct?**
 5 A. Yes.
 6 **Q. Can we show on the screen the first pages of**
 7 **CX 6 and CX 7.**
 8 **What are CX 6 and CX 7?**
 9 A. CX 6 and CX 7 are LabMD's Policy Manual.
 10 They're two different versions of the Policy Manual.
 11 **Q. Are these the policies that you were referring**
 12 **to that were in writing in 2010?**
 13 A. Yes.
 14 **Q. What did you conclude about whether these**
 15 **policies were sufficiently comprehensive?**
 16 A. I concluded that they were not sufficiently
 17 comprehensive.
 18 **Q. Why did you reach that conclusion?**
 19 A. I reached that conclusion because they were
 20 missing some key elements regarding specific policies.
 21 **Q. Can you give the court an example of one of**
 22 **those?**
 23 A. One of the most basic mechanisms that is to be
 24 used in a system is an authentication mechanism. The
 25 most commonly used authentication mechanism is the user

132

1 name and a password. The user name is your identity,
 2 and the password is your proof of the identity.
 3 So it's important to use strong passwords. And
 4 there's no information about strong password policies
 5 and the strength of passwords, the history, how often
 6 passwords should be changed, whether there's a duration
 7 in which you can reuse passwords. There's no
 8 information about the strength of passwords.
 9 **Q. Professor Hill, could LabMD have implemented a**
 10 **comprehensive information security program at relatively**
 11 **low cost?**
 12 A. Yes.
 13 **Q. How so?**
 14 A. They could have done this through consulting
 15 guidelines that were available regarding what are the
 16 best practices to secure a system.
 17 They could have done this by providing training
 18 to their employees on the consequences and the
 19 responsibilities of misconfigured systems and the
 20 consequences of the use of some of the antivirus
 21 software that -- for example, antivirus software that
 22 they're responsible for using, and the training of IT
 23 professionals on evolving threats and the best ways of
 24 mitigating risk.
 25 **Q. You mentioned available guidance.**

1 **What are some examples of organizations that**
 2 **provide such guidance?**
 3 A. Some organizations that provided such guidance
 4 include the National Research Council. They provided
 5 an actual book, and in one chapter of the book they
 6 focus specifically on security mechanisms for
 7 protecting an infrastructure that contains medical
 8 information.
 9 **Q. What is the National Research Council?**
 10 A. The National Research Council is an
 11 organization that seeks the guidance of researchers in
 12 the field in order to define and specify guidelines.
 13 **Q. When you say "researchers in the field," what**
 14 **field are you referring to?**
 15 A. For this, for the purposes of this, I'm
 16 referring to like IT-related individuals.
 17 **Q. Are there other examples of organizations that**
 18 **provide guidance for creating a comprehensive**
 19 **information security program?**
 20 A. The National Institute of Standards, NIST,
 21 provided guidelines. I've actually cited some of their
 22 guidelines on risk assessment, and so they provide a
 23 comprehensive plan for risk assessment.
 24 **Q. What is the full name of NIST?**
 25 A. The National Institute for Standards.

1 Technology.
 2 **Q. How would IT professionals know about**
 3 **organizations like NIST and their resources?**
 4 A. Organizations would know about NIST and their
 5 practices and some of these other related organizations
 6 through training.
 7 **Q. What types of topics are covered in guidance**
 8 **provided by organizations like NIST and NRC?**
 9 A. The types of guidance that's provided by these
 10 organizations in their guidelines are the same types of
 11 guidelines that I presented in the background section
 12 for a comprehensive information security program.
 13 **Q. Can you remind us what those are?**
 14 A. Okay.
 15 So they include things like don't keep what you
 16 don't need, patching your and updating your system,
 17 closing all unused ports, you know, providing physical
 18 security, specifying policies, you know, being able to
 19 probe your network for risk assessment, those types of
 20 policies, protecting your network, you know, which
 21 mechanisms are best suited to address a particular
 22 security goal. Those are the types of things that they
 23 provide guidelines and guidance on.
 24 **Q. How could LabMD have used these types of**
 25 **guidelines to create a comprehensive information**

1 **Q. What does the "T" stand for?**
 2 A. I'm trying to remember what the "T" stands for.
 3 **Q. Is there a document that would refresh your**
 4 **memory?**
 5 A. Yes, there is.
 6 JUDGE CHAPPELL: Is it "Technology"?
 7 BY MS. LASSACK:
 8 **Q. Professor Hill, Your Honor asked if it's**
 9 **"Technology."**
 10 **Is it "Technology"?**
 11 A. It probably is "Technology." Thank you,
 12 Your Honor.
 13 JUDGE CHAPPELL: And is the "S" "Science"?
 14 BY MS. LASSACK:
 15 **Q. Is the "S" "Science"?**
 16 A. I don't recall.
 17 JUDGE CHAPPELL: I'm guessing. I don't know.
 18 THE WITNESS: Yeah. Actually, the "S" is
 19 "Standards."
 20 BY MS. LASSACK:
 21 **Q. I believe you testified it's "Standards."**
 22 A. Yes.
 23 **Q. So then what is the full name of NIST for the**
 24 **record?**
 25 A. The National Institute for Standards and

1 **security program at relatively low cost?**
 2 A. They could have -- given their specific goals
 3 and the types of information that they needed to
 4 protect, they could have looked at the guidelines for
 5 specific confidentiality goals and the types of
 6 mechanisms that those guidelines recommend.
 7 And so what those guidelines do, they provide
 8 like a general and overall guidelines for like all
 9 types of computing infrastructure. But if you have
 10 additional things that differ, you are going to have to
 11 evaluate that in a more process or in an approach and
 12 really look at your structure to understand what in
 13 addition to those guidelines you need to do.
 14 **Q. How much would it cost to implement that**
 15 **process-based approach?**
 16 A. That process-based approach for a trained IT
 17 person, that -- that takes people time in order to just
 18 go through the process in evaluating the system and the
 19 infrastructure.
 20 **Q. So it's just a time cost then, not monetary?**
 21 A. It's a time cost.
 22 **Q. Professor Hill, I'd like to turn to the section**
 23 **of your report that begins with paragraph 63.**
 24 **Did complaint counsel ask you to provide an**
 25 **opinion on whether LabMD used an appropriate set of**

137

1 **readily available risk assessment measures?**
 2 A. Yes.
 3 **Q. What did you conclude?**
 4 A. I concluded that LabMD did not provide a
 5 reasonable set of readily available measures for risk
 6 assessment.
 7 **Q. What does risk assessment involve?**
 8 A. Risk assessment involves evaluating your
 9 network to determine the risks that are current in your
 10 network.
 11 **Q. Why is risk assessment important?**
 12 A. Risk assessment is important because security
 13 can only be considered within the context of what is
 14 actually happening right now, and so you -- and threats
 15 are always evolving, and so that context changes. And
 16 because that context changes, you need to do a risk
 17 assessment periodically in order to assess the overall
 18 vulnerability and the risk within your system.
 19 **Q. How does risk assessment fit into an appropriate**
 20 **defense in depth strategy?**
 21 A. Risk assessment is very -- it's very important.
 22 It's a part of the -- it's the probe part of your seven
 23 principles.
 24 **Q. How does risk assessment relate to the selection**
 25 **of security measures?**

138

1 A. Risk assessment -- so all security measures are
 2 not going to just be to protect. There are going to be
 3 security measures that are going to be about assessing
 4 the network.
 5 So you need risk assessment tools, and they
 6 become mechanisms in an overall security program. But
 7 once I've actually used those risk assessment
 8 mechanisms, they can help me to identify the
 9 vulnerabilities that are present and whether I need to
 10 reconfigure my current security mechanisms that I have
 11 and am using or I need to get additional mechanisms to
 12 protect against an emerging or a new threat.
 13 **Q. What are some examples of the types of**
 14 **mechanisms that IT professionals use to assess risk?**
 15 A. So one example would be a penetration test.
 16 And you have a tool called NMAP that is widely
 17 used for penetration testing, and that's just to probe
 18 your network to see if there are open ports.
 19 You have things like Nessus that allows you to,
 20 once you probe the network, to understand whether your
 21 operating system needs to be updated.
 22 So you have various types of techniques, I mean,
 23 tools in order to do that.
 24 You have things like Wireshark that will allow
 25 you to capture data and do some analysis of that data to

139

1 understand what data is entering and leaving your
 2 network.
 3 **Q. Can you describe for the court how a penetration**
 4 **test works?**
 5 A. One example of a penetration test, I go back to
 6 NMAP.
 7 And so with NMAP what I can do is, given the IP
 8 addresses on your network, I can try to initiate a
 9 connection to those IP addresses giving various --
 10 varying port numbers for -- and that type of assessment
 11 is called like a port scan.
 12 And so my goal when doing this penetration test
 13 is to scan all the ports that are -- that could possibly
 14 be open. And there are 216 different ports. That's over
 15 65,000 ports that could be open.
 16 And so a penetration test, one example is a port
 17 scan. I just go through the IP addresses on your
 18 network and try to find an opening.
 19 **Q. You mentioned NMAP. What is that?**
 20 A. NMAP is a freely available tool that does a
 21 variety of different penetration testing, and a port
 22 scan is just one of those.
 23 **Q. What are some other examples?**
 24 A. Other examples of penetration tests that can be
 25 done with NMAP or other examples of different types of

140

1 tools that can be used for risk assessment?
 2 **Q. Other examples of different types of penetration**
 3 **testing that can be done.**
 4 A. Okay.
 5 So one thing that NMAP allows you to do is to
 6 determine information about the level of the operating
 7 system that you're running, and so that becomes
 8 important because if the operating system contains
 9 vulnerabilities, an attacker would want to know that, so
 10 an unpatched operating system that contains
 11 vulnerabilities can be exploited by an attacker.
 12 And so discovering the level of the operating
 13 system is -- is going beyond just a port scan but trying
 14 to determine, you know, whether you're running a patched
 15 or an unpatched operating system or any other
 16 applications that communicate via the network, whether
 17 they are -- also have vulnerabilities in them.
 18 **Q. How do IT professionals decide which risk**
 19 **assessment mechanisms to use?**
 20 A. The way IT professionals decide about that, it
 21 is part of this whole process-driven approach.
 22 So if I have servers within my organization
 23 that need to communicate with the outside world and
 24 there are going to be connections that initiate it, I
 25 would want to use a penetration test to determine

141

1 whether I -- my firewall is configured properly, where
 2 I'm not just allowing those ports to be open for those
 3 servers, but you know, I would close unused ports.
 4 **Q. Can one type of risk assessment mechanism alone**
 5 **be enough to be sufficient to assess risk?**
 6 A. No.
 7 **Q. Why not?**
 8 A. Because, for example, penetration testing allows
 9 me to determine whether ports are open. Penetration
 10 testing doesn't tell me anything about the data that may
 11 be entering or leaving my network.
 12 So if I have sensitive data and I want to
 13 ensure or assess whether that sensitive data is leaving
 14 my network, I would need to actually do what we call
 15 deep packet analysis. I need to go beyond the headers,
 16 and a penetration test only looks at the header
 17 information, like IP addresses and ports. I would have
 18 to go beyond that layer within my data and look at the
 19 data itself, and so you need a tool like Wireshark in
 20 order to do that.
 21 **Q. What is Wireshark?**
 22 A. Wireshark is a data traffic monitoring tool
 23 that will capture data on your network and allow you to
 24 look at that data snapshot.
 25 So when you see data going across the network,

142

1 it's in hexadecimal form, and so you need that
 2 translation of that data into a human-readable form.
 3 **Q. I'm not even sure I can say that word again.**
 4 **What is hex- -- is it hexadecimal form?**
 5 A. Yes.
 6 **Q. Is that what you said?**
 7 A. Yes, hexadecimal.
 8 **Q. Can you explain briefly?**
 9 A. There are different -- hexadecimal form
 10 basically represents the data in -- like with 16 --
 11 first it covers like 16 bits of information.
 12 So the format is not like, you know, just our,
 13 you know, our regular alphabet, so you're not going to
 14 see -- when you're looking at data as it's being
 15 transmitted, you're not going to see A, B, C, D. You're
 16 not going to see our regular alphabet. What you're
 17 going to see are numbers and characters from zero,
 18 you know, to FFF, so -- and that's the representation
 19 of, you know, information in hexadecimal.
 20 **Q. Okay. So to come back from there to the higher**
 21 **level of risk assessment, are you saying that one type**
 22 **of risk assessment can only address one type of risk?**
 23 JUDGE CHAPPELL: Hold on.
 24 Is there an objection?
 25 MR. SHERMAN: No, sir. That's a plea for a

143

1 break.
 2 JUDGE CHAPPELL: How much time do you need to
 3 finish the witness?
 4 MS. LASSACK: I think -- I would think at least
 5 a couple more hours, Your Honor.
 6 JUDGE CHAPPELL: So there is hope that you'll
 7 finish today.
 8 MS. LASSACK: I think there's at least hope
 9 that I'll finish today. It will be today or early
 10 tomorrow.
 11 JUDGE CHAPPELL: Okay.
 12 At this time we'll take our afternoon break. We
 13 will reconvene at 3:45.
 14 We're in recess.
 15 (Recess)
 16 JUDGE CHAPPELL: Back on the record.
 17 Go ahead.
 18 MS. LASSACK: Your Honor, there was a pending
 19 question before we took a break. May I restate it?
 20 JUDGE CHAPPELL: Would you like her to read the
 21 question?
 22 MS. LASSACK: Sure.
 23 (The record was read as follows:)
 24 "QUESTION: So to come back from there to the
 25 higher level of risk assessment, are you saying that one

144

1 type of risk assessment can only address one type of
 2 risk?"
 3 THE WITNESS: Yes.
 4 BY MS. LASSACK:
 5 **Q. Professor Hill, what types of measures did LabMD**
 6 **use to assess risk on its network?**
 7 A. LabMD used logs from their firewalls. They used
 8 antivirus software. And in 2010, they did a penetration
 9 test.
 10 **Q. Why did you conclude that LabMD did not use an**
 11 **appropriate set of risk assessment measures?**
 12 A. First, the logs from the firewalls were very
 13 limited. And there's no evidence in the record of the
 14 actual log from the firewall. There's just a discussion
 15 in the transcripts that discusses reviewing the logs
 16 from the firewall. But the firewall logs are very
 17 limited. They could only collect a few days of data
 18 that had been transmitted into the network.
 19 And with regards to the antivirus software, an
 20 antivirus application can only identify malicious
 21 software that it knows about, and so -- and its purpose
 22 is to detect the presence of malicious -- known
 23 malicious software, so it has a limited functionality
 24 when you begin to look at the full scope of risk
 25 assessment.

145

1 And...

2 **Q. Are there any other reasons why you concluded**

3 **that LabMD's antivirus software was not a sufficient**

4 **risk assessment mechanism?**

5 A. There were times that some of the antivirus

6 software could not be updated and could not be run, and

7 so there was then no -- those machines who were --

8 those machines that were running that particular

9 antivirus software, no detection of viruses could occur

10 on those machines because those machines were not able

11 to update their virus signatures and actually run the

12 antivirus software.

13 So that's one reason why I say that their use of

14 antivirus software was not sufficient.

15 **Q. Professor Hill, I'd like to draw your attention**

16 **to CX 35 and page 2 in particular.**

17 **What is CX 35?**

18 A. CX 35 is an APT service invoice.

19 **Q. We talked earlier about APT.**

20 **What type of work did APT do for LabMD?**

21 A. APT deployed some firewalls. They also helped

22 with problems that were reported to them.

23 For example, in this particular case, they were

24 looking at, you know, the anti- -- a particular server

25 at LabMD and the inability to run the antivirus

146

1 software and the fact that the software hadn't been

2 updated, the virus definitions hadn't been updated

3 since 2005. And this particular service invoice is

4 dated 2006.

5 **Q. Okay. Professor Hill, are you referring to the**

6 **first entry on page 2 of CX 35?**

7 A. Yes, I am.

8 **Q. Will you read that entry aloud for the court,**

9 **please.**

10 A. "Ran a complete virus scan on the server and

11 found no issues after it had completed. The LabMD

12 server however does still have an issue. It will not

13 run a virus scan, nor will it go out and get updates for

14 the virus definitions. It has not updated since July of

15 2005. Tried to run an online virus scanner, but since

16 the server did not have Java and would not install it, I

17 was not even able to do that. Suggested that we need to

18 totally wipe and reload that server."

19 **Q. What is the date of the entry you just read?**

20 A. The date of the entry is May 3, 2006.

21 **Q. Did you consider this entry when forming your**

22 **opinion about the effectiveness of LabMD's antivirus**

23 **applications?**

24 A. Yes.

25 **Q. What did you conclude from that entry?**

147

1 A. I concluded that their use was not -- their use

2 of antivirus software was not sufficient in order to

3 protect critical servers within their infrastructure.

4 **Q. Why did this entry support that conclusion?**

5 A. Because the virus definitions had not been

6 updated since July 2005, and this particular work order

7 was for the day of May 3, 2006, and so that's

8 approximately a year without new virus definitions.

9 And as I previously stated, antivirus software can only

10 detect malware that for which it has a data signature.

11 And a signature is, just think of it as the

12 signature that we sign. And our signature is usually

13 unique to us, and so a virus signature is unique to that

14 specific virus.

15 So if the antivirus software can't update

16 itself to get new signatures, then it cannot detect the

17 new and emerging viruses that may be present on a

18 system.

19 **Q. Professor Hill, I'd like to turn your attention**

20 **to page 3 of CX 35, particularly the entry dated**

21 **June 21, 2006.**

22 **What does that entry say?**

23 A. It says, "Did check on all of the servers. Each

24 server was not updating antivirus definitions since

25 May '06. Tried to run a manual update of the

148

1 definitions, but on every server it would start the live

2 update process and then lock the program up. Suggested

3 they upgrade their antivirus since they are running

4 Symantec Corporate 7 which is not supported by

5 Symantec."

6 **Q. Did you review this entry in connection with**

7 **reaching your conclusions about LabMD's antivirus**

8 **applications?**

9 A. Yes.

10 **Q. What did you conclude from this entry?**

11 A. I concluded that they were not running antivirus

12 software that would protect their servers.

13 **Q. Professor Hill, we've discussed antivirus**

14 **software for LabMD's servers.**

15 **Did you reach any conclusions about LabMD's**

16 **antivirus software for individual employee**

17 **workstations?**

18 A. Yes. The -- for some point in time during the

19 relevant time period, the antivirus software on

20 individual employees' computers were run and -- but the

21 logs from those were not reviewed until there was a

22 problem with the machine, a noticeable problem, so maybe

23 there's a slowdown that prevented the employee from

24 performing his or her duties.

25 So at that point the employee would report to

149

1 the IT staff that I'm having problems with my computer,
 2 and at that point in time is when those logs would be --
 3 antivirus scanning logs would be reviewed.
 4 And so this is a very reactive kind of approach,
 5 and it occurred -- to securing a system or assessing the
 6 risk in a system. And it often occurred in an ad hoc
 7 manner, so there wasn't scheduled, you know, reviews of
 8 these logs for some period of time during the relevant
 9 time period.
 10 **Q. You mentioned earlier why LabMD's firewalls were**
 11 **not sufficient risk assessment tools.**
 12 **Why was that?**
 13 A. Because the main purpose of a firewall is to
 14 block unnecessary and unwanted traffic and unauthorized
 15 traffic from entering the network, and so unless it's a
 16 firewall that also has some intrusion detection
 17 functionality, it's not going to have the ability to
 18 capture large amounts of traffic in order to do some
 19 analysis on that traffic and alert IT staff of,
 20 you know, possible threats and suspicious activity
 21 within the network, and so their firewalls only had the
 22 capability of capturing a limited amount of traffic.
 23 **Q. Did LabMD's firewalls have intrusion detection**
 24 **functionality?**
 25 A. LabMD's -- one question. Which firewall are you

150

1 referring to?
 2 **Q. I'm referring to LabMD's gateway firewalls.**
 3 A. Okay. LabMD's gateway firewall, as I recall, it
 4 had intrusion detection capability, but it was not
 5 enabled.
 6 **Q. Do you recall if that's true for whether all**
 7 **LabMD gateway firewalls had that capability?**
 8 A. There was -- as I recall, there was one gateway
 9 firewall, and then the other firewalls were internal
 10 firewalls, and I don't recall them having that
 11 capability.
 12 **Q. Was any intrusion detection capability in**
 13 **operation on any LabMD firewalls during the relevant**
 14 **time period for your conclusions?**
 15 A. No.
 16 **Q. Did APT monitor LabMD firewalls in a proactive**
 17 **way?**
 18 A. No.
 19 **Q. Why do you conclude that?**
 20 A. Because there's evidence of APT only providing
 21 service in response to a request, and also there's
 22 testimony from APT -- an APT representative which said
 23 that it provided service in an ad hoc manner as a
 24 reaction to there being problems within the network.
 25 **Q. Professor Hill, I'd like to direct your**

151

1 **attention to CX 731.**
 2 **What is CX 731?**
 3 A. CX 731 is the deposition transcript of
 4 Allen Truett.
 5 **Q. Who an Allen Truett?**
 6 A. Allen Truett was the owner of APT.
 7 **Q. Is he the representative you were referring to**
 8 **earlier?**
 9 A. Yes.
 10 **Q. I'd like to direct your attention to page 69 of**
 11 **Mr. Truett's deposition transcript.**
 12 **Lines 1 through 16 in particular.**
 13 **Is this the testimony that you were referring to**
 14 **earlier?**
 15 A. Yes.
 16 **Q. What did you conclude from this testimony?**
 17 A. That APT did not do any active monitoring of
 18 LabMD's firewalls.
 19 **Q. Did LabMD conduct manual inspections?**
 20 A. Yes.
 21 **Q. What did you conclude about LabMD's manual**
 22 **inspections as effective risk assessment mechanisms?**
 23 A. I concluded that LabMD's manual inspections were
 24 not effective.
 25 **Q. Why did you conclude that?**

152

1 A. I concluded that for two main reasons.
 2 The manual inspections were performed in an
 3 ad hoc manner for some period during the relevant time
 4 period, meaning that it was usually in response to an
 5 employee noting a problem was occurring with their
 6 machines.
 7 And another reason that I concluded that the
 8 manual inspections were not effective was because it's
 9 virtually impossible for a human to inspect every
 10 aspect of a computer and determine that there has been
 11 a change in integrity of the system, basically that
 12 there's been a change that would compromise the
 13 security of a system.
 14 So a computer may have over a thousand files.
 15 There are configurations that are in multiple places,
 16 configuration of shared folders and other types, the
 17 configuration of the firewall, so there are many aspects
 18 of the computer that would need to be inspected,
 19 including antivirus logs, any logs that the operating
 20 system may generate.
 21 So there's so many places that you would have to
 22 look in order to do an assessment of the system,
 23 there's -- it's virtually impossible for it to be
 24 effective as a risk assessment tool.
 25 **Q. Earlier you talked about LimeWire being**

153

1 **installed on the billing manager's computer.**
 2 **Did LabMD's manual inspections detect LimeWire**
 3 **on the billing manager's computer?**
 4 A. No, it did not.
 5 MS. LASSACK: May I ask the witness -- may the
 6 witness approach CXD 1 again?
 7 JUDGE CHAPPELL: Go ahead.
 8 BY MS. LASSACK:
 9 **Q. Professor Hill, will you note on CXD 1 when**
 10 **LimeWire was installed on the billing manager's computer.**
 11 A. Okay. LimeWire was installed on the billings
 12 manager's computer between 2005 and 2006 (indicating).
 13 **Q. Will you note when LimeWire was removed from the**
 14 **billing manager's computer.**
 15 A. LimeWire was removed from the billings manager's
 16 computer in 2008.
 17 **Q. When was that in 2008?**
 18 A. May of 2008.
 19 **Q. Will you note that, please, on CXD 1.**
 20 A. (Witness complies.)
 21 MS. LASSACK: May the witness return to the
 22 witness stand?
 23 JUDGE CHAPPELL: Sure.
 24 BY MS. LASSACK:
 25 **Q. Professor Hill, how long then was LimeWire**

154

1 **installed on the billing manager's computer without**
 2 **being detected by LabMD's manual inspections?**
 3 A. From two to three years.
 4 **Q. Earlier you testified that LabMD's manual**
 5 **inspections were conducted in an ad hoc way; is that**
 6 **correct?**
 7 A. Yes.
 8 **Q. What did you base that conclusion on?**
 9 A. I based that conclusion on testimonies that were
 10 provided through the deposition.
 11 **Q. I'd like to draw your attention to CX 734.**
 12 **Professor Hill, what is CX 734?**
 13 A. It is the deposition transcript of
 14 Alison Simmons.
 15 **Q. Did you review Ms. Simmons' testimony in**
 16 **connection with reaching your conclusion about LabMD's**
 17 **manual inspections?**
 18 A. Yes, I did.
 19 MR. SHERMAN: Your Honor, if I could object, I
 20 don't think this is a deposition transcript. It's a CID
 21 hearing transcript.
 22 JUDGE CHAPPELL: You need to stand up to
 23 object.
 24 MR. SHERMAN: I'm sorry, Your Honor.
 25 Yes, I believe this is a CID hearing

155

1 transcript, and I would just like that corrected for
 2 the record.
 3 MS. LASSACK: That is correct, Your Honor. We
 4 will note for the record that that is -- CX 734 is
 5 Alison Simmons' investigational hearing transcript.
 6 JUDGE CHAPPELL: You're questioning the
 7 witness. Why don't you let the witness handle that.
 8 MS. LASSACK: Okay. I apologize.
 9 JUDGE CHAPPELL: Did the witness give you the
 10 wrong answer?
 11 MS. LASSACK: I believe so, Your Honor.
 12 JUDGE CHAPPELL: Then why don't you have her
 13 correct it.
 14 MS. LASSACK: Okay.
 15 BY MS. LASSACK:
 16 **Q. Professor Hill, what is CX 734?**
 17 A. CX 734 is Alison Simmons' investigational
 18 hearing testimony.
 19 **Q. Did you consider CX 734 in connection with**
 20 **forming your conclusions about LabMD's manual**
 21 **inspections?**
 22 A. Yes, I did.
 23 **Q. I'd like to draw your attention to**
 24 **pages 78 through 80 of Ms. Simmons' investigational**
 25 **hearing transcript.**

156

1 **What did you conclude from this testimony?**
 2 A. I concluded that the manual inspections were
 3 performed in an ad hoc manner.
 4 **Q. I'd now like to direct your attention to**
 5 **page 14 lines 8 through 12 of Ms. Simmons'**
 6 **investigational hearing transcript.**
 7 **What did Ms. Simmons testify about when she**
 8 **worked at LabMD?**
 9 A. She testified that her starting date was late
 10 August 2006 -- October 2006 and through August 2009.
 11 **Q. So is it correct that she testified that she was**
 12 **at LabMD from October 2006 through August 2009?**
 13 A. Yes.
 14 **Q. Professor Hill, you testified that manual**
 15 **inspections are not a sufficient risk assessment tool.**
 16 **Before May 2010, did LabMD use any automated**
 17 **risk assessment measures?**
 18 A. No.
 19 **Q. Would that be other than antivirus software?**
 20 A. Other than antivirus software, that was the only
 21 one that was an actual electronic.
 22 **Q. So I can clarify the record then, your testimony**
 23 **is that Lab- -- other than antivirus software, LabMD did**
 24 **not use any automated risk assessment mechanisms prior**
 25 **to May 2010.**

157

1 A. Yes, that's true.
 2 **Q. And Professor Hill, you testified that LabMD**
 3 **first conducted penetration testing in May 2010; is that**
 4 **correct?**
 5 A. Yes.
 6 **Q. What types of risks did LabMD's**
 7 **May 2010 penetration testing identify?**
 8 A. The -- one of the risks that was identified was
 9 that of the anonymous FTP server.
 10 **Q. Professor Hill, I'd like to direct your**
 11 **attention to CX 70.**
 12 JUDGE CHAPPELL: I want to point out something
 13 for the record here because of things I've seen in
 14 posttrial briefing in the past.
 15 This is an expert witness, and a lot of these
 16 questions are very factual based, for example, when
 17 LabMD first conducted penetration testing. And as I
 18 understand it, this is based on -- this is her opinion
 19 based on what she's read in the record. She doesn't
 20 know for a fact when it began. Am I correct?
 21 MS. LASSACK: You are correct, Your Honor. It's
 22 her conclusions based on the record.
 23 JUDGE CHAPPELL: Right. I just want to make
 24 that clear. I have seen, for example, that question and
 25 answer type cited in a brief for a factual assertion.

158

1 I'm just letting everyone know that that's not correct
 2 to do that.
 3 BY MS. LASSACK:
 4 **Q. Professor Hill, I'd like to direct your**
 5 **attention to CX 70.**
 6 **What is CX 70?**
 7 A. CX 70 is the ProviDyn report.
 8 **Q. What is the ProviDyn report?**
 9 A. The ProviDyn report is the report that was
 10 generated by the company ProviDyn, and it was --
 11 ProviDyn had been engaged by LabMD to perform an
 12 external vulnerability scan of LabMD's network.
 13 **Q. What is an external vulnerability scan?**
 14 A. So an external vulnerability scan is one -- is a
 15 risk assessment scan. I say "external" because it's
 16 performed from outside of an organization's network, and
 17 it uses various risk assessment techniques like
 18 penetration testing and, in addition to penetration
 19 testing, looking for vulnerabilities in the software
 20 that is run on specific machines for which it is
 21 probing.
 22 **Q. On page 1 of CX 70, what is shown about the**
 23 **overall security posture in connection with the external**
 24 **vulnerability scan conducted?**
 25 A. That the overall security posture was poor.

159

1 **Q. What does that mean?**
 2 A. That means that the system is not secure and
 3 it's vulnerable to risks that would actually compromise
 4 the system, compromise data that's stored on the system
 5 and even possibly take control of the system.
 6 **Q. I'd like to direct your attention to page 19 of**
 7 **CX 70, the top entry in particular.**
 8 **What does the top entry on page 19 of**
 9 **CX 70 show?**
 10 A. It shows that there is an anonymous FTP
 11 writeable root directory vulnerability.
 12 **Q. Is that the vulnerability you were referring to**
 13 **earlier?**
 14 A. Yes.
 15 **Q. Please describe for the court what that**
 16 **vulnerability is.**
 17 A. It is possible to write on the root directory of
 18 this remote anonymous FTP server. And a root directory
 19 is the administrative directory within a computer, so if
 20 you have access and write access to the root directory,
 21 you can control and reconfigure the machine, so this
 22 allows an attacker to upload arbitrary files which could
 23 be used in other attacks or to turn the FTP server into
 24 a software distribution point.
 25 **Q. What would be the consequence of that?**

160

1 A. The consequence of that is that malicious
 2 software can be loaded on this computer that would then
 3 distribute any data that is on the computer to outside
 4 of the network.
 5 So this notion of a software distribution point
 6 means that now I -- if I'm a malicious entity, I now
 7 control that computer, and any data on that computer, I
 8 can distribute it to any computer on the Internet.
 9 **Q. What computer was this vulnerability found on?**
 10 A. On mapper.
 11 **Q. And can you remind us what the mapper is?**
 12 A. The mapper server was the machine that
 13 collected the data from the doctors' offices, so
 14 doctors' offices would write, do bulk transfers into
 15 the mapper server.
 16 **Q. What types of information were stored on the**
 17 **mapper server?**
 18 A. Sensitive data information like consumer names,
 19 their Social Security numbers, their addresses, their
 20 date of birth, insurance information, banking and credit
 21 card information.
 22 **Q. When was the anonymous FTP problem first**
 23 **reported?**
 24 A. I would need to consult my expert witness
 25 document for that detail.

