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

FEDERAL TRADE COMMISSION
INDEX
IN RE LABMD, INC.
TRIAL VOLUME 1
PUBLIC RECORD
MAY 20, 2014

WITNESS:	DIRECT	CROSS	REDIRECT	RECROSS	VOIR
HILL	81				

EXHIBITS	FOR ID	IN EVID	IN CAMERA	STRICKEN/REJECTED
CX				
(none)				
RX				
(none)				
JX				
Number2		6		

2

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

```
In the Matter of                    )
                                    )
LabMD, Inc., a corporation,         ) Docket No. 9357
                                    )
                        Respondent. )
------------------------------------)
```

May 20, 2014
10:11 a.m.
TRIAL VOLUME 1
PUBLIC RECORD

BEFORE THE HONORABLE D. MICHAEL CHAPPELL
Chief Administrative Law Judge
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C.

Reported by: Josett F. Whalen, Court Reporter

3

APPEARANCES:

ON BEHALF OF THE FEDERAL TRADE COMMISSION:
LAURA RIPOSO VANDRUFF, ESQ.
ALAIN SHEER, ESQ.
MARGARET LASSACK, ESQ.
Federal Trade Commission
Bureau of Consumer Protection
Division of Privacy and Identity Protection
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580
(202) 326-2999
lvandruff@ftc.gov

ON BEHALF OF THE RESPONDENT:
WILLIAM A. SHERMAN, II, ESQ.
REED D. RUBINSTEIN, ESQ.
Dinsmore & Shohl LLP
801 Pennsylvania Avenue, N.W.
Suite 610
Washington, D.C. 20004
(202) 372-9100
william.sherman@dinsmore.com

4

APPEARANCES: (continued)

ON BEHALF OF THE RESPONDENT:
KENT G. HUNTINGTON, ESQ.
MICHAEL PEPSON, ESQ.
Cause of Action
1919 Pennsylvania Avenue, N.W.
Suite 650
Washington, D.C. 20006
(202) 499-2426
kent.huntington@causeofaction.org

5

P R O C E E D I N G S

- - - - - -

JUDGE CHAPPELL: Call to order Docket 9357, In Re LabMD, Inc.

I'm going to start with the appearances of the parties, government first.

MS. VANDRUFF: Good morning, Your Honor.

Laura VanDruff for complaint counsel.

With me at counsel table is Alain Sheer and Maggie Lassack and Jon Owens.

JUDGE CHAPPELL: And for respondent?

MR. SHERMAN: Good morning, Your Honor.

William Sherman on behalf of LabMD.

Seated next to me on my left is Mr. Michael Daugherty, who is the owner and CEO of LabMD.

Next to him is Kent Huntington, who you met last week, counsel from Cause of Action.

Next to him is my law partner, Reed Rubinstein.

And next to him is co-counsel Mike Pepson, also from Cause of Action.

JUDGE CHAPPELL: All right. Thank you.

Before I hear your opening statements, I'm going to admit -- I understand there's a JX 2, and we have copies of it?

6

MS. VANDRUFF: Your Honor, this morning we served copies -- complaint counsel served copies on Your Honor's office. I have copies for the court today as well if that would be helpful.

JUDGE CHAPPELL: Right. Let's have the original. If you want to approach the bench.

MS. VANDRUFF: Certainly, Your Honor.

(Pause in the proceedings.)

JUDGE CHAPPELL: This is the same JX 2 that was e-mailed to my office?

MS. VANDRUFF: That was e-mailed this morning, that's correct, Your Honor.

JUDGE CHAPPELL: All right. I've reviewed this exhibit and JX 2 is admitted.

(Joint Exhibit Number 2 was admitted into evidence.)

JUDGE CHAPPELL: Any other evidentiary or procedural issues to raise at this time?

MS. VANDRUFF: Two, Your Honor, if I may.

JUDGE CHAPPELL: All right.

MS. VANDRUFF: The first is that the parties had jointly submitted a prior stipulation, and I don't know, because it wasn't filed with the Office of the Secretary, whether there is any process we must dispense with in order to withdraw that stipulation.

7

JUDGE CHAPPELL: Was it part of a motion?

MS. VANDRUFF: No, Your Honor. It was submitted prior to the preliminary -- sorry -- the pretrial hearing and Your Honor rejected it, and in its stead is JX 2 which you've just admitted.

JUDGE CHAPPELL: So it was filed as a joint stipulation with the Office of the Secretary.

MS. VANDRUFF: It was submitted to Your Honor. It was not filed with the Office of the Secretary.

JUDGE CHAPPELL: If it was not filed, then don't worry about it.

MS. VANDRUFF: All right. Terrific.

JUDGE CHAPPELL: And anything that has been filed, you can always do a joint motion to withdraw, but since it was not, it's of no concern. I handled it on the record last week.

MS. VANDRUFF: That was my understanding, Your Honor, but I wanted to make sure that there wasn't something more that the parties needed to do.

On a second issue, Your Honor, it is the parties' understanding that consistent with rule 3.41(b)(6) that Your Honor typically reserves closing argument until after the parties have submitted their posttrial findings of fact and conclusions of law.

8

Is that Your Honor's intent with respect to this proceeding?

JUDGE CHAPPELL: Yes.

MS. VANDRUFF: Thank you, Your Honor.

JUDGE CHAPPELL: Is that what you would desire? Is there an objection to that?

MS. VANDRUFF: There's no objection to that, Your Honor.

JUDGE CHAPPELL: It's always been suggested by the parties. That's why I do it.

MS. VANDRUFF: There's no objection, Your Honor. Just in terms of planning, that was the reason for our inquiry.

JUDGE CHAPPELL: Okay.

MS. VANDRUFF: Thank you, Your Honor.

JUDGE CHAPPELL: Is she speaking for you, Mr. Sherman?

MR. SHERMAN: We discussed that briefly, prior to Your Honor coming on the bench. Again, just a little foreign to me, but I think that as long as we know ahead of time, we can accommodate it.

JUDGE CHAPPELL: Things flow better logically that way. All the briefing is done, and then I hear the closing at that time when it's all in front of me.

MR. SHERMAN: Very well.

9

JUDGE CHAPPELL: All right. Let's have opening statements. I'll start with the government.

And I remind you that you're not to reveal information that's been granted in camera treatment during your opening statements.

Are we going to need a timer or are you going to be well under the two hours?

MR. SHEER: Your Honor, we'll be well under two hours.

JUDGE CHAPPELL: All right.

MR. SHEER: Good morning.

May it please the court.

I'm Alain Sheer, complaint counsel.

This case is about a medical testing laboratory that failed to use reasonable measures to protect sensitive information entrusted to it.

By failing to take reasonable security measures, LabMD exposed information about hundreds of thousands of consumers, including their names, Social Security numbers and medical testing information, to people who never should have had it.

The evidence will show that in two documented incidents, one involving a popular peer-to-peer file-sharing program and the other involving identity thieves in Sacramento, sensitive personal information

10

for nearly 10,000 consumers was disclosed without authorization.

The company's security practices --

JUDGE CHAPPELL: Is it your position that the information that was on the peer-to-peer file-sharing program, LimeWire, that was a violation of the law, merely posting it on that? Is that your position?

MR. SHEER: That is a consequence of the company's unreasonable security practices and is indicative of the way the practices failed to protect sensitive information.

JUDGE CHAPPELL: But if I heard you correctly, mere posting of the information is not a violation.

MR. SHEER: The posting of the information makes the information available to anyone who searches on the P2P network to find it. It is there for the world to see. And by simply disclosing that information and making it available, the company has demonstrated that its practices were not reasonable and appropriate.

JUDGE CHAPPELL: So that's a yes or a no to my question? I asked you twice.

MR. SHEER: A breach itself may not by itself be a law violation, but it is indicative that security practices are not reasonable and appropriate, and that's

11

the circumstances here.

JUDGE CHAPPELL: All right. Go ahead.

MR. SHEER: As I was saying, the company's information security practices put at risk very sensitive information of as many as 750,000 people whose information is maintained on the company's network.

The evidence will show that LabMD's security practices were unfair under section 5 of the FTC Act because they were not reasonable.

Reasonableness is a flexible concept that takes into account all of the circumstances, including actual and potential harm from unauthorized disclosure of consumer information and the costs of preventing the harm.

Specifically, the evidence will show that LabMD's security practices caused or are likely to cause identity theft, medical identity theft and other substantial harms.

The evidence will show that consumers had no way of knowing about LabMD's security practices and thus could not reasonably avoid those harms.

And because the failures could have been corrected at low cost, there are no countervailing benefits to consumers or competition.

12

The court will hear from LabMD about extraneous issues, but the evidence will show that the company's failure to provide reasonable and appropriate security for the very sensitive information it maintains about hundreds of thousands of consumers was an unfair act or practice.

LabMD collected and maintained the most sensitive kinds of information for 750,000 consumers, including information about approximately a hundred thousand consumers for whom it never provided any services at all. In addition to names, addresses, dates of birth and Social Security numbers, LabMD also maintains their sensitive health and financial information.

The evidence will show that if this information is disclosed, it can be used to perpetrate identity theft, medical identity theft and other significant harms.

Complaint counsel's expert witnesses, Rick Kam and Jim Van Dyke, will explain that LabMD's failure to provide reasonable and appropriate security for sensitive information is likely to result in concrete and substantial harms to consumers.

In the two documented incidents of unauthorized disclosure of sensitive information involving the

13

information of approximately 10,000 consumers, Mr. Kam and Mr. Van Dyke will describe, based on their experience and research, the likelihood that consumers will suffer identity theft, medical identity theft and other substantial harms.

JUDGE CHAPPELL: Do you plan to offer any evidence of actual harm in this case?

MR. SHEER: Complaint counsel will not be putting up identity theft victims, but that does not mean that actual harm did not occur. And that is because, in many cases, identity theft victims are unable to connect up the dots. They're unable to identify the source of the information that was used to harm them.

And that's particularly the case here because LabMD did not provide notice to the 9300 consumers whose information was found on the P2P network. And that's especially true for the hundred thousand people whose information -- who did not even know that LabMD had its information, their information.

The evidence will show that these risks are particularly acute for the 9300 consumers --

JUDGE CHAPPELL: Hang on a second.

So if I understood your answer, you don't plan to introduce evidence of harm, but your position is that doesn't mean no harm occurred? Is that what you said?

14

MR. SHEER: That's correct.

JUDGE CHAPPELL: Okay.

MR. SHEER: And I'm also saying, though, that the legal standard is that we -- the legal standard is caused harm or is likely to cause harm.

JUDGE CHAPPELL: I'm aware of the standard, sir.

MR. SHEER: The evidence will show that consumers cannot avoid these harms. Physicians, rather than consumers, decide to use LabMD. Consumers do not have information about LabMD's security practices and cannot evaluate whether the practices are reasonable.

LabMD's security failures were not close to being reasonable. As a preview, consider three obvious, longstanding security issues at LabMD.

First, the evidence will show that LabMD failed to adequately assess risks, with the result that very serious, well-known and easily fixed vulnerabilities went unpatched for years on the company's servers that handled sensitive information.

For example, it did not conduct external vulnerability scans to find commonly known or reasonably foreseeable risks until 2010.

15

Second, despite it being common knowledge that easily guessed passwords are a security no-no, LabMD allowed employees with access to sensitive information to log into their computers using, quote-unquote, "LabMD" as their password. One such employee used this password for years without being required to change it. LabMD did not use the password management function already built into the Windows operating systems it was using to ensure that passwords were strong.

Third, IT employees and non-IT employees were inadequately trained. IT employees did not receive periodic security training to keep up with evolving threats and how to address them. Some non-IT employees could install unauthorized programs and disable security settings on their computers without approval, but they weren't trained that doing so could compromise the security of LabMD's networks.

These and other security failures increased the risk of unauthorized disclosure of sensitive information on LabMD's network.

One result was that an employee installed a peer-to-peer file-sharing program called LimeWire on a computer used by LabMD's billing manager. LimeWire allows users to designate files that they will share from their own computers, search for files on other computers and download them.

16

An insurance billing file that was designated for sharing from the billing manager's computer was found at IP addresses in Arizona, San Diego, Costa Rica, and London. The file, which we call the 1718 File, contained information about more than 9300 consumers.

JUDGE CHAPPELL: Excuse me. You say this information was found in these various places. How was it found?

MR. SHEER: It was found by a third party who was searching the P2P networks.

JUDGE CHAPPELL: And what was their motivation to be searching?

MR. SHEER: The motivation of the search is that the third party is in the business of trying to protect the information of its clients, and it does so by searching P2P networks, looking for information about the clients. In doing that, it came across these files.

JUDGE CHAPPELL: Is this a non-government-affiliated entity?

MR. SHEER: It is.

JUDGE CHAPPELL: Not funded by taxpayer money in any way?

MR. SHEER: It is not.

As I was saying, the file, which we call the 1718 File, has very sensitive information about 9300 consumers, including their names and Social Security numbers and medical test codes. Their test codes reveal the nature of the tests performed, such as for prostate cancer or sexually transmitted diseases or hepatitis.

The evidence will show that unauthorized disclosure of this kind of information causes or is likely to cause substantial injury in the form of identity theft, medical identity theft and other harms.

Complaint counsel's information security expert, Indiana University computer science professor Raquel Hill, will explain that the 1718 File incident was only the tip of LabMD's security iceberg. This case is not about a single, isolated failure. It's about systemic, easily addressed security failures that persisted for years.

The evidence will show that LabMD systematically failed to practice what IT practitioners call defense in depth. Although it will sound technical, some points, the main point is simple. LabMD failed to implement the basic, simple, effective security measures to protect the information in its

care.

So what's defense in depth on a computer network? A bricks-and-mortar analogy is a castle defended with a moat and sturdy inside and outside walls. These multiple defenses are effective, because if one defense fails, there will be another one to back it up.

As Professor Hill will explain, defense in depth on a computer network is the same concept. Use a variety of security measures at the network perimeter and inside the network. That way, if one measure fails, other measures will protect the network.

Professor Hill will explain that the particular security measures that accomplish reasonable defense in depth for a network start with understanding the network and its vulnerabilities and weaknesses.

JUDGE CHAPPELL: This defense in depth you're talking about, is this a law, regulation or guideline that's out there for everybody to see?