161

1 **Q. I'd like you to turn then to CX 740.**
 2 **Does paragraph 72 of CX 740 refresh your**
 3 **recollection?**
 4 A. Yes.
 5 **Q. When was the anonymous FTP problem first**
 6 **reported?**
 7 A. July 14, 1993.
 8 **Q. How long was that before it was identified by**
 9 **LabMD's penetration tests?**
 10 A. 17 years.
 11 **Q. What is secure FTP?**
 12 A. Secure FTP is an extension of the file transfer
 13 protocol that transmits data over an encrypted channel.
 14 So unlike FTP, secure FTP encrypts the data as
 15 it's being transmitted from one point to the next.
 16 **Q. Did LabMD use secure FTP?**
 17 A. No.
 18 **Q. How do you know that?**
 19 A. Because the port that's open on mapper is one
 20 for the file transfer protocol. There's no port open on
 21 mapper during the relevant time period for secure FTP.
 22 That's a different port.
 23 **Q. Could LabMD have corrected its failure to use an**
 24 **appropriate set of risk assessment measures at**
 25 **relatively low cost?**

162

1 A. Yes.
 2 **Q. How could LabMD have done that?**
 3 A. LabMD could have used some of the freely
 4 available tools for risk assessment, some of the same
 5 ones that were used by ProviDyn.
 6 **Q. What's an example of one of those tools?**
 7 A. One example is NMAP, is one example.
 8 The Nessus tool was free up until a period of
 9 time.
 10 **Q. Do you recall how long Nessus was free?**
 11 A. I would need to consult -- free until 2008.
 12 **Q. How much did the May 2010 penetration test that**
 13 **LabMD conducted cost?**
 14 A. \$450.
 15 **Q. Were there other risk assessment measures**
 16 **besides the ones you discussed that were available at**
 17 **relatively low cost?**
 18 A. Yes. Wireshark is another risk assessment
 19 measure, and it was available since 1998.
 20 **Q. Will you remind the court what Wireshark is.**
 21 A. Wireshark is a data traffic analysis tool, so
 22 it allows you to capture data off of your -- that is
 23 coming into your network and do what I call deep packet
 24 inspection of the data, look at -- look beyond the
 25 headers of the data and look explicitly at the data

163

1 itself to determine what information is flowing into and
 2 flowing out of your network.
 3 **Q. How much did Wireshark cost?**
 4 A. Wireshark is also freely available.
 5 **Q. Professor Hill, I'd like to direct your**
 6 **attention to the section of your report that begins with**
 7 **paragraph 78.**
 8 **Did complaint counsel ask you to provide an**
 9 **opinion on whether LabMD maintained more personal**
 10 **information than necessary on its network?**
 11 A. Yes.
 12 **Q. What did you conclude?**
 13 A. I concluded that LabMD maintained information
 14 about approximately a hundred thousand consumers that it
 15 never performed lab tests for.
 16 **Q. Did you conclude that LabMD needed that**
 17 **information to conduct its business?**
 18 A. I concluded that they did not need that
 19 information to conduct their business.
 20 **Q. Why did you reach that conclusion?**
 21 A. Because lab tests were never performed by LabMD
 22 or any of its associated lab testing organizations.
 23 **Q. How long did LabMD maintain that information?**
 24 A. They maintained it throughout the relevant time
 25 period.

164

1 **Q. Did LabMD ever delete that information?**
 2 A. No.
 3 **Q. Why is maintaining more information than**
 4 **necessary problematic?**
 5 A. This goes back to the -- one of the seven
 6 principles of don't keep what you don't need, because if
 7 there's a compromise with this data, you have an
 8 increased scope of harm for individuals for which were
 9 never your consumers, for which you never provided
 10 services for.
 11 So -- and also it adds an additional burden for
 12 maintaining and protecting that information.
 13 **Q. Could LabMD have deleted the approximately**
 14 **hundred thousand records that you concluded it didn't**
 15 **need to conduct its business?**
 16 A. Yes.
 17 **Q. How could LabMD have done that?**
 18 A. They could have done -- they could have removed
 19 it from their database.
 20 **Q. How so?**
 21 A. By deleting those records.
 22 **Q. What would that have cost?**
 23 A. That would have cost only the time of the IT
 24 professional who was responsible for managing their
 25 database.

165

1 **Q. Did complaint counsel ask you to provide an**
2 **opinion on whether LabMD used adequate measures to**
3 **prevent employees from accessing personal information**
4 **that they didn't need to perform their jobs?**

5 A. Yes.

6 **Q. What did you conclude?**

7 A. I concluded that LabMD did not provide adequate
8 measures to limit the data that an employee had access
9 to.

10 **Q. Why did you reach that conclusion?**

11 A. I reached that conclusion based on the
12 information that was provided in the record. When
13 asked about what information an employee needed in
14 order to do his or her job, the response was that they
15 needed various types of information at various levels
16 of access.

17 And so if you're going to implement an access
18 control policy, you would need to know what an employee
19 requires in order to do the job, and so this would
20 prevent you from implementing an access control policy.

21 **Q. Why is limiting employee access to only the**
22 **information needed to do the employee's job important?**

23 A. It is important because I've previously talked
24 about the insider threat. If an employee has access to
25 all information and if that employee is malicious, then

166

1 there is a potential of exposing a large amount of
2 information.

3 And also, the more information, the more people
4 who are able to access the information, that also
5 increases the risk to that data because they're
6 increasing the likelihood of compromise on those
7 individuals' machines.

8 So if there is not a need to access that
9 information, if you -- if you then limit access to that
10 information, you also limit the risk of inadvertent
11 exposure and compromise of that information.

12 **Q. Could LabMD have limited employees' access to**
13 **only the information needed to do the employees' job at**
14 **relatively low cost?**

15 A. Yes.

16 **Q. How would LabMD have done that?**

17 A. LabMD would have to evaluate their processes and
18 procedures and determine what information was needed to
19 perform a particular job and then use tools that were
20 provided by, for example, the Windows operating system
21 to restrict access to that data.

22 **Q. How much would that have cost?**

23 A. That would have cost people time because, since
24 they were using Windows operating systems and Windows
25 servers, that functionality was built into those servers

167

1 to limit access to data.

2 **Q. Would there have been any additional monetary**
3 **cost?**

4 A. No.

5 **Q. Professor Hill, I'd like to direct your**
6 **attention to the section of your report that begins on**
7 **paragraph 86.**

8 **Did complaint counsel ask you to provide an**
9 **opinion on whether LabMD adequately trained its**
10 **employees to safeguard personal information?**

11 A. Yes.

12 **Q. What did you conclude?**

13 A. I concluded that LabMD did not provide adequate
14 training to its employees in order to safeguard personal
15 information.

16 **Q. Does your conclusion apply to particular types**
17 **of LabMD employees or all employees?**

18 A. It -- it includes regular employees -- when I
19 say "regular employees," I mean non-IT employees,
20 non-information technology employees -- and information
21 technology employees, so all of its employees.

22 **Q. Let's start with information technology**
23 **employees.**

24 **Why is proper information security training for**
25 **information technology employees important?**

168

1 A. It's important because they're responsible for
2 defining and implementing a comprehensive security plan,
3 and so if they don't have proper training, they won't be
4 able to define that plan, they won't be able to
5 implement the mechanisms and the strategy for protecting
6 the data and the infrastructure.

7 So without adequate training, they don't know
8 about emerging threats. They may not know about how
9 they can get alerts and updates from vendors and from
10 organizations like NIST about new vulnerabilities that
11 are out there.

12 And so they're just unable to -- because they
13 don't have proper training, this lack of information
14 creates a gap for them.

15 **Q. Why is proper information security training**
16 **important for non-IT employees?**

17 A. It's important for non-IT employees because the
18 things that they do impact the overall security of a
19 system.

20 And so, for example, if they are responsible
21 for running their own antivirus application, they need
22 to understand when it's important to contact IT in order
23 to assess the risk and the vulnerability on their
24 system.

25 So it's too late to wait until the system is

169

1 running so slowly that you can't perform your job.
 2 And they also need to understand the risk of
 3 changing configurations on their system, downloading an
 4 application, and those types of things.
 5 **Q. Earlier you testified that LabMD had given**
 6 **administrative access to at least some employees during**
 7 **the relevant time period.**
 8 **How does that relate to the importance of**
 9 **training for non-IT employees?**
 10 A. So when you have administrative access on your
 11 machine, you have complete control of that machine. You
 12 can reconfigure anything on the machine.
 13 And so if you have that amount of power, you
 14 need to not -- you need to understand and have the
 15 knowledge of the consequences of making such changes,
 16 like, for example, disabling your firewall, what would
 17 that actually mean, downloading some unauthorized
 18 software and the possibilities of compromise that go
 19 along with that.
 20 So that's why they need to have training,
 21 especially when they have full control of their
 22 machines.
 23 **Q. Turning back to training for IT employees, how**
 24 **is that an important part of a defense in depth**
 25 **strategy?**

170

1 A. It's an important part of defense in depth
 2 because, as I stated, if they don't have the knowledge
 3 that they need, they won't be able to specify a
 4 comprehensive security program that applies mechanisms
 5 in a defense in depth way.
 6 And so you can -- even with the best training,
 7 there's still a possibility of human error. But with
 8 no training, you can't expect for there to be proper
 9 security measures in place, put in place, and that they
 10 will be configured properly and that they will achieve
 11 the goal that they're set to achieve. You can't even
 12 expect that there will actually -- that the proper goals
 13 will be identified.
 14 **Q. Professor Hill, why did you conclude that LabMD**
 15 **did not provide proper training for its IT employees?**
 16 A. I concluded that they didn't provide proper
 17 training for their IT employees because there were --
 18 there was testimony that stated that there was -- that
 19 IT employees did not receive training.
 20 **Q. I'd like to turn back to CX 734, which was**
 21 **Ms. Simmons' investigational hearing transcript. And**
 22 **I'd like to draw your attention to page 1 of her**
 23 **testimony -- I'm sorry -- page 61 of her testimony,**
 24 **lines 6 through 14.**
 25 **Did you consider this testimony in connection**

171

1 **with reaching your conclusion about LabMD's lack of**
 2 **IT staff training?**
 3 A. Yes.
 4 **Q. Is this one of the examples that you were**
 5 **referring to earlier?**
 6 A. Yes.
 7 **Q. Now turning to non-IT employees or regular**
 8 **employees as you called them, why did you conclude that**
 9 **those employees did not receive proper information**
 10 **security training?**
 11 A. I concluded that they didn't receive proper
 12 information security training because there was no
 13 evidence in the record that supported that they received
 14 proper IT security training.
 15 **Q. I'd like to turn back to page 61 of Ms. Simmons'**
 16 **testimony, investigational hearing testimony at CX 734.**
 17 **I'd like to turn to line 15 of page 61 through line 6 of**
 18 **page 62.**
 19 **Did you consider this testimony when reaching**
 20 **your conclusion about LabMD's lack of information**
 21 **security training for non-IT employees?**
 22 A. Yes.
 23 **Q. How did LabMD's lack of information security**
 24 **training affect how LabMD performed security?**
 25 A. Basically the lack of knowledge about, you know,

172

1 how to create a comprehensive security program in a
 2 defense in depth manner rendered them -- rendered their
 3 whole approach to one -- or relegated their whole
 4 approach to one that was ad hoc and reactive.
 5 **Q. Was there any written documentation in the**
 6 **record of information security training for LabMD**
 7 **employees?**
 8 A. No.
 9 **Q. You just testified how LabMD performed security**
 10 **in an ad hoc manner as a result of not having proper**
 11 **information security training.**
 12 **Could you provide the court some examples of**
 13 **that.**
 14 A. Can you repeat the question. I'm sorry.
 15 **Q. Sorry.**
 16 **Can you -- I believe you testified earlier that**
 17 **LabMD performed information security in an ad hoc manner**
 18 **due to its lack of information security training. Is**
 19 **that correct?**
 20 A. Yes.
 21 **Q. Will you please provide the court some examples**
 22 **of that.**
 23 A. If -- there's evidence about, you know,
 24 IT staff addressing issues once they've been told that
 25 there is a problem, and so this actually occurred --

173

1 and the problem would be my computer is running so
 2 slowly that I can't perform my job. And this not only
 3 happened, you know, with their internal employees but
 4 also with the machines that were placed in the doctors'
 5 offices.
 6 **Q. Are there any things that with respect to**
 7 **security that LabMD should have done but didn't do**
 8 **because of improper information security training?**
 9 A. Things that they should have done.
 10 **Q. Such as a security practice that should have**
 11 **been implemented?**
 12 A. They should have -- they should have done risk
 13 assessment, and that risk assessment should have been
 14 done periodically. And if they had had proper
 15 training, they would have done risk assessment
 16 periodically.
 17 **Q. Are there any other examples of those types of**
 18 **things?**
 19 A. They would have had strong passwords.
 20 They would have applied patches in a timely
 21 manner, so updating their operating systems, updating
 22 their applications to address vulnerabilities.
 23 And there's evidence in the record that show
 24 that that wasn't being done.
 25 **Q. Could LabMD have provided training, proper**

174

1 **information security training, for its IT employees at**
 2 **relatively low cost?**
 3 A. Yes.
 4 **Q. How could LabMD have done that?**
 5 A. There were low-cost and no-cost options for
 6 training.
 7 There was I think -- I recall -- I would have to
 8 look back at my report, but I think it's the
 9 National Research Alliance that would provide training,
 10 security training for small businesses, businesses with
 11 25 employees or less, at no cost.
 12 There were online training modules that were
 13 provided by the Computer Emergency Response Team at no
 14 cost. And there were some low-cost options for IT
 15 training at \$850 -- for \$850.
 16 So there were some basic -- there were some free
 17 options for training and there were low-cost options
 18 also.
 19 **Q. You mentioned the Consumer Emergency Response**
 20 **Team.**
 21 **What is that?**
 22 A. The Computer Emergency Response Team, CERT.
 23 CERT is an organization that is at Carnegie-Mellon, and
 24 it was created in response to the first Internet
 25 vulnerability. And it includes participation of

175

1 government, academic and industry professionals. They
 2 all come together to create guidelines and information
 3 that helps to secure computing systems.
 4 **Q. Are these guidelines easily found?**
 5 A. Yes.
 6 **Q. How so?**
 7 A. The guidelines are available online. If
 8 there's anything that you are specifically looking for,
 9 you can usually go to their main -- CERT's main Web site
 10 and, you know, they're available. Or you can do
 11 something as simple as a Google search for specific
 12 terms. If you're looking at confidentiality policies
 13 for small businesses, you would find some of these
 14 guidelines.
 15 **Q. Could LabMD have provided proper information**
 16 **security training for its non-IT employees at relatively**
 17 **low cost?**
 18 A. Yes.
 19 **Q. How could LabMD have done that?**
 20 A. Some of these same guidelines, they also
 21 provide some basic training not just for
 22 IT professionals but for people to understand the
 23 emerging risks that are out there so that non-IT
 24 employees, you know, have a better understanding of the
 25 consequences of, you know, their actions when they are

176

1 using a computing infrastructure.
 2 **Q. Professor Hill, I'd like to direct your**
 3 **attention to the section of your report that begins with**
 4 **paragraph 93.**
 5 **Did complaint counsel ask you to provide an**
 6 **opinion on whether LabMD required employees or others**
 7 **with remote access to its network to use common**
 8 **authentication measures?**
 9 A. Yes.
 10 **Q. Will you remind the court what an authentication**
 11 **measure is.**
 12 A. An authentication measure is a way of verifying
 13 the identity of users on your network.
 14 So a common way to do that is with a user name,
 15 which becomes your identity, and a password, which is
 16 proof of your identity.
 17 **Q. What did you conclude about LabMD's**
 18 **authentication measures?**
 19 A. I concluded that LabMD's authentication
 20 mechanisms were not reasonable and appropriate for
 21 securing LabMD's network.
 22 **Q. Why is it important to use effective**
 23 **authentication measures?**
 24 A. If you don't use effective authentication
 25 measures, you increase the risk of unauthorized access

177

1 to your system.
 2 For example, if you use weak passwords, it's
 3 likely that an attacker will be able to guess a password
 4 and gain access to your system.
 5 **Q. What is a weak password?**
 6 A. A weak password is a password that is short in
 7 length, less than eight characters, one that uses
 8 either all alphabets or all numbers, no special
 9 characters.
 10 So if you are not varying those characters and
 11 you don't have a long length, you actually reduce the
 12 uncertainty in the password, and so basically that deals
 13 with information entropy, and so what you want is there
 14 to be a lot of uncertainty, which creates a large search
 15 space for an attacker.
 16 So if I use alphabets of uppercase and
 17 lowercase, that increases the search space. If I don't
 18 use dictionary words, that also increases the search
 19 space. If I introduce numbers and special characters,
 20 like punctuation characters, that also increases the
 21 search space.
 22 So it makes it more difficult for an attacker to
 23 actually brute-force your authentication mechanism --
 24 and when I say "brute-force," I mean try all
 25 possibilities -- because that attacker will have to

178

1 search a large space in order to determine what the
 2 actual password is.
 3 **Q. You've discussed the length and required
 4 characters in connection with passwords.**
 5 **How does the history of a password relate to its
 6 strength?**
 7 A. A history of the password has to be taken under
 8 consideration in order to have strong passwords, because
 9 if you maintain the history, you can ensure that
 10 individuals don't reuse passwords.
 11 And so that's why you would want to maintain a
 12 history of passwords and require users to create unique
 13 new passwords.
 14 **Q. How often should a password be changed?**
 15 A. That should be determined by the role of the
 16 user, the types of information that the user will have
 17 access to, the sensitivity of that information.
 18 So if you have access to highly sensitive
 19 information, you would want to change your password more
 20 frequently.
 21 So it's a process for determining that, the
 22 frequency of changing passwords and the history you'd
 23 want to maintain.
 24 **Q. How should passwords be stored within a
 25 network?**

179

1 A. Passwords should be stored in a way that is not
 2 readable in the network, so it's best to store the
 3 passwords in encrypted form. And usually a hash of a
 4 password is taken and the password is stored with that
 5 hash. And in addition to that hash, you add some
 6 randomness to the password before you create that
 7 cryptographic hash of a password.
 8 **Q. I'm going to ask you some more about that to
 9 make sure I understand the technical terms here.**
 10 **What is -- a cryptographic hash you said?**
 11 A. Yes. A cryptographic hash is a transformation
 12 of a piece of information into a fixed-size
 13 information.
 14 And so what you have that's used is a function
 15 that would create a one-way mapping of your password to
 16 a numeric value that is not in alphabetic form, so it
 17 translates your password to some numeric value. And so
 18 an attacker, even if they saw it, they wouldn't
 19 understand what that value was.
 20 **Q. Why did you conclude that LabMD failed to use
 21 effective authentication measures?**
 22 A. I concluded that they failed to use effective
 23 authentication measures because they had no policy for
 24 strong passwords. And there was evidence in the record
 25 to show that individuals used very weak passwords that

180

1 included dictionary words, parts of the names of the
 2 individuals for which the password was used, and so this
 3 makes it easy for these passwords to be guessed.
 4 And they also -- there's also evidence that some
 5 users used these passwords for years and that they were
 6 never changed.
 7 **Q. Professor Hill, I'd like to direct your
 8 attention to CX 167.**
 9 **What is CX 167?**
 10 A. CX 167 is -- it's a small database of passwords
 11 that were being used within the relevant time period.
 12 **Q. Did you consider CX 167 in reaching your
 13 conclusion about the effectiveness of LabMD's
 14 authentication measures?**
 15 A. Yes.
 16 **Q. What did you conclude from CX 167?**
 17 A. I concluded that LabMD didn't have a strong -- a
 18 policy for strong passwords and that they had no
 19 mechanism in place to enforce strong passwords, so you
 20 had passwords like "LabMD."
 21 So meaning that there's some users that actually
 22 used the password "LabMD" as their password.
 23 **Q. Why is a LabMD employee using "LabMD" as a
 24 password problematic?**
 25 A. It's problematic because it would be very easy

181

1 to guess. An attacker -- that would be one of the first
 2 things that an attacker would choose, is the name of the
 3 company, as a potential password.
 4 It also -- if you see here, "labmd" is all
 5 lowercase. "LabMD" also contains a dictionary word,
 6 which is, when an attacker is trying to crack a password
 7 or determine a password, they will often use dictionary
 8 words in that approach.
 9 The password is actually less than eight
 10 characters. "LabMD" is only five characters long, which
 11 is a small search space to begin to look or to try to
 12 brute-force a password.
 13 **Q. When you say "brute-force a password," what do**
 14 **you mean?**
 15 A. When I say "brute-force," I mean I'm going to
 16 try all possible combinations to determine what the
 17 password is.
 18 So here, I only have to try the alphabet, the
 19 letters in the alphabet. I'm only -- an attacker would
 20 only have to try lowercased alphabets, and so that --
 21 and only five characters.
 22 So that defines my search space, and so in order
 23 to brute-force this, you know, I would -- as an
 24 attacker, I would actually look for five characters and
 25 change those five characters in order to search for

182

1 possible passwords.
 2 **Q. When you say "search space," what do you mean?**
 3 A. Search space is basically the different
 4 combinations of characters and -- that I would have to
 5 search across in order to possibly find this particular
 6 password.
 7 So that constitutes a search space. And the
 8 length, the number of characters I would have to
 9 consider, the alphabet that I would have to consider
 10 where I'm dealing with lowercase and uppercase, if I
 11 now, you know, add numbers to that, I've increased that
 12 search space.
 13 **Q. So what is the consequence of a smaller search**
 14 **space?**
 15 A. The consequence of a smaller space is that it
 16 takes less time to determine the actual password in a
 17 brute force attack.
 18 **Q. Professor Hill, I'd like to direct your**
 19 **attention to CX 706.**
 20 **What is CX 706?**
 21 A. CX 706 is the transcript for Sandra Brown.
 22 **Q. Who is Sandra Brown?**
 23 A. Sandra Brown -- I think that Sandra Brown is the
 24 billings manager.
 25 **Q. Is she the same billing manager who had the**

183

1 **1718 File installed on her computer?**
 2 A. No. She's not the same one that had the
 3 1718 File on her computer.
 4 **Q. Did you consider Ms. Brown's testimony when**
 5 **reaching your conclusions about LabMD's password**
 6 **practices?**
 7 A. Yes.
 8 **Q. I'd like to draw your attention to page 13 of**
 9 **Ms. Brown's testimony, lines 4 through 20 in**
 10 **particular.**
 11 **What did you conclude from this testimony?**
 12 A. I concluded that she used the same password for
 13 the duration of the time that she was there from 2006 to
 14 2013.
 15 **Q. Is this one of the examples you were referring**
 16 **to earlier?**
 17 A. Yes.
 18 **Q. Did you consider her using the same password**
 19 **from 2006 to 2013 problematic?**
 20 A. Yes, I did.
 21 **Q. Why?**
 22 A. There are a couple of reasons. She's using the
 23 same password. She has a weak password that was only
 24 five characters long, all lowercase letters, so that
 25 increases the chances that an attacker could compromise

184

1 that password.
 2 She's also logging in remotely, so if her
 3 password is compromised and she's using this weak
 4 password, there is no two-factor authentication in
 5 place for remote users.
 6 And so if I had a different way of auth-- -- an
 7 additional way of authenticating myself for remote
 8 users, it would make it harder for an attacker to gain
 9 unauthorized access.
 10 **Q. Okay. I'd like to unpack that a little bit.**
 11 **What is two-factor authentication?**
 12 A. Two-factor authentication is that I have two
 13 ways, two sources of proof that I am who I claim to be.
 14 So with regard to the user name, I present an
 15 identity to the computer and the infrastructure in order
 16 to log in.
 17 So with a one-factor authentication mechanism,
 18 I only present one source of proof, and usually that is
 19 a password. With a two-factor mechanism, in addition
 20 to presenting you some -- with something that I know,
 21 like my password, I also have to present you with
 22 something that maybe I have, like a biometric or a token
 23 that generates a random number.
 24 **Q. Did LabMD use two-factor authentication for any**
 25 **of its remote users?**

185

1 A. No.

2 **Q. How would using two-factor authentication for**

3 **remote access have implemented a defense in depth**

4 **strategy?**

5 A. Because it requires two different types of

6 proofs of identity, so even if the password is

7 compromised, an attacker would also have to gain access

8 to the thing, for instance, that you know -- I mean,

9 that you have, like a biometric or a token that's

10 generating a random number for you to enter.

11 So it decreases the likelihood of a compromised

12 access for remote users.

13 **Q. I'd like to turn now from employee passwords to**

14 **passwords that LabMD used for accounts in its doctor --**

15 **the offices of its doctor or physician clients.**

16 **What types of passwords did LabMD use for**

17 **accounts that its physician clients' offices had?**

18 A. I would also characterize those passwords as

19 weak passwords. They used nurses' initials as

20 passwords, nurses' initials with a couple of numbers,

21 so these were short passwords. They included

22 information about the users themselves, and they also

23 had a small search space.

24 **Q. When you say "information about the users**

25 **themselves," what do you mean?**

186

1 A. Information, for example, the nurses' initials.

2 **Q. Should passwords be limited to one user?**

3 A. Yes.

4 **Q. Why?**

5 A. If you share passwords, you also increase the

6 chance and likelihood of compromise.

7 **Q. Why is that?**

8 A. Because now I need to -- as I explained what an

9 authentication mechanism is, I present to you an

10 identity and I give you then proof of that identity,

11 which is the password. Now I have one identity, but

12 then I have multiple people with the proof for that

13 identity, so how then do you verify, you know, which

14 individual is actually associated with that user name

15 credential.

16 And so this becomes problematic. You don't know

17 which user -- it's -- let me back up a little bit.

18 It's giving the user the ability to impersonate

19 someone else, and so that's the first problem, so I've

20 destroyed that link between identity and proof of

21 identity. Okay?

22 And so now I'm sharing the password among

23 multiple individuals, and what prevents that individual

24 from additionally sharing it to more people, so this

25 could lead to compromise or an individual exposing that

187

1 password in some way by, for example, writing it down on

2 a sticky note or something like that.

3 So the more people who touch that password, the

4 more likely it is to compromise.

5 **Q. Are there instances where LabMD allowed**

6 **passwords to be shared during the relevant time period**

7 **for your report?**

8 A. Yes.

9 **Q. How do you know that?**

10 A. There is testimony that discusses the sharing of

11 passwords and how that was a major issue at LabMD.

12 **Q. Was that throughout the relevant time period for**

13 **your report?**

14 A. That was at least up until 2009.

15 **Q. Professor Hill, I'd like to draw your attention**

16 **to CX 719.**

17 **What is CX 719?**

18 A. CX 719 is the transcript of Robert Hyer.

19 **Q. Who is Robert Hyer?**

20 A. Robert Hyer was the -- was an IT manager at

21 LabMD.

22 **Q. I'd like to draw your attention to page 26 of**

23 **the transcript of Mr. Hyer's deposition, lines 9 through**

24 **25 in particular.**

25 **Is this an example of the testimony you were**

188

1 **referring to earlier about LabMD having instances of**

2 **employees sharing passwords?**

3 A. Yes.

4 **Q. Could LabMD have corrected its failure to use**

5 **common effective authentication measures at relatively**

6 **low cost?**

7 A. Yes.

8 **Q. How could LabMD have done that?**

9 A. They could have used mechanisms that are

10 provided by the Windows server in order to implement

11 strong password policies.

12 **Q. What would that have cost?**

13 A. That -- there would be no additional cost

14 because those mechanisms were provided.

15 **Q. Would there be a cost in terms of time?**

16 A. There would be a cost in the form of employee

17 time, the IT staff.

18 **Q. Would there be any monetary cost?**

19 A. There would be no monetary cost.

20 **Q. Professor Hill, I'd like to draw your attention**

21 **to the section of your report that begins with**

22 **paragraph 97.**

23 **Did complaint counsel ask you to offer an**

24 **opinion on whether LabMD maintained and updated**

25 **operating systems and applications on its network?**

189

1 A. Yes.
 2 **Q. What did you conclude?**
 3 A. I concluded that LabMD did not update its
 4 operating systems and other applications in a timely
 5 manner to address risk and vulnerabilities in those
 6 software applications.
 7 **Q. I believe you testified about this earlier, but**
 8 **will you remind the court why it's important to maintain**
 9 **and update operating systems and applications.**
 10 A. It's important, and I'll repeat the example that
 11 I gave. For every ten lines of software, there is on
 12 average one vulnerability.
 13 So in something like Windows operating system,
 14 which has 50 million lines of code, there are at least
 15 on average five million coding mistakes and flaws in
 16 that code. And it's virtually impossible for a vendor
 17 to identify and fix all of those vulnerabilities before
 18 they are released to consumers.
 19 **Q. Why is it not possible to fix those**
 20 **vulnerabilities before the software is released to**
 21 **consumers?**
 22 A. One of the reasons that it's impossible is
 23 because in order to identify some of those
 24 vulnerabilities, you would need a large user base to get
 25 a large coverage of all of the functionality within that

190

1 piece of software.
 2 So if -- some of those problems won't be
 3 discovered until they're released to the consumer.
 4 **Q. And is there another reason?**
 5 A. Is there another reason?
 6 **Q. Why all of the flaws couldn't be fixed before**
 7 **the software is released.**
 8 A. That even -- even with automated testing, they
 9 won't get, you know, the type of coverage.
 10 And also, usually the time from completion of a
 11 project to the release date is preset, and companies
 12 are going to release their data to -- release their
 13 products to consumers, so that may also have an effect,
 14 that window from coding completion to testing
 15 completion.
 16 **Q. Professor Hill, will you please provide the**
 17 **court an example of why you concluded that LabMD did**
 18 **not adequately update and maintain its operating**
 19 **systems.**
 20 A. LabMD -- one example would be that in 2006,
 21 LabMD was still using the Windows NT server on some
 22 of -- server operating system on some of its servers,
 23 and Microsoft had discontinued support for Windows NT in
 24 2004.
 25 **Q. Will you please provide the court an example of**

191

1 **why you concluded that LabMD did not adequately maintain**
 2 **and update its applications.**
 3 A. There -- after the -- the ProviDyn
 4 vulnerability scan identified applications with
 5 vulnerabilities. And one of those applications was the
 6 Veritas backup software. And this software had a
 7 Level 5 risk, which meant that that risk gave an
 8 attacker administrative access and control over the
 9 machine that was actually running that software. And it
 10 was a default password vulnerability.
 11 So that was one of the vulnerabilities with
 12 that software. And the second vulnerability with that
 13 software was a buffer overflow vulnerability, which
 14 allowed an attacker to execute code remotely and gave
 15 them partial access to the data on the machine.
 16 **Q. Professor Hill, I'd like to direct your**
 17 **attention to CX 67.**
 18 **What is CX 67?**
 19 A. CX 67 is the ProviDyn report.
 20 **Q. Is this a different ProviDyn report from the one**
 21 **we looked at earlier at CX 70?**
 22 A. No. It is the same ProviDyn.
 23 **Q. The company is the same; is that what you're**
 24 **saying?**
 25 A. Yes.

192

1 **Q. What computer does CX 67 cover, if you recall?**
 2 A. I am --
 3 **Q. Do you not recall?**
 4 A. I don't recall the --
 5 **Q. I'd like to show a document -- split the screen.**
 6 **I'd like to show you CX 51 page 4.**
 7 **And I'd like to turn to CX 67 page 22.**
 8 **Professor Hill, do these two excerpts --**
 9 A. Yes.
 10 **Q. -- refresh your memory as to which computer?**
 11 A. Yes, it does.
 12 **Q. Which computer?**
 13 A. It was the LabNet computer.
 14 **Q. Is the LabNet computer a server?**
 15 A. Yes, it was.
 16 **Q. What did the LabNet server do?**
 17 A. The LabNet server maintained sensitive
 18 information that was used for the collection and the
 19 processing of test results.
 20 **Q. What types of information were on the LabNet**
 21 **server?**
 22 A. The LabNet server contained consumer names,
 23 Social Security numbers, insurance information, types of
 24 tests, test results, date of birth, those types of
 25 information.

193

1 **Q. So I'd like to draw your attention to the bottom**
 2 **entry on page 22 of CX 67.**
 3 **Is this the buffer flow vulnerability that**
 4 **you -- buffer overflow vulnerability that you discussed**
 5 **earlier?**
 6 A. Yes.
 7 **Q. What could happen if that vulnerability were**
 8 **exploited?**
 9 A. That vulnerability gave an attacker the ability
 10 to execute code remotely, so an attacker could
 11 execute -- exploit this vulnerability and execute code
 12 that could then take over partial control of that
 13 computer.
 14 **Q. When did LabMD first identify this**
 15 **vulnerability?**
 16 A. LabMD first identified this vulnerability in
 17 2010.
 18 **Q. When was the risk first identified within the IT**
 19 **community?**
 20 A. I would have to consult my expert witness
 21 document to determine that.
 22 (Pause in the proceedings.)
 23 The problem was detected and a solution was
 24 available in July of 2007.
 25 **Q. How do you know that?**

194

1 A. I know that because there was an alert and an
 2 announcement made by the vendor, Symantec, regarding
 3 this vulnerability. And that announcement provided
 4 information about when a solution was available.
 5 **Q. Could LabMD have corrected its failure to**
 6 **update operating systems and applications at relatively**
 7 **low cost?**
 8 A. Yes.
 9 **Q. How could LabMD have done that?**
 10 A. They could have just downloaded the update from
 11 the vendor.
 12 **Q. What would that have cost?**
 13 A. There would not have been any cost.
 14 **Q. So I'd just like to turn back to page 1 of**
 15 **CX 67 for a moment.**
 16 **What was the overall security posture from the**
 17 **ProviDyn scan of the LabNet server?**
 18 A. It was poor.
 19 **Q. Professor Hill, I'd like you to turn to the next**
 20 **section of your report, which begins with paragraph 102.**
 21 **Did complaint counsel ask you to provide an**
 22 **opinion on whether LabMD used readily available measures**
 23 **to prevent or detect unauthorized access to personal**
 24 **information on its network?**
 25 A. Yes.

195

1 **Q. What did you conclude?**
 2 A. I concluded that LabMD did not use readily
 3 available measures to prevent and detect unauthorized
 4 access to their personal information.
 5 **Q. Why are measures to prevent and detect**
 6 **unauthorized access to personal information an important**
 7 **part of a defense in depth strategy?**
 8 A. It's important because there are a variety of
 9 ways that an attacker may try to gain access to a
 10 system, and so it's part of any defense in depth
 11 strategy to try to prevent and then to detect that
 12 unauthorized access. Detecting it allows you to know
 13 that it is occurring and would help you to remediate the
 14 problem.
 15 **Q. Professor Hill, I'd like to turn to**
 16 **paragraph 104 of your expert report.**
 17 **What does this paragraph discuss?**
 18 A. This paragraph discusses the various measures
 19 that can be put in place to prevent the unauthorized
 20 sharing of personal information.
 21 **Q. Paragraph 104(a) discusses that employees**
 22 **should be given nonadministrative accounts on**
 23 **workstations.**
 24 A. Yes.
 25 **Q. You talked about this earlier this afternoon.**

196

1 **Can you just summarize why it's important for**
 2 **employees to have nonadministrative accounts.**
 3 A. It's important for employees to have
 4 nonadministrative accounts because giving them limited
 5 control of their machine prevents the inadvertent
 6 downloading of software that could compromise not only
 7 their system but compromise the entire network.
 8 Employees often don't understand the
 9 consequences of reconfiguring or changing things on
 10 their system, and so by limiting the power that they
 11 have over their system, you can help prevent inadvertent
 12 compromise.
 13 **Q. You testified earlier today that there are**
 14 **instances where LabMD gave employees administrative**
 15 **accounts.**
 16 **Was one of those instances the billing manager**
 17 **whose computer had LimeWire installed?**
 18 A. Yes.
 19 **Q. I'd like to turn to paragraph 104(b), which**
 20 **discusses backups of personal information.**
 21 **Why is it important to store backups of personal**
 22 **information on devices that are separate from other**
 23 **employee activities?**
 24 A. Because employees, they use their computers in a
 25 variety of ways, especially those who are given full

197

1 power over those devices, the power to download software
 2 and to change security settings.
 3 So because these are multiuse environments
 4 where they're reading their e-mail, they may
 5 inadvertently open an attachment that has malicious
 6 software embedded in it, any of those things put that
 7 computer, any information that's stored on that
 8 computer, at risk for exposure, so you would want to
 9 store backups on a machine where those types of
 10 activities are not occurring.
 11 **Q. Did LabMD store backups on devices that were not**
 12 **isolated from other employee activities?**
 13 A. Yes.
 14 **Q. Paragraph 104(e) of your report.**
 15 **It says that a firewall should be configured to**
 16 **block all unwanted traffic from entering the network.**
 17 **Why is that important?**
 18 A. That is important because if you restrict
 19 communication that's initiated from outside for
 20 unauthorized applications, then that would block that
 21 traffic from entering your network.
 22 **Q. What did you conclude about the configuration of**
 23 **LabMD's firewalls?**
 24 A. I concluded that LabMD's firewalls were not
 25 configured to block all traffic that wasn't necessary

198

1 for LabMD to conduct its business.
 2 **Q. Why did you reach that conclusion?**
 3 A. I reached that conclusion because the Veritas
 4 backup software had a port open, port 10,000, and the
 5 Veritas backup software also had a vulnerability that
 6 was a Level 5 vulnerability that gave an attacker
 7 administrative access to that software and to the
 8 machine that was running that software. There was no
 9 business need for that port to be open. Backups were
 10 done within the local area network and not across the
 11 Internet.
 12 **Q. Professor Hill, I'd like to turn back to CX 67,**
 13 **page 22, and the top entry.**
 14 **Is this the vulnerability that you were just**
 15 **referring to?**
 16 A. Yes.
 17 **Q. In your opinion, if LabMD's firewalls had been**
 18 **properly configured, would that have prevented the**
 19 **LimeWire application on the billing manager's computer**
 20 **from sharing files?**
 21 A. No.
 22 **Q. Why not?**
 23 A. Because LimeWire can still share files even if
 24 the request for files is not initiated from outside of
 25 an organization's network.

199

1 If a computer that's using LimeWire within the
 2 organization initiates a connection with the LimeWire
 3 network, then data can be transferred to that computer
 4 through that already-established communication channel.
 5 **Q. How does the fact that a properly configured**
 6 **firewall would not have prevented the LimeWire**
 7 **application from sharing files relate to the importance**
 8 **of a proper defense in depth strategy?**
 9 A. It's a great example of why you need to use
 10 defense in depth, because, as I stated earlier, it's an
 11 arms race and applications become more and more
 12 stealthy. If there's a mechanism in place, they try to
 13 determine -- application -- malicious application
 14 developers try to determine ways to circumvent that
 15 mechanism to achieve its goal, and its goal is to gain
 16 unauthorized access to a system.
 17 So that's why you would need to deploy
 18 mechanisms, heterogeneous mechanisms, in a layered
 19 manner to combat that.
 20 **Q. How did LabMD allowing the billing manager to**
 21 **have an administrative account on her machine relate to**
 22 **the LimeWire application being present on her computer?**
 23 A. Given that the billings manager had
 24 administrative access, the billings manager was able to
 25 download and install applications onto the machine.

200

1 **Q. How long was the LimeWire application on the**
 2 **billing manager's computer?**
 3 A. The application was installed somewhere between
 4 2005 and 2006. It was not removed until 2008.
 5 **Q. Are there security measures that LabMD could**
 6 **have used to detect the application sooner?**
 7 A. Can you repeat the question, please.
 8 **Q. Are there automated security measures that LabMD**
 9 **could have used that would have detected -- could have**
 10 **detected LimeWire before May 2008?**
 11 A. Yes.
 12 **Q. Can you give us and the court an example?**
 13 A. They could have used a file integrity monitor
 14 to detect the presence of the application.
 15 **Q. What is a file integrity monitor?**
 16 A. A file integrity monitor is an application that
 17 first creates a base profile for your computer. And the
 18 assumption when you create the base profile is that that
 19 system is in a trustworthy state, so it actually creates
 20 a list of all the files that's stored on your computer,
 21 and periodically you can use it to check the integrity
 22 of the computer.
 23 And what I mean by "integrity" is determine
 24 whether files have been added, the size of files have
 25 changed, and those types of things.

201

1 And so when you -- when you do this integrity
 2 check, by comparing the current state of the computer,
 3 the current list of files, to the list of files that's
 4 in your base profile, you can detect that there has
 5 been a change.
 6 A change doesn't necessarily mean that it is
 7 malicious, but a change will help you to identify that,
 8 you know, there's -- further investigation is needed,
 9 and so you can further investigate those changes to
 10 determine whether, for example, an unauthorized
 11 file-sharing application has been downloaded.
 12 JUDGE CHAPPELL: We're about at 5:30. What's
 13 your status?
 14 MS. LASSACK: I think that we could finish in
 15 ten minutes or so, so...
 16 JUDGE CHAPPELL: What do you think, Bailiff?
 17 MR. MITCHELL: It's your call, sir.
 18 JUDGE CHAPPELL: Press on.
 19 BY MS. LASSACK:
 20 **Q. Professor Hill, did LabMD use file integrity**
 21 **monitoring?**
 22 A. No.
 23 **Q. Could LabMD have corrected its failure to use**
 24 **readily available measures to prevent or detect**
 25 **unauthorized access to personal information on its**

202

1 **network at relatively low cost?**
 2 A. Yes.
 3 **Q. How could LabMD have done that?**
 4 A. LabMD could have enforced a policy that
 5 prevented employees from having administrative access.
 6 They could have used file integrity monitoring
 7 software that was freely available.
 8 **Q. How much would it have cost to prevent employees**
 9 **from having administrative accounts?**
 10 A. Nothing. It would only cost people time, so no
 11 additional monetary cost.
 12 **Q. How much would it have cost to store backups of**
 13 **personal information on machines that weren't used for**
 14 **other employee purposes?**
 15 A. There were other machines like servers
 16 available, so no additional machines would need to be
 17 purchased.
 18 **Q. Professor Hill, earlier this afternoon, you**
 19 **said no -- there's no such thing as perfect security.**
 20 **And His Honor asked whether this means that there is**
 21 **always the likelihood of a security problem. Do you**
 22 **recall that testimony?**
 23 A. Yes.
 24 **Q. If a company that maintains personal**
 25 **information cannot achieve perfect security, what, in**

203

1 **your opinion, should be a company's goal with regard to**
 2 **its security?**
 3 A. The company's goal is to do what is reasonable
 4 and appropriate and to apply strategies that would limit
 5 the probability of compromise.
 6 **Q. Professor Hill, now that we've discussed all of**
 7 **your specific opinions about LabMD's security practices,**
 8 **I'd like to turn back to your overall conclusion about**
 9 **LabMD's security practices.**
 10 **What is your overall conclusion about the**
 11 **reasonableness and appropriateness of LabMD's security**
 12 **practices?**
 13 A. My overall conclusion is that LabMD did not
 14 practice reasonable and appropriate security to ensure
 15 the protection of its infrastructure and its data.
 16 **Q. What time period does that conclusion cover?**
 17 A. January 2005 until July 2010.
 18 **Q. Do you offer any opinion about the**
 19 **reasonableness of LabMD's security practices after**
 20 **July 2010?**
 21 A. No, I do not.
 22 **Q. Could LabMD have corrected its security failures**
 23 **at little or no cost?**
 24 A. Yes.
 25 MS. LASSACK: Your Honor, that's my final

204

1 question.
 2 JUDGE CHAPPELL: All right. Thank you.
 3 MS. LASSACK: I would like to move admission of
 4 CDX 01, which is the version of the IT employee timeline
 5 that was not discussed with Professor Hill. And I'd
 6 also like to move the admission of CDX 02.
 7 JUDGE CHAPPELL: Any objection?
 8 MR. SHERMAN: Yes. I was informed that this
 9 was a demonstrative exhibit and not something that was
 10 going to be admitted into evidence, so I would object
 11 on that basis. I thought this was a demonstrative.
 12 MS. LASSACK: Well, it's also a summary without
 13 Professor Hill's markup, which is what I would move
 14 first, CDX -- sorry -- CXD 01, which is a summary
 15 exhibit of testimony, which I believe we established the
 16 foundation for with Professor Hill's testimony.
 17 I also have here binders with testimony that
 18 supports the summary exhibit that is CXD 1, the LabMD IT
 19 employee timeline.
 20 And I'd also like to move a third exhibit, which
 21 is the LabMD IT employee timeline with Professor Hill's
 22 markup, which we'll give a new --
 23 JUDGE CHAPPELL: Okay. What's the first exhibit
 24 you're offering?
 25 MS. LASSACK: So the first exhibit would be

205

1 CDX 01, which would be the -- what we'll call the clean
 2 version.
 3 JUDGE CHAPPELL: What's the next exhibit?
 4 MS. LASSACK: CDX 02 is the -- Professor Hill's
 5 network diagram.
 6 MR. SHERMAN: Isn't that in her report?
 7 MS. LASSACK: It's the additional description
 8 with when the animation is shown through the PowerPoint
 9 slide.
 10 JUDGE CHAPPELL: All right. You are objecting
 11 to the marked-up poster board?
 12 MR. SHERMAN: I'm objecting to all three. They
 13 represented to us that these were demonstrative
 14 exhibits and that they weren't going -- well, they
 15 didn't say they weren't going to move them for
 16 admission, but they're demonstrative. I think they've
 17 served their purpose in assisting the witness in
 18 testifying today, and I will object to them being
 19 admitted as exhibits.
 20 JUDGE CHAPPELL: Right.
 21 Are you offering them as demonstrative and not
 22 for evidence?
 23 MS. LASSACK: We're using them as demonstrative
 24 exhibits today, and I believe we've established the
 25 foundation necessary.

206

1 JUDGE CHAPPELL: I don't believe you have, so
 2 those are not going to be admitted into evidence over
 3 objection. If you want them to be merely demonstrative,
 4 I'll allow that, but not for evidence.
 5 MS. LASSACK: Then at present we will leave them
 6 as merely demonstrative exhibits.
 7 JUDGE CHAPPELL: I didn't understand you.
 8 MS. LASSACK: Then we will leave them as merely
 9 demonstrative exhibits.
 10 JUDGE CHAPPELL: Any objection for them as
 11 demonstrative?
 12 MR. SHERMAN: No objection, Your Honor.
 13 JUDGE CHAPPELL: Okay. That will be allowed.
 14 They will be admitted as demonstrative.
 15 And just so you know, I don't believe you laid
 16 a proper foundation for all those time periods that are
 17 on that chart, just for your own personal knowledge
 18 there.
 19 Any cross?
 20 MR. SHERMAN: Yes, Your Honor.
 21 JUDGE CHAPPELL: I just want to get that on the
 22 record. We won't do it today.
 23 Anything further from you?
 24 MS. LASSACK: Not at this time.
 25 JUDGE CHAPPELL: Do you pass the witness now?

207

1 MS. LASSACK: Yes.
 2 JUDGE CHAPPELL: All right.
 3 We will reconvene tomorrow at 0930.
 4 MR. SHERMAN: Your Honor, one housekeeping.
 5 JUDGE CHAPPELL: Okay. Go ahead.
 6 MR. SHERMAN: I've had discussions with
 7 complaint counsel regarding calling Mr. Eric Johnson in
 8 their case. Well, they're going to allow me to call him
 9 as if in my case but on Friday. And I believe we
 10 anticipate that Mr. Van Dyke will be testifying on
 11 Friday?
 12 MS. VANDRUFF: Yes, that's correct, Your Honor.
 13 Respondent's counsel reached out yesterday to ask for
 14 our consent to call Mr. Johnson in our case, if you
 15 will, on Friday because of his scheduling constraints.
 16 Mr. Van Dyke, our expert, likewise has
 17 scheduling constraints, and as long as we can conclude
 18 Mr. Van Dyke's examination, we have no objection to
 19 respondent calling Mr. Johnson on Friday, even if our
 20 case hasn't concluded.
 21 MR. SHERMAN: The reason I bring it up is
 22 because Friday may be one of the days where we request
 23 additional time. We may go overtime, if that's -- if
 24 we can arrange that with the court and the court
 25 personnel.

208

1 JUDGE CHAPPELL: Nobody is going to be driving
 2 on freeways around here Friday anyway in the afternoon
 3 because they actually start on Thursday morning to get
 4 out of town, so we're stuck here anyway basically, so as
 5 long as it's okay with the -- everyone else involved, we
 6 can go late on Friday.
 7 MR. SHERMAN: And we're not saying we have --
 8 JUDGE CHAPPELL: What do you think there,
 9 Officer Proctor? Is it okay with you?
 10 OFFICER PROCTOR: It sounds good to me,
 11 Your Honor.
 12 JUDGE CHAPPELL: Why don't we -- we'll plan to
 13 do that and -- so in other words, you're going to
 14 direct-examine this witness.
 15 MR. SHERMAN: Yes, sir.
 16 JUDGE CHAPPELL: And without a jury, it's no big
 17 deal to take somebody out of time, so that's not a
 18 problem.
 19 All right. Anything further?
 20 MR. SHERMAN: Nothing further, Your Honor.
 21 JUDGE CHAPPELL: All right. Until 9:30 in the
 22 morning we're in recess.
 23 (Whereupon, the foregoing hearing was adjourned
 24 at 5:38 p.m.)
 25

1 CERTIFICATION OF REPORTER

2

3 DOCKET/FILE NUMBER: 9357

4 CASE TITLE: LabMD, Inc.

5 HEARING DATE: May 20, 2014

6

7 I HEREBY CERTIFY that the transcript contained
8 herein is a full and accurate transcript of the notes
9 taken by me at the hearing on the above cause before the
10 FEDERAL TRADE COMMISSION to the best of my knowledge and
11 belief.

12

13 DATED: MAY 24, 2014

14

15

16 JOSETT F. WHALEN, RMR

17

18

19 CERTIFICATION OF PROOFREADER

20

21 I HEREBY CERTIFY that I proofread the transcript
22 for accuracy in spelling, hyphenation, punctuation and
23 format.

24

25 ELIZABETH M. FARRELL

<p>A</p> <p>\$450 26:9 162:14</p> <p>\$850 174:15,15</p> <p>a.m 2:8 79:7</p> <p>ability 69:18 84:12 102:2 111:19 149:17 186:18 193:9</p> <p>able 23:19 32:13 42:16 61:2 63:7 64:17 68:8 72:1 73:19 90:18 111:19 116:2 126:15 135:18 145:10 146:17 166:4 168:4,4 170:3 177:3 199:24</p> <p>Absolutely 54:17 70:15 71:15</p> <p>academia 87:8</p> <p>academic 109:18 175:1</p> <p>accept 88:1</p> <p>access 15:3 22:18 33:4 34:17,21 35:1 36:21,24 37:3,8,9 41:10,22,24 42:8 42:10,11,16,16,19 47:9 48:5,10 65:21 65:25 66:1,2,3,12 66:17 67:8 68:24 69:9 72:10,11,22 90:6,25 92:12 94:13,22 95:4,19 95:19 101:13,23 101:24 102:1 103:5,7,10,10,20 109:7,8 115:11,17 115:20 116:3,6,23 116:25 118:2 126:9 159:20,20 165:8,16,17,20,21 165:24 166:4,8,9 166:12,21 167:1 169:6,10 176:7,25</p>	<p>177:4 178:17,18 184:9 185:3,7,12 191:8,15 194:23 195:4,6,9,12 198:7 199:16,24 201:25 202:5</p> <p>accessed 46:23 47:9 115:3 116:10</p> <p>accessible 42:6 43:1 126:18</p> <p>accessing 48:11 115:22 165:3</p> <p>accommodate 8:21</p> <p>accommodating 49:18</p> <p>accomplish 18:14</p> <p>account 11:12 24:11 43:12 101:10,11 101:14 102:4,22 199:21</p> <p>accounts 111:18 185:14,17 195:22 196:2,4,15 202:9</p> <p>accuracy 209:22</p> <p>accurate 209:8</p> <p>accurately 128:3</p> <p>achieve 43:20 44:2 170:10,11 199:15 202:25</p> <p>achieved 96:3 104:11</p> <p>acronym 86:9,13,15</p> <p>act 11:9 12:5 24:7 48:20 50:14,17,17 50:18</p> <p>Action 4:6 5:18,21</p> <p>actions 175:25</p> <p>active 151:17</p> <p>activities 196:23 197:10,12</p> <p>activity 39:11 99:6 149:20</p> <p>actual 11:12 13:7,10 39:4 67:11 86:10 86:12,12 133:5 144:14 156:21 178:2 182:16</p>	<p>acute 13:22</p> <p>ad 44:6 149:6 150:23 152:3 154:5 156:3 172:4 172:10,17</p> <p>adapter 90:1</p> <p>add 179:5 182:11</p> <p>added 200:24</p> <p>addition 12:11 28:6 37:5 39:13 42:18 104:3 125:1 136:13 158:18 179:5 184:19</p> <p>additional 26:23 83:2 105:7 111:21 116:17 136:10 138:11 164:11 167:2 184:7 188:13 202:11,16 205:7 207:23</p> <p>additionally 186:24</p> <p>address 15:13 24:15 24:16 38:20 58:25 59:15 82:18 90:5,6 90:6,7 92:15,16,19 92:20,23,24 93:2 94:10,14 97:14 98:19 114:3 126:4 135:21 142:22 144:1 173:22 189:5</p> <p>addressed 17:18 86:6,7 100:20 110:3</p> <p>addresses 12:11 16:4 22:11 26:1 42:4 59:3 139:8,9 139:17 141:17 160:19</p> <p>addressing 44:4 172:24</p> <p>adds 164:11</p> <p>adequate 21:4 41:24 76:10,12 165:2,7 167:13 168:7</p> <p>adequately 14:19 38:15 40:17 48:2,3</p>	<p>48:4,7 71:5 167:9 190:18 191:1</p> <p>adjourned 208:23</p> <p>admin 73:4</p> <p>administrative 2:13 37:6,11,14,17 40:15,19 101:23 101:24 102:1 159:19 169:6,10 191:8 196:14 198:7 199:21,24 202:5,9</p> <p>admission 204:3,6 205:16</p> <p>admit 5:24 56:19</p> <p>admitted 6:14,15 7:5 204:10 205:19 206:2,14</p> <p>adware 24:6</p> <p>affect 103:13 171:24</p> <p>afternoon 79:10,11 79:22 80:5 81:4,5 143:12 195:25 202:18 208:2</p> <p>agencies 87:4</p> <p>aging 59:10,11,14</p> <p>Aging_6.05.071.pdf 30:6</p> <p>agreed 62:11</p> <p>ahead 8:20 11:2 24:20 38:21 41:3 80:15 88:7 103:1 111:1 116:20 127:16 129:4,12 143:17 153:7 207:5</p> <p>Alain 3:5 5:9 9:13</p> <p>alert 149:19 194:1</p> <p>alerts 168:9</p> <p>algorithm 118:5</p> <p>Alison 154:14 155:5 155:17</p> <p>allegation 63:11</p> <p>allege 51:12</p> <p>alleged 51:18,25 52:24 53:11</p> <p>allegedly 58:17</p>	<p>62:24</p> <p>Allen 151:4,5,6</p> <p>Alliance 174:9</p> <p>allocate 82:12</p> <p>allow 39:11,19 100:24 112:23 120:4 138:24 141:23 206:4 207:8</p> <p>allowed 15:3 32:4 32:14 112:18 187:5 191:14 206:13</p> <p>allowing 92:5 141:2 199:20</p> <p>allows 15:24 25:4 37:13 55:14 95:18 101:4 118:24 138:19 140:5 141:8 159:22 162:22 195:12</p> <p>aloud 85:7 114:25 146:8</p> <p>alphabet 142:13,16 181:18,19 182:9</p> <p>alphabetic 179:16</p> <p>alphabets 177:8,16 181:20</p> <p>already-established 199:4</p> <p>America 2:1 24:4</p> <p>amount 24:13 27:19 43:14 102:14,15 149:22 166:1 169:13</p> <p>amounts 103:3 112:14 149:18</p> <p>analogy 18:3 54:7,8</p> <p>analysis 54:16 115:25 116:1 138:25 141:15 149:19 162:21</p> <p>anew 46:17</p> <p>angle 91:6</p> <p>animation 205:8</p> <p>announcement 194:2,3</p>
---	---	---	--	--

<p>anomaly 60:25</p> <p>anonymous 25:4,18 36:25 37:3 113:23 157:9 159:10,18 160:22 161:5</p> <p>answer 13:24 27:10 65:8 116:5 155:10 157:25</p> <p>anti 145:24</p> <p>anticipate 207:10</p> <p>anticipated 49:9</p> <p>antispyware 23:20</p> <p>antivirus 20:19 23:12,16,20 24:1 27:1,3,5,8 85:16 85:22 108:12 132:20,21 144:8 144:19,20 145:3,5 145:9,12,14,25 146:22 147:2,9,15 147:24 148:3,7,11 148:13,16,19 149:3 152:19 156:19,20,23 168:21</p> <p>antivirusware 64:3</p> <p>anybody 56:3 62:20 66:11</p> <p>anyway 67:19 208:2 208:4</p> <p>apologize 30:1 50:4 155:8</p> <p>apparently 74:13</p> <p>appearance 52:24 53:11</p> <p>appearances 3:1 4:1 5:5</p> <p>appears 51:7 53:8 84:8</p> <p>applauded 71:12</p> <p>application 93:12 93:14,15,17,22,25 94:1,3,21 95:6,9 97:10,15,17,19,23 98:1 113:13,15 115:6,7,10 118:15 118:16,18,20,22</p>	<p>118:24,25 119:5,7 119:18,20 120:3 144:20 168:21 169:4 198:19 199:7,13,13,22 200:1,3,6,14,16 201:11</p> <p>applications 82:13 93:20 100:4 105:15 115:8 118:10 119:3,4 122:8 140:16 146:23 148:8 173:22 188:25 189:4,6,9 191:2,4 191:5 194:6 197:20 199:11,25</p> <p>applied 65:14 173:20</p> <p>applies 43:11 170:4</p> <p>apply 167:16 203:4</p> <p>appreciate 50:5</p> <p>appreciates 90:16</p> <p>approach 6:6 80:19 90:10 110:13 128:18,18 136:11 136:15,16 140:21 149:4 153:6 172:3 172:4 181:8</p> <p>appropriate 10:20 10:25 12:3,21 21:17 26:24 31:9 38:24 45:22 46:5,8 47:16 48:10 71:25 72:13,14 79:11 84:21 85:2 102:3 102:21 103:13 104:15 110:8 124:12 136:25 137:19 144:11 161:24 176:20 203:4,14</p> <p>appropriately 48:9</p> <p>appropriateness 203:11</p> <p>approval 15:15 37:14,20 79:14,14</p>	<p>approximately 12:9 13:1 42:3,19 46:1 46:21 124:16 147:8 163:14 164:13</p> <p>APT 77:1,3 85:23 86:1,3 145:18,19 145:20,21 150:16 150:20,22,22 151:6,17</p> <p>arbitrary 159:22</p> <p>area 89:17,18,22 90:8,23 92:8,25 93:1 97:11 198:10</p> <p>areas 76:25 81:13 81:14 127:3</p> <p>argument 7:23 77:25</p> <p>Arizona 16:4</p> <p>arms 38:22 110:3 199:11</p> <p>arrange 207:24</p> <p>arrives 68:23 93:7,9</p> <p>arrows 92:10</p> <p>article 58:11 61:7</p> <p>asked 10:22 52:8 65:8,9 134:8 165:13 202:20</p> <p>asking 67:18 125:1</p> <p>asks 56:4</p> <p>aspect 51:6 152:10</p> <p>aspects 152:17</p> <p>assertion 157:25</p> <p>assess 14:19 84:21 137:17 138:14 141:5,13 144:6 168:23</p> <p>assessing 108:20 138:3 149:5</p> <p>assessment 21:2,6,7 21:17 23:2,12 26:24 27:10,15 28:16 36:6 85:17 133:22,23 135:19 137:1,6,7,8,11,12 137:17,19,21,24 138:1,5,7 139:10</p>	<p>140:1,19 141:4 142:21,22 143:25 144:1,11,25 145:4 149:11 151:22 152:22,24 156:15 156:17,24 158:15 158:17 161:24 162:4,15,18 173:13,13,15</p> <p>assessments 21:4</p> <p>assessor 46:9</p> <p>assisting 205:17</p> <p>associate 81:8</p> <p>associated 120:14 163:22 186:14</p> <p>assume 39:25 52:8 84:13 97:3,9 128:11</p> <p>assumed 88:14</p> <p>assumes 61:7</p> <p>assuming 107:24</p> <p>assumption 88:18 88:19,19 200:18</p> <p>Atlanta 82:2</p> <p>ATP 86:3</p> <p>attachment 197:5</p> <p>attachments 130:24</p> <p>attack 20:16 96:20 97:1,3 109:9 110:11 182:17</p> <p>attacker 97:3,7 110:12 140:9,11 159:22 177:3,15 177:22,25 179:18 181:1,2,6,19,24 183:25 184:8 185:7 191:8,14 193:9,10 195:9 198:6</p> <p>attacking 110:13</p> <p>attacks 27:1,6 159:23</p> <p>attempt 70:7,10 104:9</p> <p>attention 84:7 87:15 104:18 145:15 147:19 151:1,10</p>	<p>154:11 155:23 156:4 157:11 158:5 159:6 163:6 167:6 170:22 176:3 180:8 182:19 183:8 187:15,22 188:20 191:17 193:1</p> <p>attorneys 57:11</p> <p>audience 92:7</p> <p>audio 82:12,25</p> <p>audits 46:7</p> <p>August 156:10,10 156:12</p> <p>auth 184:6</p> <p>authenticate 48:3 101:13</p> <p>authenticated 122:10</p> <p>authenticating 184:7</p> <p>authentication 31:7 31:10 123:14 131:24,25 176:8 176:10,12,18,19 176:23,24 177:23 179:21,23 180:14 184:4,11,12,17,24 185:2 186:9 188:5</p> <p>authentication-rel... 31:10</p> <p>authority 50:15</p> <p>authorization 10:2 28:19 46:12</p> <p>authorized 30:14 42:13</p> <p>automated 28:14,15 86:16 156:16,24 190:8 200:8</p> <p>availability 126:6 126:16,17</p> <p>available 10:15,18 18:22 24:15 30:7 30:11 31:4 36:20 37:12 38:24 45:18 50:7 85:10,18,20 85:21,25 119:11</p>
---	--	---	--	---