MR. SHEER: This is the practice that information security professionals use and have used for many, many years. It is available in many forms, including in standards that have been produced by the government, the National Institute of Science and Technology, as well as many other private organizations

that supply information to --

JUDGE CHAPPELL: I'm talking about government only. My question goes to the government only.

MR. SHEER: Yes.

JUDGE CHAPPELL: Law, regulation or guideline published by the government.

MR. SHEER: There are guidelines that have been published, for example, having to do with the security of health information that have these same basic concepts built into them. They're not always called defense in depth, but there are a series of standard steps, which we're going to talk about, that will illustrate what "defense in depth" means.

JUDGE CHAPPELL: These guidelines have been published. Can you cite me to them right now?

MR. SHEER: I can point you to the -- I can point you to pieces of it right now. I can point you to the HIPAA security rule which has -- which lays out in some detail what defense in depth requires.

JUDGE CHAPPELL: Did you say HIPAA?

MR. SHEER: I did.

JUDGE CHAPPELL: Okay.

MR. SHEER: And I can point you, if you will give me a few moments, to other sources at the National Institute of Standards and Technology.

JUDGE CHAPPELL: That's fine. I don't expect you to in your opening. I'm just wondering if you're going to do it here in the trial.

Is it part of your case?

MR. SHEER: References have been made to those things by our experts.

As I was saying, Professor Hill will explain the particular security measures that constitute reasonable defense in depth for a network start with the network and its vulnerabilities and weaknesses. Defense in depth counters these threats by putting in place a series of roadblocks to close the vulnerabilities and weaknesses at different layers of the network.

Reasonable defense in depth is proactive, not static. This is because threats and attack methods change quickly, and security has to keep pace to be effective. That, for example, is the point of regularly updating antivirus programs.

At least for networks that connect to the Internet, like LabMD's, defense in depth is not a "set it up and forget it" endeavor.

Can we have slide 1, please.

I'd like to turn to LabMD's security failures. The evidence -- the evidence will show that there were a number of them.

First up is risk assessment.

The evidence will show that LabMD failed to conduct adequate risk assessments.

Professor Hill will explain that risk assessment is an essential part to reasonable security.

Risk assessment is just like it sounds. It's tools to spot commonly known or reasonably foreseeable vulnerabilities on a network so that they can be closed before they're exploited.

Companies can't fix vulnerabilities they don't know about. And because no one tool can find all the different types of vulnerabilities that may be present on a network, a variety of tools are needed to evaluate exposure to the different types of risks.

The evidence will show that LabMD did not use an appropriate set of risk assessment tools.

For example, it did not perform external vulnerability scans, which are also called penetration tests. Penetration tests help companies find vulnerabilities and close them before intruders can exploit them.

LabMD performed no penetration tests of its network until at least 2010, after the commission investigation began. The 2010 test results show why

this failure was unreasonable.

First, the tests found urgent the most -- or the most serious vulnerabilities in two of LabMD's servers.

Second, the servers with these urgent vulnerabilities handled sensitive information which identity thieves use to conduct identity theft.

Using a file transfer protocol or FTP program, this server had received information about hundreds of thousands of consumers from physicians, including their names and addresses and Social Security numbers and medical information.

The other server had this information plus laboratory tests and also was used to keep a backup copy of the information -- of this information and the other information on LabMD's systems.

Third, the vulnerabilities could be exploited to access sensitive consumer information handled by the servers.

Fourth, the vulnerabilities identified in 2010 penetration tests were publicly identified and commonly known to IT practitioners years before.

And finally, the vulnerabilities could have been found at very low cost and then fixed at low cost. But to use these low-cost fixes, LabMD first had to know

the vulnerabilities were there. That's the point of risk assessment.

To illustrate these points, let's turn to the penetration tests run on the server that --

JUDGE CHAPPELL: Hold on a second. I'm trying to follow you here.

Are you saying that respondent didn't even have some type of spyware or virus program on their system? Is that what you're saying?

MR. SHEER: No, it isn't.

What I am saying is that there are a variety of risk assessment tools, of which antivirus programs and spyware programs are one type. The distinction is that no one program, no one tool can identify all of the vulnerabilities that may be present on a system.

So, for example, an antivirus program can find viruses, but it can't tell whether there's an unauthorized program on a computer, and so it goes, and so it isn't generally enough to be able to say, I have an antivirus program and I have an antispyware program. And the reason for that is because those programs are not capable of identifying other very significant risks that may confront a network.

This is an example of that. The vulnerabilities that we are talking about cannot be identified using an

antivirus program or a spyware program.

JUDGE CHAPPELL: So if I understand your position, any company out there today, in the United States of America, operating with customer information, who only has, let's say, McAfee or Norton spyware, adware, malware, virus protection, they're in violation of the FTC Act section 5?

MR. SHEER: We're not saying that.

Reasonable security, reasonable defense in depth depends on the circumstances. It takes into account all of the circumstances, including the size and complexity of the network, the kinds of information it has, the amount of information it has, the harm that could be done with that information, and the available -- and the cost of measures to address -- to address the risks and vulnerabilities.

And so it is based on the totality of the circumstances rather than a laundry list of things that you check off and say yes, I have or don't have.

JUDGE CHAPPELL: Go ahead.

MR. SHEER: Turning to the penetration test that was run on the server that received sensitive information about hundreds of thousands of consumers, it is Exhibit CX 070.

The test found that the server's overall

25

security posture was poor, partly because of the urgent risk to the FTP program used to receive the information.

This vulnerability allows anonymous log-in to the FTP program. What that means is that anyone -- it was set up so that anyone could log in without having a user name and password.

In conducting the test, the penetration tester passed through LabMD's firewall, found the FTP program, and tested it and found the vulnerability. An intruder could do exactly the same.

The urgent risk identified in Exhibit CX 070 was well-known years before the 2010 pen test was conducted. It shows that the vulnerability was identified in 1999, if not earlier, in free national databases of vulnerabilities and exposures, along with an easy fix.

The fix is to change the settings in the FTP program to disable anonymous log-in.

JUDGE CHAPPELL: You said this Exhibit CX 70 was some type of penetration test? Who generated this document?

MR. SHEER: This test was prepared by a company named ProviDyn. It is an outside information security firm. LabMD engaged it, well after the commission's investigation began, to test -- to conduct penetration

26

tests on nine IP addresses. It did so.

JUDGE CHAPPELL: So this was a company that was retained by respondent.

MR. SHEER: It was.

JUDGE CHAPPELL: All right.

MR. SHEER: The cost to LabMD of finding this vulnerability and other vulnerabilities was low. The company performing the penetration tests charged $450 for nine tests, including the test in Exhibit CX 070.

This cost is well within LabMD's reach given that it is a very profitable company that since 2005 had revenues of between 35 and 40 million dollars.

The penetration tester found --

JUDGE CHAPPELL: Is that million or billion, M or B?

MR. SHEER: M, millions.

The penetration tester found the FTP vulnerability using a free program called Nessus, which is often used by penetration testers and IP practitioners to spot a variety of network vulnerabilities. LabMD did not run Nessus on its own.

Additional evidence will show that LabMD failed to use other appropriate risk assessment tools or did not use them properly. It did not use an intrusion

27

detection program to warn of attacks. Its antivirus program at times provided little or no protection.

For example, the antivirus program on a server would not run a scan for about a year and did not have up-to-date antivirus definitions to warn of newly discovered attacks.

Untrained employees were expected to respond to warnings on their computers from the antivirus programs on the computers.

LabMD's answer to its risk assessment failures is that it had a firewall and manually inspected computers for vulnerabilities.

The evidence will show, however, that the firewall does not have or does not eliminate the need for risk assessment. The firewall let some traffic through, opening doors through which vulnerabilities and intruders could enter the network.

And although the firewall logged a limited amount of information that might have given some insight into risks, the information was overwritten every few days and was not systematically reviewed. LabMD actually only reviewed the firewall logs when users complained that their computers were not performing as they wished.

As for manual inspections, which are also known

28

as walk-around inspections here, through at least mid-2008, these inspections were not systematic. LabMD conducted manual inspections only when a user complained that their computer was not working correctly.

In addition, the inspections were cursory, seeking only to resolve the complaint.

JUDGE CHAPPELL: You're talking about computer users. Are you talking about employees of LabMD?

MR. SHEER: Yes.

The manual inspections were not thorough.

As Professor Hill will explain, even though systematic manual inspections are a poor substitute for automated -- she will explain that systematic manual inspections are a poor substitute for automated risk assessment tools.

As the 1718 File incident shows, the evidence shows or will show that the 1718 File was disclosed without authorization to a public P2P network through LimeWire. It was a program for which LabMD had no business need.

File-sharing programs, like LimeWire, present well-known risks.

Georgetown University computer science professor Clay Shields, complaint counsel's expert on

P2P file-sharing programs, will explain that by 2005, IT practitioners were well aware of the risk that P2P programs and their users would inadvertently share files they did not intend to share, such as business files containing sensitive information. Inadvertent file sharing occurs because users mistakenly designate files for sharing.

The evidence will show that LimeWire was installed on the LabMD computer in 2006. The billing manager used LimeWire to share music.

Also designated for sharing from the computer was every file in the Windows My Documents folder, which is the default folder for a user's files.

In all, more than 900 files were designated for sharing from the computer, including, most likely inadvertently, the 1718 File and other LimeWire LabMD business files.

Would you bring up slide 6, please.

Slide 6 is a screen shot of LimeWire taken from the computer used by LabMD's billing manager.

And now can we have slide 7, please.

Slide 7 has two highlighted lines. One shows a file -- it's the lower one I believe --

JUDGE CHAPPELL: Is that my glasses or is that blurred?

MR. SHEER: It is blurry. And I apologize for that. This is the best that we can do with what we received.

But if you look at the lower box, you will see three files. One of them is being highlighted now in yellow. It's called the Insurance Aging_6.05.071.pdf, and it's available for sharing. This is the 1718 File's true name.

The upper bullet or the upper box has a highlighted line, and it shows that there were 950 files available for sharing from this computer.

The evidence will show that LabMD's ordinary inspections did not find the LimeWire program.

JUDGE CHAPPELL: Was this employee authorized to use LimeWire?

MR. SHEER: LabMD is going to tell you no. And what the evidence is going to show, however, is that there were inadequate controls, as we will get to, inadequate controls to prevent this employee from downloading -- from installing -- downloading and installing LimeWire on the computer and using it.

JUDGE CHAPPELL: Was that a no?

MR. SHEER: That was a no.

The evidence will show that LabMD's ordinary manual inspections did not find the LimeWire program.

LabMD found it on the computer two years after the program was installed and then only because it was informed by a third party that the 1718 File was available on a public P2P network.

I'm going to turn now to the next of the security failures at LabMD, so we'll go back to slide 1, and this is authentication.

The evidence will show that LabMD did not require employees and others to use appropriate authentication -- authentication-related security measures.

Professor Hill will explain that LabMD did not have a strong password policy and did not use measures to ensure that employees use strong passwords.

Could you pull up slide 8 now, please.

Slide 8 is a 2010 table of user names and passwords.

JUDGE CHAPPELL: Let's back up the truck here.

This LimeWire program you're talking about, if that had never been downloaded by an employee, would we not be here today?

MR. SHEER: It is likely that we would not know about the defects in LabMD's security practices had we not known that LimeWire was out on the -- that -- rather, that the 1718 File was on the P2P network.

JUDGE CHAPPELL: So whatever information got out there in cyberspace was a result of LimeWire?

MR. SHEER: It was a result of the company's security failures that allowed LimeWire to be used by an employee to --

JUDGE CHAPPELL: But directly, was it a result of LimeWire directly? Is that how it got on the Internet?

MR. SHEER: Yes, it is.

JUDGE CHAPPELL: Thank you.

MR. SHEER: Going back to this exhibit, it is a 2010 table of user names and passwords at LabMD. It shows that a number of employees were able to use or allowed to use, quote-unquote, "LabMD" as their password. The vertical line in yellow identifies all of the instances in which that password "LabMD" was used.

The evidence will show that reasonable security -- password security practices would have prevented employees from using "LabMD" or other easily guessed passwords.

The last entry in the billing department's section on this exhibit -- it's the horizontal line -- identifies "sbrown" as a user name and "labmd" as the corresponding password.

Sandra Brown was LabMD's billing manager in 2005 and thereafter its insurance claim processor. She did most of the insurance claim processing work from her home computer and had access to very sensitive information, including files like the 1718 File. She used these same credentials -- "sbrown" plus "labmd" -- without changing them between 2006 and 2013.

The evidence will show that LabMD also provided computers to physician offices for them to use to transmit information to LabMD, including names, Social Security numbers and medical information. It did not set these computers up with strong passwords.

JUDGE CHAPPELL: What's the operator password of the employee who downloaded LimeWire?

MR. SHEER: I do not know. The employee who downloaded LimeWire is named Ros -- I'm sorry. Let me backtrack.

We do not know, LabMD does not know, the name of the employee who installed LimeWire on the billing manager's computer.

What we do know is that that computer was used by Ros Woodson, who was LabMD's billing manager. Her credentials, her user name and password are not included on this table.

JUDGE CHAPPELL: Why is that?

MR. SHEER: Because she was dismissed from the company before this table was created.

JUDGE CHAPPELL: So did you tell me this S. Brown is also a billing manager?

MR. SHEER: For a time, for one year in 2005, Ms. Brown, Mrs. Brown, was the billing manager, and thereafter she was the insurance claim processor, working from home mainly.

JUDGE CHAPPELL: All right. Thank you.

MR. SHEER: Going back to the computers and the passwords for them set up in the physicians' offices, LabMD did not set these computers up with strong passwords, and the evidence will show that passwords -- that the passwords were easy to guess.

LabMD did not effectively secure these computers, exposing them to vulnerabilities that could be used to reach into LabMD's network and access sensitive consumer information there.

Professor Hill will explain that the dangers of weak passwords are well-known. They can be exploited to obtain unauthorized access to networks and the computers and the information on them.

The weak passwords used at LabMD on the computers in the company and the computers that the company provided to physician offices could be misused

to obtain unauthorized access to sensitive consumer information. This is the kind of information that identity thieves want and use to conduct identity theft.

JUDGE CHAPPELL: These computers you're talking about provided to physician offices?

MR. SHEER: Yes.

JUDGE CHAPPELL: Am I mistaken or does the document here say they were not networked?

MR. SHEER: They were networked. I don't think that's what the document says. The way --

JUDGE CHAPPELL: In the column that says "Notes or Changes"?