<p>119:20,21 120:6,7 120:13 121:12 132:15,25 137:1,5 139:20 162:4,16 162:19 163:4 175:7,10 193:24 194:4,22 195:3 201:24 202:7,16 Avenue 2:15 3:10,19 4:7 average 105:17,22 189:12,15 avoid 11:22 14:11 48:24 avoidable 50:20 avoided 37:23 aware 14:8 29:2 65:14 80:24 awful 44:14</p> <hr/> <p style="text-align: center;">B</p> <hr/> <p>B 26:16 52:5 142:15 bachelor's 81:25 back 18:6 31:6,18 32:11 34:10 36:16 38:8 39:17 41:4 48:1 49:22 50:12 59:24 61:17 62:5 69:17,17 78:10 79:3 87:19 92:7 108:3 111:17 113:2 121:6 124:7 139:5 142:20 143:16,24 164:5 169:23 170:20 171:15 174:8 186:17 194:14 198:12 203:8 backed 38:6,10 103:18 background 62:5 88:23 89:14 124:7 135:11 backtrack 33:17 backup 22:14 41:8 41:16 103:21 117:8,16 191:6</p>	<p>198:4,5 backups 117:9,22 196:20,21 197:9 197:11 198:9 202:12 backwards 39:12,19 bad 116:8,9,12,14 Bailiff 201:16 balancing 125:21,21 bandwidth 82:12 83:2 banking 124:19 160:20 barrier 95:17 98:14 base 154:8 189:24 200:17,18 201:4 based 13:2 24:17 64:18 92:22 98:18 110:9 115:25 116:1 154:9 157:16,18,19,22 165:11 basic 17:24 19:9 131:23 174:16 175:21 basically 65:23 91:2 94:3,7,20 99:24 106:7 108:6 112:18 113:7 114:19 142:10 152:11 171:25 177:12 182:3 208:4 basis 44:2 60:24 65:14 68:5 76:25 204:11 began 21:25 25:25 41:7 157:20 begins 124:5 136:23 163:6 167:6 176:3 188:21 194:20 behalf 3:3,15 4:3 5:13 90:3 belief 209:11 believe 29:23 59:3 64:8 70:4 74:8,15 77:8 78:2 109:20</p>	<p>134:21 154:25 155:11 172:16 189:7 204:15 205:24 206:1,15 207:9 believed 76:10 bench 6:6 8:19 benefit 59:6 67:15 67:20 69:2 benefits 11:25 49:3 50:21 best 30:2 72:18 96:11 132:16,23 135:21 170:6 179:2 209:10 better 8:22 69:6 175:24 beyond 140:13 141:15,18 162:24 big 208:16 billing 15:23 16:2,3 29:9,20 32:22 33:1 33:19,22 34:4,6 37:16 38:8 42:7 45:14 59:10,20 60:9,22,23 66:1,3 66:3,22 114:14,16 114:17 118:19 153:1,3,10,14 154:1 182:25 196:16 198:19 199:20 200:2 billings 117:7,9 118:17 153:11,15 182:24 199:23,24 billings-related 117:10,11 billion 26:15 bin 73:23 binders 80:17,22 204:17 biometric 184:22 185:9 birth 12:12 114:5 160:20 192:24 bit 51:4 184:10 186:17</p>	<p>bits 142:11 blank 87:24 bleed 55:2 bleeding 69:11 blink 90:15 block 69:9 98:16,20 149:14 197:16,20 197:25 blocked 98:18 blood 54:4 55:2 67:12 77:22 blue 91:1 92:10 blurred 29:25 blurry 30:1 board 72:25 205:11 Boback 56:17 58:23 boggling 61:1 book 133:5,5 bottom 193:1 box 30:4,9 89:21 91:1,2 92:9,10 93:23 Boyle 77:4,5 breach 10:23 39:16 62:4 76:13 breaches 55:17 breadth 55:15 break 49:14,17,19 78:9 79:9,10,20,22 143:1,12,19 bricks-and-mortar 18:3 bridge 52:16 brief 157:25 briefing 8:23 157:14 briefly 8:18 118:23 142:8 bring 29:18 207:21 Brown 33:1 34:4,6,6 182:21,22,23,23 Brown's 183:4,9 browser 122:2 brute 182:17 brute-force 177:23 177:24 181:12,13 181:15,23 buffer 191:13 193:3</p>	<p>193:4 building 66:21 77:19 79:18,19 built 15:8 19:10 37:24 42:9 166:25 built-in 36:11 37:19 bulk 113:16 160:14 bullet 30:9 burden 105:7 164:11 Bureau 3:8 burning 74:10 business 16:16 28:21 29:4,17 35:19 47:3 60:7 65:13 69:14,15 70:8,12 71:9,10,11 71:12 72:16,16,17 72:18 76:8 77:19 77:22 97:25 105:6 115:19 118:11 123:15 163:17,19 164:15 198:1,9 businesses 174:10 174:10 175:13</p> <hr/> <p style="text-align: center;">C</p> <hr/> <p>C 5:1 52:5 142:15 209:1,1,19,19 Cadillac 71:22 California 58:25 63:13 call 5:3 16:5 17:2,22 69:16 78:11 80:3,7 98:21 141:14 162:23 201:17 205:1 207:8,14 called 15:22 19:10 21:19 26:19 30:6 43:16 60:22 77:2 80:13 90:5 95:15 114:16,17 119:3 138:16 139:11 171:8 calling 207:7,19 calls 59:20 camera 1:12 9:4</p>
--	---	---	---	---

cancer 17:7 67:13 69:4 72:17	certain 38:7 65:5	57:7,10,13 58:16	check 24:19 147:23 200:21 201:2	190:14
capabilities 55:11 62:11	certainly 6:7 51:9	59:5,24 60:13,17	checked 73:10	collaboration 57:16
capability 149:22 150:4,7,11,12	CERTIFY 209:7,21	60:19 61:14 63:10	chief 2:13 77:5	collect 56:4 59:21 60:21 144:17
capable 23:22	cetera 39:3	64:13 66:6,11,19	choose 46:9 181:2	collected 12:7 42:23 59:12 114:19 160:13
capacities 55:11	chance 97:4,7 110:12,15 111:6,6 186:6	67:3,7,24 69:13,22 70:1,13,18,21 71:8 71:14 73:3,15,19 73:24 74:5,15,22 75:2,7,17,20,23 76:18,22 77:9,24 78:8 79:3 80:3,8 80:15,21 83:16,19 83:24 84:2,11,17 86:9 87:22 88:7 90:12,14,17 91:3,6 91:9,15,18,24 92:2 92:5 94:9,12,15 110:18,21 111:1 111:12,23 115:15 115:24 116:7,12 116:16,19 121:24 122:15,23 123:8 123:19,23 127:14 127:16 128:20 129:4,10,12 134:6 134:13,17 142:23 143:2,6,11,16,20 153:7,23 154:22 155:6,9,12 157:12 157:23 201:12,16 201:18 204:2,7,23 205:3,10,20 206:1 206:7,10,13,21,25 207:2,5 208:1,8,12 208:16,21	CID 154:20,25	College 57:2,4,18,25 57:25 62:13,15
capture 138:25 141:23 149:18 162:22	chances 183:25	99:12,14,17 91:3,6 91:9,15,18,24 92:2 92:5 94:9,12,15 110:18,21 111:1 111:12,23 115:15 115:24 116:7,12 116:16,19 121:24 122:15,23 123:8 123:19,23 127:14 127:16 128:20 129:4,10,12 134:6 134:13,17 142:23 143:2,6,11,16,20 153:7,23 154:22 155:6,9,12 157:12 157:23 201:12,16 201:18 204:2,7,23 205:3,10,20 206:1 206:7,10,13,21,25 207:2,5 208:1,8,12 208:16,21	circumstances 11:1 11:12 24:10,11,18 45:22 46:5	column 35:12
capable 23:22	change 15:6 20:17 25:17 37:18 39:3 40:20 66:7,9 67:8 113:7 126:13,13 126:15 152:11,12 178:19 181:25 197:2 201:5,6,7	90:12,14,17 91:3,6 91:9,15,18,24 92:2 92:5 94:9,12,15 110:18,21 111:1 111:12,23 115:15 115:24 116:7,12 116:16,19 121:24 122:15,23 123:8 123:19,23 127:14 127:16 128:20 129:4,10,12 134:6 134:13,17 142:23 143:2,6,11,16,20 153:7,23 154:22 155:6,9,12 157:12 157:23 201:12,16 201:18 204:2,7,23 205:3,10,20 206:1 206:7,10,13,21,25 207:2,5 208:1,8,12 208:16,21	circumvent 199:14	combination 181:16 182:4
capacities 55:11	changed 132:6 178:14 180:6 200:25	90:12,14,17 91:3,6 91:9,15,18,24 92:2 92:5 94:9,12,15 110:18,21 111:1 111:12,23 115:15 115:24 116:7,12 116:16,19 121:24 122:15,23 123:8 123:19,23 127:14 127:16 128:20 129:4,10,12 134:6 134:13,17 142:23 143:2,6,11,16,20 153:7,23 154:22 155:6,9,12 157:12 157:23 201:12,16 201:18 204:2,7,23 205:3,10,20 206:1 206:7,10,13,21,25 207:2,5 208:1,8,12 208:16,21	cite 19:15	combined 114:9
capture 138:25 141:23 149:18 162:22	changes 35:13 113:8 137:15,16 169:15 201:9	90:12,14,17 91:3,6 91:9,15,18,24 92:2 92:5 94:9,12,15 110:18,21 111:1 111:12,23 115:15 115:24 116:7,12 116:16,19 121:24 122:15,23 123:8 123:19,23 127:14 127:16 128:20 129:4,10,12 134:6 134:13,17 142:23 143:2,6,11,16,20 153:7,23 154:22 155:6,9,12 157:12 157:23 201:12,16 201:18 204:2,7,23 205:3,10,20 206:1 206:7,10,13,21,25 207:2,5 208:1,8,12 208:16,21	cited 133:21 157:25	come 52:8 64:17 78:10 109:14 123:9 142:20 143:24 175:2
card 89:24,25 90:1,4 90:5 124:19 160:21	changing 33:7 38:2 169:3 178:22 196:9	90:12,14,17 91:3,6 91:9,15,18,24 92:2 92:5 94:9,12,15 110:18,21 111:1 111:12,23 115:15 115:24 116:7,12 116:16,19 121:24 122:15,23 123:8 123:19,23 127:14 127:16 128:20 129:4,10,12 134:6 134:13,17 142:23 143:2,6,11,16,20 153:7,23 154:22 155:6,9,12 157:12 157:23 201:12,16 201:18 204:2,7,23 205:3,10,20 206:1 206:7,10,13,21,25 207:2,5 208:1,8,12 208:16,21	claim 33:2,3 34:7 184:13	combat 199:19
care 18:1	channel 82:23 83:5 89:4 161:13 199:4	90:12,14,17 91:3,6 91:9,15,18,24 92:2 92:5 94:9,12,15 110:18,21 111:1 111:12,23 115:15 115:24 116:7,12 116:16,19 121:24 122:15,23 123:8 123:19,23 127:14 127:16 128:20 129:4,10,12 134:6 134:13,17 142:23 143:2,6,11,16,20 153:7,23 154:22 155:6,9,12 157:12 157:23 201:12,16 201:18 204:2,7,23 205:3,10,20 206:1 206:7,10,13,21,25 207:2,5 208:1,8,12 208:16,21	clarify 99:17 156:22	combinations 181:16 182:4
careful 112:23	CHAPPELL 2:12 5:3,11,22 6:5,9,13 6:17,20 7:1,6,10 7:13 8:3,5,9,14,16 8:22 9:1,10 10:4 10:12,21 11:2 13:6 13:23 14:4,8 16:8 16:13,21,24 18:17 19:2,5,14,20,22 20:1 23:5 24:2,20 25:19 26:2,5,15 28:8 29:24 30:14 30:22 31:18 32:1,6 32:10 33:13,25 34:3,9 35:5,8,12 35:22 36:1 39:1,21 40:8 41:1 47:1 49:5,8,13,16,22,25 50:6,9 51:15 53:14 54:7,15,23 55:16 55:20,23 56:14,21	90:12,14,17 91:3,6 91:9,15,18,24 92:2 92:5 94:9,12,15 110:18,21 111:1 111:12,23 115:15 115:24 116:7,12 116:16,19 121:24 122:15,23 123:8 123:19,23 127:14 127:16 128:20 129:4,10,12 134:6 134:13,17 142:23 143:2,6,11,16,20 153:7,23 154:22 155:6,9,12 157:12 157:23 201:12,16 201:18 204:2,7,23 205:3,10,20 206:1 206:7,10,13,21,25 207:2,5 208:1,8,12 208:16,21	Clay 28:25 123:25	comes 53:25 57:21 84:18 102:1 108:23
Carnegie-Mellon 174:23	channel 82:23 83:5 89:4 161:13 199:4	90:12,14,17 91:3,6 91:9,15,18,24 92:2 92:5 94:9,12,15 110:18,21 111:1 111:12,23 115:15 115:24 116:7,12 116:16,19 121:24 122:15,23 123:8 123:19,23 127:14 127:16 128:20 129:4,10,12 134:6 134:13,17 142:23 143:2,6,11,16,20 153:7,23 154:22 155:6,9,12 157:12 157:23 201:12,16 201:18 204:2,7,23 205:3,10,20 206:1 206:7,10,13,21,25 207:2,5 208:1,8,12 208:16,21	clean 205:1	coming 8:19 69:9 123:11 162:23
case 9:14 13:7,15 17:16 20:4 40:4 50:10 51:5,5,7 54:24,25 63:10,24 65:7,16 71:9 72:4 83:21 145:23 207:8,9,14,20 209:4	CHAPPELL 2:12 5:3,11,22 6:5,9,13 6:17,20 7:1,6,10 7:13 8:3,5,9,14,16 8:22 9:1,10 10:4 10:12,21 11:2 13:6 13:23 14:4,8 16:8 16:13,21,24 18:17 19:2,5,14,20,22 20:1 23:5 24:2,20 25:19 26:2,5,15 28:8 29:24 30:14 30:22 31:18 32:1,6 32:10 33:13,25 34:3,9 35:5,8,12 35:22 36:1 39:1,21 40:8 41:1 47:1 49:5,8,13,16,22,25 50:6,9 51:15 53:14 54:7,15,23 55:16 55:20,23 56:14,21	90:12,14,17 91:3,6 91:9,15,18,24 92:2 92:5 94:9,12,15 110:18,21 111:1 111:12,23 115:15 115:24 116:7,12 116:16,19 121:24 122:15,23 123:8 123:19,23 127:14 127:16 128:20 129:4,10,12 134:6 134:13,17 142:23 143:2,6,11,16,20 153:7,23 154:22 155:6,9,12 157:12 157:23 201:12,16 201:18 204:2,7,23 205:3,10,20 206:1 206:7,10,13,21,25 207:2,5 208:1,8,12 208:16,21	clear 75:25 84:11 157:24	commission 1:1 2:1 2:14 3:3,7 21:24 50:14,15 209:10
case-by-case 65:14	chapter 133:5	90:12,14,17 91:3,6 91:9,15,18,24 92:2 92:5 94:9,12,15 110:18,21 111:1 111:12,23 115:15 115:24 116:7,12 116:16,19 121:24 122:15,23 123:8 123:19,23 127:14 127:16 128:20 129:4,10,12 134:6 134:13,17 142:23 143:2,6,11,16,20 153:7,23 154:22 155:6,9,12 157:12 157:23 201:12,16 201:18 204:2,7,23 205:3,10,20 206:1 206:7,10,13,21,25 207:2,5 208:1,8,12 208:16,21	clearly 71:3	commission's 25:24 41:7
cases 13:11	characterize 185:18	90:12,14,17 91:3,6 91:9,15,18,24 92:2 92:5 94:9,12,15 110:18,21 111:1 111:12,23 115:15 115:24 116:7,12 116:16,19 121:24 122:15,23 123:8 123:19,23 127:14 127:16 128:20 129:4,10,12 134:6 134:13,17 142:23 143:2,6,11,16,20 153:7,23 154:22 155:6,9,12 157:12 157:23 201:12,16 201:18 204:2,7,23 205:3,10,20 206:1 206:7,10,13,21,25 207:2,5 208:1,8,12 208:16,21	clerks 80:20	common 15:1 96:22 101:21 176:7,14 188:5
castle 18:3 48:17	characters 142:17 177:7,9,10,19,20 178:4 181:10,10 181:21,24,25 182:4,8 183:24	90:12,14,17 91:3,6 91:9,15,18,24 92:2 92:5 94:9,12,15 110:18,21 111:1 111:12,23 115:15 115:24 116:7,12 116:16,19 121:24 122:15,23 123:8 123:19,23 127:14 127:16 128:20 129:4,10,12 134:6 134:13,17 142:23 143:2,6,11,16,20 153:7,23 154:22 155:6,9,12 157:12 157:23 201:12,16 201:18 204:2,7,23 205:3,10,20 206:1 206:7,10,13,21,25 207:2,5 208:1,8,12 208:16,21	client 55:25 59:5 60:2 68:21 69:14 76:18 82:22 93:18 94:4 115:10,11,12	commonly 14:24 21:8 22:22 131:25
category 37:11	charge 45:18 56:24 77:7	90:12,14,17 91:3,6 91:9,15,18,24 92:2 92:5 94:9,12,15 110:18,21 111:1 111:12,23 115:15 115:24 116:7,12 116:16,19 121:24 122:15,23 123:8 123:19,23 127:14 127:16 128:20 129:4,10,12 134:6 134:13,17 142:23 143:2,6,11,16,20 153:7,23 154:22 155:6,9,12 157:12 157:23 201:12,16 201:18 204:2,7,23 205:3,10,20 206:1 206:7,10,13,21,25 207:2,5 208:1,8,12 208:16,21	close 14:15 20:12 21:21 94:23 106:7 141:3	communicate 90:2 140:16,23
causal 52:23 53:10	charged 26:8	90:12,14,17 91:3,6 91:9,15,18,24 92:2 92:5 94:9,12,15 110:18,21 111:1 111:12,23 115:15 115:24 116:7,12 116:16,19 121:24 122:15,23 123:8 123:19,23 127:14 127:16 128:20 129:4,10,12 134:6 134:13,17 142:23 143:2,6,11,16,20 153:7,23 154:22 155:6,9,12 157:12 157:23 201:12,16 201:18 204:2,7,23 205:3,10,20 206:1 206:7,10,13,21,25 207:2,5 208:1,8,12 208:16,21	closed 21:9 41:13 95:13,14,14	communication 197:19 199:4
cause 4:6 5:18,21 11:17 14:7 17:11 48:21 50:19 63:9 63:23 209:9	chart 206:17	90:12,14,17 91:3,6 91:9,15,18,24 92:2 92:5 94:9,12,15 110:18,21 111:1 111:12,23 115:15 115:24 116:7,12 116:16,19 121:24 122:15,23 123:8 123:19,23 127:14 127:16 128:20 129:4,10,12 134:6 134:13,17 142:23 143:2,6,11,16,20 153:7,23 154:22 155:6,9,12 157:12 157:23 201:12,16 201:18 204:2,7,23 205:3,10,20 206:1 206:7,10,13,21,25 207:2,5 208:1,8,12 208:16,21	closing 7:23 8:24 95:11 135:17	communications 82:23 83:5 89:4
caused 11:17 14:7 48:21 71:8	chasm 52:17	90:12,14,17 91:3,6 91:9,15,18,24 92:2 92:5 94:9,12,15 110:18,21 111:1 111:12,23 115:15 115:24 116:7,12 116:16,19 121:24 122:15,23 123:8 123:19,23 127:14 127:16 128:20 129:4,10,12 134:6 134:13,17 142:23 143:2,6,11,16,20 153:7,23 154:22 155:6,9,12 157:12 157:23 201:12,16 201:18 204:2,7,23 205:3,10,20 206:1 206:7,10,13,21,25 207:2,5 208:1,8,12 208:16,21	cloud 98:11	community 65:13 67:18 193:19
causes 17:10 50:18		90:12,14,17 91:3,6 91:9,15,18,24 92:2 92:5 94:9,12,15 110:18,21 111:1 111:12,23 115:15 115:24 116:7,12 116:16,19 121:24 122:15,23 123:8 123:19,23 127:14 127:16 128:20 129:4,10,12 134:6 134:13,17 142:23 143:2,6,11,16,20 153:7,23 154:22 155:6,9,12 157:12 157:23 201:12,16 201:18 204:2,7,23 205:3,10,20 206:1 206:7,10,13,21,25 207:2,5 208:1,8,12 208:16,21	co-counsel 5:20 90:9	companies 21:11,20 45:20 67:25 72:11 72:13 190:11
CDX 204:4,6,14 205:1,4		90:12,14,17 91:3,6 91:9,15,18,24 92:2 92:5 94:9,12,15 110:18,21 111:1 111:12,23 115:15 115:24 116:7,12 116:16,19 121:24 122:15,23 123:8 123:19,23 127:14 127:16 128:20 129:4,10,12 134:6 134:13,17 142:23 143:2,6,11,16,20 153:7,23 154:22 155:6,9,12 157:12 157:23 201:12,16 201:18 204:2,7,23 205:3,10,20 206:1 206:7,10,13,21,25 207:2,5 208:1,8,12 208:16,21	coarse-grained 101:2	company 10:18 24:3
cease 69:22		90:12,14,17 91:3,6 91:9,15,18,24 92:2 92:5 94:9,12,15 110:18,21 111:1 111:12,23 115:15 115:24 116:7,12 116:16,19 121:24 122:15,23 123:8 123:19,23 127:14 127:16 128:20 129:4,10,12 134:6 134:13,17 142:23 143:2,6,11,16,20 153:7,23 154:22 155:6,9,12 157:12 157:23 201:12,16 201:18 204:2,7,23 205:3,10,20 206:1 206:7,10,13,21,25 207:2,5 208:1,8,12 208:16,21	code 105:17,21 189:14,16 191:14 193:10,11	
ceased 70:22		90:12,14,17 91:3,6 91:9,15,18,24 92:2 92:5 94:9,12,15 110:18,21 111:1 111:12,23 115:15 115:24 116:7,12 116:16,19 121:24 122:15,23 123:8 123:19,23 127:14 127:16 128:20 129:4,10,12 134:6 134:13,17 142:23 143:2,6,11,16,20 153:7,23 154:22 155:6,9,12 157:12 157:23 201:12,16 201:18 204:2,7,23 205:3,10,20 206:1 206:7,10,13,21,25 207:2,5 208:1,8,12 208:16,21	codes 17:5,6	

<p>25:22 26:2,8,12 34:2,24,25 36:13 39:19 40:16,18 41:9,12 42:22,23 42:25 43:2,18,24 44:6 45:3,25 46:6 46:9 47:10,17 48:15 55:8,16,20 55:25 58:16 77:2 86:10,10 158:10 181:3 191:23 202:24 company's 10:3,9 11:3,6 12:2 14:21 32:3 40:19 44:17 44:19 75:4 102:4 203:1,3 compare 89:11 comparing 55:10 201:2 compete 71:13 competition 11:25 49:3 50:22 complained 27:23 28:4 complaint 5:8 6:2 9:13 12:19 13:8 17:13 28:7,25 45:24 50:3 59:3 80:6 84:20 88:20 123:24 125:3,8 136:24 163:8 165:1 167:8 176:5 188:23 194:21 207:7 complaints 71:20 complete 146:10 169:11 completed 146:11 completely 47:2 completion 190:10 190:14,15 complex 76:25 complexity 24:12 43:13 complies 153:20 component 82:14</p>	<p>components 120:20 120:23 composed 106:15 composition 89:2 comprehensive 43:6 43:16,23 44:22 45:16 46:4 48:14 102:10 106:14,18 106:19,21 107:6 107:22,22 108:1 125:10,15,17,19 126:3,21,23 129:18,25 131:15 131:17 132:10 133:18,23 135:12 135:25 168:2 170:4 172:1 compromise 15:16 105:9 122:20 152:12 159:3,4 164:7 166:6,11 169:18 183:25 186:6,25 187:4 196:6,7,12 203:5 compromised 122:21 184:3 185:7,11 computer 15:23 16:3 17:14 18:2,9 23:18 28:4,8,24 29:9,11,15,20 30:11,21 31:1 33:4 33:20,21 37:16 38:21 43:10 45:13 46:22 61:4 67:8 73:9,10,12 74:8 75:16 76:6 81:9,16 81:24,25 82:2,3,5 84:22 86:4 90:2,7 92:18,19 93:8,10 93:10,16 95:3,5,7 99:21 101:23 102:2 103:24 105:17 109:4,6 117:8,10 118:17 118:19 119:16,17 121:13 122:13,13</p>	<p>122:16,25,25 123:10,12,14 149:1 152:10,14 152:18 153:1,3,10 153:12,14,16 154:1 159:19 160:2,3,7,7,8,9 173:1 174:13,22 183:1,3 184:15 192:1,10,12,13,14 193:13 196:17 197:7,8 198:19 199:1,3,22 200:2 200:17,20,22 201:2 computer's 90:2 computers 15:4,15 15:25 16:1 27:8,9 27:12,23 33:9,12 34:10,12,16,22,24 34:24 35:5,19,22 35:24 36:9 37:7,12 37:19,25 38:7 40:15,21 45:9 68:4 76:7 89:2,22 90:23 92:17,22,24 97:11 99:24 115:14 116:22 117:4 118:11 121:10,14 123:6 148:20 196:24 computing 81:11,12 87:5 94:22 136:9 175:3 176:1 concealing 74:14 concept 11:11 18:9 68:3 concepts 19:10 concern 7:15 concerning 71:20 76:14 concerns 57:15 conclude 84:25 124:10 125:13 126:20 129:17 131:14 137:3 144:10 146:25</p>	<p>148:10 150:19 151:16,21,25 156:1 163:12,16 165:6 167:12 170:14 171:8 176:17 179:20 180:16 183:11 189:2 195:1 197:22 207:17 concluded 85:1 124:11 125:14 126:22 129:23 131:16 137:4 145:2 147:1 148:11 151:23 152:1,7 156:2 163:13,18 164:14 165:7 167:13 170:16 171:11 176:19 179:22 180:17 183:12 189:3 190:17 191:1 195:2 197:24 207:20 conclusion 85:3 86:19 124:8 131:18,19 147:4 154:8,9,16 163:20 165:10,11 167:16 171:1,20 180:13 198:2,3 203:8,10 203:13,16 conclusions 7:24 112:3 125:2 148:7 148:15 150:14 155:20 157:22 183:5 concrete 12:22 concur 55:20 conduct 14:23 21:4 22:7 25:25 35:3 47:13 151:19 163:17,19 164:15 198:1 conducted 25:13 28:3 57:18 154:5 157:3,17 158:24</p>	<p>162:13 conducting 25:8 35:16 confidentiality 126:5,7,8 136:5 175:12 configuration 100:15 152:16,17 197:22 configurations 152:15 169:3 configured 37:2 65:24 141:1 170:10 197:15,25 198:18 199:5 confirm 53:9 confront 23:23 Congress 55:12 connect 13:12 20:20 83:20 94:4 98:13 112:12 122:2 connected 69:19 89:3,23 92:18 112:11 connecting 51:18 connection 52:23 53:10 83:13 90:11 98:21,24 100:19 101:2 139:9 148:6 154:16 155:19 158:23 170:25 178:4 199:2 connections 140:24 consent 207:14 consequence 10:8 159:25 160:1 182:13,15 consequences 97:21 132:18,20 169:15 175:25 196:9 consider 14:16 45:20 65:8 86:18 103:21 112:4 146:21 155:19 170:25 171:19 180:12 182:9,9 183:4,18</p>
---	--	---	--	---

<p>consideration 102:12,17 104:1 178:8</p> <p>considered 65:16 86:20,22,24 87:9 88:4 137:13</p> <p>consistent 7:21 58:23 67:17</p> <p>constitute 20:8</p> <p>constitutes 182:7</p> <p>constraints 207:15 207:17</p> <p>consult 75:7 160:24 162:11 193:20</p> <p>consulting 132:14</p> <p>consumer 3:8 11:14 22:18 34:18 35:1 36:8 38:5 51:14 69:3 124:16 160:18 174:19 190:3 192:22</p> <p>consumers 9:19 10:1 11:20,25 12:5 12:8,10,23 13:1,3 13:16,22 14:11,12 14:12 16:7 17:4 22:10 24:23 42:3 42:20,21 46:2,11 46:13,22 47:7,18 47:23 48:23 49:3 50:19,20,22 70:2 88:13,15 124:18 163:14 164:9 189:18,21 190:13</p> <p>contact 168:22</p> <p>contain 102:14 121:15 129:19</p> <p>contained 16:6 38:6 92:16 192:22 209:7</p> <p>containing 29:5 130:23</p> <p>contains 59:23 133:7 140:8,10 181:5</p> <p>contend 117:19</p> <p>content 121:17</p>	<p>context 66:24 137:13,15,16</p> <p>continue 91:22 101:6 128:19</p> <p>continued 4:1 41:17</p> <p>continues 71:3</p> <p>contract 55:24 57:5 57:6,15</p> <p>contractors 44:19</p> <p>contracts 56:10,20</p> <p>control 37:11,12,14 37:17 40:15,20 42:8 90:6 91:1 92:12 94:13 101:25 112:25 121:17 159:5,21 160:7 165:18,20 169:11,21 191:8 193:12 196:5</p> <p>controls 30:18,19 37:6 41:22,24 42:11,17 48:10</p> <p>copied 113:20</p> <p>copies 5:25 6:2,2,3</p> <p>copy 22:14 80:24,25</p> <p>core 43:19</p> <p>corporate 130:20,21 148:4</p> <p>corporation 2:4</p> <p>correct 6:12 14:3 50:7 55:19 67:6 73:6,6 87:10 110:19 131:4 154:6 155:3,13 156:11 157:4,20 157:21 158:1 172:19 207:12</p> <p>corrected 11:24 49:2 124:23 155:1 161:23 188:4 194:5 201:23 203:22</p> <p>correctly 10:12 28:5 53:15</p> <p>corresponding 32:25 93:12</p> <p>corresponds 92:20</p>	<p>cost 11:24 22:24,24 24:15 26:6,11 36:13 37:23 38:25 42:17 45:16 49:2 124:24 132:11 136:1,14,20,21 161:25 162:13,17 163:3 164:22,23 166:14,22,23 167:3 174:2,11,14 175:17 188:6,12 188:13,15,16,18 188:19 194:7,12 194:13 202:1,8,10 202:11,12 203:23</p> <p>Costa 16:5 74:25</p> <p>costly 102:18</p> <p>costs 11:14</p> <p>Council 133:4,9,10</p> <p>counsel 5:8,9,18 6:2 9:13 13:8 45:24 50:3 51:22 59:4 80:6,18 84:20 88:20 125:3,8 136:24 163:8 165:1 167:8 176:5 188:23 194:21 207:7,13</p> <p>counsel's 12:19 17:13 28:25 123:25</p> <p>counters 20:11</p> <p>countervailing 11:24 49:2 50:21 67:15 69:2</p> <p>country 74:23 79:13</p> <p>couple 113:11 143:5 183:22 185:20</p> <p>course 60:7</p> <p>court 2:19 6:3 9:12 12:1 49:12 50:2,23 51:17,20,24 52:1 54:19 63:16 65:17 79:24 80:9 81:7,23 82:8,20 85:13,19 86:14 96:25 104:25 112:2</p>	<p>117:6 124:6 125:18 130:5 131:21 139:3 146:8 159:15 162:20 172:12,21 176:10 189:8 190:17,25 200:12 207:24,24</p> <p>court's 50:5</p> <p>cover 43:23 85:3 192:1 203:16</p> <p>coverage 189:25 190:9</p> <p>covered 135:7</p> <p>covers 142:11</p> <p>crack 181:6</p> <p>create 135:25 172:1 175:2 178:12 179:6,15 200:18</p> <p>created 34:2 39:15 40:3 45:15 59:10 59:16,18 60:9,21 61:4 174:24</p> <p>creates 112:21 168:14 177:14 200:17,19</p> <p>creating 37:8 72:18 106:18 133:18</p> <p>credential 186:15</p> <p>credentials 33:6,23</p> <p>credit 124:19 160:20</p> <p>critical 147:3</p> <p>cross 1:8 206:19</p> <p>crossed 74:19</p> <p>crowd 91:10,20</p> <p>cryptographic 179:7,10,11</p> <p>cubicles 66:22</p> <p>current 107:12 137:9 138:10 201:2,3</p> <p>currently 69:21 70:11</p> <p>cursory 28:6</p> <p>customer 24:4 60:2</p> <p>cut 53:21,24 54:3,3</p>	<p>54:19,21,24 55:1 67:20,22 71:24</p> <p>cuts 54:5</p> <p>cutting 71:11</p> <p>CV 84:13</p> <p>CX 1:13 24:24 25:12 25:19 26:10 36:6 84:7,9,10 87:15,17 87:18,20 117:14 117:15,16 130:13 131:7,7,8,8,9,9 145:16,17,18 146:6 147:20 151:1,2,3 154:11 154:12 155:4,16 155:17,19 157:11 158:5,6,7,22 159:7 159:9 161:1,2 170:20 171:16 180:8,9,10,12,16 182:19,20,21 187:16,17,18 191:17,18,19,21 192:1,6,7 193:2 194:15 198:12</p> <p>CXD 89:7,8,9,11,14 90:11 93:22 98:3 100:9 101:7 127:12,20,21,23 128:3,5,7,24 153:6 153:9,19 204:14 204:18</p> <p>CYA 75:13</p> <p>cyber 57:16,16</p> <p>cyberspace 32:2</p>
<p>D</p>				
<p>D 1:2 2:12 3:17 5:1 52:5 142:15 209:19</p> <p>D.C 2:16 3:11,21 4:9</p> <p>daily 60:16,18,24 76:25</p> <p>dangers 34:19 69:20</p> <p>Dartmouth 57:2,4 57:18,25,25 62:8,9 62:10,13,15</p>				

Dartmouth's 62:11	68:15	106:13 168:2	97:1,2,13 98:4,7	193:23 200:9,10
data 51:13,19 52:4	day 52:21 59:7,19	definition 122:23	98:25 99:8 100:17	Detecting 195:12
52:24 53:4,8 58:7	59:22 60:20,21	definitions 27:5	101:7,9 102:4,9,22	detection 27:1 36:17
58:11 62:3,3 65:12	61:14,15,19,24	146:2,14 147:5,8	103:13 104:23	39:14 72:17 99:2,3
67:19,22 71:2	62:2 79:15,24	147:24 148:1	110:8 111:4	99:4 108:24 145:9
72:18 81:14,15	103:20 147:7	definitively 116:5	137:20 169:24	149:16,23 150:4
82:25 83:3,9,11	days 27:21 79:12	degree 81:25 82:2	170:1,5 172:2	150:12
90:22,24 92:14,15	144:17 207:22	delay 50:4	185:3 195:7,10	determine 39:8
92:22 93:3,7,9,11	deal 72:7 79:4	delete 164:1	199:8,10	40:12 116:2 137:9
93:12 94:4,5,6,8	208:17	deleted 164:13	describe 13:2 76:21	140:6,14,25 141:9
95:6,8,8,9,19	dealing 51:6 182:10	deleting 42:25	77:15 81:22 82:8	152:10 163:1
101:13 102:14	deals 177:12	164:21	82:20 83:12 98:3	166:18 178:1
112:14,16,18,20	decide 14:12 140:18	demographic	99:15 112:2 139:3	181:7,16 182:16
113:14 115:10,11	140:20	114:10	159:15	193:21 199:13,14
117:16 118:1,5,7	decision 83:7,10	demonstrated 10:19	describing 98:2	200:23 201:10
124:9,13 125:2,4	declare 50:16	demonstrative	description 116:10	determined 178:15
126:10,14,18	decreases 185:11	127:14 204:9,11	205:7	determining 178:21
129:20 130:8,10	deep 141:15 162:23	205:13,16,21,23	descriptions 86:6	develop 125:14
130:11,23 138:25	deface 129:4	206:3,6,9,11,14	designate 15:24	developed 125:9,20
138:25 139:1	default 29:13 41:8	department 44:15	29:6 119:25 120:4	developers 199:14
141:10,12,13,18	191:10	59:20 60:23,23	designated 16:2	developing 45:20
141:19,22,23,24	defects 31:23	66:23 72:24 76:21	29:11,14 99:10	126:25
141:25 142:2,10	defended 18:4	department's 32:22	designating 99:11	device 91:1 92:10,12
142:14 144:17	defense 17:22 18:2,6	depends 24:10 75:9	119:22	92:17 93:21 95:14
147:10 159:4	18:8,14,17 19:11	deploy 97:13 99:9	designations 59:17	113:1
160:3,7,13,18	19:13,19 20:9,11	101:12 104:9	designed 82:10,18	devices 40:24 98:12
161:13,14 162:21	20:15,21 24:9 43:9	108:7 199:17	83:13 111:13	99:18,20,21 100:7
162:22,24,25,25	46:18 47:24 48:19	deployed 96:16,18	desire 8:5	196:22 197:1,11
164:7 165:8 166:5	96:12,13,14,22,25	96:19 98:24	desktop 66:18	diagnosis 67:13
166:21 167:1	97:2,12 98:4,7,25	104:23 105:25	desktops 67:2,25	diagram 205:5
168:6 190:12	99:8 100:17 101:7	107:2 111:5	despite 15:1	dictate 53:16
191:15 199:3	101:9 102:3,9,21	145:21	destination 93:7,9	dictionary 177:18
203:15	103:13 104:23	deploying 96:11	93:10 95:5,7	180:1 181:5,7
database 42:18 56:5	110:8 111:3	104:14 108:17	destined 93:13	Diego 16:4 58:25
60:9 68:15,17	137:20 169:24	110:14 111:9	100:25	differ 136:10
69:18 70:1 100:4	170:1,5 172:2	depose 73:20	destroyed 59:18	different 20:13
164:19,25 180:10	185:3 195:7,10	deposition 58:24	186:20	21:13,15 100:7
databases 25:15	199:8,10	59:1,17 75:1 85:16	detail 19:19 88:21	113:12 114:21
42:3,6 43:1 87:6	defenses 18:5	151:3,11 154:10	113:24 160:25	131:10 139:14,21
date 114:5 146:19	deficient 51:18	154:13,20 187:23	details 86:8	139:25 140:2
146:20 156:9	define 96:4 106:15	depositions 58:5	detect 36:21 48:5	142:9 161:22
160:20 190:11	109:25 125:24,24	depth 17:22 18:2,8	99:5 108:13	182:3 184:6 185:5
192:24 209:5	133:12 168:4	18:15,17 19:11,13	126:15 144:22	191:20
dated 146:4 147:20	defined 104:13	19:19 20:9,11,15	147:10,16 153:2	difficult 121:5,7
209:13	106:24 109:17	20:21 24:10 43:10	194:23 195:3,5,11	177:22
dates 12:11 127:25	defines 94:8 181:22	46:19 47:24 48:19	200:6,14 201:4,24	digital 62:18 121:16
Daugherty 5:15	defining 102:10	96:12,13,14,22	detected 154:2	123:19,21

<p>Dinsmore 3:18 direct 1:8 81:2 84:6 87:19 104:17 114:23 117:13 123:5 124:4 130:13 150:25 151:10 156:4 157:10 158:4 159:6 163:5 167:5 176:2 180:7 182:18 191:16 direct-examine 208:14 directly 32:6,7 58:6 112:11 directory 159:11,17 159:18,19,20 disable 15:14 25:18 disabling 169:16 disclosed 10:1 12:16 28:18 46:12 disclosing 10:17 88:17 disclosure 11:13 12:25 15:19 17:10 37:10 discontinued 190:23 discover 45:13 discovered 27:6 75:18 77:12 190:3 discovering 140:12 discuss 88:21 195:17 discussed 8:18 85:24 148:13 162:16 178:3 193:4 203:6 204:5 discusses 144:15 187:10 195:18,21 196:20 discussion 144:14 discussions 207:6 disease 69:5 diseases 17:8 disks 113:8 dismissed 34:1 47:11</p>	<p>dispense 6:25 disputed 63:12 dissertation 82:9,10 82:15 83:17 dissolve 47:2 dissolving 46:16 47:5,6 distinction 23:13 distribute 160:3,8 distribution 94:4 159:24 160:5 diverse 85:10 Division 3:9 Docket 2:4 5:3 DOCKET/FILE 209:3 doctor 68:11,23 185:14,15 doctor's 113:18,19 113:21 doctors 35:20 36:8 68:6 69:16 71:20 112:17,17 113:10 113:11,25 160:13 160:14 173:4 document 25:21 35:9,11,23,25 58:13,17 60:1 61:21 63:21 80:21 129:6 134:3 160:25 192:5 193:21 documentation 172:5 documented 9:22 12:24 65:5 documents 29:12 52:25 53:2,6,12 63:12,17,19 80:17 80:23 85:24 86:1 87:4 107:11 doing 15:16 16:19 37:25 43:2 45:9 49:11 58:10,11 61:6 64:20,21 66:23 67:4,15 71:17 72:17 83:6</p>	<p>115:3 123:15 139:12 dollars 26:13 56:12 door 94:25 95:1 106:6 doors 27:16 doorway 94:20 dots 13:12 doubt 71:5 download 16:1 61:11 62:25 72:23 73:1 74:6,9 76:7 97:21 98:8 102:2 111:13,16,19 120:18 122:3,21 197:1 199:25 downloadable 62:20 downloaded 31:20 33:14,16 56:7 74:10 120:21 194:10 201:11 downloading 30:20 30:20 97:10,15,17 97:20 122:14 169:3,17 196:6 Dr 52:4,14 64:6 69:7 71:23 80:7 81:4,8 81:10 123:25 draw 87:15 145:15 154:11 155:23 170:22 183:8 187:15,22 188:20 193:1 driving 208:1 due 172:18 duly 80:14 duration 132:6 183:13 duties 75:11,14 148:24 Dyke 12:20 13:2 52:7 65:5,6,9 207:10,16 Dyke's 207:18</p> <hr/> <p style="text-align: center;">E</p> <hr/> <p>E 1:2 5:1,1 52:5 79:1</p>	<p>79:1 209:1,1,1,19 209:19,19 e-mail 58:14 79:6 93:18 100:4 130:8 130:10,12,17,20 130:21,23 197:4 e-mailed 6:10,11 e-mails 45:5 E-N-F-O-R-C-E-D 130:3 earlier 25:15 36:6 94:9 109:20 115:14 125:16 129:22 145:19 149:10 151:8,14 152:25 154:4 159:13 169:5 171:5 172:16 183:16 188:1 189:7 191:21 193:5 195:25 196:13 199:10 202:18 early 76:20 86:4 121:3 143:9 earn 81:20 82:5 earned 81:21 easier 64:24 easily 14:20 15:2 17:18 32:20 37:1 38:9 41:12 62:20 175:4 easy 25:16 34:14 121:5 180:3,25 edge 71:11 education 81:23 effect 117:19 190:13 effective 17:24 18:5 20:18 45:2 95:21 95:23 151:22,24 152:8,24 176:22 176:24 179:21,22 188:5 effectively 34:15 effectiveness 146:22 180:13 efforts 77:16</p>	<p>eight 177:7 181:9 either 40:6 63:15 74:16 94:5 177:8 electronic 62:3 67:19 68:22 109:9 113:18 156:21 electronically 61:20 61:23 68:18,25 71:18 130:8 elements 131:20 eliminate 27:14 ELIZABETH 209:25 embedded 83:3 97:20 120:20 197:6 embedding 83:6 Emergency 174:13 174:19,22 emerging 138:12 147:17 168:8 175:23 employed 128:1 employee 15:5,21 30:14,19 31:20 32:5 33:14,15,19 37:15 41:24 44:16 65:22,22 73:14 111:13,15 115:14 117:4 127:21 129:14,17,19 148:16,23,25 152:5 165:8,13,18 165:21,24,25 180:23 185:13 188:16 196:23 197:12 202:14 204:4,19,21 employee's 165:22 employees 15:3,10 15:10,11,13 27:7 28:9 31:9,14 32:13 32:20 37:6,18 38:1 38:7,15,16,19,21 38:24 39:2 40:15 40:17,19 42:7,10 42:13,15,18 43:2</p>
---	--	--	--	---

<p>43:25 44:3,9,11,14 44:20 45:4 47:11 48:7,11 65:20 66:24 67:2 72:9,21 73:4 75:21 76:2,9 111:18 116:22,25 128:8,10,16 132:18 148:20 165:3 166:12,13 167:10,14,17,17 167:18,19,19,20 167:21,21,23,25 168:16,17 169:6,9 169:23 170:15,17 170:19 171:7,8,9 171:21 172:7 173:3 174:1,11 175:16,24 176:6 188:2 195:21 196:2,3,8,14,24 202:5,8 employment 44:13 75:13 enabled 71:12 150:5 enables 115:11 enclosed 92:9 encompass 123:1 encrypt 45:4 130:25 encrypted 44:24 117:22 118:8 130:24 161:13 179:3 encrypting 103:21 encryption 117:24 117:25 118:2,3,4 130:9,17 encrypts 161:14 end-to-end 82:22 endeavor 20:22 endpoints 83:4 enforce 126:1 180:19 enforced 127:4 130:3,6 202:4 enforcing 96:7 106:25 engaged 25:24</p>	<p>47:21 158:11 enhances 100:10 ensure 15:9 31:14 45:25 46:18 47:17 109:3 126:9,12,17 141:13 178:9 203:14 enter 27:17 185:10 entered 113:13 entering 98:16 108:11 139:1 141:11 149:15 197:16,21 entire 196:7 entities 87:7 entity 16:22 63:7 112:23,25 160:6 entropy 177:13 entrusted 9:16 entry 32:22 67:22 146:6,8,19,20,21 146:25 147:4,20 147:22 148:6,10 159:7,8 193:2 198:13 environments 197:3 equally 43:11 equivalent 48:17 Eric 53:6 58:1 73:13 73:15,17 207:7 error 111:7 170:7 escape 53:6 63:20 escaped 52:19,21 53:3 62:2,24 63:21 especially 13:18 100:14 112:24 169:21 196:25 ESQ 3:4,5,6,16,17 4:4,5 essential 21:6 establish 48:13 51:12 53:13 72:2 123:18 established 123:16 204:15 205:24 et 39:3 Ethernet 90:3</p>	<p>evade 110:5 evaluate 14:14 21:14 136:11 166:17 evaluating 62:10 96:8 114:13 136:18 137:8 evaluation 82:16,17 everybody 18:19 everyone's 115:18 EVID 1:12 evidence 6:16 9:22 11:8,16,20 12:2,15 13:7,21,25 14:10 14:18 17:9,20 20:25,25 21:3,16 26:23 27:13 28:17 29:8 30:12,17,24 31:8 32:18 33:8 34:13 36:10,19 37:5 38:2,9,14,23 39:4,7,23 40:16,23 41:17,23 42:14 44:5,18,21 45:11 46:20 47:20 50:10 51:11,18,22 52:3,7 52:18,20 53:1 55:6 55:9 56:9,16,25 57:22 61:9,19 62:1 62:22 63:7,21 64:9 64:12 65:2,6,15,17 65:19 67:14 68:2,6 68:15 69:19 70:6,9 70:17 71:19 77:3 77:12 78:5,5 80:23 86:20 88:11,12 126:24 127:10 130:11 144:13 150:20 171:13 172:23 173:23 179:24 180:4 204:10 205:22 206:2,4 evidentiary 6:17 evolve 110:4 evolving 15:12 38:20 47:16</p>	<p>109:25 132:23 137:15 exact 89:13 exactly 25:11 90:19 115:21 examination 80:13 81:2 207:18 examine 84:12 examined 80:14 example 14:23 19:8 20:18 21:18 23:16 23:24 27:3 44:23 45:3 47:14 60:14 65:21 85:19 90:3 93:17 97:8,12 98:2 98:6 99:8 100:9,19 101:6,21 108:9 110:14,17 111:8 117:6,7 122:1,24 130:5,6 131:21 132:21 138:15 139:5,16 141:8 145:23 157:16,24 162:6,7,7 166:20 168:20 169:16 177:2 186:1 187:1 187:25 189:10 190:17,20,25 199:9 200:12 201:10 examples 93:19 126:2,5 133:1,17 138:13 139:23,24 139:25 140:2 171:4 172:12,21 173:17 183:15 excerpts 192:8 exchange 62:10 Excuse 16:8 83:16 execute 191:14 193:10,11,11 executed 93:16 99:13 exfiltration 40:4 exhibit 6:14,15 24:24 25:12,19 26:10 32:11,23</p>	<p>57:3 91:19 128:18 204:9,15,18,20,23 204:25 205:3 exhibits 1:12 205:14 205:19,24 206:6,9 exigent-type 69:5 exist 40:10,13 65:5 69:20,21 existence 60:25 expect 20:1 74:20 78:10 105:21 170:8,12 expected 27:7 expedition 74:23 experience 13:3 77:6 81:10 109:14 experiences 44:17 expert 12:19 17:13 28:25 51:24 53:25 64:18 83:23 84:10 84:12,17 85:6 87:12,13,18,20,25 88:1 89:6 104:18 123:25 157:15 160:24 193:20 195:16 207:16 expertise 81:13,14 experts 20:6 45:17 65:16 121:2 explain 12:20 17:15 18:8,13 20:7 21:5 28:12,14 29:1 31:12 34:19 37:1 37:22 38:18 41:5 43:8 63:11,15 85:13 94:1 96:25 100:10 104:25 105:11 113:10 118:22 142:8 explained 186:8 explicitly 162:25 exploit 21:22 193:11 exploited 21:10 22:17 34:20 140:11 193:8 exploiting 97:5 expose 103:11</p>
--	--	---	---	---

exposed 9:18 122:17 122:21	failures 11:23 14:15 15:18 17:18 20:24 27:10 31:6 32:4 36:17 38:13 39:10 40:2,22 41:21 43:5 49:1 124:23 203:22	120:15,19 121:5 121:10,21 201:11	101:2 108:9 141:1 144:14,16,16 149:13,16,25 150:3,9 152:17 169:16 197:15 199:6	flophouse 63:12 flow 8:22 43:13 83:4 193:3 flowed 112:16 flowing 102:15 163:1,2
exposing 34:16 166:1 186:25	far 58:21 74:22 83:19 122:23	filed 6:23 7:6,9,10 7:14 58:1	firewalls 48:16 64:2 76:15,16 144:7,12 145:21 149:10,21 149:23 150:2,7,9 150:10,13,16 151:18 197:23,24 198:17	focus 133:6 folder 29:12,13 folders 152:16 follow 23:6 44:9 72:12
exposure 21:15 166:11 197:8	far-reaching 77:23	files 15:24,25 16:20 29:4,5,7,13,14,17 30:5,10 33:5 59:17 60:7 74:10 113:4,6 113:17,19 119:1,6 119:11,20 120:13 120:18,22 126:14 152:14 159:22 198:20,23,24 199:7 200:20,24 200:24 201:3,3	firm 25:24	followed 73:12 following 53:15 54:11,23
exposures 25:16	FARRELL 209:25	final 203:25	first 5:6 6:21 14:18 21:2 22:2,25 39:23 46:16 78:11 80:3 80:13 95:24 98:3,9 104:10,19,25 105:2 107:11 125:8 126:24 131:6 142:11 144:12 146:6 157:3,17 160:22 161:5 174:24 181:1 186:19 193:14,16,18 200:17 204:14,23 204:25	follows 43:19 80:14 143:23
extension 161:12	fashion 96:16,18,19 104:10,14	finally 22:23 38:4 46:10 48:13	fit 137:19	footprint 62:18 force 182:17 foregoing 208:23 foreign 8:20 51:5,6 foremost 126:24 foreseeable 14:25 21:8
extensive 77:5	fed 58:13	financial 12:13 57:20 66:1	fits 51:5	forget 20:22
extent 69:15 88:3	federal 1:1 2:1,14 3:3,7 50:14 61:2 64:16 67:17 69:7 73:22 209:10	find 10:16 14:24 21:12,20 23:16 30:13,25 61:2 63:2 63:5,7 64:18 69:5 70:17 72:7 73:8,22 73:23 121:14 139:18 175:13 182:5	five 66:7,10,14,16 105:22 181:10,21 181:24,25 183:24 189:15	form 17:11 61:24 68:22 127:13 130:12 142:1,2,4,9 179:3,16 188:16
external 14:23 21:18 112:23,25 158:12,13,14,15 158:23	feel 49:18	finding 26:6	fix 21:11 25:16,17 189:17,19	format 142:12 209:23
extracts 95:8	FFF 142:18	findings 7:24	fixed 14:20 22:24 190:6	forming 146:21 155:20
extraneous 12:1	field 133:12,13,14	fine 20:1	fixed-size 179:12	forms 18:22
extremely 112:23	figure 60:4 89:11,13	fine-grained 101:3	fixes 22:25	forum 51:4 72:7
eyes 90:15	file 16:2,5,6 17:2,3 17:15 22:8 28:17 28:18 29:6,12,16 29:23 31:3,25 33:5 38:6 46:13 52:19 55:4 57:21 58:5,17 58:24 59:7,9,14,16 59:25 60:5,8,11,12 60:13,14,17,25 61:4,8,17 62:15,17 62:20,23 63:1,2,5 63:8 93:18 94:2,7 113:16,23 119:8,8 119:9,12,13,25 120:1,4,4,17,21 121:4,6,11,15,18 121:19 161:12,20 183:1,3 200:13,15 200:16 201:20 202:6	fingers 53:21 54:3 54:18,21 71:24 74:19	flat 76:21	forward 46:19 70:16 93:3,11
F	File's 30:7	Firefox 122:1,8	flaw 105:18	forwarded 92:14
F 2:19 52:5 79:1 209:1,1,16,19,19 209:19	file-sharing 9:24 10:5 15:22 28:22 29:1 118:15 119:4 119:5,17,18,19	firewall 25:9 27:11 27:14,15,18,22 69:8 95:15,16,17 98:10,14,18,19 99:12,12 100:10 100:11,19,21,22	flawed 54:16	forwarding 92:21
face 47:15 64:22			flaws 105:22 189:15 190:6	found 13:17 16:4,9 16:10,11 22:2,24 24:25 25:9,10 26:14,18 31:1 52:21 55:4,7,8 58:5,10,17,18,25 59:2 73:9,10,23 74:1 105:16 106:2 146:11 160:9
faces 43:24 87:24			flexible 11:11	
facilitate 42:24				
fact 7:24 36:4 52:18 57:4 61:6,20 62:22 71:1 106:5 112:22 127:10 146:1 157:20 199:5				
factored 65:5				
facts 65:7,16				
factual 157:16,25				
fail 47:22				
failed 9:15 10:10 14:18 17:21,24 21:3 26:23 38:14 40:23 41:23 48:2,3 48:4,7 179:20,22				
failing 9:17				
fails 18:6,11 54:25				
failure 12:3,20 17:17 22:1 39:18 43:7 48:19 161:23 188:4 194:5 201:23				

<p>175:4 foundation 204:16 205:25 206:16 fourth 22:20 38:12 130:15 frame 57:5 free 25:15 26:19 41:13 162:8,10,11 174:16 freely 139:20 162:3 163:4 202:7 freeways 208:2 frequency 178:22 frequently 178:20 Friday 58:2 207:9 207:11,15,19,22 208:2,6 front 8:24 FTC 11:9 24:7 48:20 50:11 71:2 FTP 22:8 25:2,5,9 25:17 26:18 36:5,7 36:25 37:2 68:9 93:18,23 94:1,2,3 94:4,5,7 157:9 159:10,18,23 160:22 161:5,11 161:12,14,14,16 161:21 full 66:21 101:25 103:10 133:24 134:23 144:24 169:21 196:25 209:8 fully 49:11 function 15:7 93:16 179:14 functionalities 102:1 functionality 36:11 36:13 37:24 42:8 101:17,19 144:23 149:17,24 166:25 189:25 fundamental 39:18 funded 16:24 56:11 funding 55:21</p>	<p>further 64:12 201:8 201:9 206:23 208:19,20 future 46:17</p> <hr/> <p style="text-align: center;">G</p> <hr/> <p>G 4:4 5:1 52:6 gain 95:4 177:4 184:8 185:7 195:9 199:15 gaining 77:18 gap 168:14 Garrett 74:7 gateway 98:12 150:2,3,7,8 general 79:5 136:8 generally 23:19 79:7 79:20 119:3 generate 152:20 generated 25:20 158:10 generates 184:23 generating 185:10 gentleman 56:21 Georgetown 28:24 Georgia 82:1,2,3 getting 37:20 122:5 122:6,9 give 19:24 69:18 85:19 89:14 101:22 103:6 117:6 130:5 131:21 155:9 186:10 200:12 204:22 given 26:11 27:19 37:6 40:14 64:20 78:3 103:9 110:16 136:2 139:7 169:5 195:22 196:25 199:23 gives 101:24 giving 139:9 186:18 196:4 glasses 29:24 go 11:2 24:20 31:6 36:16 39:11 41:3</p>	<p>47:3 62:25 67:19 68:19 76:6 79:14 79:18 80:15 88:7 103:1 111:1,17 116:20 127:16 129:4,12 136:18 139:5,17 141:15 141:18 143:17 146:13 153:7 169:18 175:9 207:5,23 208:6 goal 94:23 106:16 108:13 126:7,8,8 126:11,12,16,17 135:22 139:12 170:11 199:15,15 203:1,3 goals 43:20,20,21,25 44:2 96:2,5,7 104:11,13 106:24 106:25 125:21,23 125:25 126:1,2 136:2,5 170:12 God 53:5 goes 19:3 23:18 84:17 164:5 going 5:5,23 9:6,6 19:12 20:3 30:16 30:17 31:5 32:11 34:10 39:6 46:19 48:1 54:3 56:15 64:22 65:11,17 66:17 70:21 73:1 78:9,11,13 79:7 83:20 88:1 98:6 107:16 136:10 138:2,2,3 140:13 140:24 141:25 142:13,15,16,17 149:17 165:17 179:8 181:15 190:12 204:10 205:14,15 206:2 207:8 208:1,13 good 5:7,12 9:11 50:1 53:22,23 64:4 64:5,7,8,9 74:14</p>	<p>78:3 80:5 81:4,5 103:6 208:10 Google 55:12 175:11 Gormley 58:3 gotten 73:7 government 5:6 9:2 18:24 19:2,3,6 39:22 50:24,24 51:2,11 52:16 53:13 54:6 55:17 55:24 56:10,19 61:2 62:19 63:14 63:16 64:17 65:9 65:11 67:18 69:7 71:9 72:1 73:22 77:20 78:10 86:22 87:1,3,4,7 109:17 175:1 government's 54:8 73:3 grant 62:9 granted 9:4 great 199:9 green 91:11,14 grid 74:24 grounds 50:17 growing 47:16 guarantee 121:12 guess 34:14 67:4 68:24 115:17 177:3 181:1 guessed 15:2 32:21 180:3 guessing 134:17 guidance 107:23 132:25 133:2,3,11 133:18 135:7,9,23 guide 107:12 128:14 guideline 18:18 19:5 guidelines 19:7,14 86:23 87:5 109:17 132:15 133:12,21 133:22 135:10,11 135:23,25 136:4,6 136:7,8,13 175:2,4 175:7,14,20</p>	<p>guy 75:8</p> <hr/> <p style="text-align: center;">H</p> <hr/> <p>hacked 122:15,16 122:18 half 48:17 hand 59:22 90:12 handbook 129:15 129:17,19 handed 59:19 handle 155:7 handled 7:15 14:22 22:6,18 77:1 hands 52:10 handwriting 68:19 Hang 13:23 happen 39:25,25 51:8 63:25 64:14 79:17 193:7 happened 39:8,12 40:4,9,12 51:8,9 51:10 64:1 72:5 75:17 114:6 173:3 happening 39:16,20 137:14 happens 47:6 63:25 93:8 hard 66:23 89:20 91:13 113:8 harder 184:8 hardware 99:21 100:11 harm 11:13,15 13:7 13:10,14,25 14:1,7 14:7 24:13 51:13 51:16,19 52:2 53:16 55:2 63:9,23 64:22,23,25 88:15 88:19 105:10 164:8 harmed 63:18 64:10 64:11 65:10 harms 11:19,22 12:18,23 13:5 14:11 17:12 48:22 48:25 Harvard 82:4</p>
---	---	---	--	---

<p>hash 179:3,5,5,7,10 179:11</p> <p>head 75:8,10</p> <p>header 141:16</p> <p>headers 83:3,7 141:15 162:25</p> <p>health 12:13 19:9 58:8 71:4 77:17 113:18</p> <p>hear 5:23 8:23 12:1 84:14</p> <p>heard 10:12 74:1,11</p> <p>hearing 7:4 154:21 154:25 155:5,18 155:25 156:6 170:21 171:16 208:23 209:5,9</p> <p>heart 84:3</p> <p>heavyweight 83:1</p> <p>help 21:20 57:19 86:14 89:14 104:21 138:8 195:13 196:11 201:7</p> <p>helped 145:21</p> <p>helpful 6:4 85:23 92:3</p> <p>helps 38:21 175:3</p> <p>hemorrhaging 58:7 58:11</p> <p>hepatitis 17:8</p> <p>heterogeneous 111:4 199:18</p> <p>hex 142:4</p> <p>hexadecimal 142:1 142:4,7,9,19</p> <p>Hey 53:25</p> <p>higher 142:20 143:25</p> <p>highest 37:11</p> <p>highlighted 29:22 30:5,10</p> <p>highly 103:14,19 178:18</p> <p>Hill 1:9 17:15 18:8 18:13 20:7 21:5 28:12 31:12 34:19</p>	<p>37:1,22 38:18 41:5 43:8 51:24 52:4 64:6 69:7 80:7,12 81:4,8,10,22 82:8 82:14 84:6,9,20 85:5 86:18 87:19 88:9,21 89:5,8 90:10,22 93:5 94:17 95:21 98:3 99:7 102:3,21 104:5,17 109:11 111:25 114:23 117:13 121:22 124:4 127:20 128:23 129:14,22 132:9 134:8 136:22 144:5 145:15 146:5 147:19 148:13 150:25 153:9,25 154:12 155:16 156:14 157:2,10 158:4 163:5 167:5 170:14 176:2 180:7 182:18 187:15 188:20 190:16 191:16 192:8 194:19 195:15 198:12 201:20 202:18 203:6 204:5</p> <p>Hill's 71:23 204:13 204:16,21 205:4</p> <p>HIPAA 19:18,20 70:4</p> <p>hired 76:4 77:4</p> <p>history 132:5 178:5 178:7,9,12,22</p> <p>hoc 44:6 149:6 150:23 152:3 154:5 156:3 172:4 172:10,17</p> <p>hold 23:5 41:1 115:15 142:23</p> <p>hole 83:20</p> <p>holes 48:17</p> <p>home 33:4 34:8</p>	<p>62:25 74:9 122:25 122:25</p> <p>Homeland 57:5</p> <p>Honor 5:7,12 6:1,7 6:12,19 7:2,4,8,18 7:20,22 8:4,8,11 8:15,19 9:8 49:7 49:24 50:1,4 51:2 53:1 54:13 55:1 56:12,25 60:6 61:20 63:6 69:25 70:6 71:10 73:8,21 76:1 77:13 78:7 80:1,5,16,19,25 83:18,23 84:1,16 88:6 90:9,20 91:8 92:3 111:22 115:21 116:18 123:24 127:11 128:17 129:8 134:8,12 143:5,18 154:19,24 155:3 155:11 157:21 202:20 203:25 206:12,20 207:4 207:12 208:11,20</p> <p>Honor's 6:3 8:1</p> <p>HONORABLE 2:12</p> <p>honors 82:1</p> <p>hope 111:9 143:6,8</p> <p>hopefully 100:20</p> <p>horizontal 32:23</p> <p>host 119:10,15,16 119:16</p> <p>hours 9:7,9 49:11 143:5</p> <p>house 63:17 94:25 95:1,1</p> <p>housekeeping 207:4</p> <p>huge 56:5</p> <p>human 111:6 152:9 170:7</p> <p>human-readable 142:2</p> <p>humanly 118:6</p> <p>humans 100:14</p> <p>hundred 12:9 13:18</p>	<p>42:20 66:24 163:14 164:14</p> <p>hundreds 9:18 12:5 22:9 24:23 70:1</p> <p>Huntington 4:4 5:17</p> <p>Hyer 187:18,19,20</p> <p>Hyer's 187:23</p> <p>hyphenation 209:22</p> <hr/> <p style="text-align: center;">I</p> <hr/> <p>iceberg 17:16</p> <p>ID 1:12</p> <p>idea 62:19,19 66:19 66:25 120:19</p> <p>identification 68:13 68:21</p> <p>identified 22:20,21 23:25 25:12,14 36:22 41:7 55:25 96:11 105:24 106:22 107:1 109:1 157:8 161:8 170:13 191:4 193:16,18</p> <p>identifies 32:15,24 90:7 92:19</p> <p>identify 13:13 23:14 42:12,15 45:8 48:2 95:24 96:1,6 104:22 109:11 121:18 138:8 144:20 157:7 189:17,23 193:14 201:7</p> <p>identifying 23:22 68:12</p> <p>identity 3:9 9:24 11:18,18 12:16,17 13:4,4,9,11 17:12 17:12 22:7,7 35:3 35:3 43:3 48:21,22 88:16,16 122:11 132:1,2 176:13,15 176:16 184:15 185:6 186:10,10 186:11,13,20,21</p> <p>II 3:16</p>	<p>illustrate 19:13 23:3 93:22</p> <p>illustrates 89:9,22 93:24</p> <p>image 89:9</p> <p>immediately 62:23</p> <p>impact 168:18</p> <p>imperative 103:15</p> <p>impersonate 186:18</p> <p>implement 17:24 43:21 46:3 48:13 136:14 165:17 168:5 188:10</p> <p>implemented 82:11 125:10 132:9 173:11 185:3</p> <p>implementing 165:20 168:2</p> <p>importance 95:11 128:5 169:8 199:7</p> <p>important 91:18 105:4,5 106:17 108:15 132:3 137:11,12,21 140:8 165:22,23 167:25 168:1,16 168:17,22 169:24 170:1 176:22 189:8,10 195:6,8 196:1,3,21 197:17 197:18</p> <p>impossible 121:17 152:9,23 189:16 189:22</p> <p>improper 173:8</p> <p>inability 145:25</p> <p>inadequacies 51:25 52:24</p> <p>inadequacy 53:11 62:4 71:2</p> <p>inadequate 30:18,19 52:5,9</p> <p>inadequately 15:11</p> <p>inadvertent 29:5 61:7 120:17 166:10 196:5,11</p> <p>inadvertently 29:3</p>
---	--	---	---	--