MR. SHEER: I understand.

That is referring to the inside physicians at LabMD who are actually reading the tests and conducting them.

What I'm talking about, however, is LabMD's business model, which was to put computers into the doctors' offices so that they could use them to place orders with LabMD.

JUDGE CHAPPELL: And those computers are not on this document?

MR. SHEER: Those computers are not on this document.

JUDGE CHAPPELL: But they were part of the network.

MR. SHEER: They were part of the network.

In fact, as we'll talk in a few moments, the FTP program vulnerability that we were talking about earlier and the risk assessment as part of CX 070, that FTP program is one of the principal ways in which doctors' offices transmitted sensitive consumer information to LabMD using these computers.

The evidence will show that LabMD's Windows operating system had built-in functionality to manage passwords and that LabMD could have used this functionality at low cost. The company didn't do so, and it didn't use other methods to test password strength.

I'd like to go back now to slide 1 and to the third of the security failures, which is detection and prevention.

The evidence will show that LabMD did not use readily available security measures to prevent and detect unauthorized access to its network.

The 2010 penetration tests identified urgent vulnerabilities that could have been used to obtain unauthorized access to LabMD's network, such as through the anonymous FTP log-in.

Professor Hill will explain that LabMD easily could have configured the FTP program to prohibit anonymous log-in and prevent unauthorized access into its system in that way.

In addition, the evidence will show that some employees were given administrative controls over their computers, and some had Internet -- unrestricted Internet access as well, creating unnecessary security risks that could lead to unauthorized access and disclosure of sensitive information.

Administrative control is the highest category of control available on Windows computers, and it allows users to install unauthorized programs without prior approval. Without administrative control, an employee could not have installed LimeWire on the billing manager's computer.

Administrative control also means that employees could change security settings on their computers, such as by turning off built-in Windows security settings, without getting approval from anyone.

Professor Hill will explain that LabMD could have avoided these risks at low cost using functionality already built into the Windows operating system on its computers. By doing so, it could have

prevented employees from installing unauthorized programs and changing security settings. The evidence will show it did not do that.

Finally, LabMD required sensitive -- required sensitive consumer information, such as the information contained in the 1718 File, to be backed up on computers used by certain employees, including the billing manager. The need to back up information is obvious, but the evidence will show that LabMD easily could have backed up the information to a more secure location on its network.

I'd like to turn now to the fourth of the security failures, its training.

The evidence will show that LabMD failed to adequately train employees about information security. IT employees did not receive periodic security training.

Professor Hill will explain that such training is intended to keep IT employees up-to-date about evolving threats and how to address them. IT training helps the employees stay ahead in the computer security arms race.

The evidence will show that IT training appropriate for LabMD's employees was available from a number of sources at little or no cost.

JUDGE CHAPPELL: Regarding the training and the step above that where you said that employees could change security settings, et cetera, do you plan to introduce evidence of actual penetration of the network?

MR. SHEER: We are not going to introduce evidence of that sort. And the reason for that is that we are unable to determine whether it happened. And the reason for that is that among LabMD's security failures is that it did not keep records and logs of activity on its network, which would allow one to go backwards and look and see what had actually happened.

In addition, because it did not use an intrusion detection program, there were no warnings and records that would be created by that program to say something is happening here, there may be a breach, and there would be records to look back at. It is a fundamental security failure not to keep records that allow the company to look backwards and see what's happening on its network.

JUDGE CHAPPELL: So if I understand your position as the United States government, because, first of all, you don't have evidence of penetration of the network, but because they don't have records showing it didn't happen, I'm to assume it did happen?

MR. SHEER: No. What we are saying here is that these vulnerabilities, these security failures, created an unreasonable risk of an intrusion or, if you will, as happened in this case, the exfiltration of information by an insider.

Either way, the security vulnerabilities were such that it put the information at risk.

JUDGE CHAPPELL: So you're not suggesting an inference that something happened just because records don't exist.

MR. SHEER: No. We are saying simply that there is no way to determine whether something happened because the records don't exist.

As I mentioned, LabMD had given non-IT employees administrative control over their computers.

The evidence will show that the company did not adequately train non-IT employees about the security measures the company used or about the security risks to the company's networks if employees used administrative control to install unauthorized programs or change the security settings on their computers.

The next of the security failures is updates.

The evidence will show that LabMD failed to maintain and update operating systems and other devices on its network.

JUDGE CHAPPELL: Can you hold on a second?
(Pause in the proceedings.)
Go ahead.
MR. SHEER: Back to updates.
Professor Hill will explain that the penetration tests LabMD performed after the commission's investigation began identified an urgent default password vulnerability in the backup program that the company used. The vulnerability could be used to obtain unauthorized access to sensitive information on LabMD's network.

The company easily could have updated the program and closed the vulnerability using a free update the program vendor provided in 2005. It didn't do that.

Besides not updating the backup program, the evidence also will show that LabMD continued to run a Windows NT 4.0 operating system on a server for two years after Microsoft had stopped supporting it and had recommended using a more secure product.

Turning to the sixth of the security failures, this is access controls.

The evidence will show that LabMD failed to use adequate controls to limit employee access to just the sensitive information they needed to perform their

jobs.

LabMD maintained very sensitive information about approximately 750,000 consumers in databases on its network, including their names, addresses, Social Security numbers, and medical information. The databases were accessible to managers and laboratory, IT and billing employees.

LabMD did not use access control functionality built into its operating systems to limit the information employees could access. Because these access controls have to be programmed to actually work, the measures themselves can identify the types of information that employees were authorized to view.

The evidence will show, however, that LabMD cannot identify the types of information employees were able to access. It could have used these access controls at low cost, but it didn't.

In addition, included in the database employees could access was information about approximately a hundred thousand consumers to whom LabMD never provided any service at all. These consumers had no reason to know that the company had their information.

The company collected the information to facilitate test ordering, but it didn't use it. And instead of deleting it, the company permanently retained

the information in databases where it was accessible to many company employees. Doing so put the information at risk of misuse through identity theft.

And now we turn to number 7, the last of the security failures that we'll talk about. It is a written comprehensive information security program failure.

Professor Hill will explain that the specific security measures that provide reasonable defense in depth on a particular computer network are the result of a security strategy. This strategy applies equally to large and small networks, and it takes into account the size and complexity of the network, the flow of information into and within the network, and the amount and sensitivity of the information on the network. The result is called a written comprehensive information security program.

A written program is the road map the company follows to protect the network. At the core are specific goals, security goals, policies to achieve those goals, and procedures and tools to implement the policies.

Comprehensive programs cover all rather than just some of the security issues that a company faces. The program tells IT employees what the security goals

are, as well as the policies, procedures and tools to use to achieve those goals. It also provides a basis for training non-IT employees about risks and their responsibilities in addressing them.

The evidence will show that LabMD's security was ad hoc. The company did not have written security policies and procedures until 2010.

As a result, until at least 2010, there was no written road map for LabMD's employees to follow to know how to secure the network. A road map was necessary for LabMD's employees.

Would you please put up slide 9.

This is an employment timeline for LabMD's IT employees. What it shows is there's an awful lot of turnover in the IT department and there's no long-term IT employee to pass on institutional knowledge about the company's security practices and experiences.

The evidence will show that LabMD replaced outside IT contractors with the company's own IT employees, who are not network security specialists.

The evidence will also show that LabMD's security practices were not comprehensive.

For example, there was no policy about whether information was to be encrypted while it was stored on the network.

And some of the practices simply were not effective.

For example, although the company had a policy recommending that employees encrypt sensitive information in e-mails, it provided no means for them to do that. There were no tools.

Similarly, LabMD says it had a policy to identify and remove unauthorized programs from computers. The method for doing that was the manual or walk-around inspections we've talked about.

The evidence will show, however, that for more than two years these walk-around inspections did not discover that LimeWire was installed on a LabMD computer used by the billing manager.

LabMD could have created a written comprehensive information security program at low cost using model programs from national experts that had been available at no charge for years. The model programs provide a menu of security policies and procedures that companies can consider in developing their own information security programs that are appropriate for their circumstances.

Turning now to relief, the order proposed by complaint counsel is not intended to punish LabMD. It is to ensure that the company protects the very

sensitive information it maintains about approximately 750,000 consumers.

It requires LabMD to implement a written comprehensive information security program that is appropriate to its circumstances.

The proposed order also requires the company to obtain periodic third-party audits to verify that the program is providing reasonable and appropriate security. The company can choose its own assessor.

Finally, the proposed order requires LabMD to provide notice to consumers whose information may have been disclosed without authorization, such as the 9300 consumers whose information was in the 1718 File.

An order is necessary, even though LabMD is no longer providing testing services, for several reasons.

First, LabMD has no intention of dissolving and may in the future start anew. Were it to do so, an order could ensure that it practices reasonable defense in depth going forward.

Second, the evidence will show that LabMD maintains sensitive information about approximately 750,000 consumers on a computer network that can be accessed over the Internet. The information includes names, Social Security numbers, and medical information.

JUDGE CHAPPELL: If I understood you properly, you're saying that should LabMD completely dissolve and go out of business, that's irrelevant?

MR. SHEER: They are telling us that they are not planning on dissolving, and the issue still would be, if they were dissolving, what happens to the information about 750,000 consumers.

So it's got this information on a network that has access to the Internet and can be accessed through the Internet. The company operates the network, but it's dismissed all of its IT employees, so there are no IT personnel to manage the network security.

There are no plans to conduct penetration tests, for example.

LabMD's security is static in the face of evolving and growing threats. An appropriate order would ensure that the company protected the very sensitive information about 750,000 consumers that it maintains on this network.

To sum up, the evidence will show that LabMD engaged in a number of practices that taken together fail to provide reasonable security for the most sensitive information of as many as 750,000 consumers. It did not practice defense in depth and its security was not proactive.

In particular, going back to slide 1, LabMD failed to adequately identify risks.

It failed to adequately authenticate users.

It failed to adequately use reasonable measures to detect and prevent unauthorized access to its networks.

It failed to adequately train employees about security.

It did not appropriately update its systems, and it didn't use access controls that were appropriate to prevent employees from using or accessing information that they did not need to do their jobs.

And finally, it did not establish and implement a comprehensive information security program.

Although the company may point to walk-around inspections and routers and firewalls, its security was equivalent to a castle with half a moat and with holes in the inner and outer walls.

LabMD's failure to practice defense in depth is an unfair practice under section 5 of the FTC Act. It caused or is likely to cause identity theft, medical identity theft and other substantial harms.

Consumers had no way of knowing about LabMD's security practices and thus could not reasonably avoid those harms.

49

And because the failures could have been corrected at low cost, there are no countervailing benefits to consumers or competition.

Thank you.

JUDGE CHAPPELL: Thank you.

Who will speak for LabMD?

MR. SHERMAN: I will, Your Honor.

JUDGE CHAPPELL: Are you prepared?

MR. SHERMAN: I had anticipated, as they represented last week, that their opening would be two hours. And in doing so, I can't say that I'm fully prepared, but if the court wants, we can proceed.

JUDGE CHAPPELL: Are you requesting a short break?

MR. SHERMAN: Yes, sir.

JUDGE CHAPPELL: Subtly, though, but requesting a short break.

I feel really accommodating this morning, so we'll take a break and we'll return at 11:30.

We're in recess.

(Recess)

JUDGE CHAPPELL: We're back on the record.

Is everyone ready?

MR. SHERMAN: We are, Your Honor.

JUDGE CHAPPELL: Proceed.

50

MR. SHERMAN: Good morning, Your Honor.

May it please the court.

Complaint counsel.

Your Honor, I apologize for the delay and appreciate the court's indulgence.

JUDGE CHAPPELL: This is a laptop that will be available from now on; correct?

MR. SHERMAN: Yes, sir.

JUDGE CHAPPELL: Okay.

MR. SHERMAN: The evidence in this case will show that the FTC initiated its investigation of LabMD for unfair trade practices back in January of 2010.

And the law is section 5 of the Federal Trade Commission Act. In pertinent part, it reads that "The Commission shall have no authority under this section or section 57a of this title to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."

And I submit to the court that that is what the government must prove and that is what the government cannot prove.

51

And what portion of it is there that the government cannot prove, Your Honor? Well, let me start by saying this.

As I mentioned before that this forum is a bit foreign to me, that being the case, this case fits within that foreign aspect that we're dealing with here because it appears that this case is more about what could have happened, it's more about what might happen, what might have happened, but it's certainly not about what happened.

And the evidence will show that the government is unable to establish the link between what they allege are LabMD's data security practices and any harm to any consumer.

JUDGE CHAPPELL: What about the likelihood of harm?

MR. SHERMAN: I submit to the court that the evidence will be deficient in connecting LabMD's alleged data security practices and the likelihood of harm. And I submit to the court that that is precisely what they will be unable to prove.

What the evidence will show -- and counsel did a very thorough and succinct job in terms of presenting to the court what their expert witness, Professor Hill, has laid out as LabMD's alleged inadequacies. But as the court has lasered in on, what about the likelihood of this harm?

52

Well, the problem with the evidence is, Dr. Hill says LabMD's data security practices are inadequate because they didn't do A, B, C, D, E, F and G.

The evidence will show that Mr. Van Dyke will come in and say, Well, I was asked to assume that the practices were inadequate, and oh, by the way, if the information gets out and if it's in the hands of unauthorized third parties, the rate of injury is 30.5 percent, not the likelihood of injury but the rate of injury.

Dr. Kam or Professor Kam makes the same type of leap.

Now, it's up to the government to bridge that chasm. They won't. They can't.

In fact, the evidence will show that they don't know how the 1718 File escaped the possession of LabMD.

The evidence will show that they don't know how the day sheets that were found in Sacramento escaped the possession of LabMD.

So there's no causal connection between the alleged data security inadequacies and the appearance of these documents.

And what the evidence will show, Your Honor, is that there are a number of ways that these documents could have escaped the possession of LabMD even if LabMD's data security practices were perfect.

And we've joked over and over again, thank God for Eric (sic) Snowden, because if documents can escape the NSA, then there is no perfect security. And every data security witness that appears on the stand will confirm that there is no perfect security.

And so without this causal connection between this alleged inadequacy and the appearance of these documents outside of LabMD's possession, how does the government establish likelihood?

JUDGE CHAPPELL: So you're saying, if I'm following you correctly, if there's no such thing as a perfect system, logic would dictate that harm would always be likely.

MR. SHERMAN: It's not quite that simple, Judge.