<p>29:16 61:11 119:23 121:4 197:5 incident 17:15 28:17 75:3 77:10,11 incidents 9:23 12:24 include 67:25 124:17 126:5 133:4 135:15 included 33:23 42:18 124:18 180:1 185:21 includes 46:23 107:3 167:18 174:25 including 9:19 11:12 12:9 17:4 18:23 22:10 24:11 26:9 29:15 33:5,10 38:7 42:4 62:19 85:16 152:19 incorrect 56:13 increase 105:9 176:25 186:5 increased 15:18 164:8 182:11 increases 166:5 177:17,18,20 183:25 increasing 166:6 Indiana 17:14 81:9 81:17,18 indicate 128:23 129:3 indicated 55:12 indicating 89:20 90:25 92:9 129:2 153:12 indicative 10:10,24 individual 97:20,22 99:13,25 103:7,11 105:8 119:1 148:16,20 186:14 186:23,25 individual's 103:5 103:23 individuals 100:1</p>	<p>107:3,16 114:12 118:1,24 127:23 133:16 164:8 166:7 178:10 179:25 180:2 186:23 indulgence 50:5 industry 57:20,20 86:23 87:8,9 96:23 109:18 175:1 inference 40:9 information 9:4,16 9:18,20,25 10:5,11 10:13,14,15,18 11:4,5,6,14 12:4,8 12:9,14,15,22,25 13:1,13,17,19,20 13:20 14:13,22 15:3,19 16:6,9,17 16:18 17:3,10,13 17:25 18:21 19:1,9 22:6,9,12,13,15,15 22:16,18 24:5,12 24:13,14,23 25:3 25:23 27:19,20 29:5 32:1 33:5,10 33:11 34:18,22 35:2,2 36:9 37:10 38:5,5,8,10,15 40:5,7 41:10,25 42:2,5,10,13,15,19 42:22,23 43:1,2,6 43:14,15,16 44:24 45:5,16,21 46:1,4 46:11,13,21,23,25 47:7,8,18,23 48:11 48:14 52:10 56:4,5 56:8 57:17 61:12 61:22,23 64:19 65:21 66:2,3,17 67:16 68:8,9,14,16 70:5 71:4,21 77:6 77:17 79:5 83:6 84:22 85:10,15,17 88:13,15,17 102:10,15,23 103:4,6,7,10,11,12</p>	<p>103:14,15,17,18 103:20,22,23 104:2,4 105:6,8 106:14,19,21 107:6,22 108:2 113:13,25 114:4,6 114:8,10,11,13,14 114:20,20,21 115:4,13,17,18,19 115:23 116:2,3,4 116:11,23 117:3 117:11,12,12 122:14 124:14,17 124:19,20,20,21 125:10,15,17,19 125:22 126:3,21 126:23 127:6,8,8 128:6,13,24 129:18,24 130:22 131:3 132:4,8,10 133:8,19 135:12 135:25 136:3 140:6 141:17 142:11,19 160:16 160:18,20,21 163:1,10,13,17,19 163:23 164:1,3,12 165:3,12,13,15,22 165:25 166:2,3,4,9 166:10,11,13,18 167:10,15,20,22 167:24,25 168:13 168:15 171:9,12 171:20,23 172:6 172:11,17,18 173:8 174:1 175:2 175:15 177:13 178:16,17,19 179:12,13 185:22 185:24 186:1 192:18,20,23,25 194:4,24 195:4,6 195:20 196:20,22 197:7 201:25 202:13,25 informed 31:3 204:8 infrastructure 87:5</p>	<p>109:4 129:21 133:7 136:9,19 147:3 168:6 176:1 184:15 203:15 initials 185:19,20 186:1 initiate 115:12 139:8 140:24 initiated 50:11 98:17 197:19 198:24 initiates 199:2 injured 65:4 injury 17:11 50:19 52:11,12,13 inner 48:18 inquiry 8:13 inside 18:4,11 35:15 insider 40:5 103:8,9 165:24 insight 27:20 inspect 152:9 inspected 27:11 152:18 inspection 162:24 inspections 27:25 28:1,2,3,6,11,13 28:15 30:13,25 45:10,12 48:16 151:19,22,23 152:2,8 153:2 154:2,5,17 155:21 156:2,15 install 15:14 37:13 40:20 146:16 199:25 installed 15:21 29:9 31:2 33:19 37:15 45:13 68:4 118:10 118:16,18,20 153:1,10,11 154:1 183:1 196:17 200:3 installing 30:20,21 38:1 instance 185:8 instances 32:16</p>	<p>187:5 188:1 196:14,16 Institute 18:24 19:25 82:1 133:20 133:25 134:25 institutional 44:16 insurance 16:2 30:6 33:2,3 34:7 59:9 59:11,14 60:1 70:11 72:11,13 114:3 124:20 160:20 192:23 integrity 126:5,11 126:12 152:11 200:13,15,16,21 200:23 201:1,20 202:6 intend 29:4 61:12 intended 38:19 45:24 intent 8:1 intention 46:16 interact 123:4 interaction 123:6 interested 119:13 interesting 57:22 112:15,21,22 interface 89:24,25 90:1 intermediary 123:2 intermediate 123:5 123:7 internal 150:9 173:3 Internet 20:21 32:8 37:7,8 46:23 47:9 47:10 69:20 72:10 72:22,23 82:13 83:9 92:16 98:11 98:18,21,24 100:19 101:2 123:17 160:8 174:24 198:11 introduce 13:25 39:4,6 81:6 177:19 introduces 97:18,24 98:1 105:7 introduction 120:11</p>
---	--	---	--	---

<p>intruder 25:10 intruders 21:21 27:17 76:16 intrusion 26:25 39:14 40:3 99:1,3 99:4 108:24 149:16,23 150:4 150:12 investigate 201:9 investigated 71:2 investigation 21:25 25:25 41:7 50:11 64:19 201:8 investigational 155:5,17,24 156:6 170:21 171:16 invoice 145:18 146:3 involve 137:7 involved 79:16,18 100:14 123:2 208:5 involvement 57:24 involves 137:8 involving 9:23,24 12:25 IP 16:4 26:1,20 58:25 59:3 92:15 92:20 139:7,9,17 141:17 irrelevant 47:3 isolated 17:17 197:12 issue 7:20 47:5 106:1 127:5 146:12 187:11 issued 55:10 issues 6:18 12:2 14:17 43:24 79:4 146:11 172:24 IT-related 133:16</p> <hr/> <p style="text-align: center;">J</p> <hr/> <p>January 50:12 69:24 70:23 85:4 203:17 Java 146:16</p>	<p>Jim 12:20 job 51:23 64:24 66:1 165:14,19,22 166:13,19 169:1 173:2 jobs 42:1 48:12 65:22 165:4 John 77:4,5 Johnson 58:1,6,13 207:7,14,19 joint 6:15 7:6,14 jointly 6:22 joked 53:5 Jon 5:10 Josett 2:19 209:16 Judge 2:13 5:3,11 5:22 6:5,9,13,17 6:20 7:1,6,10,13 8:3,5,9,14,16,22 9:1,10 10:4,12,21 11:2 13:6,23 14:4 14:8 16:8,13,21,24 18:17 19:2,5,14,20 19:22 20:1 23:5 24:2,20 25:19 26:2 26:5,15 28:8 29:24 30:14,22 31:18 32:1,6,10 33:13,25 34:3,9 35:5,8,12 35:22 36:1 39:1,21 40:8 41:1 47:1 49:5,8,13,16,22,25 50:6,9 51:15 53:14 53:19 54:7,15,23 55:6,16,20,23 56:14,21 57:7,10 57:13 58:16,22 59:5,24 60:13,17 60:19 61:14 62:7 63:10 64:13 65:2 66:6,11,14,19 67:3 67:7,24 69:13,22 70:1,13,16,18,21 71:8,14,18 73:3,15 73:19,24 74:5,15 74:22 75:2,7,17,20 75:23 76:18,22</p>	<p>77:9,24 78:2,8 79:3 80:3,8,15,21 83:16,19,24 84:2 84:11,17 86:9 87:22 88:7 90:12 90:14,17 91:3,6,9 91:15,18,24 92:2,5 94:9,12,15 110:18 110:21 111:1,12 111:23 115:15,24 116:7,12,16,19 121:24 122:15,23 123:8,19,23 127:14,16 128:20 129:4,10,12 134:6 134:13,17 142:23 143:2,6,11,16,20 153:7,23 154:22 155:6,9,12 157:12 157:23 201:12,16 201:18 204:2,7,23 205:3,10,20 206:1 206:7,10,13,21,25 207:2,5 208:1,8,12 208:16,21 juggle 53:20 54:2,4 juggler 54:10,11 jugglers 54:2 juggling 53:23,23 54:20 July 60:11 85:4 146:14 147:6 161:7 193:24 203:17,20 June 60:11 147:21 jury 208:16 JX 1:19 5:24 6:9,14 7:5</p> <hr/> <p style="text-align: center;">K</p> <hr/> <p>Kam 12:19 13:1 52:14,14 65:6,7,9 keep 15:12 20:17 22:14 38:19 39:10 39:18 54:20 64:10 66:14 105:2,5 135:15 164:6</p>	<p>Kent 4:4 5:17 kent.huntington... 4:11 key 77:18 118:2,3,4 131:20 kind 17:10 35:2 61:17 66:19 89:19 91:13 149:4 kinds 12:8 24:12 knew 73:7 77:18 knife 54:1,9,10 knives 53:20,23,24 54:2,4,21 69:10 know 6:23 8:20 13:19 21:12 22:25 31:22 33:15,18,18 33:21 42:22 44:9 52:19,20 54:1 56:1 59:6 61:5 63:11 65:1 66:15,20,22 68:7,20,22 69:3,4 69:8 74:1,1,2,5,12 74:18,22 75:23 76:13 79:15 96:8 97:8 100:12 106:14 109:15 115:25,25 116:13 116:15 121:9 123:13,15 127:7 134:17 135:2,4,17 135:18,20 140:9 140:14 141:3 142:12,13,18,19 145:24 149:7,20 157:20 158:1 161:18 165:18 168:7,8 171:25 172:23 173:3 175:10,24,25 181:23 182:11 184:20 185:8 186:13,16 187:9 190:9 193:25 194:1 195:12 201:8 206:15 knowing 11:21 48:23 119:24</p>	<p>knowledge 15:1 44:16 86:24 169:15 170:2 171:25 206:17 209:10 known 14:24 21:8 22:22 27:25 31:24 72:25 92:25 93:1 93:10 109:13 144:22 knows 144:21</p> <hr/> <p style="text-align: center;">L</p> <hr/> <p>lab 66:2,4 76:5 156:23 163:15,21 163:22 LabCorp 71:14,14 labmd 1:3 2:4 5:4 5:13,16 9:18 12:1 12:7,12 13:16,19 14:12,17,18 15:2,5 15:7 17:20,23 21:3 21:16,23 22:25 25:24 26:6,22,23 27:22 28:2,9,20 29:9,16 30:16 31:1 31:6,8,12 32:12,14 32:16,20,24 33:6,8 33:10,18 34:12,15 34:23 35:16,21 36:9,12,19 37:1,22 38:4,9,14 40:14,23 41:6,17,23 42:2,8 42:14,20 44:18 45:7,13,15,24 46:3 46:10,14,16,20 47:2,20 48:1 49:6 50:11 52:19,22 53:3 59:11,21 61:23,24 62:24 63:3 64:2,2 65:20 66:20 67:17 68:3 69:10,17,22 70:7,9 70:22,24 71:1,13 71:16 72:9,16,25 75:21 76:8,15 77:16,21 84:21</p>
--	--	--	--	--

86:4,7 88:12 113:15,20 114:1 115:2,14 116:22 116:25,25 117:3 117:19 118:11 124:11,14,23 125:4,9 126:20 127:5,7,21 128:1 128:24 129:14 130:25 131:3 132:9 135:24 136:25 137:4 144:5,7,10 145:20 145:25 146:11 150:7,13,16 151:19 156:8,12 156:16,23 157:2 157:17 158:11 161:16,23 162:2,3 162:13 163:9,13 163:16,21,23 164:1,13,17 165:2 165:7 166:12,16 166:17 167:9,13 167:17 169:5 170:14 171:24 172:6,9,17 173:7 173:25 174:4 175:15,19 176:6 179:20 180:17,20 180:22,23,23 181:4,5,10 184:24 185:14,16 187:5 187:11,21 188:1,4 188:8,24 189:3 190:17,20,21 191:1 193:14,16 194:5,9,22 195:2 196:14 197:11 198:1 199:20 200:5,8 201:20,23 202:3,4 203:13,22 204:18,21 209:4 LabMD's 11:8,17 11:21 12:20 14:13 14:15 15:17,20,23 17:16 20:21,24	22:3,16 25:9 26:11 27:10 29:20 30:12 30:24 31:23 33:1 33:22 34:17 35:18 36:10,24 38:24 39:9 41:11 44:5,9 44:11,13,21 47:15 48:19,23 51:13,18 51:25 52:4 53:4,12 59:10 60:7 62:2,24 68:14,17 76:10,15 76:21 87:13 112:1 112:2,4,15,18 113:6,8,22,22 114:7,9,14,16,17 114:22 115:3,4 116:23 118:7 124:9 125:2 129:23 130:20 131:9 145:3 146:22 148:7,14 148:15 149:10,23 149:25 150:2,3 151:18,21,23 153:2 154:2,4,16 155:20 157:6 158:12 161:9 171:1,20,23 176:17,19,21 180:13 183:5 197:23,24 198:17 203:7,9,11,19 LabNet 192:13,14 192:16,17,20,22 194:17 laboratory 9:14 22:14 42:6 114:11 labs 71:13 lack 168:13 171:1 171:20,23,25 172:18 Laden 73:23 laid 51:25 70:14 206:15 laptop 50:6 laptops 100:5 112:10	large 43:12 103:3 112:14 149:18 166:1 177:14 178:1 189:24,25 larger 102:18 laser 90:10,19 91:3 91:12,23 lasered 52:1 Lassack 3:6 5:10 80:5,6,16 81:3 83:18,22 84:4,5,16 84:19 86:16,17 88:8 90:9,13,16,18 90:21 91:16,22 92:3 93:4 94:16 111:21,24 116:17 116:21 123:24 124:3 127:11,15 127:17,19 128:17 128:21,22 129:8 129:11,13 134:7 134:14,20 143:4,8 143:18,22 144:4 153:5,8,21,24 155:3,8,11,14,15 157:21 158:3 201:14,19 203:25 204:3,12,25 205:4 205:7,23 206:5,8 206:24 207:1 late 79:14,18 156:9 168:25 208:6 laundry 24:18 Laura 3:4 5:8 law 2:13 5:19 7:25 10:6,24 18:18 19:5 50:13 75:13 layer 92:13 97:6,6 98:22,24 99:11,16 99:19,23 100:3,6,8 100:20,21,23 101:3,4,10,11,15 104:23 141:18 layered 96:16,18,19 104:10,14 110:13 199:18 layers 20:13 110:15	lays 19:18 lead 37:9 186:25 leap 52:15 54:19 learning 62:23 leave 94:25 206:5,8 leaves 121:17 leaving 139:1 141:11,13 left 5:14 87:24 91:17 legal 14:6,6 88:3 length 177:7,11 178:3 182:8 let's 6:5 9:1 23:3 24:5 31:18 60:10 73:25 77:24 97:3,8 127:5 167:22 letters 181:19 183:24 letting 158:1 level 75:11,15 140:6 140:12 142:21 143:25 191:7 198:6 levels 165:15 liability's 71:7 life's 77:22 lifetime 112:8 lightweight 82:11 likelihood 13:3 51:15,19 52:1,12 53:13,21,22 97:1,2 110:11,22 111:11 166:6 185:11 186:6 202:21 likewise 207:16 LimeWire 10:6 15:22,23 28:20,22 29:8,10,16,19 30:13,15,21,25 31:19,24 32:2,4,7 33:14,16,19 37:15 45:13 61:3,6,10 62:20,25 73:9 74:3 74:11 75:15,18,25 77:9,11,11 111:14 111:16 118:15,22 118:24 152:25	153:2,10,11,13,15 153:25 196:17 198:19,23 199:1,2 199:6,22 200:1,10 limit 41:24 42:9 95:19 101:13,16 101:19 103:5 109:6 110:10 165:8 166:9,10 167:1 203:4 limited 27:18 144:13,17,23 149:22 166:12 186:2 196:4 limiting 109:8 165:21 196:10 line 30:10 32:15,23 70:18 171:17,17 lines 29:22 105:16 105:21 151:12 156:5 170:24 183:9 187:23 189:11,14 link 51:12 186:20 list 24:18 74:16,18 200:20 201:3,3 listed 109:12 127:23 listening 95:10 little 8:19 27:2 38:25 61:13 62:6 77:21 107:20 128:9,15 184:10 186:17 203:23 live 148:1 living 53:20 LLP 3:18 loaded 160:2 local 89:17,18,22 90:7,23 92:8,25 93:1 97:11 198:10 located 99:18 location 38:11 lock 148:2 locked 109:6,6 log 15:4 25:6 66:13 144:14 184:16 log-in 25:4,18 36:25
--	--	--	--	--

37:3	174:2 175:17	60:8 61:20 114:20	111:15	meaning 76:22,23
logged 27:18	188:6 194:7 202:1	117:3 125:10	managing 107:21	152:4 180:21
logging 184:2	low-cost 22:25	163:9,13,24	115:9 164:24	means 19:13 25:5
logic 53:16	174:5,14,17	188:24 192:17	manner 104:4	37:17 45:5 73:4
logically 8:22	lower 29:23 30:4	maintaining 60:5	112:16 121:20	79:14 85:13,14
logs 27:22 39:10	lowercase 177:17	70:3 107:5,25	149:7 150:23	105:14 108:6
108:23 144:7,12	181:5 182:10	164:3,12	152:3 156:3 172:2	113:4,7 159:2
144:15,16 148:21	183:24	maintains 12:4,13	172:10,17 173:21	160:6 202:20
149:2,3,8 152:19	lowercased 181:20	46:1,21 47:19	189:5 199:19	meant 191:7
152:19	ludicrous 77:23	88:12 202:24	manual 27:25 28:3	measure 18:11
London 16:5	lunch 78:9,15 79:9	maintenance 86:4	28:11,13,14 30:25	162:19 176:11,12
long 8:20 81:16	79:21	major 120:11	45:9 131:9,10	measures 9:15,18
120:5 153:25	lvandruff@ftc.gov	187:11	147:25 151:19,21	17:25 18:10,12,14
161:8 162:10	3:13	making 10:18 79:17	151:23 152:2,8	20:8 24:15 31:11
163:23 177:11	Lytec 114:17	118:1 121:11	153:2 154:2,4,17	31:13 36:20 40:18
181:10 183:24		169:15	155:20 156:2,14	42:12 43:9 48:4
200:1 207:17	M	malicious 97:19	manually 27:11	104:5,7 137:1,5,25
208:5	M 26:15,17 209:25	99:5 103:9 108:14	113:14	138:1,3 144:5,11
long-term 44:15	M-A-C 94:10,11	120:20,23 123:9	map 43:18 44:9,10	156:17 161:24
longer 46:15	Ma'am 94:9	144:20,22,23	89:10	162:15 165:2,8
longstanding 14:17	MAC 90:5 92:19,23	160:1,6 165:25	mapper 114:9,18,19	170:9 176:8,18,23
look 30:4 39:12,17	92:24 93:2 94:10	197:5 199:13	160:10,11,12,15	176:25 179:21,23
39:19 85:5 89:18	machine 101:1,25	201:7	160:17 161:19,21	180:14 188:5
89:21 92:15,15	113:5,20 148:22	malware 24:6	mapping 179:15	194:22 195:3,5,18
105:19 111:17	159:21 160:12	147:10	maps 94:21	200:5,8 201:24
136:12 141:18,24	169:11,11,12	man 56:24	MARGARET 3:6	mechanism 95:17
144:24 152:22	191:9,15 196:5	manage 36:11 47:12	marked 89:7	95:18 97:6 98:15
162:24,24,25	197:9 198:8	managed 87:7	marked-up 205:11	99:1 108:9 131:24
174:8 181:11,24	199:21,25	111:13	marking 129:6	131:25 141:4
looked 67:11 136:4	machines 102:13	management 15:7	markup 204:13,22	145:4 177:23
191:21	113:15 119:1	manager 15:23	master's 82:2	180:19 184:17,19
looking 16:18	145:7,8,10,10	29:10,20 33:1,22	material 86:18	186:9 199:12,15
102:13 142:14	152:6 158:20	34:4,6 38:8 45:14	matter 2:3 57:19	mechanisms 82:18
145:24 158:19	166:7 169:22	59:10 60:9 75:12	62:22 80:17 84:3	83:12,14 96:6,10
175:8,12	173:4 202:13,15	75:15 76:19,23	86:25	96:12,15,15 97:14
looks 141:16	202:16	182:24,25 187:20	McAfee 24:5	98:23 99:10
losing 70:25	Maggie 5:10 80:6	196:16 199:20,23	mean 13:10 14:1	101:12 102:19
loss 71:20	main 17:23 94:23	199:24	54:3 66:11,13,14	104:9,14,22 107:1
lot 44:14 64:24	149:13 152:1	manager's 16:3	66:16,24 87:2,3	108:7,8,12,16
79:16 87:23 128:7	175:9,9	33:20 37:16 117:7	90:12 101:19	110:1,14 111:5,8
157:15 177:14	maintain 40:24	117:10 118:17,19	108:5 112:20	111:10 120:3
low 11:24 22:24,24	102:16 107:17	153:1,3,10,12,14	113:3 138:22	125:24,25 130:25
26:7 36:13 37:23	125:15 163:23	153:15 154:1	159:1 167:19	131:23 133:6
42:17 45:16 49:2	178:9,11,23 189:8	198:19 200:2	169:17 177:24	135:21 136:6
124:24 132:11	190:18 191:1	managers 42:6 72:8	181:14,15 182:2	138:6,8,10,11,14
136:1 161:25	maintained 11:6	72:9,22	185:8,25 200:23	140:19 151:22
162:17 166:14	12:7 42:2 59:25	manages 94:3	201:6	156:24 168:5

<p>170:4 176:20 188:9,14 199:18 199:18 medical 9:14,20 11:18 12:17 13:4 17:5,12 22:12 33:11 42:5 46:24 48:21 57:20 67:4,4 67:10,11,18,19 68:6 70:14 88:16 133:7 medium 90:6,25 92:12 94:13 meet 71:23 88:3 members 75:23 memory 134:4 192:10 mention 87:23 mentioned 40:14 51:4 59:4 94:17 95:11 115:14 120:16 132:25 139:19 149:10 174:19 menu 45:19 mere 10:13 merely 10:7 206:3,6 206:8 messages 130:24 131:1 met 5:17 method 45:9 methodology 58:7 62:17 methods 20:16 36:14 Michael 2:12 4:5 5:15 Microsoft 41:19 105:25 190:23 mid-2008 28:2 midst 73:13 Mike 5:20 million 26:13,15 105:21,22 189:14 189:15 millions 26:17</p>	<p>mine 54:4 minutes 201:15 misconfiguration 100:18 misconfigured 132:19 missing 65:3 131:20 mistake 100:20 105:17 mistaken 35:8 mistakenly 29:6 mistakes 67:22 100:16 105:23,24 106:1 189:15 misuse 43:3 misused 34:25 MITCHELL 201:17 mitigate 110:2,5 mitigating 132:24 moat 18:4 48:17 model 35:19 45:17 45:18 71:9,10,11 71:12 modules 174:12 moment 194:15 moments 19:24 36:4 monetary 136:20 167:2 188:18,19 202:11 money 16:24 59:12 59:13,21 70:25 monitor 91:7 150:16 200:13,15,16 monitoring 108:23 141:22 151:17 201:21 202:6 monitors 93:24 month 70:25 morning 5:7,12 6:1 6:11 9:11 49:18 50:1 79:10,20 208:3,22 motion 7:1,14 58:1 motivation 16:13,15 74:3 move 62:6 70:16 84:16 204:3,6,13</p>	<p>204:20 205:15 moved 56:21 multiple 18:5 76:15 111:9 113:17 152:15 186:12,23 multiple-use 103:24 multiuse 197:3 music 29:10 61:11 74:6,9,10 120:12</p> <hr/> <p style="text-align: center;">N</p> <hr/> <p>N 1:2 5:1 79:1,1,1 209:1,19 N.W 2:15 3:10,19 4:7 name 25:7 30:8 32:24 33:18,23 55:9 59:15 63:1,5 71:15 81:8 86:10 86:12 114:2 124:18 132:1,1 133:24 134:23 176:14 181:2 184:14 186:14 named 25:23 33:16 55:17 names 9:19 12:11 17:4 22:11 31:16 32:12 33:10 42:4 46:24 160:18 180:1 192:22 national 18:24 19:25 25:15 45:17 87:6 133:4,9,10,20 133:25 134:25 174:9 nature 17:6 130:22 nearly 10:1 necessarily 116:8 201:6 necessary 44:10 46:14 65:22 70:10 76:7 118:11 163:10 164:4 197:25 205:25 need 9:6 27:14 28:21 38:8 48:12</p>	<p>66:12 73:1 80:21 84:14 92:6,6 95:25 96:1,2,8 97:25 102:19 103:4,16 103:19 104:1,12 105:3 106:23 111:18,19 123:6 135:16 136:13 137:16 138:5,9,11 140:23 141:14,15 141:19 142:1 143:2 146:17 152:18 154:22 160:24 162:11 163:18 164:6,15 165:4,18 166:8 168:21 169:2,14 169:14,20 170:3 186:8 189:24 198:9 199:9,17 202:16 needed 7:19 21:14 41:25 65:25 66:4 68:14 97:25 126:19 136:3 163:16 165:13,15 165:22 166:13,18 201:8 needs 138:21 neither 57:25 58:4 Nessus 26:19,22 138:19 162:8,10 net 67:7 network 10:16 11:7 13:17 15:20 18:3,9 18:10,11,12,15,15 20:9,10,14 21:9,14 21:24 23:23 24:12 26:21 27:17 28:19 31:4,25 34:17 36:2 36:3,21,24 38:11 39:5,11,20,24 40:25 41:11 42:4 43:10,13,14,15,19 44:10,20,25 46:22 47:8,10,12,19 55:5 55:8 62:21 63:4</p>	<p>77:7 84:23 86:8 88:23 89:1,2,15,17 89:18,22,23,23,23 89:25 90:1,8,23 92:8,22,25 93:1,2 94:21 95:4,4,20,22 95:24 96:17 97:11 97:19 98:16,17 99:5 100:24 102:5 102:13,14,15,18 102:20,24 106:6 107:25 108:11,23 109:19 111:10 112:1,2,4,5,6,8,11 112:12,13,16,17 112:19,21,24 113:3,6,9,22 114:7 114:22 115:4 116:25 118:7,25 119:17 120:13,19 121:11,21 135:19 135:20 137:9,10 138:4,18,20 139:2 139:8,18 140:16 141:11,14,23,25 144:6,18 149:15 149:21 150:24 158:12,16 160:4 162:23 163:2,10 176:7,13,21 178:25 179:2 188:25 194:24 196:7 197:16,21 198:10,25 199:3 202:1 205:5 networked 35:9,10 networking 92:13 networks 15:17 16:12,18 20:20 34:21 40:19 43:12 48:6 55:14 88:23 89:15 98:13 120:22 never 9:21 12:10 31:20 42:20 66:15 163:15,21 164:9,9 180:6</p>
--	--	--	---	---

<p>new 69:23 76:6 107:23 110:2 138:12 147:8,16 147:17 168:10 178:13 204:22 newly 27:5 nice 74:12 nine 26:1,9 81:19 NIST 133:20,24 134:23 135:3,4,8 168:10 NMAP 138:16 139:6,7,19,20,25 140:5 162:7 no-cost 174:5 no-no 15:2 nodes 121:10 non-government-... 16:22 non-information 167:20 non-IT 15:10,13 40:14,17 44:3 167:19 168:16,17 169:9 171:7,21 175:16,23 nonadministrative 195:22 196:2,4 nonelectronic 121:19 normal 60:7 91:12 Norton 24:5 note 79:23 153:9,13 153:19 155:4 187:2 notes 35:13 209:8 notice 13:16 46:11 noticeable 148:22 noting 152:5 notion 160:5 November 59:2 NRC 135:8 NSA 53:7 NT 41:18 190:21,23 number 6:15 21:1 32:13 38:25 43:4 47:21 53:2 59:15</p>	<p>68:13,21 93:11 95:6,8 98:19 102:13 114:3 124:19 182:8 184:23 185:10 209:3 Number2 1:20 numbers 9:20 12:12 17:5 22:11 33:11 42:5 46:24 139:10 142:17 160:19 177:8,19 182:11 185:20 192:23 numeric 118:4 179:16,17 nurses 185:19,20 186:1</p> <hr/> <p style="text-align: center;">O</p> <hr/> <p>O 5:1 79:1,1,1 209:1 209:1,1,19,19,19 209:19 object 154:19,23 204:10 205:18 objecting 205:10,12 objection 8:6,7,11 83:24 84:15 88:2 142:24 204:7 206:3,10,12 207:18 obtain 34:21 35:1 36:23 41:10 46:7 obvious 14:16 38:9 67:21 occur 13:10 64:22 145:9 occurred 14:1 68:4 149:5,6 172:25 occurring 64:23 113:1 152:5 195:13 197:10 occurs 29:6 October 156:10,12 offer 13:6 85:11 188:23 203:18 offered 88:3 offering 204:24</p>	<p>205:21 office 6:3,10,23 7:7 7:9 67:16 113:18 113:20,21 officer 58:3 77:5 208:9,10 offices 33:9 34:11,25 35:6,20 36:8 68:6 112:17,18 113:10 113:11 114:1 160:13,14 173:5 185:15,17 oftentimes 107:19 oh 52:9 54:20 99:22 okay 8:14 14:4 19:22 50:9 60:10 60:19 75:17 80:22 84:4,16 88:25 98:5 99:22 100:12 116:16 135:14 140:4 142:20 143:11 146:5 150:3 153:11 155:8,14 184:10 186:21 204:23 206:13 207:5 208:5,9 old 66:16 on-the-job 76:3,4 once 59:17 67:23 93:7,9 95:7,25 96:10 114:8 121:16 125:23 138:7,20 172:24 one-eighth 110:16 one-factor 184:17 one-half 110:16 one-hour 79:9 one-way 179:15 ones 107:4 128:10 162:5,16 online 146:15 174:12 175:7 open 61:21 94:24,25 95:1,2 106:6 138:18 139:14,15 141:2,9 161:19,20</p>	<p>197:5 198:4,9 opening 5:23 9:1,5 20:2 27:16 49:10 54:12 77:25 127:12 139:18 operate 70:11 77:19 operates 47:10 operating 15:8 24:4 36:11 37:24 40:24 41:18 42:9 69:13 70:22 77:5 105:15 105:20,20,23 138:21 140:6,8,10 140:12,15 152:19 166:20,24 173:21 188:25 189:4,9,13 190:18,22 194:6 operation 66:20 150:13 operations 58:3 operator 33:13 opinion 125:9 136:25 146:22 157:18 163:9 165:2 167:9 176:6 188:24 194:22 198:17 203:1,18 opinions 83:21 85:11 88:3,4,22 125:3,7 203:7 opportunities 119:23 opportunity 95:3 opposing 80:18,23 options 174:5,14,17 174:17 order 5:3 6:25 45:23 46:6,10,14,18 47:16 55:1 68:11 72:22 93:2 97:14 104:13 108:17 111:19 115:13 130:10 133:12 136:17 137:17 138:23 141:20 147:2,6 149:18 152:22 165:14,19</p>	<p>167:14 168:22 178:1,8 181:22,25 182:5 184:15 188:10 189:23 ordered 115:2 ordering 42:24 orders 35:21 ordinary 30:12,24 organization 100:1 107:19 133:11 140:22 174:23 199:2 organization's 158:16 198:25 organizations 18:25 109:18 133:1,3,17 135:3,4,5,8,10 163:22 168:10 original 6:6 Osama 73:23 ourself 72:7 outer 48:18 outside 18:4 25:23 44:19 53:12 67:25 92:25 95:4 98:17 121:20 140:23 158:16 160:3 197:19 198:24 outweighed 50:21 overall 24:25 96:7 106:13 111:11 124:7 125:1 136:8 137:17 138:6 158:23,25 168:18 194:16 203:8,10 203:13 overflow 191:13 193:4 overlap 107:20 128:9,15 overtime 207:23 overview 78:3 overwritten 27:20 owed 59:12,21 60:2 60:2 Owens 5:10 owes 60:10</p>
--	---	--	---	--