If I juggle knives for a living, there's a likelihood I will get my fingers cut. There's a likelihood. But I don't because I'm really, really good at juggling knives. Or I'm good enough at juggling knives that I don't get my finger cut.

Now, if some expert comes in and says, Hey, for

the most part, you know, we did a survey of knife jugglers and 30.5 percent of people who juggle knives cut their fingers, that doesn't mean I'm going to cut mine. And if after I juggle knives there is no blood, there are no cuts.

The government has submitted --

JUDGE CHAPPELL: But in your analogy, in your analogy, though, the government's position from what I take it would be that you wouldn't be that knife juggler who's well-trained, you would be the knife juggler who's not as prepared, just following their opening statement.

MR. SHERMAN: Even so, Your Honor, I'm prepared enough.

JUDGE CHAPPELL: You're saying that the predictability analysis is flawed.

MR. SHERMAN: Absolutely.

I'm prepared enough that my fingers did not get cut. But they want this court to make the quantum leap that, Oh, Mr. Sherman, if you keep juggling those knives, you're likely to cut your fingers. Well, that's true. But I haven't. And is that enough?

JUDGE CHAPPELL: But again, following their case, you've already cut yourself.

MR. SHERMAN: That's where their case fails,

Your Honor. Because in order to -- if you cut, you bleed. There's no blood here. There's no harm.

There's even a question as to whether or not they can prove that this file was found on a peer-to-peer network.

But what the evidence will show, Judge, on top of this, is that even if it were found on a peer-to-peer network, it was found by a company by the name of Tiversa. And the evidence will show that Tiversa has issued press releases comparing its search capabilities and its search capacities to that of Google, that Tiversa has indicated even to the Congress of the United States that it has patented technology which allows it to search peer-to-peer networks in an unprecedented breadth and volume.

JUDGE CHAPPELL: And Tiversa was the company not named by the government trolling for breaches in security?

MR. SHERMAN: That's correct.

JUDGE CHAPPELL: Do you concur that that company has no taxpayer funding?

MR. SHERMAN: I do not.

JUDGE CHAPPELL: Are you saying they were under government contract when they were trolling and identified your company, your client?

MR. SHERMAN: I don't know who they were providing services for or if they were providing services for anybody or if they just trolled. Because they collect information, and when somebody asks them if my information is out there, they have a huge database where they can search what they've already trolled and downloaded and tell someone whether or not their information is out there.

But I will suggest that the evidence will show that they have government contracts.

And so to say that they're not funded in any way by taxpayer dollars, Your Honor, I think is incorrect.

JUDGE CHAPPELL: And what you're telling me you're going to provide in the record in this trial. You have evidence.

MR. SHERMAN: Mr. Boback has been testified (sic) to show up here, and if he tells the truth, he must admit that they have government contracts.

JUDGE CHAPPELL: That's the gentleman who moved to quash the subpoena?

MR. SHERMAN: Yes, sir. That is the CEO, owner, president, man in charge of Tiversa, Inc.

What the evidence will show here, Your Honor, is

57

that Tiversa was a research partner with Dartmouth College.

You can put that exhibit up now.

Dartmouth College in fact, in the 2004, '5, '6 time frame, had a contract with Homeland Security.

It's not that contract; it's the other one.

JUDGE CHAPPELL: Who are you talking to?

MR. SHERMAN: I'm talking to my technical people.

JUDGE CHAPPELL: I can't --

MR. SHERMAN: It's actually my attorneys actually. They've just --

JUDGE CHAPPELL: Nothing I can do about that screen.

MR. SHERMAN: This contract concerns itself with cyber sharing, cyber security collaboration and information sharing. It's RX 404.

And Dartmouth College conducted research, with the help of Tiversa, on this very subject matter for the financial industry and for the medical industry.

And here's where the 1718 File comes into play.

But what's interesting about what the evidence will show with regard to this research, Tiversa's involvement as a research partner with Dartmouth College, is that neither Dartmouth College

58

professor Eric Johnson, who also filed a motion to quash his subpoena but will be here on Friday, nor Mr. Gormley, who was the operations officer at Tiversa during this time, neither of them could tell me during their depositions how the 1718 File was found.

Mr. Johnson couldn't directly tie it to his research methodology in his data hemorrhaging in the health sector report that he put out.

Tiversa could not tell me whether or not they found it as a result of work they were doing on the data hemorrhaging article, whether they were doing it for one of their other clients, or whether they just fed Mr. Johnson this document to, as he says in an e-mail to his research partner at Tiversa, to spice up my report.

JUDGE CHAPPELL: So you're saying the company that allegedly found the document, 1718 File, can't tell you or tell us how it came to be, how they found it?

MR. SHERMAN: Not from anyone we've talked to thus far.

Now, let me say this, Judge.

If Mr. Boback testifies consistent with his deposition testimony, he will say that the 1718 File was found at an IP address in San Diego, California.

59

He will also say that prior to his deposition, which was taken in November of 2013, that it was also found on three separate IP addresses. I believe complaint counsel mentioned that.

JUDGE CHAPPELL: Since it's your client, for the benefit of all these people here that don't know what we're talking about, what is the 1718 File and a day sheet?

MR. SHERMAN: The 1718 File is an insurance aging report that LabMD's billing manager created. And what LabMD did with these insurance aging reports is they collected money from those people who owed them money for tests that they had performed.

On the 1718 File, the insurance aging report, name, address, Social Security number for most people, and so they created the file. And there is testimony in the deposition designations that once these files were created, they were destroyed. They were shredded at the end of the day because they would be handed out to billing department, and they would then make calls to collect the money owed to LabMD.

A day sheet, on the other hand, is a sheet which again contains --

JUDGE CHAPPELL: Let me back up there.

The 1718 File then was maintained as a

60

reconciliation document, so after your insurance paid, this is what the client owed or the customer owed in the end?

I'm just trying to figure out the purpose for maintaining the file.

MR. SHERMAN: See, that's just it, Your Honor. In the normal course of LabMD's business, files like the 1718 File were not maintained. They were actually created using a database which the billing manager will put in parameters, okay, let's see who still owes us from June to July, print off a file similar to the 1718 File.

JUDGE CHAPPELL: Is it a 1718 File like 1718 File, for example, they do them all the time or was it --

MR. SHERMAN: Daily.

JUDGE CHAPPELL: -- one, one file?

MR. SHERMAN: Daily.

JUDGE CHAPPELL: Okay.

MR. SHERMAN: Or every other day or until the pages that were created that day to collect were actually called upon by the people in the billing department. People in the billing department shredded them on a daily basis.

The anomaly of the existence of the 1718 File is still boggling because, even with all the resources of the federal government, no one has been able to find Ros Woodson, the very person who was using LimeWire on her computer, the very person who created the 1718 File.

And there's testimony that she didn't know what she was doing when she was using LimeWire. And in fact, the article that's on the screen assumes inadvertent file sharing.

And so if you take all of the evidence that's presented about how this LimeWire works and how people use it to download music and inadvertently share other information that they didn't intend to share, the story makes a little more sense.

JUDGE CHAPPELL: And what's a day sheet?

MR. SHERMAN: A day sheet is a sheet again that's used for collection purposes. I think what it shows -- it's kind of like a back end of the 1718 File that shows who paid, what payments were received.

And so the day sheets, the evidence will show, Your Honor, are not electronically maintained. In fact, it's the type of document that you open up, you populate it with the information, but you cannot save the information electronically, and so LabMD would print the day sheets and store them in their paper form on LabMD premises.

So part of what the evidence will show is that the day sheets could not have escaped LabMD's possession as a result of a data -- an electronic data security-type breach or inadequacy.

But back to the background of the story, and I'll -- I have to move along a little quicker than I am, Judge.

Dartmouth and Tiversa are research partners. Dartmouth has the grant. The testimony is that Tiversa, in exchange for Dartmouth evaluating its search capabilities, agreed to be Dartmouth's research partner and therefore receive no remuneration for their participation with Dartmouth College.

But again, it was from Tiversa that Dartmouth College received the 1718 File and made representations in this report that they received this 1718 File as a result of their research methodology, their digital footprint, and therefore gave the public this idea, including the government, this idea that this file was easily downloadable by anybody using LimeWire or a peer-to-peer network.

The fact of the matter is, the evidence will show that upon immediately learning that this file had allegedly escaped LabMD's possession, LabMD had one of its IT personnel go home, download LimeWire and use

precisely -- precisely -- the file name and search for the file. They didn't find it.

A few years later, LabMD had another of its IT persons search using a peer-to-peer network using the precise file name. He didn't find it.

I think it's significant, Your Honor, that the evidence will show that the only entity able to find this file has patented technology.

Likely to cause substantial harm I think not.

JUDGE CHAPPELL: If that's the case, how do you explain the allegation -- I don't know if it's disputed -- of the documents turning up in a flophouse in California?

MR. SHERMAN: We don't. The government doesn't explain it either.

The government, again, wants this court to say, Well, the documents showed up in a house in Sacramento. Somebody must be harmed.

Who is it? When? How did the documents escape? I submit to you, there's no -- there will be no evidence of how the document escaped. And what they must prove is that the practice was unfair and that unfair practice is likely to cause harm.

But again, this case is not about what actually happens but what might happen, what could have

happened.

LabMD had firewalls in place. LabMD had spyware and antivirusware in place and they had routers and they had all these things in place, but it just wasn't good enough. Yeah, they had it, but it wasn't good enough for Dr. Hill.

It wasn't good enough for Professor Shields, I believe it is. It just wasn't good enough.

But the evidence will show that it was good enough to keep someone from likely being harmed, because nobody has been harmed.

The evidence will further show that --

JUDGE CHAPPELL: Wait a second.

So your position is, if it did not happen, it is not likely?

MR. SHERMAN: My position is that the federal government should not be able to come in and say that we find, through our expert, based on a three-year investigation and all of the information that you've given us about what you were doing, that what you were doing was unfair and not have to prove how likely it is that substantial harm is going to occur in face of no harm occurring.

I think that their job would be a lot easier if they could show some harm. But without it, they have to prove "likely," and I don't know that they will present -- all the evidence that I've seen, Judge, "likely" is missing.

The rate at which people will be injured if certain factors exist is documented by Van Dyke and Kam, but the evidence will show that when Van Dyke and Kam are questioned about the facts in this case, "Well, I wasn't asked to consider that" is their answer. When Van Dyke and Kam are asked, Well, did the government tell you that no one had been harmed? Well, why no.

And so if the government is going to take the position, which they have, that the data security standards which the regulated business community should be aware of will be applied on a case-by-case basis, it seems to me that the evidence should show that their experts considered the facts in this case. And I submit to the court that the evidence is not going to show that.

What the evidence will show is that when the LabMD employees were questioned about what was in place, for example, who had access to information necessary to do their jobs, employee after employee after IT person basically said, Well, it was my understanding that the workstations were configured such that people only had access to what they needed

for their job. Billing did not have access to financial information. The people in the lab didn't have access to billing information, but billing did have access to people in the lab because they needed the codes, so they had.

JUDGE CHAPPELL: What about his slide that showed people didn't change passwords for over five years?

MR. SHERMAN: People didn't change passwords for over five years.

JUDGE CHAPPELL: But does that mean anybody can sit there and access whatever they need to?

MR. SHERMAN: It doesn't mean they didn't log off, Judge. I mean, I can keep my password for five years and you'll never know what it is. That doesn't mean because my password is five years old that somehow you're going to have access to the information on my desktop.

JUDGE CHAPPELL: Well, I have no idea what kind of operation LabMD was running. I don't know if it was a 15-story building full of people, one room with three cubicles, so when you said billing didn't know what the other department was doing, it's hard for me to put that in context. I mean, were there a hundred employees? I have no idea.

MR. SHERMAN: There were anywhere between 25 to 35 employees, 15 to 20 desktops.

JUDGE CHAPPELL: Now, you had at some point I guess technicians or medical personnel doing medical tests.

MR. SHERMAN: That's correct.

JUDGE CHAPPELL: Are they part of this net that had access to the computer system and didn't change passwords?

MR. SHERMAN: The medical personnel were not -- the medical personnel looked at the actual slides, tissue, urine, blood samples, and they made their diagnosis of cancer.

What the evidence will show is that the countervailing benefit to doing it this way, to having physician clients transfer information from their office to LabMD, was consistent with what the federal government was asking the medical community to do anyway, which was to go to electronic medical data.

And the benefit is, you cut down on paper. That's obvious.

Secondly, you cut down on data entry mistakes. Once it's there, it's there.

JUDGE CHAPPELL: These 15 or 20 personnel who had desktops, does that include the outside companies?

MR. SHERMAN: No, it does not.

And the evidence will show that the -- this concept about all physician clients having LabMD computers installed is something that may have occurred on a more regular basis in 2005, '6 and '7, but the evidence will show that as medical doctors' offices became more technologically savvy, you know, they were able to transfer this information using their own information technology through a secure FTP. And that's how it was done.

And the speed with which a doctor could order a test was simply by identifying the patient identification number and the test that that patient needed. That information was already on LabMD's database -- the evidence will show and Mr. Daugherty will testify to it -- that information was already on LabMD's database.

It's transferred electronically. No one has to go in and read someone's sloppy handwriting about, you know, what test is performed and what is the identification number for the client. It's already there. It's in electronic form. You know what test you want to perform. The sample arrives. The doctor does the test. And guess what? The physician has access to the test results electronically. He doesn't have to

69

wait.

And so there is countervailing benefit to the consumer, to someone who wants to know whether or not they've got cancer, which, as we know, is an exigent-type disease. The sooner you find out, the better.

And so when Dr. Hill and the federal government says, Well, you know, yeah, you had a firewall, but you didn't block access to every port coming in, well, yeah, maybe LabMD didn't, but they're playing with knives and they're not bleeding.

And so --

JUDGE CHAPPELL: What's the operating status of your client? Are they in business?

MR. SHERMAN: They are in business to the extent that if doctors call and say, "What was the result of that test back in 2006 or back in 2010?" LabMD has the ability to give them that result. Their database is not, the evidence will show, is not connected to the Internet, so these dangers that would exist don't currently exist.

JUDGE CHAPPELL: At what point did LabMD cease testing new samples?

MR. SHERMAN: In January of this year, Your Honor.

70

JUDGE CHAPPELL: So this database of hundreds of thousands of consumers, what's the purpose of maintaining that?

MR. SHERMAN: I believe HIPAA requires that that information be retained for a period of years.

And the evidence will show, Your Honor, that LabMD, if it succeeds here, will attempt to restart its business.

The evidence will show that LabMD, if it's successful here, will attempt to get the necessary insurance that it's unable to get currently to operate its business.

JUDGE CHAPPELL: So the scientific or technical and medical personnel have been laid off or fired or --

MR. SHERMAN: Absolutely.

Judge, if I might move forward, what you will find from the evidence is that only --

JUDGE CHAPPELL: Let me finish my line of questioning.

MR. SHERMAN: Yes, sir.

JUDGE CHAPPELL: And what's going to be your position of the reason why LabMD ceased operating in January of 2014?

MR. SHERMAN: It's my understanding that LabMD was losing money every month as a result of physicians

71

being very wary of the fact that LabMD is being investigated by the FTC for data security inadequacy.

And clearly, if a physician then continues to send protected health information to a place where there is some doubt as to whether or not it's adequately protected, then that physician is putting itself in liability's way.

JUDGE CHAPPELL: So your position is, caused by the government case, not by the business model?

MR. SHERMAN: Your Honor, the business model was cutting edge at its time. The business model was applauded by the physicians. The business model enabled LabMD to compete with labs ten times its size.

JUDGE CHAPPELL: LabCorp? Like LabCorp?

MR. SHERMAN: To name one. Absolutely.

LabMD had clients in six or seven states across the south. Why? Because they were doing things electronically, Judge.

And the evidence will show that they had no complaints from doctors concerning the loss of patient information.

They didn't have the Cadillac of systems. They didn't meet Dr. Hill's standard. They didn't. But they didn't cut their fingers.

They took the appropriate precautions, and

72

because they did so, the government will not be able to establish "likely," because everything points against "likely."

But I do understand that this case is not about what actually happened but what might and what could have and what might have and those types of things, so we have to deal with the forum in which we find ourself, but what you will get from the IT managers and from the employees of LabMD is that, well, only the managers had access to the Internet, and the purpose for that was so that they could access the insurance companies' Web sites so that they could follow the regulations set out by the insurance companies and use the appropriate codes for the appropriate tests and services that they provided so that they could get paid.

LabMD was a small business in the business of doing business, cancer detection. They were not in the business of creating the best data security system out there. It's simply just not how it works in the real world.

What the employees will say is that even the managers who had access to the Internet, in order to download programs from the Internet, were supposed to get permission from the IT department. That was a policy. It was known across the board at LabMD. If you're going to download something, you need to get permission from IT to do it.

JUDGE CHAPPELL: The government's position is those employees had admin privileges, which means they didn't have to get permission.

MR. SHERMAN: That's correct. That's correct. But they knew that they should have gotten permission.

And what you find, Your Honor, is after the peer -- after LimeWire was found on one computer, it wasn't found on any other. They checked every computer. There were no peer-to-peer programs on any other computer. The policy was being followed. But you always have an Eric Snowden in your midst. And you can't protect against a rogue employee.

JUDGE CHAPPELL: So who is Eric Snowden in this scenario?

MR. SHERMAN: Eric Snowden is Ros Woodson, potentially.

JUDGE CHAPPELL: And no one has been able to depose Ros?

MR. SHERMAN: Your Honor, it's the strangest thing. The federal government cannot find Ros Woodson. Found Osama bin Laden. We can't find Ros Woodson.

JUDGE CHAPPELL: Well, that took a while.

But let's talk about Ros Woodson. If no one has

found her, how do we know -- and I don't know if I heard it today or I read it in pleadings -- how do we know her motivation for LimeWire?

MR. SHERMAN: We don't.

JUDGE CHAPPELL: So we don't know if it was just to download music.

MR. SHERMAN: We have testimony from Ms. Garrett I believe that Ros Woodson didn't have a computer at home and she just wanted to download music and she was burning music files, and that's why she downloaded LimeWire and -- that's what we heard.

It would have been nice to know from Ms. Woodson why she did what she did, but apparently she's -- she's pretty good at concealing her whereabouts.

JUDGE CHAPPELL: I don't believe she's on any witness list, is she, on either side?

MR. SHERMAN: I don't think she is. We may have put her on our witness list, you know, with our fingers crossed that she would somehow -- but I don't expect that Ms. Woodson will show up and testify. She has not been subpoenaed.

JUDGE CHAPPELL: So as far as you know, she has taken off to some country without an expedition treaty to the United States? Off the grid?

MR. SHERMAN: She could be in Costa Rica.

What you will see from the deposition --

JUDGE CHAPPELL: Regarding her, I just want to make sure, was she fired over this incident? Is that the company's position?

MR. SHERMAN: There's testimony from the person --

JUDGE CHAPPELL: Do you want to consult with the guy shaking his head?

MR. SHERMAN: It depends on which way he was shaking his head because -- there's testimony that she was fired for not performing her duties up to the level of a manager.

Now, maybe that's some employment law CYA, but she was fired because, in not performing her duties up to the level of a manager, she had LimeWire on her computer.

JUDGE CHAPPELL: Okay. But it happened to be right after LimeWire was discovered.

MR. SHERMAN: Yes, it was.

JUDGE CHAPPELL: All right.

MR. SHERMAN: What the IT employees at LabMD will say --

JUDGE CHAPPELL: And I know there's members of the press out there. They're not saying she was fired just for LimeWire, just so we're clear.

MR. SHERMAN: Thank you, Your Honor.

The IT employees will say over and over again that they received on-the-job training. They received on-the-job training to do what they were hired to do. Many of them were just lab technicians -- I'm sorry -- computer technicians, who would go around and set up new computers, download the necessary software, so that LabMD could do business.

What the IT employees will say is that they believed that LabMD's security was adequate. Was it perfect? I don't think any of them can say that. But they will say that it was adequate. They will testify that they themselves know of no security breach.

As I said before, they will testify concerning LabMD having multiple firewalls in place, that LabMD's firewalls prevented unauthorized intruders into their system.

JUDGE CHAPPELL: Does your client have an IT manager? A webmaster? Anything like that?

MR. SHERMAN: In the early years, 2005, 2006, 2007, I would describe LabMD's IT department as flat.

JUDGE CHAPPELL: Meaning?

MR. SHERMAN: Meaning there was no manager. There were three people who did what they had to do on a daily basis, and the more complex areas of IT were handled by third-party providers, such as -- APT? Is that what it was called? Truett's company -- such as APT. The evidence will show this.

In or about 2007, John Boyle was hired as the chief operating officer. And John Boyle has extensive experience in terms of information technology and network security, and he was in charge from 2007 all the way up until I believe 2011.

JUDGE CHAPPELL: And when was the LimeWire incident?

MR. SHERMAN: The LimeWire incident -- LimeWire was discovered in May of 2008. There will be evidence to show that, Your Honor.

But again, there will be testimony from those who were there that will describe the technological processes and efforts that were put in place by LabMD to protect the protected health information, which they knew was key to gaining the trust of their physician clients and building a business that would operate.

And so to suggest, as the government has, that LabMD willy-nilly did as little as possible to protect the very life's blood of their business is I think a far-reaching, ludicrous --

JUDGE CHAPPELL: And let's remember, this is opening statement, not argument.

MR. SHERMAN: I understand.

And so with that, Judge, I believe that I've given you a pretty good overview of what the respondent's position is with regard to really what the evidence will show and mainly what evidence will not be shown.

Thank you, Your Honor.

JUDGE CHAPPELL: Thank you.

All right. We're going to take a lunch break.

When we come back, I expect the government to be prepared to call their first witness. We're going to get after this.

We're going to return at 1:45.

We're in recess.

(Whereupon, at 12:37 p.m., a lunch recess was taken.)

AFTERNOON SESSION

(1:51 p.m.)

JUDGE CHAPPELL: Back on the record.

We have a few scheduling issues to deal with.

Some general information if you're -- I think this was in our e-mail to the parties.

We're generally going to be here from 9:30 a.m. to 5:30 p.m. starting tomorrow, we're at 9:30.

We'll take a one-hour lunch break sometime in the afternoon, a ten-minute break in the morning and afternoon as appropriate.

There will be days when we have a witness from out of town or out of the country, and with prior approval, we can go late. The "prior approval" means you let me know no later than the day before. And that's simply because there's a lot more people involved in making this happen than who you see up here. We've got building personnel and others involved to go late in this building.

Generally, the morning break will be between 11:00 and 11:30, lunch sometime between 1:00 and 2:00, afternoon break sometime between 3:30 and 4:00.

And make a note, this Thursday, the 22nd, we will end court no later than 5:00 p.m. on that day.

Any questions on that?

MS. VANDRUFF: No, Your Honor.

MR. SHERMAN: No, sir.

JUDGE CHAPPELL: All right. Call your first witness.

MS. LASSACK: Good afternoon, Your Honor. Maggie Lassack for complaint counsel.

We'd like to call to the stand Dr. Raquel Hill.

JUDGE CHAPPELL: All right. Step up here, and the court reporter will swear you in.

- - - - -

Whereupon --

RAQUEL HILL, Ph.D.

a witness, called for examination, having been first duly sworn, was examined and testified as follows:

JUDGE CHAPPELL: All right. Go ahead.

MS. LASSACK: Your Honor, one preliminary matter. We have binders of documents for the witness and opposing counsel that we may use today. May I approach to provide one to Your Honor and to your clerks?

JUDGE CHAPPELL: If I need a document, I'll ask for it. And it's okay to provide binders to the witness if the documents are in evidence and the opposing party is aware or has a copy of it.

MR. SHERMAN: I do have a copy, Your Honor.

- - - - -

DIRECT EXAMINATION

BY MS. LASSACK:

Q. Good afternoon, Dr. Hill.

A. Good afternoon.

Q. Would you please introduce yourself to the court.

A. My name is Dr. Raquel Hill. I'm an associate professor of computer science at Indiana University.

Q. Dr. Hill, how much experience do you have in computing?

A. I have over 25 years in computing.

Q. What are your areas of expertise?

A. My areas of expertise are data security, system security and data privacy.

Q. How long have you been a professor of computer science at Indiana University?

A. I've been a professor at Indiana University for nine years.

Q. When did you earn tenure?

A. I earned tenure in 2012.

Q. Professor Hill, would you please describe for the court your education that you received to become a professor in computer science.

A. I received my bachelor's degree in computer science with honors from Georgia Institute of Technology in Atlanta, Georgia; my master's degree in computer science from Georgia Tech; and my Ph.D. in computer science from Harvard University.

Q. When did you earn your Ph.D. in computer science?

A. In 2002.

Q. Professor Hill, would you describe for the court your dissertation research.

A. My dissertation research, I designed and implemented a lightweight reservation protocol that would allocate bandwidth for audio and video applications so that they could run over the Internet.

Q. Professor Hill, was there any security component to your dissertation research?

A. Yes. I did an evaluation of the -- of the protocol and -- a security evaluation of the protocol, and I designed mechanisms to address the vulnerabilities in the protocol.

Q. Describe for the court how the protocol worked.

A. The way that the protocol worked is that it was an end-to-end protocol, so you had a client user on one side of the communications channel and then maybe there was a server on the other side that it wanted to retrieve the video or audio data from, and so instead of using more heavyweight signaling protocols that would require you to use additional bandwidth, my protocol actually embedded the request in the headers of the data packets that flow between the two endpoints of the communications channel.

And so by doing that embedding of information in the headers, routers along the path can make a decision about whether they could support the traffic, and so as that data was propagated from one router in the Internet to the next, each router made a decision about whether it would support that data.

Q. Would you describe the security mechanisms that you designed in connection with that work.

A. So one of the security mechanisms was to prevent --

JUDGE CHAPPELL: Excuse me. Are we still talking about the dissertation?

MS. LASSACK: Yes, Your Honor.

JUDGE CHAPPELL: And before we get too far down the rabbit hole, are you going to connect what she's saying now to her opinions in this case?

MS. LASSACK: This is to qualify her as an expert, Your Honor.

JUDGE CHAPPELL: Is there an objection to her qualification?

MR. SHERMAN: No, sir, Your Honor.

JUDGE CHAPPELL: Why don't we just get to the heart of the matter here.

MS. LASSACK: Okay.

BY MS. LASSACK:

Q. Professor Hill, I'd like to direct your attention to CX 740.

It also appears on the screen as well.

Professor Hill, what is CX 740?

A. CX 740 is my expert report.

JUDGE CHAPPELL: And just so we're clear, I'm not stepping on your ability to examine your expert witness, but I assume her CV is somewhere in the record, so I don't think we need to hear it unless there's an objection to her qualification.

MS. LASSACK: Okay, Your Honor. We'll move on.

JUDGE CHAPPELL: And that goes for any expert that comes in here.

BY MS. LASSACK:

Q. Professor Hill, did complaint counsel ask you to assess whether LabMD provides reasonable and appropriate security for personal information within its computer network?

A. Yes.

Q. What did you conclude?

85

A. I concluded that they did not provide reasonable and appropriate security.

Q. What time period does your conclusion cover?

A. January 2005 until July of 2010.

Q. Professor Hill, I'd like you to look at paragraph 48 of your expert report.

Will you please read aloud the second sentence of that paragraph.

A. "From my review of the record, there are not sufficiently diverse types of information available after the relevant time period for me to offer opinions about that period."

Q. Please explain to the court what that means.

A. That means that during the relevant time period, there were a variety of types of information, including antivirus scans, deposition testimony, risk assessment scans, and all of this information wasn't available after the relevant time period.

Q. Can you give the court an example of something that was not available?

A. One of the things that was not available was the antivirus scans. There were -- another thing that was very helpful were the vendor reports, like the APT documents that discussed the specific things that had been done, so those types of things were not available.

86

Q. When you say "the APT documents," what are those?

A. The ATP -- APT was a vendor that provided services, computer maintenance services for LabMD early in the relevant time period, and that there were descriptions of the vulnerabilities that they addressed or other problems that they addressed on the LabMD network, and so that provided specific details.

JUDGE CHAPPELL: Is that an acronym for the company or is that the actual name of the company?

THE WITNESS: I don't recall, sir, if that was the actual -- if that's the actual name or it is an acronym.

MR. SHERMAN: If it would help the court, it's an acronym.

MS. LASSACK: It's Automated PC Technologies.

BY MS. LASSACK:

Q. Professor Hill, what material did you consider in reaching your conclusion?

A. I considered the record evidence that was provided to me.

I also considered government standards and guidelines and industry standards.