<p>owner 5:15 56:23 119:9 151:6</p> <hr/> <p style="text-align: center;">P</p> <hr/> <p>P 5:1 209:1,19 p.m 78:15 79:2,8,24 208:24 P2P 10:16 13:17 16:12,18 28:19 29:1,2 31:4,25 pace 20:17 packet 141:15 162:23 packets 83:4 page 117:14,15,16 130:13 145:16 146:6 147:20 151:10 156:5 158:22 159:6,8 170:22,23 171:15 171:17,18 183:8 187:22 192:6,7 193:2 194:14 198:13 pages 60:21 131:6 155:24 paid 60:1 61:18 72:15 paper 61:24 67:20 paragraph 85:6,8 87:21 88:10 89:5 104:18,20 109:1 109:12 114:24 115:16 116:7 121:22 124:5 136:23 161:2 163:7 167:7 176:4 188:22 194:20 195:16,17,18,21 196:19 197:14 parameters 60:10 part 7:1 20:4 21:6 36:1,3,6 50:14 54:1 62:1 67:7 98:9,25 106:17 112:13,15 118:5 118:25 137:22,22</p>	<p>140:21 169:24 170:1 195:7,10 partial 191:15 193:12 participation 62:13 174:25 particular 18:13 20:8 43:10 48:1 87:20 92:20 95:10 101:17 110:3,17 119:10,12 130:15 135:21 145:8,16 145:23,24 146:3 147:6 151:12 159:7 166:19 167:16 182:5 183:10 187:24 particularly 13:15 13:22 147:20 parties 5:6 6:21 7:19 7:21,23 8:10 52:11 79:6 partly 25:1 partner 5:19 57:1 57:24 58:14 62:11 partners 62:8 parts 98:7 180:1 party 16:11,16 31:3 80:23 pass 44:16 206:25 passed 25:9 password 15:5,6,7 25:7 31:13 32:15 32:16,19,25 33:13 33:23 36:14 41:8 66:14,16 132:1,2,4 176:15 177:3,5,6,6 177:12 178:2,5,7 178:14,19 179:4,4 179:6,7,15,17 180:2,22,22,24 181:3,6,7,9,12,13 181:17 182:6,16 183:5,12,18,23,23 184:1,3,4,19,21 185:6 186:11,22 187:1,3 188:11</p>	<p>191:10 passwords 15:2,9 31:14,17 32:12,21 33:12 34:11,13,13 34:14,20,23 36:12 66:7,9 67:9 132:3 132:5,6,7,8 173:19 177:2 178:4,8,10 178:12,13,22,24 179:1,3,24,25 180:3,5,10,18,19 180:20 182:1 185:13,14,16,18 185:19,20,21 186:2,5 187:6,11 188:2 patch 105:13 patched 140:14 patches 106:1 173:20 patching 135:16 patented 55:13 63:8 path 83:7 patient 68:12,13 71:20 113:13,17 115:22 116:3 patient's 114:2 patients 115:20 116:4,6,6 Pause 6:8 41:2 129:7 193:22 payments 61:18 PC 86:16 peer 73:9 122:6 123:9,12,13 peer-to-peer 9:23 10:5 15:22 55:5,8 55:14 62:21 63:4 73:11 119:4,5,17 119:19 120:5,7,15 120:19,22 121:5 121:20,25 122:4 122:24 123:3,4 124:1 peers 120:13 123:17 pen 25:13 pending 143:18</p>	<p>penetrated 111:9 penetration 21:19 21:20,23 22:21 23:4 24:21 25:8,20 25:25 26:8,14,18 26:20 36:22 39:4 39:23 41:6 47:13 108:22 138:15,17 139:3,5,12,16,21 139:24 140:2,25 141:8,9,16 144:8 157:3,7,17 158:18 158:18 161:9 162:12 Pennsylvania 2:15 3:10,19 4:7 people 9:21 11:5 13:18 54:2 57:9 59:6,12,15 60:22 60:23 61:10 65:4 65:25 66:2,4,7,9 66:21 76:24 79:16 107:21 136:17 166:3,23 175:22 186:12,24 187:3 202:10 Pepson 4:5 5:20 percent 52:12 54:2 97:4,7 110:12 perfect 53:4,7,9,16 76:11 100:13 109:21,24 110:7 110:19 202:19,25 perform 21:18 41:25 68:23 158:11 165:4 166:19 169:1 173:2 performed 17:6 21:23 41:6 59:13 68:20 114:5 152:2 156:3 158:16 163:15,21 171:24 172:9,17 performing 26:8 27:24 75:11,14 148:24</p>	<p>perimeter 18:10 period 70:5 85:3,11 85:12,15,18 86:5 112:3,9,9 117:20 148:19 149:8,9 150:14 152:3,4 161:21 162:8 163:25 169:7 180:11 187:6,12 203:16 periodic 15:12 38:16 46:7 periodically 137:17 173:14,16 200:21 periods 206:16 permanently 42:25 permission 72:24 73:2,5,7 perpetrate 12:16 persisted 17:19 person 61:3,4 65:23 75:6 136:17 personal 9:25 84:22 88:13 115:3,17,18 116:23 117:3 124:14 130:11 163:9 165:3 167:10,14 194:23 195:4,6,20 196:20 196:21 201:25 202:13,24 206:17 personnel 47:12 62:25 67:4,10,11 67:24 70:14 79:18 207:25 persons 63:4 pertinent 50:14 Ph.D 80:12 82:3,5 physical 109:2,3,7,8 135:17 physically 109:4 physician 33:9 34:25 35:6 67:16 68:3,24 71:3,6 77:18 115:1,5 185:15,17 physicians 14:11</p>
--	--	---	--	--

<p>22:10 34:11 35:15 70:25 71:12 114:12 115:17 piece 93:15 95:15 122:21 179:12 190:1 pieces 19:17 place 20:12 35:20 64:2,3,4 65:21 71:4 76:15 77:16 113:4,6 126:25 170:9,9 180:19 184:5 195:19 199:12 placed 90:2 173:4 places 16:9 121:18 152:15,21 plain 117:25 plan 13:6,24 39:3 102:10 106:14,18 106:20,21 107:23 108:2 129:18 133:23 168:2,4 208:12 planning 8:12 47:5 plans 47:13 128:24 129:1 play 57:21 playing 69:10 plea 142:25 pleadings 74:2 please 9:12 20:23 29:18,21 31:15 44:12 50:2 81:6,22 85:7,13 96:25 104:20,25 105:11 112:2 114:25 117:6 128:23 129:3 130:5 146:9 153:19 159:15 172:21 190:16,25 200:7 plus 22:13 33:6 point 17:23 19:16,17 19:17,23 20:18 23:1 48:15 67:3 69:22 91:19 111:2</p>	<p>148:18,25 149:2 157:12 159:24 160:5 161:15 pointed 91:20 pointer 90:10,19 91:4,23 points 17:23 23:3 72:2 policies 43:20,22 44:1,7 45:19 96:4 96:15,16 104:12 104:22 106:12,15 106:17,24 125:25 127:1,2,3,6,8 128:6 129:20 130:2,6 131:4,11 131:15,20 132:4 135:18,20 175:12 188:11 policy 31:13 44:23 45:3,7 72:25 73:12 111:17 117:8,16 117:17,19 130:9 130:15,16,18,19 131:9,10 165:18 165:20 179:23 180:18 202:4 poor 25:1 28:13,15 158:25 194:18 popped 93:24 popular 9:23 populate 61:21 port 69:9 93:11 94:19,20,21,24 95:2,5,8,10,13,14 98:19 106:6 139:10,11,16,21 140:13 161:19,20 161:22 198:4,4,9 portal 113:13 115:3 portion 51:1 ports 94:17,24 95:12 98:20 106:4,5,8 135:17 138:18 139:13,14,15 141:2,3,9,17 position 10:4,7</p>	<p>13:25 24:3 39:22 54:8 64:14,16 65:12 70:22 71:8 73:3 75:4 78:4 positions 128:11 possession 52:19,22 53:3,12 62:2,24 possibilities 169:18 177:25 possibility 170:7 possible 77:21 97:12 149:20 159:17 181:16 182:1 189:19 possibly 139:13 159:5 182:5 poster 127:13 205:11 posting 10:7,13,14 posttrial 7:24 157:14 posture 25:1 158:23 158:25 194:16 potential 11:13 166:1 181:3 potentially 73:18 power 169:13 196:10 197:1,1 PowerPoint 205:8 practice 12:6 17:21 18:20 47:24 48:19 48:20 50:17,18,18 63:22,23 96:22 101:21 103:6 173:10 203:14 practices 10:3,9,10 10:19,25 11:4,9,17 11:21 14:13,14 31:23 32:19 44:17 44:22 45:1 46:18 47:21 48:24 50:12 51:13,19 52:4,9 53:4 105:7 107:12 125:2,4 132:16 135:5 183:6 203:7 203:9,12,19 practitioners 17:21</p>	<p>22:22 26:21 29:2 precautions 71:25 precise 63:5 precisely 51:20 63:1 63:1 predictability 54:16 preliminary 7:3 80:16 premises 61:25 prepared 25:22 49:8 49:12 54:11,13,18 78:11 presence 108:13 144:22 200:14 present 21:13 23:15 28:22 65:2 98:6 121:18 138:9 147:17 184:14,18 184:21 186:9 199:22 206:5 presented 61:10 135:11 presenting 51:23 184:20 presents 95:3 preset 190:11 president 56:24 press 55:10 75:24 201:18 pretrial 7:4 pretty 74:14 78:3 prevent 30:19 36:20 37:3 48:5,11 83:15 108:10 109:9 110:1 165:3,20 194:23 195:3,5,11 195:19 196:11 201:24 202:8 prevented 32:20 38:1 76:16 148:23 198:18 199:6 202:5 preventing 11:14 prevention 36:18 prevents 186:23 196:5 preview 14:16</p>	<p>previous 128:9 previously 98:15 110:11 128:12 147:9 165:23 principal 36:7 principle 105:13 106:7 principles 104:21 105:1,2,12 106:3 106:11,12 108:4 108:18,19,25 109:12,13,15,16 110:9 137:23 164:6 print 60:11 61:23 prior 6:22 7:3 8:18 37:14 59:1 79:13 79:14 156:24 privacy 3:9 81:15 private 18:25 88:17 privileges 73:4 112:24 proactive 20:15 47:25 95:18 108:9 150:16 proactively 108:10 probability 96:20 97:4 203:5 probably 102:18 134:11 probe 108:19,20 135:19 137:22 138:17,20 probing 158:21 problem 52:3 97:14 110:23 111:14,16 148:22,22 152:5 160:22 161:5 172:25 173:1 186:19 193:23 195:14 202:21 208:18 problematic 164:4 180:24,25 183:19 186:16 problems 86:7 145:22 149:1</p>
--	---	---	---	---

<p>150:24 190:2 procedural 6:18 procedures 43:21 44:1,7 45:20 166:18 proceed 49:12,25 proceeding 8:2 proceedings 6:8 41:2 129:7 193:22 process 6:24 94:8 96:8 102:11 106:13 117:25 122:10 123:14 125:20,21 126:25 136:11,18 148:2 178:21 process-based 136:15,16 process-driven 140:21 processes 77:16 166:17 processing 33:3 192:19 processor 33:2 34:7 Proctor 208:9,10 produced 18:23 product 41:20 products 190:13 profession 101:22 professional 164:24 professionals 18:21 107:13,24 132:23 135:2 138:14 140:18,20 175:1 175:22 professor 17:14 18:8,13 20:7 21:5 28:12,25 31:12 34:19 37:1,22 38:18 41:5 43:8 51:24 52:14 58:1 64:7 81:9,16,18,22 81:24 82:8,14 84:6 84:9,20 85:5 86:18 87:19 88:9,21 89:5 89:8 90:10,22 93:5</p>	<p>94:17 95:21 98:3 99:7 102:3,21 104:5,17 109:11 111:25 114:23 117:13 121:22 124:4 127:20 128:23 129:14,22 132:9 134:8 136:22 144:5 145:15 146:5 147:19 148:13 150:25 153:9,25 154:12 155:16 156:14 157:2,10 158:4 163:5 167:5 170:14 176:2 180:7 182:18 187:15 188:20 190:16 191:16 192:8 194:19 195:15 198:12 201:20 202:18 203:6 204:5,13,16 204:21 205:4 profile 200:17,18 201:4 profitable 26:12 program 9:24 10:6 15:22 22:8 23:8,14 23:16,18,20,20 24:1,1 25:2,5,9,18 26:19 27:1,2,3 28:20 30:13,25 31:2,19 36:5,7 37:2 39:14,15 41:8 41:13,14,16 43:6 43:17,18,25 45:16 46:4,8 48:14 107:7 121:5 125:11,15 125:17,19 126:3 126:21,23 129:24 132:10 133:19 135:12 136:1 138:6 148:2 170:4 172:1 programmed 42:11 programs 15:14</p>	<p>20:19 23:12,13,21 27:8 28:22 29:1,3 37:13 38:2 40:20 43:23 45:8,17,19 45:21 72:23 73:11 120:5,7,15 128:14 prohibit 37:2 project 190:11 proof 132:2 176:16 184:13,18 186:10 186:12,20 proofread 209:21 proofs 185:6 propagated 83:9 proper 88:3 167:24 168:3,13,15 170:8 170:12,15,16 171:9,11,14 172:10 173:14,25 175:15 199:8 206:16 properly 26:25 47:1 141:1 170:10 198:18 199:5 proposed 45:23 46:6 46:10 prostate 17:7 protect 9:15 10:10 16:17 17:25 18:12 43:19 73:14 77:17 77:21 98:8 103:15 103:17 108:4,6,7 108:15,17 110:1,1 125:23 136:4 138:2,12 147:3 148:12 protected 47:17 71:4,6 77:17 95:25 96:1,9 106:23 109:5 protecting 109:18 129:20 133:7 135:20 164:12 168:5 protection 3:8,9 24:6 27:2 95:17 96:3 98:15 109:3</p>	<p>203:15 protects 45:25 protocol 22:8 82:11 82:17,17,19,20,21 82:22 83:2 92:16 93:19 94:2,7 98:18 113:23 161:13,20 protocols 83:1 prove 50:24,25 51:2 51:21 55:4 63:22 64:21 65:1 provide 12:3,21 13:16 43:9 45:19 46:11 47:22 56:15 80:19,22 85:1 95:22,23 104:6,8 124:11 125:3,9 130:25 133:2,18 133:22 135:23 136:7,24 137:4 163:8 165:1,7 167:8,13 170:15 170:16 172:12,21 174:9 175:21 176:5 190:16,25 194:21 provided 12:10 27:2 33:8 34:25 35:6 41:14 42:20 45:5 72:15 86:3,8,21 87:4 88:20 109:16 113:21 120:24 124:6 127:10 133:3,4,21 135:8,9 150:23 154:10 164:9 165:12 166:20 173:25 174:13 175:15 188:10,14 194:3 providers 77:1 provides 44:2 84:21 94:22 107:12,23 120:3 providing 46:8,15 56:2,2 93:16 121:2 128:13 132:17 135:17 150:20</p>	<p>ProviDyn 25:23 158:7,8,9,10,11 162:5 191:3,19,20 191:22 194:17 public 1:5 2:10 28:19 31:4 62:18 publicly 22:21 published 19:6,8,15 pull 31:15 punctuation 177:20 209:22 punish 45:24 purchase 122:9 purchased 202:17 purpose 60:4 70:2 72:10 99:5 118:12 144:21 149:13 205:17 purposes 61:16 88:14 133:15 202:14 push 112:18,20 put 11:4 35:19 40:7 43:2 44:12 57:3 58:8 60:10 66:23 74:18 77:16 126:25 128:24 129:1 170:9 195:19 197:6 putting 13:9 20:11 71:6</p> <hr/> <p style="text-align: center;">Q</p> <p>qualification 83:25 84:15 qualify 83:22 87:25 quantum 54:19 quash 56:22 58:2 question 10:22 19:3 55:3 121:24 143:19,21,24 149:25 157:24 172:14 200:7 204:1 questioned 65:7,20 questioning 70:19 155:6</p>
---	--	---	--	---

<p>questions 79:25 88:5,6,23 111:22 116:18 157:16 quicker 62:6 quickly 20:17 quite 53:18 quote-unquote 15:4 32:14</p> <hr/> <p style="text-align: center;">R</p> <hr/> <p>R 5:1 79:1 209:1,1,1 209:1,19,19,19,19 rabbit 83:20 race 38:22 110:3 199:11 raise 6:18 Ran 146:10 random 184:23 185:10 randomness 179:6 Raquel 17:15 80:7 80:12 81:8 rate 52:11,12 65:4 reach 26:11 34:17 131:18 148:15 163:20 165:10 198:2 reached 88:22 124:8 131:19 165:11 198:3 207:13 reaching 86:19 148:7 154:16 171:1,19 180:12 183:5 reaction 150:24 reactive 108:12 149:4 172:4 read 68:19 74:2 85:7 87:12 88:9 104:19 114:25 143:20,23 146:8,19 157:19 readable 118:6 179:2 readily 36:20 120:13 137:1,5 194:22 195:2 201:24</p>	<p>reading 35:16 197:4 reads 50:15 ready 49:23 real 72:19 really 49:18 53:22 53:22 78:4 123:18 136:12 reason 8:12 23:21 39:7,9 42:21 70:22 100:22 103:7 107:14,18 121:16 145:13 152:7 190:4,5 207:21 reasonable 9:15,17 10:19,25 11:10 12:3,21 14:14,16 18:14 20:9,15 21:6 24:9,9 32:18 43:9 46:8,18 47:22 48:4 84:21 85:1 95:22 95:23 104:6,8,15 124:12 137:5 176:20 203:3,14 reasonableness 11:11 124:8 203:11,19 reasonably 11:22 14:24 21:8 48:24 50:20 reasons 46:15 100:16 107:10 120:11 121:9 128:13 129:23 145:2 152:1 183:22 189:22 rebuttal 87:18 recall 86:11 134:16 150:3,6,8,10 162:10 174:7 192:1,3,4 202:22 receive 15:11 25:2 38:16 62:12 170:19 171:9,11 received 22:9 24:22 30:3 61:18 62:15 62:16 76:3,3 81:23 81:25 171:13</p>	<p>receives 95:7 recess 49:20,21 78:14,15 143:14 143:15 208:22 recollection 161:3 recommend 136:6 recommended 41:20 130:22 recommending 45:4 reconciliation 60:1 reconfigure 138:10 159:21 169:12 reconfiguring 196:9 reconvene 143:13 207:3 record 1:5 2:10 7:16 49:22 56:15 79:3 84:13 85:9 86:20 87:23 88:10,12 113:18 127:10 130:10 134:24 143:16,23 144:13 155:2,4 156:22 157:13,19,22 165:12 171:13 172:6 173:23 179:24 206:22 records 39:10,15,17 39:18,24 40:9,13 124:16 164:14,21 RECROSS 1:8 red 91:11,12 REDIRECT 1:8 reduce 96:20 110:15 111:10 177:11 reduces 97:1,2 Reed 3:17 5:19 References 20:5 referring 35:15 117:17 131:11 133:14,16 146:5 150:1,2 151:7,13 159:12 171:5 183:15 188:1 198:15 reflect 128:3 refresh 134:3 161:2 192:10</p>	<p>regard 57:23 78:4 184:14 203:1 regarded 130:7 regarding 39:1 75:2 111:18 115:20 131:20 132:15 194:2 207:7 regards 107:20 144:19 regular 68:5 101:22 142:13,16 167:18 167:19 171:7 regularly 20:18 regulated 65:13 regulation 18:18 19:5 regulations 72:12 rejected 7:4 relate 137:24 169:8 178:5 199:7,21 related 135:5 relationship 122:13 relatively 124:24 132:10 136:1 161:25 162:17 166:14 174:2 175:16 188:5 194:6 202:1 release 190:11,12,12 released 189:18,20 190:3,7 releases 55:10 relegated 172:3 relevant 85:11,14,18 86:5 112:3,9 117:20 124:6 148:19 149:8 150:13 152:3 161:21 163:24 169:7 180:11 187:6,12 relief 45:23 reload 146:18 remediate 195:13 remember 77:24 134:2</p>	<p>remind 9:3 135:13 160:11 162:20 176:10 189:8 remote 113:5 159:18 176:7 184:5,7,25 185:3 185:12 remotely 112:12 116:11 117:1 184:2 191:14 193:10 remove 45:8 removed 153:13,15 164:18 200:4 remuneration 62:12 rendered 172:2,2 repeat 172:14 189:10 200:7 replaced 44:18 report 58:8,15 59:10 59:14 62:16 84:10 85:6 87:12,18,20 88:14 89:6,12 104:18 109:1,12 114:24 121:23 124:5 136:23 148:25 158:7,8,9,9 163:6 167:6 174:8 176:3 187:7,13 188:21 191:19,20 194:20 195:16 197:14 205:6 reported 2:19 145:22 160:23 161:6 reporter 2:19 80:9 reports 59:11 85:23 representation 142:18 representations 62:16 representative 150:22 151:7 represented 49:10 205:13 represents 142:10 request 83:3 115:12</p>
---	--	---	---	---

119:7,12 150:21 198:24 207:22 requested 124:21 requester 119:12 requesting 49:13,16 require 31:9 83:2 178:12 required 15:6 38:4,4 105:6 111:20 176:6 178:3 requires 19:19 46:3 46:6,10 70:4 165:19 185:5 research 13:3 57:1 57:18,23,24 58:7 58:14 62:8,11,17 82:9,10,15 120:21 133:4,9,10 174:9 researchers 105:16 133:11,13 reservation 82:11 reserves 7:22 resolve 28:7 resource 126:10,10 resources 61:1 95:25 96:1 101:14 106:23 109:7,9 129:20 135:3 respect 8:1 173:6 respond 27:7 110:25 respondent 2:5 3:15 4:3 5:11 23:7 26:3 207:19 respondent's 78:4 207:13 response 150:21 152:4 165:14 174:13,19,22,24 responsibilities 44:4 132:19 responsibility 107:24 responsible 92:21 114:12 115:9 132:22 164:24 168:1,20 restart 70:7	restate 143:19 restrict 95:19 166:21 197:18 result 12:22 14:19 15:21 32:2,3,6 43:10,16 44:8 58:10 62:3,17 69:16,18 70:25 104:15 110:8,10 172:10 results 21:25 68:25 115:2 192:19,24 retained 26:3 42:25 70:5 reticent 129:6 retrieve 82:25 94:6 115:13 119:1,8 retrieved 115:1 retrieving 119:14 122:12,19 return 49:19 78:13 93:6 129:9 153:21 returned 119:9 reuse 132:7 178:10 reveal 9:3 17:6 revenues 26:13 review 85:9 148:6 154:15 reviewed 6:13 27:21 27:22 127:22 148:21 149:3 reviewing 108:22 144:15 reviews 149:7 Rica 16:5 74:25 Rick 12:19 right 5:22 6:5,13,20 7:12 9:1,10 11:2 19:15,17 26:5 34:9 75:18,20 78:9 80:3 80:8,15 91:15 98:10 106:9 123:23 137:14 157:23 204:2 205:10,20 207:2 208:19,21 RIPOSO 3:4	risk 11:4 15:19 21:2 21:4,5,7,17 23:2 23:12 25:2,12 26:24 27:10,15 28:15 29:2 36:6 40:3,7 43:3 85:16 97:16,18,24 98:1 108:20 110:2,2,4,6 132:24 133:22,23 135:19 137:1,5,7,8 137:11,12,16,18 137:19,21,24 138:1,5,7,14 140:1 140:18 141:4,5 142:21,22,22 143:25 144:1,2,6 144:11,24 145:4 149:6,11 151:22 152:24 156:15,17 156:24 158:15,17 161:24 162:4,15 162:18 166:5,10 168:23 169:2 173:12,13,15 176:25 189:5 191:7,7 193:18 197:8 risks 13:21 14:19,25 21:15 23:22 24:16 27:20 28:23 37:9 37:23 40:18 44:3 48:2 120:14,24 137:9 157:6,8 159:3 175:23 RMR 209:16 road 43:18 44:9,10 roadblocks 20:12 Robert 187:18,19,20 rodeo 92:2 rogue 73:14 role 178:15 room 66:21 87:24 109:5,5 rooms 109:6 root 159:11,17,18 159:20 Ros 33:16,22 61:3	73:17,20,22,23,25 74:8 router 83:9,10 98:11 98:11,12 100:11 routers 48:16 64:3 83:7 98:12 Rubinstein 3:17 5:19 rule 7:22 19:18 101:2,4 run 23:4 24:22 26:22 27:4 41:17 82:13 100:3 145:6 145:11,25 146:13 146:15 147:25 148:20 158:20 running 66:20 140:7 140:14 145:8 148:3,11 168:21 169:1 173:1 191:9 198:8 RX 1:16 57:17	54:15 55:23 58:16 75:24 83:21 88:2 94:9 106:7 110:21 115:16,18 116:8,9 142:21 143:25 191:24 208:7 says 35:11,12 45:7 52:4 53:25 58:13 69:8 130:20 147:23 197:15 sbrown 32:24 33:6 scan 27:4 139:11,13 139:17,22 140:13 146:10,13 158:12 158:13,14,15,24 191:4 194:17 scanner 146:15 scanning 149:3 scans 14:24 21:19 85:16,17,22 scenario 73:16 97:9 110:17 112:22 scheduled 149:7 scheduling 79:4 207:15,17 science 17:14 18:24 28:24 81:9,17,24 82:1,3,4,6 134:13 134:15 scientific 70:13 scope 105:9 121:20 144:24 164:8 screen 29:19 57:14 61:7 84:8 87:16 89:6 91:20,21 92:7 127:17 130:14 131:6 192:5 search 15:25 16:15 55:10,11,14 56:6 62:10 63:1,4 119:1 119:10,10 121:14 175:11 177:14,17 177:18,21 178:1 181:11,22,25 182:2,3,5,7,12,13 185:23 searches 10:15
S				
S 5:1 34:4 79:1,1,1 134:13,15,18 Sacramento 9:25 52:21 63:17 safeguard 167:10,14 salespeople 112:10 sample 68:23 samples 67:12 69:23 San 16:4 58:25 Sandra 33:1 182:21 182:22,23,23 satisfy 104:13 106:16 125:24,25 satisfying 96:5 106:25 save 61:22 saved 113:14,14 savvy 68:7 saw 87:23 179:18 saying 11:3 14:5 17:2 20:7 23:7,9 23:11 24:8 40:1,11 47:2 51:3 53:14				

<p>searching 16:12,14 16:18 Seated 5:14 second 7:20 13:23 15:1 22:5 23:5 41:1 46:20 64:13 85:7 96:4 105:11 105:13 113:2 115:15 191:12 Secondly 67:22 Secretary 6:24 7:7,9 section 11:9 24:7 32:23 48:20 50:13 50:16,16 124:5 135:11 136:22 163:6 167:6 176:3 188:21 194:20 sector 58:8 secure 34:15 38:10 41:20 44:10 68:9 102:19 104:4 105:8 107:13 132:16 159:2 161:11,12,14,16 161:21 175:3 securing 87:5 107:5 107:25 109:19 149:5 176:21 security 9:17,20 10:3,9,24 11:4,8 11:17,21 12:3,12 12:21 14:13,15,17 15:2,12,14,17,18 17:5,13,16,18,25 18:10,14,21 19:8 19:18 20:8,17,24 21:6 22:11 24:9 25:1,23 31:6,10,23 32:4,19,19 33:11 36:17,20 37:8,18 37:20 38:2,13,15 38:16,21 39:3,9,18 40:2,6,17,18,21,22 41:21 42:5 43:5,6 43:9,11,17,20,24 43:25 44:5,6,17,20 44:22 45:16,19,21</p>	<p>46:4,9,24 47:12,15 47:22,24 48:8,14 48:16,24 51:13,19 52:4,24 53:4,7,8,9 55:18 57:5,16 59:15 65:12 71:2 72:18 76:10,13 77:7 81:14,15 82:14,17 83:12,14 84:22 85:2 88:24 89:15 94:23 95:18 95:22,24 96:5,10 96:15,16 99:9,20 100:11,13 102:10 104:5,6,7,8,15,23 106:14,16,18,19 106:21 107:6,23 108:2,22 109:21 109:24 110:7,19 114:3 121:2 124:9 124:12,19,23 125:2,4,11,15,17 125:19,21 126:3 126:21,23 127:1,6 127:8 128:6,13,24 129:18,24 130:17 130:21 131:4 132:10 133:6,19 135:12,18,22 136:1 137:12,25 138:1,3,6,10 152:13 158:23,25 160:19 167:24 168:2,15,18 170:4 170:9 171:10,12 171:14,21,23,24 172:1,6,9,11,17,18 173:7,8,10 174:1 174:10 175:16 192:23 194:16 197:2 200:5,8 202:19,21,25 203:2,7,9,11,14,19 203:22 security-type 62:4 see 10:17 18:19 30:4 39:12,19 60:6,10</p>	<p>75:1 79:17 91:3 93:23 98:9 122:2 138:18 141:25 142:14,15,16,17 181:4 seeking 28:7 seeks 133:11 seen 65:2 157:13,24 sees 119:13 select 120:1 selection 137:24 send 71:4 95:6 sends 95:9 sense 61:13 sensitive 9:16,25 10:11 11:5 12:4,8 12:13,22,25 14:22 15:3,19 17:3 22:6 22:18 24:22 29:5 33:4 34:18 35:1 36:8 37:10 38:4,5 41:10,25 42:2 45:4 46:1,21 47:18,23 103:14,19,23 104:1,4 106:22 112:14 117:12 126:10 130:7,10 130:22,23 141:12 141:13 160:18 178:18 192:17 sensitivity 43:15 102:23 103:12 178:17 sensor 99:4 sent 130:23 sentence 85:7 104:19 sentences 88:10 separate 59:3 196:22 separated 123:17 series 19:11 20:12 serious 14:20 22:3 served 6:2,2 205:17 server 22:9,13 23:4 24:22 27:3 41:18 82:24 93:18,18,19</p>	<p>94:3,5,5,6 99:15 99:19,23 100:2,3,6 100:8 109:5,5 113:20,22 114:9 114:10,18,19 115:9,13 119:2 122:7,11,19 123:2 123:5,7 145:24 146:10,12,16,18 147:24 148:1 157:9 159:18,23 160:12,15,17 188:10 190:21,22 192:14,16,17,21 192:22 194:17 server's 24:25 servers 14:21 22:4,5 22:19 89:3 99:14 100:2,4,4 112:8 113:7 114:21 116:23 140:22 141:3 147:3,23 148:12,14 166:25 166:25 190:22 202:15 serves 107:15 service 42:21 145:18 146:3 150:21,23 services 12:11 46:15 56:2,3 72:14 86:4 86:4 115:2 164:10 serving 115:10 set 20:22 21:17 25:6 33:12 34:11,12 72:12 76:6 111:4 136:25 137:5 144:11 161:24 170:11 settings 15:15 25:17 37:18,20 38:2 39:3 40:21 130:21 197:2 seven 71:16 104:21 105:1,2,11 106:3 106:11,12 108:3 108:18,19,25 109:11,13,15,16</p>	<p>110:9 137:22 164:5 sexually 17:7 shaking 75:8,10 share 15:24 29:3,4 29:10 61:11,12 119:6,20,23 186:5 198:23 shared 120:2,4 121:4,19 152:16 187:6 sharing 16:3 29:6,7 29:11,15 30:7,11 57:16,17 61:8 119:11,21,22,25 120:12,17,22 121:12 186:22,24 187:10 188:2 195:20 198:20 199:7 Sheer 3:5 5:9 9:8,11 9:13 10:8,14,23 11:3 13:8 14:3,5 14:10 16:11,15,23 17:1 18:20 19:4,7 19:16,21,23 20:5 23:10 24:8,21 25:22 26:4,6,17 28:10 30:1,16,23 31:22 32:3,9,11 33:15 34:1,5,10 35:7,10,14,24 36:3 39:6 40:1,11 41:4 47:4 127:12 sheet 59:8,22,22 61:14,15,15 sheets 52:21 61:19 61:24 62:2 Sherman 3:16 5:12 5:13 8:17,18,25 49:7,9,15,24 50:1 50:8,10 51:17 53:18 54:13,17,20 54:25 55:19,22 56:1,17,23 57:8,11 57:15 58:20 59:9 60:6,16,18,20</p>
--	--	---	--	---