I also considered my own knowledge about the subject matter.

87

Q. When you say "government standards," what do you mean by that?

A. When I say "government standards," I mean documents that have been provided by government agencies as guidelines for securing computing infrastructure, also national vulnerability databases and those types of things that are managed by government entities and industry and academia.

Q. You considered industry standards as well; correct?

A. Yes, I did.

Q. Have you read the expert report submitted by LabMD's expert?

A. Yes, I have.

Q. I'd like to draw your attention to CX 737.

It's up on the screen as well.

What is CX 737?

A. CX 737 is my rebuttal of the expert report.

Q. Now, Professor Hill, I'd like to direct you back to your expert report at CX 740, in particular paragraph 49.

JUDGE CHAPPELL: Before you do that, I want to mention something for the record because I saw a lot of blank faces on the left side of the room when you were trying to qualify your expert.

88

I'm going to accept someone as an expert unless there's an objection, but what I'm saying is that to the extent any opinions offered meet the proper legal standards, those opinions will be considered.

Any questions on that?

MR. SHERMAN: No questions, Your Honor.

JUDGE CHAPPELL: Go ahead.

BY MS. LASSACK:

Q. Professor Hill, will you read the last two sentences of that paragraph starting with "Record evidence."

A. "Record evidence shows that LabMD maintains personal information about more than 750,000 consumers. For purposes of this report, I have assumed that these types of information can be used to harm consumers, through identity theft, medical identity theft, and disclosing private information."

Q. Why did you make that assumption?

A. I made that assumption -- the assumption of harm was provided to me by complaint counsel.

Q. Professor Hill, before we discuss in detail how you reached your opinions, I'd like to ask you some background questions about networks and network security.

A. Okay.

Q. What is a network?

A. A network is a composition of computers, servers, workstations that are connected via some type of communications channel.

Q. Professor Hill, will you turn to paragraph 17 of your expert report. And I'm also showing on the screen what's been marked as CXD 2.

Professor Hill, what is CXD 2?

A. CXD 2 is an image that illustrates a very simple map.

Q. How does CXD 2 compare to figure 17 in your report?

A. It's the exact same figure.

Q. Will CXD 2 help you give background testimony about networks and network security?

A. Yes, it will.

Q. What is a local area network?

A. A local area network, if you look -- I'm sorry. I'm trying to get it on the -- it's kind of hard (indicating).

But if you look in the square box, that illustrates a local area network. The computers on the network are connected to the network via a network interface card.

Q. What is a network interface card?

A. A network interface card is an adapter that's placed in a computer to communicate on the computer's behalf, an example of which would be like an Ethernet card.

And each card has a unique address called a MAC address, a medium access control address. And that address uniquely identifies that computer on the local area network.

MS. LASSACK: Your Honor, may co-counsel approach Professor Hill with a laser pointer to use in connection with CXD 2?

JUDGE CHAPPELL: You mean to hand it to her?

MS. LASSACK: Yes.

JUDGE CHAPPELL: Sure. I didn't want him to just blink it in her eyes or anything.

MS. LASSACK: I'm sure she appreciates that.

JUDGE CHAPPELL: Did you try this out?

MS. LASSACK: We weren't able to try it out here beforehand with the laser pointer exactly, Your Honor.

BY MS. LASSACK:

Q. Professor Hill, how is data transferred between computers with a local area network?

A. Data is transferred via the use of this switch (indicating). And a switch is a medium access

control device. The switch is the box here, this blue box. And the switch basically --

JUDGE CHAPPELL: Does anyone see the laser pointer?

UNIDENTIFIED SPEAKER: Yes.

JUDGE CHAPPELL: It must be the angle here.

MS. VANDRUFF: May I turn the monitor, Your Honor?

JUDGE CHAPPELL: Try turning it toward the crowd.

UNIDENTIFIED SPEAKER: It's green, not red. A red laser would be like normal.

THE WITNESS: It's kind of hard because it's green.

JUDGE CHAPPELL: Is it on the one at the right?

MS. LASSACK: No. It's only on the one on the left.

JUDGE CHAPPELL: If this is very important, she can step down and point to the exhibit, because the screen is being pointed toward the crowd. That's what it's for. I've got my own screen here.

MS. LASSACK: And I think we can continue without the laser pointer.

JUDGE CHAPPELL: All of that for nothing.

THE WITNESS: Would you like for me to step

down?

JUDGE CHAPPELL: It's her rodeo.

MS. LASSACK: Your Honor, if it would be helpful to you, may the witness step down?

JUDGE CHAPPELL: It's your show. I'm allowing her if you need her to. But we do need to turn that screen back towards the audience.

THE WITNESS: So this is the local area network here that's enclosed in the box (indicating). And this device here, the blue box with the arrows on top, is a switch.

And a switch is a medium access control device, and it works at that layer of the networking stack. And as data is forwarded to the switch, the switch will look at the data and it will look at the IP address, the Internet protocol address, that's contained within this device, and then it will ask the computers that are connected to this switch which computer has the MAC address that uniquely identifies that computer that corresponds to that particular IP address.

So the switch is responsible for forwarding any data to the computers on this network based on the MAC address.

And the MAC address for these computers that are on this local area network are not known outside of that

93

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

BY MS. LASSACK:

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

Once the data arrives at the destination computer, what happens?

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

Q. What is an application?

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

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

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

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

94

Q. Can you explain what an FTP application does?

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

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

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

THE WITNESS: M-A-C.

JUDGE CHAPPELL: Does that stand for something?

THE WITNESS: Yes. Medium access control address.

JUDGE CHAPPELL: Thank you.

BY MS. LASSACK:

Q. Professor Hill, you mentioned ports.

A. Yeah.

Q. What is a port?

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

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

95

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

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

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

Q. You mentioned the importance of closing unused ports.

How is a port closed?

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

Q. What is a firewall?

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

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

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

96

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

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

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

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

Q. What is defense in depth?

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

Q. Why are they deployed in a layered fashion?

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

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

A. Yes.

Q. Please explain for the court how defense in

depth reduces the likelihood of an attack.

A. Defense in depth reduces the likelihood of an attack -- let's just assume that an attacker has a probability of -- a 50 percent chance of being successful in exploiting a vulnerability, and so at each layer of a mechanism -- at each layer of your system, the attacker has a 50 percent chance.

So if, for an example, you know, let's just assume that we have a scenario where there is an unauthorized application downloading on one of the computers that's on your local area network, and so if I want to have -- an example of a possible defense in depth strategy would be one where I want to deploy mechanisms throughout in order to address that problem.

Q. Why is downloading an unauthorized application a risk?

A. Downloading an unauthorized application is a risk because it introduces a vulnerability in the network. That application could have a malicious software embedded within it. The individual downloading it may not understand the consequences of the download. It may not -- the individual may not also understand how the application works.

So it just introduces a risk. If it's not needed for -- if there's no business need for the

application, then it introduces a risk.

Q. In the example you're describing, Professor Hill, will you use CXD 2 to describe the first step of defense in depth.

A. Okay.

So with this example, I'm going to present some parts of what would be a defense in depth strategy to protect against an unauthorized download.

So the first part that we see here is the firewall that is at -- that's right between the Internet cloud and the router. That router there is a gateway router. And routers are devices that are used to connect networks together.

And so what a firewall does, it's a barrier protection mechanism, as I've previously stated, and it can be used to block traffic from entering the network. Traffic that is initiated outside of the network can be blocked by the firewall based on the Internet protocol address and port number, so you can use the firewall to block those ports.

So in here I call that the Internet connection layer.

Q. Are there any other types of mechanisms that could be deployed at the Internet connection layer as part of a defense in depth strategy?

A. Another type of mechanism would be an intrusion detection system.

Q. What is an intrusion detection system?

A. An intrusion detection system is like a sensor in your network, and its purpose is to detect malicious activity.

Q. Professor Hill, what is the next step in your example of a defense in depth strategy?

A. The next step would be to deploy security mechanisms at what I've designated as the workstation layer. And here, I'm designating the use of a -- another firewall. And this would be a software firewall that would be executed on individual workstations and servers.

Q. How would you describe the workstation server layer?

A. Can you clarify?

Q. What types of devices are located at the workstation server layer?

A. Security devices?

Q. More computer hardware devices.

A. Oh, okay.

At the workstation and server layer we basically have our computers. We have -- and these are workstations that are used by individual -- by

individuals within an organization.

There are servers at the workstation and server layer, and they are used to run like your server applications, like e-mail servers, database servers, and those types of things. You can have laptops at this workstation and server layer.

And so those are some of the different devices that are at the workstation and server layer.

Q. In the example you have up here at CXD 2, will you explain how the software firewall enhances the security with the hardware firewall at the router.

A. Okay. One thing that we should all know is that there's no such thing as perfect security, especially whenever there are humans involved in the configuration of the software. There can always be mistakes, and that's one of the reasons why we want to do defense in depth.

So if there's been a misconfiguration, for example, of the firewall at the Internet connection layer, this mistake could hopefully be addressed by having a software firewall at the workstation layer.

Another reason for having a firewall at the workstation layer is that there is some traffic that you want to allow into your network, but you don't want -- that traffic should be destined for a specific machine, and maybe you want to have a simple coarse-grained firewall rule at the Internet connection layer, and you can have a more stringent fine-grained rule at the workstation layer, so this allows you to do that.

Q. Will you continue on in your example at CXD 2 and show the next step in the defense in depth strategy.

A. The next step in the defense in depth strategy is the user account layer.

And so at the user account layer, what you want to deploy are mechanisms that can be used to authenticate a user, limit access to data and resources, and those can be done at the user account layer.

And also you would want to limit the functionality that the user has within that particular workstation.

Q. What do you mean by "limit the functionality that the user has"?

A. So, for example, it's a common practice in the IT profession to not give regular users of a system administrative access to their computer.

What administrative access does, it gives you full control over that machine. And one of the

functionalities that comes with administrative access is the ability to download software onto the computer.

Q. Professor Hill, does an appropriate defense in depth strategy take into account the size of a company's network?

A. Yes, it does.

Q. How does it do that?

A. It takes it -- it takes -- as I said before, the -- a defense in depth strategy -- and when you're defining a comprehensive information security plan, it's a process.

It takes into consideration the size of the network by looking at the number of machines that the network may contain, the amount of data that would be flowing into the network, the amount of information that the system will maintain and store, so all of those things are taken into consideration because the larger the network, the -- probably the more costly the mechanisms that you would need to use to secure that network.

Q. Professor Hill, does an appropriate defense in depth strategy take into account the volume and sensitivity of the types of information stored on the network?

A. Yes.

Go ahead.

Q. How so?

A. If the -- if there are large amounts of information that's stored on the system, you need to think about how to limit an individual's access to that information. It is not a good practice to give an individual access to all information. And the reason for that is the insider threat.

So you could have a malicious insider. If given access, full access to all information, then that one individual could expose all of that information.

Q. How does the sensitivity of the information affect an appropriate defense in depth strategy?

A. If the information is highly sensitive, then it is imperative that you protect that information.

So you would need to think more about how do I protect that information when it's stored.

If the information is being backed up and it's highly sensitive, and I'm not -- there is no need to access that information throughout the day, you may want to consider encrypting that backup.

You would not want to store this information, this sensitive information, on an individual's multiple-use computer.

So those are some of the things that you would

need to take into consideration when you have sensitive information.

In addition, you want to think about how do I transmit this sensitive information in a secure manner.

Q. Professor Hill, do technical security measures alone provide reasonable security?

A. No, technical security measures alone do not provide reasonable security.

You can attempt to just deploy mechanisms even in a layered fashion, but if you don't first understand the goals that are to be achieved, if you don't understand the policies that need to be specified and defined in order to satisfy those goals, then simply deploying mechanisms, even in a layered fashion, will not result in reasonable and appropriate security for your system.

Q. Professor Hill, I'd like to direct your attention to paragraph 31 of your expert report.

Will you read the first sentence of that paragraph, please.

A. "There are seven principles that help to specify the policies and identify the mechanisms that are to be deployed at each layer of a defense in depth security strategy."

Q. Please explain to the court the first of those

seven principles.

A. The first of the seven principles is don't keep what you don't need.

Q. Why is that important?

A. That's important because if you keep information that is not required for your business practices, then that introduces an additional burden on the individual to secure that information, and it could also, if there is a compromise, increase the scope of harm.

Q. Please explain the second of the seven principles.

A. The second principle is to patch. And what that means is that software is -- will have vulnerabilities. Applications. Operating systems. Researchers have found that for every ten lines of computer code, there is on average one coding mistake or flaw.

And so if we look at something like the operating system Windows 2003, that operating system has 50 million lines of code, and so you would expect on average there to be five million flaws, coding mistakes, in that operating system software. And so all of those mistakes will not be identified before that software is deployed, and so vendors, like Microsoft,

will issue updates and patches to coding mistakes that are found in their software.

Q. What is the third of the seven principles?

A. This third is ports.

And so we've talked about ports and the fact that a port is an open door to your network, and so this principle is basically saying close all used and unneeded ports.

Q. All right. That was unused?

A. Unused.

Q. What's the next of the seven principles?

A. The next of the seven principles is policies.

And the overall process for defining a comprehensive information security plan, you know, is composed of a step where you are to define the policies that will satisfy your security goal.

So specifying policies is an important part of creating a comprehensive security plan.

Q. What is a comprehensive information security plan?

A. A comprehensive information security plan is one in which you have identified the sensitive resources that need to be protected, you've specified your goals, you have also defined policies for enforcing and satisfying those goals and you have

identified the mechanisms and the way they would be deployed.

It also includes training of individuals who will be using the systems and the ones that will be maintaining and securing the system.

Q. Should a comprehensive information security program be in writing?

A. Yes, it should.

Q. Why is that?

A. It should be in writing for several reasons.

One of the first is because it documents the current practices and it provides a guide for the IT professionals on how to secure the system.

Another reason that it should be in writing is because it serves as a training tool also for individuals who are going to use the system and also maintain it.

Another reason that it should be in writing is because oftentimes in an organization there's turnover, and so if there is little or no overlap with regards to the people who are managing the system, then that comprehensive -- that written comprehensive information security plan provides the guidance for the new IT professionals who are assuming the responsibility for maintaining and securing the network.

Q. We'll be talking about a comprehensive information security plan shortly.

I'd like to turn back to the next of the seven principles, which is protect.

What does that mean?

A. "Protect" basically means that you should deploy mechanisms that will protect your system. And we've talked about some of those mechanisms, for example, a firewall, which is a proactive mechanism and because it proactively tries to prevent unauthorized traffic from entering the network.

We also have reactive mechanisms, like antivirus software, that whose goal is to detect the presence of malicious software.

And so protect is very important because it talks about the mechanisms that you are actually deploying in order to protect your system.

Q. What is the next of the seven principles?

A. The next of the seven principles is probe.

And probe is all about assessing the risk and the vulnerabilities within your system and through things like penetration testing, reviewing of security logs, monitoring traffic that comes into your network, intrusion detection, those types of things.

Q. What is the last of the seven principles

109

identified in paragraph 31 of your report?

A. The last is physical.

So with physical protection, you want to ensure that your computer infrastructure is physically protected. You have a server room and the server room is locked. Your computer rooms are locked and you limit the physical access to these resources.

Q. Does limiting the physical access to the resources prevent electronic attack?

A. No, it does not.

Q. Professor Hill, how did you identify the seven principles listed in paragraph 31 of your report?

A. These seven principles are known. And through my training and experience, that's how I've come to understand and know these seven principles.

But these seven principles are also provided in guidelines that have been defined by various government, industry, and academic organizations for protecting and securing a network.

Q. I believe earlier you testified that there's no such thing as perfect security.

A. Yes.

Q. Why is that?

A. There's no such thing as perfect security because threats are always evolving. And as we define

110

mechanisms to protect or protect against or prevent or mitigate a risk, there's a new risk, and so it's an arms race. And even if I've addressed a particular risk and vulnerability, that vulnerability could evolve to evade the techniques that I'm using to mitigate that risk.

Q. If there's no such thing as perfect security, what is the result of an appropriate defense in depth strategy based on the seven principles?

A. The result is is that you want to limit the likelihood of an attack. And as I was previously stating, if an attacker has a 50 percent chance of attacking your system, if you have a layered approach of deploying your mechanisms, then in the example that I gave where we had three layers, you reduce your chance of success from one-half to one-eighth, given that particular example scenario.

JUDGE CHAPPELL: You say there's no such thing as perfect security; is that correct?

THE WITNESS: Yes, sir.

JUDGE CHAPPELL: Isn't that also saying then that in every system there always is a likelihood of a problem?

THE WITNESS: Yes, sir.

And if I could respond --

111

JUDGE CHAPPELL: Go ahead.

THE WITNESS: -- to that point.

And that is why you would want to use a defense in depth and you want to use a set of heterogeneous mechanisms deployed throughout, because there's a chance of a vulnerability, there's a chance of human error.

And so if, for example, one of those mechanisms are penetrated, the hope is by deploying multiple mechanisms throughout your network, you could reduce the overall likelihood.

JUDGE CHAPPELL: But with all that, even a system you designed, if an employee managed to download LimeWire, you'd still have a problem.

THE WITNESS: If an employee manages to download LimeWire, you would have a problem. But you would also have to go back and look at your policy regarding user accounts and whether employees need the ability -- need to be able to download software in order to do the work that they are required to do.

MS. LASSACK: Do you have any additional questions, Your Honor?

JUDGE CHAPPELL: No.

BY MS. LASSACK:

Q. Professor Hill, I'd like to turn to the next

112

topic, which is LabMD's network.

Please describe for the court LabMD's network during the relevant time period for your conclusions.

A. LabMD's network, I consider it to be a small network, maybe no more than 50 workstations on the network.

There were I don't think no more than ten servers throughout the lifetime of the network during the relevant period, time period.

There were laptops of the salespeople that weren't directly connected to the network but could connect remotely to the network.

And another part about the network is that it did store large amounts of sensitive data.

And another interesting part about LabMD's network is the manner in which data flowed into the network from the doctors' offices, and so doctors' offices were allowed to basically push data into LabMD's network.

So what I mean by "push" is to write data into the network, and so that creates an interesting scenario and interesting in the fact that you have to be extremely careful when you allow an external entity write privileges within your network, especially an external entity for which you have no control over the

113

device from which the writing is occurring.

Q. I'd like to back up for a second.

What does it mean to write to a network?

A. So what it means is, to write is to place files that are stored on your -- on the remote machine, to actually place those files within LabMD's network on one of their servers, so it means to basically change, make changes to the hard disks that are stored within LabMD's network.

Q. Will you explain how doctors' offices did that.

A. Doctors' offices did that in a couple of different ways. One was -- one way was through a Web portal application. They entered patient information manually and that data was saved on through -- saved on the LabMD machines via the Web application.

Another way was through bulk file transfer of multiple patient files at a time. And if -- if the doctor's office had their own electronic health record system, those files would be taken from that doctor's office server, copied to the machine that LabMD had provided to the doctor's office, and then written to LabMD's server within LabMD's network. And this was done via an anonymous file transfer protocol.

Q. We'll talk about that in more detail later.

What types of information did the doctors' offices transmit to LabMD?

114

A. They transmitted things like the patient's name, the address, Social Security number, insurance information, the types of tests that were to be performed, and those are some of the -- date of birth.

Q. What happened when that information got to LabMD's network?

A. Once the -- the information was written into LabMD's mapper server, and then it was combined with information on their demographic server and stored for the use of their laboratory information system that -- the physicians and the individuals who were responsible for evaluating tests actually used that information, and the information was also used for LabMD's billing system.

Q. What was LabMD's billing system called?

A. LabMD's billing system was called Lytec.

Q. What did the mapper server do?

A. The mapper server basically collected this information and maintained that information and then transferred that information to the different servers within LabMD's network.

Q. Professor Hill, I'd like to direct you to paragraph 38 of your report.

Will you please read that aloud.

115

A. "Physician clients typically retrieved the results of the services they ordered from LabMD through LabMD's Web portal. In doing so, they accessed personal information stored on LabMD's network."

Q. How did the physician clients do that?

A. Through their Web application.

Q. How did the Web application work?

A. Web applications, the way they work, typically there's a Web server that's responsible for managing and serving the data, and then there is a client application that enables a client to access that data.

And so a client would initiate a request to the Web server in order to retrieve information.

Q. You mentioned LabMD employee computers earlier.

JUDGE CHAPPELL: Hold on a second.

In your paragraph 38, you're saying they, I guess as the physicians, access personal information.

Are you saying everyone's personal information or just that information which they had business to access regarding their own patients?

THE WITNESS: Your Honor, I'm not exactly sure. I would think that they were accessing the patient information --

JUDGE CHAPPELL: I don't want you to think. I want to know what you know based on your analysis.

116

THE WITNESS: Based on my analysis, I didn't have information to determine whether they were able to access other patient information that were not their patients. I didn't have that information, so I can't answer definitively whether they -- whether or not they had access to patients that were not their patients.

JUDGE CHAPPELL: So that paragraph 38, you're not saying that's a bad thing necessarily.

THE WITNESS: No, I'm not saying that's a bad thing. It's just a description of how they accessed the information remotely.

JUDGE CHAPPELL: It could be a bad thing, but you don't know.

THE WITNESS: It could be a bad thing, but I don't know.

JUDGE CHAPPELL: Okay.

MS. LASSACK: Did you have any additional questions, Your Honor?

JUDGE CHAPPELL: No. I'll ask them if I have them. Go ahead.

BY MS. LASSACK:

Q. Did LabMD employees use their computers to access personal information stored on LabMD's servers?

A. Yes.

Q. Did any LabMD employees access the LabMD network

117

remotely?

A. Yes.

Q. Was any personal information maintained on LabMD employee computers?

A. Yes.

Q. Can you give the court an example, please.

A. One example was the billings manager's computer. There was a specific backup policy which stated that there would be backups to the billings manager's computer of I think it was billings-related information, but it was -- that billings-related information was sensitive information.

Q. Professor Hill, I'd like to direct you to CX 6 page 10.

What is CX 6 page 10?

A. CX 6 page 10 is a data backup policy.

Q. Is this the policy that you were referring to?

A. Yes.

Q. Did LabMD contend that this policy was in effect during the relevant time period?

A. Yes.

Q. Were these backups encrypted?

A. No.

Q. What is encryption?

A. Encryption is a process for taking plain text data and making it unreadable by individuals who don't have access to the encryption key.

118

Q. What is an encryption key?

A. An encryption key is a numeric value that's used as a part of the algorithm to transform the data into something that is not humanly readable.

Q. Was any other data on LabMD's network encrypted?

A. No.

Q. Were there any applications installed on any LabMD computers that were not necessary for business purpose?

A. Yes.

Q. What are those?

A. One was the LimeWire file-sharing application.

Q. Where was that application installed?

A. On the billings manager's computer.

Q. When was that application installed on the billing manager's computer?

A. That application was installed at some time between 2005 and 2006.

Q. Can you explain what the LimeWire application does briefly?

A. The LimeWire application allows individuals who are part of the network and using the application to

119

search and retrieve files from individual machines and not from a central server.

Q. What are those applications called generally?

A. Peer-to-peer file-sharing applications.

Q. How does a peer-to-peer file-sharing application work to share files?

A. A request is actually made by one application to retrieve for a specific file, and that file is then returned by the owner of the file, so then there's a search -- there could be a search of a particular host for all files that are available for sharing on that particular file, and then the requester makes a request for that file if it sees something that it is interested in retrieving.

Q. What is a host?

A. A host is just a computer. And a host in a peer-to-peer file-sharing network is just a computer that's using the file-sharing application.

Q. How do users of a peer-to-peer file-sharing application make files available to share?

A. They make them available for sharing by designating them as sharing. But there's some -- there are opportunities for them to inadvertently share without them knowing.

Q. How does a user designate a file for sharing?

120

A. They would actually have to select this file and say that it is to be shared.

So the application provides mechanisms that will allow them to designate the file as a shared file.

Q. How long have peer-to-peer programs been available?

A. Peer-to-peer programs have been available since 1999.

Q. How widely were they used?

A. They've been widely used since their introduction. One of the major reasons for this is that they were -- they made the sharing of music and video files readily available to peers on the network.

Q. Are there any types of risks associated with peer-to-peer file-sharing programs?

A. Yes. The one I've already mentioned is the inadvertent file sharing.

Another is that if you download files from a peer-to-peer file-sharing network, you have no idea of whether malicious components are embedded within the file that you've downloaded. And research has shown that many of the files on peer-to-peer sharing networks actually have malicious components.

Q. Has anyone provided warnings about these risks?

A. Yes.

Q. Who?

A. Security experts have been providing warnings about these as early as 2005.

Q. If a file is inadvertently shared using a peer-to-peer file-sharing program, how easy or difficult is it to get the file back?

A. Very difficult.

Q. Why?

A. One of the reasons why is that you may not know all of the nodes or computers on the file-sharing network that may have that file and are making it available for sharing, because there's no guarantee that a computer will actually be on at the time that you're trying to search and find all of the computers that actually contain that file.

Another reason is that once you have digital content and it leaves your control, it's impossible to identify all the places that this file is now present, because a file can also be shared in a nonelectronic manner outside of the scope of the peer-to-peer file-sharing network.

Q. Professor Hill, I'd like to turn to paragraph 49 of your report.

JUDGE CHAPPELL: Let me ask you a question about peer-to-peer.

What about, for example, you have Firefox browser and you see there's an update and you connect and get the download or the update. Isn't that similar to a peer-to-peer?

THE WITNESS: That is -- you are not getting that update from a peer. You're getting that update from a trusted server.

So with Firefox and other applications that you purchase from vendors where you're getting an update, that process of updating is typically authenticated, so you verify the identity of the server that you're retrieving the update from, and so there's this trusted relationship between your computer and the computer from which you are downloading that information.

JUDGE CHAPPELL: But if someone had hacked onto that other computer, hacked into that system, you could still be exposed.

THE WITNESS: If someone had hacked into the server that from which you're retrieving the update, there's a compromise there and you could -- you could be exposed. You could download then a compromised piece of software.

JUDGE CHAPPELL: And as far as your definition of "peer-to-peer," is it always, for example, my computer at home to your computer at home, or does it

also encompass a system where there might be an intermediary server involved?

THE WITNESS: In peer-to-peer, that was the value of peer-to-peer. You don't have to interact through an intermediate server. You could have direct interaction between two computers, so there's no need for the intermediate server.

JUDGE CHAPPELL: So anything untoward or malicious would have to come from the other peer or computer.

THE WITNESS: Yes, it's coming from the other peer computer.

And you don't know anything about a peer computer. There's no authentication process. And it's like doing business with someone you don't know, and so there's no trust that has been established between the two peers, because you're separated by the Internet, and so there's really no way to establish trust.

JUDGE CHAPPELL: Are we talking about digital trust?

THE WITNESS: Yes, I'm talking about digital trust.

JUDGE CHAPPELL: All right. Thank you.

MS. LASSACK: And Your Honor, complaint counsel's expert, Dr. Clay Shields, will be here later

in the week to talk more about peer-to-peer software as well.

BY MS. LASSACK:

Q. Professor Hill, I'd like to direct you to section 7 of your report which begins on paragraph 49.

Now that you've provided the court the relevant background, I'd like to turn back to your overall conclusion that you've reached about the reasonableness of LabMD's data security.

What did you conclude?

A. I concluded that LabMD did not provide reasonable and appropriate security for their systems and the data that they stored within their system.

Q. How much personal information did LabMD store on its system?

A. Approximately 750,000 consumer records.

Q. What types of information did that include?

A. That included the name of consumers, their Social Security number, credit card information, banking information, insurance information, types of tests that had been requested. That's some of the information that was stored.

Q. Could LabMD have corrected its security failures at relatively low cost?

A. Yes.

125

Q. So in addition to asking you about your overall conclusions about LabMD's data security practices, did complaint counsel also ask you to provide opinions about specific data security practices at LabMD?

A. Yes.

Q. I'd like to ask you about some of those specific opinions now, actually all of them.

So first, did complaint counsel ask you to provide an opinion on whether LabMD developed, implemented and maintained a comprehensive information security program?

A. Yes.

Q. What did you conclude?

A. I concluded that they did not develop and maintain a comprehensive information security program.

Q. And you testified earlier about what a comprehensive information security program is. Can you summarize that for the court again?

A. A comprehensive information security program is one that is developed by a process, and it's a balancing process of balancing what your security goals are with the types of information that you're trying to protect. And once you specify those goals, you then also define mechanisms that will satisfy -- define policies that will satisfy those goals and mechanisms to enforce those goals.