61:15 63:14 64:16 66:9,13 67:1,6,10 68:1 69:15,24 70:4 70:15,20,24 71:10 71:15 73:6,17,21 74:4,7,17,25 75:5 75:9,19,21 76:1,20 76:23 77:11 78:1 80:2,25 84:1 86:14 88:6 142:25 154:19,24 204:8 205:6,12 206:12 206:20 207:4,6,21 208:7,15,20 Shields 28:25 64:7 123:25 Shohl 3:18 short 49:13,17 177:6 185:21 shortly 108:2 shot 29:19 show 9:22 11:8,16 11:20 12:2,15 13:21 14:10,18 17:9,20 20:25 21:3 21:16,25 26:23 27:13 28:18 29:8 30:12,17,24 31:8 32:18 33:8 34:13 36:10,19 37:5 38:3 38:9,14,23 40:16 40:23 41:17,23 42:14 44:5,18,21 45:11 46:20 47:20 50:11 51:11,22 52:7,18,20 53:1 55:6,9 56:9,18,25 57:23 61:19 62:1 62:23 63:7 64:9,12 64:25 65:6,15,17 65:19 67:14 68:2,6 68:15 69:19 70:6,9 71:19 74:20 77:3 77:13 78:5 92:5 101:7 127:11,17 128:5 131:6 159:9 173:23 179:25	192:5,6 showed 63:17 66:7 127:12 showing 39:25 89:6 shown 78:6 120:21 158:22 205:8 shows 25:14 28:17 28:18 29:22 30:10 32:13 44:14 61:17 61:18 88:12 128:7 130:11 159:10 shredded 59:18 60:23 sic 53:6 56:18 side 74:16 82:23,24 87:24 sign 147:12 signaling 83:1 signature 147:10,11 147:12,12,13 signatures 145:11 147:16 significant 12:17 23:22 63:6 similar 60:11 122:3 Similarly 45:7 Simmons 154:14,15 155:5,17,24 156:5 156:7 170:21 171:15 simple 17:23,24 53:18 89:9 101:1 175:11 simply 10:17 40:11 45:1 68:12 72:19 79:16 104:13 single 17:17 sir 14:9 49:15 50:8 56:23 70:20 80:2 84:1 86:11 110:20 110:24 142:25 201:17 208:15 sit 66:12 site 175:9 sites 72:12 six 71:16 sixth 41:21	size 24:11 43:13 71:13 102:4,12 200:24 slide 20:23 29:18,19 29:21,22 31:6,15 31:16 36:16 44:12 48:1 66:6 205:9 slides 67:11 sloppy 68:19 slowdown 148:23 slowly 169:1 173:2 small 43:12 72:16 112:4 174:10 175:13 180:10 181:11 185:23 smaller 182:13,15 snapshot 141:24 Snowden 53:6 73:13 73:15,17 Social 9:20 12:12 17:5 22:11 33:11 42:5 46:24 59:15 114:3 124:19 160:19 192:23 software 76:7 93:15 95:15 97:20 99:12 100:10,15,21 102:2 105:14,23 105:25 106:2 108:13,14 111:19 122:22 124:1 132:21,21 144:8 144:19,21,23 145:3,6,9,12,14 146:1,1 147:2,9,15 148:12,14,16,19 156:19,20,23 158:19 159:24 160:2,5 169:18 189:6,11,20 190:1 190:7 191:6,6,9,12 191:13 196:6 197:1,6 198:4,5,7 198:8 202:7 solution 193:23 194:4 somebody 56:4	63:18 208:17 someone's 68:19 sooner 69:5 200:6 sorry 7:3 33:16 76:5 89:18 154:24 170:23 172:14,15 204:14 sort 39:7 sound 17:22 sounds 21:7 208:10 source 13:13 184:18 sources 19:24 38:25 184:13 south 71:17 space 177:15,17,19 177:21 178:1 181:11,22 182:2,3 182:7,12,14,15 185:23 speak 49:6 SPEAKER 91:5,11 speaking 8:16 special 177:8,19 specialists 44:20 specific 43:8,20 85:24 86:8 100:25 117:8 119:8 125:4 125:6 129:19 131:20 136:2,5 147:14 158:20 175:11 203:7 specifically 11:16 133:6 175:8 specified 104:12 106:23 specify 96:2 104:21 125:23 133:12 170:3 specifying 106:17 135:18 speed 68:11 spelling 209:22 spice 58:14 split 192:5 spot 21:8 26:21 spyware 23:8,13 24:1,6 64:2	square 89:21 stack 92:13 staff 149:1,19 171:2 172:24 188:17 stand 53:8 80:7 93:6 93:21 94:12 129:9 134:1 153:22 154:22 standard 14:6,6,8 19:11 71:23 standards 18:23 19:25 65:13 86:22 86:23 87:1,3,9 88:4 133:20,25 134:19,21,25 stands 94:2 134:2 start 5:5 9:2 18:15 20:9 46:17 51:2 127:5 148:1 167:22 208:3 starting 79:8 88:10 156:9 state 200:19 201:2 stated 98:15 117:9 128:12 130:9 147:9 170:2,18 199:10 statement 54:12 77:25 statements 5:23 9:2 9:5 states 2:1 24:4 39:22 55:13 71:16 74:24 static 20:16 47:15 stating 110:12 status 69:13 201:13 stay 38:21 stead 7:5 stealthy 199:12 step 39:2 80:8 91:19 91:25 92:4 96:4,6 98:4 99:7,9 101:7 101:9 106:15 stepping 84:12 steps 19:12 sticky 187:2 stipulation 6:22,25
---	---	---	--	---

<p>7:7 stopped 41:19 store 61:24 102:16 103:22 112:14 124:14 179:2 196:21 197:9,11 202:12 stored 44:24 102:23 103:4,17 113:5,8 114:10 115:4 116:23 124:13,22 126:14 159:4 160:16 178:24 179:1,4 197:7 200:20 story 61:12 62:5 strangest 73:21 strategies 203:4 strategy 43:11,11 96:11,14 97:13 98:7,25 99:8 101:8 101:9 102:4,9,22 103:13 104:24 110:9 137:20 168:5 169:25 185:4 195:7,11 199:8 strength 36:15 132:5,8 178:6 STRICKEN/REJ... 1:12 stringent 101:3 strong 15:9 31:13,14 33:12 34:12 132:3 132:4 173:19 178:8 179:24 180:17,18,19 188:11 structure 136:12 stuck 208:4 sturdy 18:4 subject 57:19 86:25 submit 50:23 51:17 51:20 63:20 65:16 submitted 6:22 7:3 7:8,23 54:6 87:12 subpoena 56:22</p>	<p>58:2 subpoenaed 74:21 substantial 11:19 12:23 13:5 17:11 48:22 50:19 63:9 64:22 substitute 28:13,15 Subtly 49:16 succeeds 70:7 success 110:16 successful 70:10 96:21 97:5 succinct 51:23 suffer 13:4 sufficient 127:2 141:5 145:3,14 147:2 149:11 156:15 sufficiently 85:10 129:24 131:15,16 suggest 56:9 77:20 suggested 8:9 146:17 148:2 suggesting 40:8 Suite 3:20 4:8 suited 135:21 sum 47:20 summarize 125:18 196:1 summary 204:12,14 204:18 supply 19:1 support 83:8,11 147:4 190:23 supported 148:4 171:13 supporting 41:19 supports 204:18 supposed 72:23 sure 7:18 75:3 90:14 90:16 115:21 142:3 143:22 153:23 179:9 survey 54:1 suspicious 149:20 swear 80:9 switch 90:25,25 91:1</p>	<p>91:2 92:11,12,14 92:14,18,21 93:2 sworn 80:14 Symantec 148:4,5 194:2 system 23:8,15 36:11 37:4,25 41:18 53:16 67:8 72:18 76:17 81:14 94:22,24 96:9 97:6 99:2,3,4 101:22 102:16 103:4 104:16 105:20,20 105:23 107:5,13 107:16,21 108:7 108:17,21 110:13 110:22 111:13 113:19 114:11,15 114:16,17 122:16 123:1 124:13,15 126:14,14,18 130:21 131:24 132:16 135:16 136:18 137:18 138:21 140:7,8,10 140:13,15 147:18 149:5,6 152:11,13 152:20,22 159:2,4 159:4,5 166:20 168:19,24,25 169:3 177:1,4 189:13 190:22 195:10 196:7,10 196:11 199:16 200:19 systematic 28:2,13 28:14 systematically 17:21 27:21 systemic 17:18 systems 15:8 22:16 40:24 42:9 48:9 71:22 105:15 107:4 124:12 132:19 166:24 173:21 175:3 188:25 189:4,9</p>	<p>190:19 194:6 <hr/> T <hr/> T 79:1 134:1,2 209:1 209:1,1,19,19 table 5:9 31:16 32:12 33:24 34:2 take 9:17 49:19 54:9 61:9 65:11 78:9 79:9 102:4,22 104:1 143:12 159:5 193:12 208:17 taken 29:19 47:21 59:2 74:23 78:16 102:17 113:19 178:7 179:4 209:9 takes 11:11 24:10 43:12 102:8,8,12 136:17 182:16 talk 19:12 36:4 43:5 73:25 113:24 124:1 talked 45:10 58:20 106:5 108:8 145:19 152:25 165:23 195:25 talking 18:18 19:2 23:25 28:8,9 31:19 35:5,18 36:5 57:7 57:8 59:7 83:17 108:1 123:19,21 talks 108:16 taxpayer 16:24 55:21 56:12 Team 174:13,20,22 Tech 82:3 technical 17:23 57:8 70:13 104:5,7 179:9 technicians 67:4 76:5,6 techniques 110:5 138:22 158:17 technological 77:15 technologically 68:7 Technologies 86:16</p>	<p>technology 18:25 19:25 55:13 63:8 68:9 77:6 82:1 134:6,9,10,11 135:1 167:20,21 167:22,25 tell 23:17 30:16 34:3 56:7 58:4,9,18,18 65:10 141:10 telling 47:4 56:14 tells 43:25 56:18 ten 71:13 105:16 112:7 189:11 201:15 ten-minute 79:10 tenure 81:20,21 terms 8:12 51:23 77:6 175:12 179:9 188:15 Terrific 7:12 test 17:5,6 21:25 24:21,25 25:8,13 25:20,22,25 26:9 36:14 42:24 68:12 68:13,20,22,24,25 69:17 138:15 139:4,5,12,16 140:25 141:16 144:9 162:12 192:19,24 tested 25:10 tester 25:8 26:14,18 testers 26:20 testified 56:18 80:14 109:20 125:16 129:22 134:21 154:4 156:9,11,14 157:2 169:5 172:9 172:16 189:7 196:13 testifies 58:23 testify 68:16 74:20 76:12,14 127:25 156:7 testifying 205:18 207:10 testimonies 154:9</p>
---	--	---	--	--

testimony 58:24 59:16 61:5 62:9 74:7 75:5,10 77:14 85:16 89:14 127:22 128:3,19 150:22 151:13,16 154:15 155:18 156:1,22 170:18 170:23,23,25 171:16,16,19 183:4,9,11 187:10 187:25 202:22 204:15,16,17	116:12,14 129:5 140:5 185:8 202:19 things 8:22 20:6 24:18 64:4 71:17 72:6 85:21,24,25 87:7 96:8 100:5 102:17 103:25 108:22,24 114:2 135:15,22 136:10 138:19,24 157:13 168:18 169:4 173:6,9,18 181:2 196:9 197:6 200:25 think 8:20 35:10 56:12 61:16 63:6,9 64:24 74:17 76:11 77:22 79:5 84:14 91:22 93:5 103:5 103:16 104:3 112:7 115:22,24 117:10 143:4,4,8 147:11 154:20 174:7,8 182:23 201:14,16 205:16 208:8 third 15:10 16:11,16 22:17 31:3 36:17 52:11 96:6 106:3,4 204:20 third-party 46:7 77:1 thorough 28:11 51:23 thought 204:11 thousand 12:10 13:18 42:20 152:14 163:14 164:14 thousands 9:19 12:5 22:10 24:23 70:2 threat 103:8 138:12 165:24 threats 15:13 20:11 20:16 38:20 47:16 109:25 132:23	137:14 149:20 168:8 three 14:16 30:5 59:3 66:21 76:24 110:15 154:3 205:12 three-year 64:18 Thursday 79:23 208:3 tie 58:6 time 6:18 8:21,24 34:5 57:5 58:4 60:14 71:11 85:3 85:11,14,18 86:5 112:3,9 113:17 117:20 118:20 121:13 136:17,20 136:21 143:2,12 148:18,19 149:2,8 149:9 150:14 152:3 161:21 162:9 163:24 164:23 166:23 169:7 180:11 182:16 183:13 187:6,12 188:15 188:17 190:10 202:10 203:16 206:16,24 207:23 208:17 timeline 44:13 127:21 204:4,19 204:21 timely 173:20 189:4 timer 9:6 times 27:2 71:13 145:5 tip 17:16 tissue 67:12 title 50:16 209:4 Tiversa 55:9,10,12 55:16 56:24 57:1 57:19 58:3,9,14 62:8,9,14 Tiversa's 57:23 today 6:3 24:3 31:21 74:2 80:18 127:13	143:7,9,9 196:13 205:18,24 206:22 token 184:22 185:9 told 172:24 tomorrow 79:8 143:10 207:3 tool 21:12 23:14 107:15 138:16 139:20 141:19,22 152:24 156:15 162:8,21 tools 21:8,14,17 23:12 26:24 28:16 43:21 44:1 45:6 130:9 138:5,23 140:1 149:11 162:4,6 166:19 top 55:6 92:10 159:7 159:8 198:13 topic 112:1 topics 135:7 totality 24:17 totally 146:18 touch 187:3 town 79:13 208:4 trade 1:1 2:1,14 3:3 3:7 50:12,14 209:10 traffic 27:15 83:8 98:16,17 100:23 100:25 108:11,23 141:22 149:14,15 149:18,19,22 162:21 197:16,21 197:25 train 38:15 40:17 48:7 trained 15:11,16 136:16 167:9 training 15:12 38:13 38:17,18,20,23 39:1 44:3 76:3,4 107:3,15 109:14 132:17,22 135:6 167:14,24 168:3,7 168:13,15 169:9 169:20,23 170:6,8	170:15,17,19 171:2,10,12,14,21 171:24 172:6,11 172:18 173:8,15 173:25 174:1,6,9 174:10,12,15,17 175:16,21 transcript 151:3,11 154:13,20,21 155:1,5,25 156:6 170:21 182:21 187:18,23 209:7,8 209:21 transcripts 144:15 transfer 22:8 67:16 68:8 93:18 94:2,5 94:7 113:16,23 161:12,20 transferred 68:18 90:22,24 114:21 199:3 transferring 94:8 transfers 160:14 transform 118:5 transformation 179:11 transition 128:8 translates 179:17 translation 142:2 transmission 130:7 transmit 33:10 104:4 114:1 130:10 transmits 161:13 transmitted 17:7 36:8 114:2 130:11 142:15 144:18 161:15 treatment 9:4 treaty 74:23 trial 1:4 2:9 20:3 56:15 Tried 146:15 147:25 tries 108:10 trolled 56:3,6 trolling 55:17,24 truck 31:18
---	--	---	--	---

true 13:18 30:8
 54:22 150:6 157:1
Truett 151:4,5,6
Truett's 77:2 151:11
trust 77:18 123:16
 123:18,20,22
trusted 122:7,12
trustworthy 200:19
truth 56:19
try 90:17,18 91:9
 139:8,18 177:24
 181:11,16,18,20
 195:9,11 199:12
 199:14
trying 16:16 23:5
 60:4 87:25 89:19
 121:14 125:22
 134:2 140:13
 181:6
turn 20:24 23:3 31:5
 38:12 43:4 89:5
 91:7 92:6 108:3
 111:25 121:22
 124:7 136:22
 147:19 159:23
 161:1 170:20
 171:15,17 185:13
 192:7 194:14,19
 195:15 196:19
 198:12 203:8
turning 24:21 37:19
 41:21 45:23 63:12
 91:9 169:23 171:7
turnover 44:15
 107:19 128:8,15
twice 10:22
two 6:19 9:7,8,22
 12:24 22:3 29:22
 31:1 41:18 45:12
 49:10 83:4 88:9
 123:6,17 131:10
 152:1 154:3
 184:12,13 185:5
 192:8
two-factor 184:4,11
 184:12,19,24
 185:2

type 23:8,13 25:20
 52:14 61:21 89:3
 99:1 139:10 141:4
 142:21,22 144:1,1
 145:20 157:25
 190:9
types 21:13,15 42:12
 42:15 72:6 85:10
 85:15,25 87:6
 88:15 98:23 99:18
 100:5 102:23
 108:24 113:25
 114:4 120:14
 124:17,20 125:22
 126:2 135:7,9,10
 135:19,22,24
 136:3,5,9 138:13
 138:22 139:25
 140:2 144:5
 152:16 157:6
 160:16 165:15
 167:16 169:4
 173:17 178:16
 185:5,16 192:20
 192:23,24 197:9
 200:25
typically 7:22 115:1
 115:8 122:10

U

unable 13:12,12
 39:8 51:12,21
 70:11 168:12
unauthorized 11:13
 12:24 15:14,19
 17:9 23:18 34:21
 35:1 36:21,24 37:3
 37:9,13 38:1 40:20
 41:10 45:8 48:5
 52:11 76:16 97:10
 97:15,17 98:8
 108:10 126:9,13
 149:14 169:17
 176:25 184:9
 194:23 195:3,6,12
 195:19 197:20
 199:16 201:10,25

uncertainty 177:12
 177:14
understand 5:24
 24:2 35:14 39:21
 72:4 78:1 97:21,22
 104:10,12 109:15
 136:12 138:20
 139:1 157:18
 168:22 169:2,14
 175:22 179:9,19
 196:8 206:7
understanding 7:17
 7:21 18:15 65:24
 70:24 175:24
understood 13:24
 47:1
unencrypted 130:12
unfair 11:9 12:5
 48:20 50:12,18
 63:22,23 64:21
UNIDENTIFIED
 91:5,11
unique 90:5 147:13
 147:13 178:12
uniquely 90:7 92:19
United 2:1 24:4
 39:22 55:13 74:24
University 17:14
 28:24 81:9,17,18
 82:4
unlawful 50:17
unnecessary 37:8
 149:14
unnneeded 106:8
unpack 184:10
unpatched 14:21
 140:10,15
unprecedented
 55:15
unreadable 118:1
unreasonable 10:9
 22:1 40:3
unrestricted 37:7
untoward 123:8
Untrained 27:7
unused 94:24 95:11
 106:9,10 135:17

141:3
unwanted 149:14
 197:16
up-to-date 27:5
 38:19
update 40:24 41:14
 48:9 122:2,3,6,6,9
 122:12,19 145:11
 147:15,25 148:2
 189:3,9 190:18
 191:2 194:6,10
updated 41:12
 138:21 145:6
 146:2,2,14 147:6
 188:24
updates 40:22 41:4
 106:1 146:13
 168:9
updating 20:19
 41:16 122:10
 135:16 147:24
 173:21,21
upgrade 148:3
upload 159:22
upper 30:9,9
uppercase 177:16
 182:10
urgent 22:2,5 25:1
 25:12 36:22 41:7
urine 67:12
use 9:15 14:12 15:7
 18:9,21 21:16 22:7
 22:25 26:24,25,25
 30:15 31:9,13,14
 32:13,14 33:9 35:3
 35:20 36:14,19
 39:13 41:23 42:8
 42:24 44:2 48:4,10
 61:11 62:25 72:13
 80:18 83:2 90:10
 90:24 95:5,14
 96:11 98:3,19
 99:11 102:19
 107:16 111:3,4
 114:11 116:22
 132:3,20 138:14
 140:19,25 144:6

144:10 145:13
 147:1,1 156:16,24
 161:16,23 166:19
 176:7,22,24 177:2
 177:16,18 179:20
 179:22 181:7
 184:24 185:16
 188:4 195:2
 196:24 199:9
 200:21 201:20,23
user 25:7 28:3 31:16
 32:12,24 33:23
 82:22 101:10,11
 101:13,14,17,20
 111:18 119:25
 131:25 132:1
 176:14 178:16,16
 184:14 186:2,14
 186:17,18 189:24
user's 29:13
users 15:24 27:23
 28:9 29:3,6 37:13
 48:3 101:22
 119:19 176:13
 178:12 180:5,21
 184:5,8,25 185:12
 185:22,24
uses 93:2,10 158:17
 177:7
usually 147:12
 152:4 175:9 179:3
 184:18 190:10

V

value 118:4 123:4
 179:16,17,19
Van 12:20 13:2 52:7
 65:5,6,9 207:10,16
 207:18
VanDruff 3:4 5:7,8
 6:1,7,11,19,21 7:2
 7:8,12,17 8:4,7,11
 8:15 80:1 91:7
 207:12
variety 18:10 21:14
 23:11 26:21 85:15
 139:21 195:8

196:25
various 16:9 109:17
 138:22 139:9
 158:17 165:15,15
 195:18
varying 139:10
 177:10
vendor 41:14 85:23
 86:3 189:16 194:2
 194:11
vendors 105:25
 122:9 168:9
verify 46:7 122:11
 186:13
verifying 176:12
Veritas 191:6 198:3
 198:5
version 204:4 205:2
versions 131:10
vertical 32:15
victims 13:9,11
video 82:12,25
 120:13
view 42:13
violation 10:6,13,24
 24:7
virtually 152:9,23
 189:16
virus 23:8 24:6
 145:11 146:2,10
 146:13,14,15
 147:5,8,13,14
viruses 23:17 145:9
 147:17
VOIR 1:8
volume 1:4 2:9
 55:15 102:22
vulnerabilities
 14:20 18:16 20:10
 20:13 21:9,11,13
 21:21 22:3,6,17,20
 22:23 23:1,15,24
 24:16 25:16 26:7
 26:22 27:12,16
 34:16 36:23 40:2,6
 82:18 86:6 105:15
 108:21 138:9

140:9,11,17
 158:19 168:10
 173:22 189:5,17
 189:20,24 191:5
 191:11
vulnerability 14:24
 21:19 25:4,10,14
 26:7,19 36:5 41:8
 41:9,13 87:6 97:5
 97:18 110:4,4
 111:6 137:18
 158:12,13,14,24
 159:11,12,16
 160:9 168:23
 174:25 189:12
 191:4,10,12,13
 193:3,4,7,9,11,15
 193:16 194:3
 198:5,6,14
vulnerable 159:3

W

wait 64:13 69:1
 168:25
walk 95:1
walk-around 28:1
 45:10,12 48:15
walls 18:5 48:18
want 6:6 35:3 54:19
 68:23 75:2,7 87:22
 90:14 97:12,13
 100:16,24,25
 101:1,11,16
 103:20,22 104:3
 109:3 110:10
 111:3,4 115:24,25
 140:9,25 141:12
 157:12,23 177:13
 178:11,19,23
 197:8 206:3,21
wanted 7:18 74:9
 82:24
wants 49:12 63:16
 69:3
warn 27:1,5
warnings 27:8 39:14
 120:24 121:2

wary 71:1
Washington 2:16
 3:11,21 4:9
wasn't 6:23 7:18
 64:4,5,7,8 65:8
 73:10 85:17 149:7
 173:24 197:25
way 8:23 10:10
 11:20 16:25 18:11
 35:11 37:4 40:6,12
 48:23 52:9 56:12
 67:15 71:7 75:9
 77:8 82:21 95:21
 95:23 107:1
 113:12,16 115:8
 123:18 140:20
 150:17 154:5
 170:5 176:12,14
 179:1 184:6,7
 187:1
ways 36:7 53:2
 113:12 132:23
 184:13 195:9
 196:25 199:14
we'll 9:8 31:6 36:4
 43:5 49:19,19 79:9
 84:16 108:1
 113:24 143:12
 204:22 205:1
 208:12
we're 19:12 24:8
 49:20,22 51:6 59:7
 75:25 78:9,11,13
 78:14 79:7,8 84:11
 143:14 201:12
 205:23 208:4,7,22
we've 45:10 53:5
 58:20 79:17 106:5
 108:8 148:13
 203:6 205:24
weak 34:20,23 177:2
 177:5,6 179:25
 183:23 184:3
 185:19
weaknesses 18:16
 20:10,13
Web 72:12 93:17

113:12,15 115:3,6
 115:7,8,9,13 175:9
webmaster 76:19
week 5:18 7:16
 49:10 124:1
well-known 14:20
 25:13 28:23 34:20
well-trained 54:10
went 14:21
weren't 15:16 90:18
 112:11 202:13
 205:14,15
Whalen 2:19 209:16
whereabouts 74:14
widely 120:9,10
 138:16
William 3:16 5:13
william.sherman...
 3:23
willy-nilly 77:21
window 190:14
Windows 15:8
 29:12 36:10 37:12
 37:19,24 41:18
 105:20 166:20,24
 166:24 188:10
 189:13 190:21,23
wipe 146:18
Wireshark 138:24
 141:19,21,22
 162:18,20,21
 163:3,4
wished 27:24
withdraw 6:25 7:14
witness 1:8 51:24
 53:8 74:16,18
 78:11 79:12 80:4
 80:13,17,22 84:13
 86:11 91:13,25
 92:4,8 93:6,21
 94:11,13 110:20
 110:24 111:2,15
 115:21 116:1,9,14
 122:5,18 123:3,11
 123:21 127:12
 128:17,18 129:9,9
 134:18 143:3

144:3 153:5,6,20
 153:21,22 155:7,7
 155:9 157:15
 160:24 193:20
 205:17 206:25
 208:14
witnesses 12:19
wondering 20:2
Woodson 33:22
 61:3 73:17,22,23
 73:25 74:8,12,20
word 142:3 181:5
words 177:18 180:1
 181:8 208:13
work 33:3 42:11
 58:10 83:13
 111:20 115:7,8
 119:6 145:20
 147:6
worked 82:20,21
 156:8
working 28:4 34:8
works 61:10 72:19
 92:13 97:23 139:4
workstation 99:10
 99:15,19,23 100:2
 100:6,8,21,23
 101:4,18
workstations 65:24
 89:3 99:13,25
 112:5 148:17
 195:23
world 10:17 72:20
 140:23
worry 7:11
wouldn't 54:9
 179:18
write 112:20,24
 113:3,4 159:17,20
 160:14
writable 159:11
writing 107:7,10,14
 107:18 113:1
 128:25 129:1,15
 129:25 131:12
 187:1
written 43:6,16,18

<p>44:6,9 45:15 46:3 107:22 113:21 114:8 127:1,6,8 128:6,13 131:3 172:5 wrong 155:10</p> <hr/> <p style="text-align: center;">X</p> <hr/> <p>X 1:2</p> <hr/> <p style="text-align: center;">Y</p> <hr/> <p>yeah 64:5 69:8,9 94:18 134:18 year 27:4 34:5 69:24 147:8 years 14:21 15:6 17:19 18:22 22:22 25:13 31:1 41:19 45:12,18 63:3 66:8 66:10,15,16 70:5 76:20 81:12,19 154:3 161:10 180:5 yellow 30:6 32:15 yesterday 207:13</p> <hr/> <p style="text-align: center;">Z</p> <hr/> <p>zero 142:17</p> <hr/> <p style="text-align: center;">0</p> <hr/> <p>01 204:4,14 205:1 02 204:6 205:4 06 147:25 070 24:24 25:12 26:10 36:6 0930 207:3</p> <hr/> <p style="text-align: center;">1</p> <hr/> <p>1 1:4 2:9 20:23 31:6 36:16 48:1 127:12 127:20,21,23 128:3,5,7,24 151:12 153:6,9,19 158:22 170:22 194:14 204:18 1:00 79:21 1:45 78:13 1:51 79:2</p>	<p>10 117:14,15,16 10,000 10:1 13:1 198:4 10:11 2:8 102 194:20 104 195:16 104(a) 195:21 104(b) 196:19 104(e) 197:14 11:00 79:21 11:30 49:19 79:21 12 156:5 12:37 78:15 13 183:8 14 156:5 161:7 170:24 15 67:2,24 171:17 15-story 66:21 16 142:10,11 151:12 167 180:8,9,10,12,16 17 89:5,11 161:10 1718 16:6 17:3,15 28:17,18 29:16 30:7 31:3,25 33:5 38:6 46:13 52:19 57:21 58:5,17,24 59:7,9,14,25 60:8 60:12,13,14,25 61:4,17 62:15,17 183:1,3 19 159:6,8 1919 4:7 1993 161:7 1998 162:19 1999 25:14 120:8</p> <hr/> <p style="text-align: center;">2</p> <hr/> <p>2 5:24 6:9,14,15 7:5 89:7,8,9,11,14 90:11 93:22 98:3 100:9 101:7 145:16 146:6 2:00 79:21 20 1:6 2:7 67:2,24 183:9 209:5 20004 3:21 20006 4:9</p>	<p>2002 82:7 2003 105:20 2004 57:4 190:24 2005 26:12 29:1 33:2 34:5 41:14 68:5 76:20 85:4 118:21 121:3 146:3,15 147:6 153:12 200:4 203:17 2006 29:9 33:7 69:17 76:20 118:21 146:4,20 147:7,21 153:12 156:10,10,12 183:13,19 190:20 200:4 2007 76:21 77:4,7 193:24 2008 77:12 153:16 153:17,18 162:11 200:4,10 2009 156:10,12 187:14 2010 14:25 21:24,25 22:21 25:13 31:16 32:12 36:22 44:7,8 50:12 69:17 85:4 127:1,9 129:1 131:4,12 144:8 156:16,25 157:3,7 162:12 193:17 203:17,20 2011 77:8 2012 81:21 2013 33:7 59:2 183:14,19 2014 1:6 2:7 70:23 209:5,13 202 3:12,22 4:10 20580 3:11 21 147:21 216 139:14 22 192:7 193:2 198:13 22nd 79:23 24 209:13</p>	<p>25 67:1 81:12 174:11 187:24 26 187:22</p> <hr/> <p style="text-align: center;">3</p> <hr/> <p>3 146:20 147:7,20 3.41(b)(6) 7:22 3:30 79:22 3:45 143:13 30.5 52:12 54:2 31 104:18 109:1,12 326-2999 3:12 35 26:13 67:2 145:16,17,18 146:6 147:20 372-9100 3:22 38 114:24 115:16 116:7</p> <hr/> <p style="text-align: center;">4</p> <hr/> <p>4 183:9 192:6 4.0 41:18 4:00 79:22 40 26:13 404 57:17 48 85:6 49 87:21 121:22 124:5 499-2426 4:10</p> <hr/> <p style="text-align: center;">5</p> <hr/> <p>5 11:9 24:7 48:20 50:13 57:4 191:7 198:6 5:00 79:24 5:30 79:8 201:12 5:38 208:24 50 97:4,7 105:21 110:12 112:5 189:14 51 192:6 57a 50:16</p> <hr/> <p style="text-align: center;">6</p> <hr/> <p>6 1:20 29:18,19 57:4 68:5 117:14,15,16 130:13,13 131:7,8</p>	<p>131:9 170:24 171:17 600 2:15 3:10 61 170:23 171:15,17 610 3:20 62 171:18 63 136:23 65,000 139:15 650 4:8 67 191:17,18,19 192:1,7 193:2 194:15 198:12 69 151:10</p> <hr/> <p style="text-align: center;">7</p> <hr/> <p>7 29:21,22 43:4 68:5 124:5 131:7,8,9 148:4 70 25:19 157:11 158:5,6,7,22 159:7 159:9 191:21 706 182:19,20,21 719 187:16,17,18 72 161:2 731 151:1,2,3 734 154:11,12 155:4 155:16,17,19 170:20 171:16 737 87:15,17,18 740 84:7,9,10 87:20 161:1,2 750,000 11:5 12:8 42:3 46:2,22 47:7 47:18,23 88:13 124:16 78 155:24 163:7</p> <hr/> <p style="text-align: center;">8</p> <hr/> <p>8 31:15,16 156:5 80 155:24 801 3:19 81 1:9 86 167:7</p> <hr/> <p style="text-align: center;">9</p> <hr/> <p>9 44:12 187:23 9:30 79:7,8 208:21</p>
--	--	--	---	--

900 29:14
93 176:4
9300 13:16,22 16:7
17:4 46:13
9357 2:4 5:3 209:3
950 30:10
97 188:22

--	--	--	--	--