126

Q. What are some examples of the types of goals a comprehensive information security program should address?

A. Some examples include confidentiality, integrity and availability.

Q. What is a confidentiality goal?

A. A confidentiality goal is a goal in which you ensure that there will be no unauthorized access to a sensitive resource, like a data resource.

Q. What is an integrity goal?

A. An integrity goal is one in which you ensure that if there is a change, an unauthorized change to the system or to data or to files stored within the system, that you will be able to detect that change.

Q. What is an availability goal?

A. An availability goal is one in which you ensure that your system and data are accessible when they are needed.

Q. Why did you conclude that LabMD did not have a comprehensive information security program?

A. I concluded that they did not have a comprehensive information security program because there was no evidence, first and foremost, that a process for developing one had been put in place.

127

There were no written security policies until 2010. Then the policies themselves were not sufficient in some areas. And then there were policies that were not enforced.

Q. Let's start with the issue of whether LabMD had written information security policies.

How do you know that LabMD did not have information -- written information security policies until 2010?

A. This fact was provided in the record evidence.

MS. LASSACK: Your Honor, I'd like to show the witness CXD 1, which Mr. Sheer showed during his opening today, but in poster form.

JUDGE CHAPPELL: A demonstrative?

MS. LASSACK: Yes.

JUDGE CHAPPELL: Go ahead.

MS. LASSACK: And can we show it on the screen as well.

BY MS. LASSACK:

Q. Professor Hill, what is CXD 1?

A. CXD 1 is a LabMD IT employee timeline.

Q. Have you reviewed the testimony of the individuals listed in CXD 1?

A. Yes, I have.

Q. Did they testify about the dates when they were employed at LabMD?

128

A. Yes.

Q. Does CXD 1 accurately reflect their testimony?

A. Yes, it does.

Q. What does CXD 1 show about the importance of having written information security policies?

A. What CXD 1 shows is that there's a lot of transition of the -- and turnover of the IT employees. Sometimes there's very little overlap in the previous IT employees and the ones that were -- that would assume those positions.

And as I previously stated, that one of the reasons for providing written information security programs is so that they can be a guide when there is this turnover, and there's very little overlap between employees.

MS. LASSACK: Your Honor, may the witness approach the exhibit and may I approach the witness to continue our testimony to --

JUDGE CHAPPELL: Yes and yes.

MS. LASSACK: Thank you.

BY MS. LASSACK:

Q. Professor Hill, will you please indicate on CXD 1 when LabMD put its information security plans in writing.

129

A. They put their plans in writing in 2010, so -- (indicating).

Q. Will you indicate that, please.

JUDGE CHAPPELL: Go ahead and deface that thing.

She's reticent about marking up your document.

(Pause in the proceedings.)

MS. LASSACK: Thank you, Your Honor. May the witness return to the witness stand?

JUDGE CHAPPELL: That's all?

MS. LASSACK: For now.

JUDGE CHAPPELL: Go ahead.

BY MS. LASSACK:

Q. Professor Hill, did LabMD have an employee handbook in writing?

A. Yes.

Q. Why did you conclude that the employee handbook was not a comprehensive information security plan?

A. The employee handbook did not contain specific policies about protecting data resources and the infrastructure.

Q. Professor Hill, earlier you testified that there were other reasons why you concluded that LabMD's information security program was not sufficiently comprehensive other than not being in writing?

130

A. Yes.

Q. Was one of those that some of its policies were not being enforced, E-N-F-O-R-C-E-D?

A. Yes.

Q. Can you give the court an example, please.

A. One example of the policies not being enforced was one that regarded the transmission of sensitive data electronically via e-mail, and it said that -- the policy stated that encryption tools would be used in order to transmit sensitive data via e-mail, but record evidence shows that data was transmitted via personal e-mail in an unencrypted form.

Q. I'd like to direct you to page 6 of CX 6, and it will be up on the screen as well.

And in particular, the fourth policy down.

What is that policy?

A. That's the e-mail security and encryption policy.

Q. What does that policy say should be done?

A. It says that corporate e-mail -- LabMD's corporate e-mail system has security settings, and it's recommended that information of a sensitive nature and containing sensitive data should not be sent via e-mail unless messages and attachments are encrypted.

Q. Did LabMD provide mechanisms to encrypt

131

messages?

A. No.

Q. You said that LabMD had no written information security policies until 2010; is that correct?

A. Yes.

Q. Can we show on the screen the first pages of CX 6 and CX 7.

What are CX 6 and CX 7?

A. CX 6 and CX 7 are LabMD's Policy Manual. They're two different versions of the Policy Manual.

Q. Are these the policies that you were referring to that were in writing in 2010?

A. Yes.

Q. What did you conclude about whether these policies were sufficiently comprehensive?

A. I concluded that they were not sufficiently comprehensive.

Q. Why did you reach that conclusion?

A. I reached that conclusion because they were missing some key elements regarding specific policies.

Q. Can you give the court an example of one of those?

A. One of the most basic mechanisms that is to be used in a system is an authentication mechanism. The most commonly used authentication mechanism is the user

132

name and a password. The user name is your identity, and the password is your proof of the identity.

So it's important to use strong passwords. And there's no information about strong password policies and the strength of passwords, the history, how often passwords should be changed, whether there's a duration in which you can reuse passwords. There's no information about the strength of passwords.

Q. Professor Hill, could LabMD have implemented a comprehensive information security program at relatively low cost?

A. Yes.

Q. How so?

A. They could have done this through consulting guidelines that were available regarding what are the best practices to secure a system.

They could have done this by providing training to their employees on the consequences and the responsibilities of misconfigured systems and the consequences of the use of some of the antivirus software that -- for example, antivirus software that they're responsible for using, and the training of IT professionals on evolving threats and the best ways of mitigating risk.

Q. You mentioned available guidance.

133

What are some examples of organizations that provide such guidance?

A. Some organizations that provided such guidance include the National Research Council. They provided an actual book, and in one chapter of the book they focus specifically on security mechanisms for protecting an infrastructure that contains medical information.

Q. What is the National Research Council?

A. The National Research Council is an organization that seeks the guidance of researchers in the field in order to define and specify guidelines.

Q. When you say "researchers in the field," what field are you referring to?

A. For this, for the purposes of this, I'm referring to like IT-related individuals.

Q. Are there other examples of organizations that provide guidance for creating a comprehensive information security program?

A. The National Institute of Standards, NIST, provided guidelines. I've actually cited some of their guidelines on risk assessment, and so they provide a comprehensive plan for risk assessment.

Q. What is the full name of NIST?

A. The National Institute for Standards.

134

Q. What does the "T" stand for?

A. I'm trying to remember what the "T" stands for.

Q. Is there a document that would refresh your memory?

A. Yes, there is.

JUDGE CHAPPELL: Is it "Technology"?

BY MS. LASSACK:

Q. Professor Hill, Your Honor asked if it's "Technology."

Is it "Technology"?

A. It probably is "Technology." Thank you, Your Honor.

JUDGE CHAPPELL: And is the "S" "Science"?

BY MS. LASSACK:

Q. Is the "S" "Science"?

A. I don't recall.

JUDGE CHAPPELL: I'm guessing. I don't know.

THE WITNESS: Yeah. Actually, the "S" is "Standards."

BY MS. LASSACK:

Q. I believe you testified it's "Standards."

A. Yes.

Q. So then what is the full name of NIST for the record?

A. The National Institute for Standards and

135

Technology.

Q. How would IT professionals know about organizations like NIST and their resources?

A. Organizations would know about NIST and their practices and some of these other related organizations through training.

Q. What types of topics are covered in guidance provided by organizations like NIST and NRC?

A. The types of guidance that's provided by these organizations in their guidelines are the same types of guidelines that I presented in the background section for a comprehensive information security program.

Q. Can you remind us what those are?

A. Okay.

So they include things like don't keep what you don't need, patching your and updating your system, closing all unused ports, you know, providing physical security, specifying policies, you know, being able to probe your network for risk assessment, those types of policies, protecting your network, you know, which mechanisms are best suited to address a particular security goal. Those are the types of things that they provide guidelines and guidance on.

Q. How could LabMD have used these types of guidelines to create a comprehensive information

136

security program at relatively low cost?

A. They could have -- given their specific goals and the types of information that they needed to protect, they could have looked at the guidelines for specific confidentiality goals and the types of mechanisms that those guidelines recommend.

And so what those guidelines do, they provide like a general and overall guidelines for like all types of computing infrastructure. But if you have additional things that differ, you are going to have to evaluate that in a more process or in an approach and really look at your structure to understand what in addition to those guidelines you need to do.

Q. How much would it cost to implement that process-based approach?

A. That process-based approach for a trained IT person, that -- that takes people time in order to just go through the process in evaluating the system and the infrastructure.

Q. So it's just a time cost then, not monetary?

A. It's a time cost.

Q. Professor Hill, I'd like to turn to the section of your report that begins with paragraph 63.

Did complaint counsel ask you to provide an opinion on whether LabMD used an appropriate set of

137

readily available risk assessment measures?

A. Yes.

Q. What did you conclude?

A. I concluded that LabMD did not provide a reasonable set of readily available measures for risk assessment.

Q. What does risk assessment involve?

A. Risk assessment involves evaluating your network to determine the risks that are current in your network.

Q. Why is risk assessment important?

A. Risk assessment is important because security can only be considered within the context of what is actually happening right now, and so you -- and threats are always evolving, and so that context changes. And because that context changes, you need to do a risk assessment periodically in order to assess the overall vulnerability and the risk within your system.

Q. How does risk assessment fit into an appropriate defense in depth strategy?

A. Risk assessment is very -- it's very important. It's a part of the -- it's the probe part of your seven principles.

Q. How does risk assessment relate to the selection of security measures?

138

A. Risk assessment -- so all security measures are not going to just be to protect. There are going to be security measures that are going to be about assessing the network.

So you need risk assessment tools, and they become mechanisms in an overall security program. But once I've actually used those risk assessment mechanisms, they can help me to identify the vulnerabilities that are present and whether I need to reconfigure my current security mechanisms that I have and am using or I need to get additional mechanisms to protect against an emerging or a new threat.

Q. What are some examples of the types of mechanisms that IT professionals use to assess risk?

A. So one example would be a penetration test.

And you have a tool called NMAP that is widely used for penetration testing, and that's just to probe your network to see if there are open ports.

You have things like Nessus that allows you to, once you probe the network, to understand whether your operating system needs to be updated.

So you have various types of techniques, I mean, tools in order to do that.

You have things like Wireshark that will allow you to capture data and do some analysis of that data to

139

understand what data is entering and leaving your network.

Q. Can you describe for the court how a penetration test works?

A. One example of a penetration test, I go back to NMAP.

And so with NMAP what I can do is, given the IP addresses on your network, I can try to initiate a connection to those IP addresses giving various -- varying port numbers for -- and that type of assessment is called like a port scan.

And so my goal when doing this penetration test is to scan all the ports that are -- that could possibly be open. And there are 216 different ports. That's over 65,000 ports that could be open.

And so a penetration test, one example is a port scan. I just go through the IP addresses on your network and try to find an opening.

Q. You mentioned NMAP. What is that?

A. NMAP is a freely available tool that does a variety of different penetration testing, and a port scan is just one of those.

Q. What are some other examples?

A. Other examples of penetration tests that can be done with NMAP or other examples of different types of

140

tools that can be used for risk assessment?

Q. Other examples of different types of penetration testing that can be done.

A. Okay.

So one thing that NMAP allows you to do is to determine information about the level of the operating system that you're running, and so that becomes important because if the operating system contains vulnerabilities, an attacker would want to know that, so an unpatched operating system that contains vulnerabilities can be exploited by an attacker.

And so discovering the level of the operating system is -- is going beyond just a port scan but trying to determine, you know, whether you're running a patched or an unpatched operating system or any other applications that communicate via the network, whether they are -- also have vulnerabilities in them.

Q. How do IT professionals decide which risk assessment mechanisms to use?

A. The way IT professionals decide about that, it is part of this whole process-driven approach.

So if I have servers within my organization that need to communicate with the outside world and there are going to be connections that initiate it, I would want to use a penetration test to determine whether I -- my firewall is configured properly, where I'm not just allowing those ports to be open for those servers, but you know, I would close unused ports.

Q. Can one type of risk assessment mechanism alone be enough to be sufficient to assess risk?

A. No.

Q. Why not?

A. Because, for example, penetration testing allows me to determine whether ports are open. Penetration testing doesn't tell me anything about the data that may be entering or leaving my network.

So if I have sensitive data and I want to ensure or assess whether that sensitive data is leaving my network, I would need to actually do what we call deep packet analysis. I need to go beyond the headers, and a penetration test only looks at the header information, like IP addresses and ports. I would have to go beyond that layer within my data and look at the data itself, and so you need a tool like Wireshark in order to do that.

Q. What is Wireshark?

A. Wireshark is a data traffic monitoring tool that will capture data on your network and allow you to look at that data snapshot.

So when you see data going across the network,

it's in hexadecimal form, and so you need that translation of that data into a human-readable form.

Q. I'm not even sure I can say that word again.
What is hex- -- is it hexadecimal form?

A. Yes.

Q. Is that what you said?

A. Yes, hexadecimal.

Q. Can you explain briefly?

A. There are different -- hexadecimal form basically represents the data in -- like with 16 -- first it covers like 16 bits of information.

So the format is not like, you know, just our, you know, our regular alphabet, so you're not going to see -- when you're looking at data as it's being transmitted, you're not going to see A, B, C, D. You're not going to see our regular alphabet. What you're going to see are numbers and characters from zero, you know, to FFF, so -- and that's the representation of, you know, information in hexadecimal.

Q. Okay. So to come back from there to the higher level of risk assessment, are you saying that one type of risk assessment can only address one type of risk?

JUDGE CHAPPELL: Hold on.

Is there an objection?

MR. SHERMAN: No, sir. That's a plea for a

break.

JUDGE CHAPPELL: How much time do you need to finish the witness?

MS. LASSACK: I think -- I would think at least a couple more hours, Your Honor.

JUDGE CHAPPELL: So there is hope that you'll finish today.

MS. LASSACK: I think there's at least hope that I'll finish today. It will be today or early tomorrow.

JUDGE CHAPPELL: Okay.

At this time we'll take our afternoon break. We will reconvene at 3:45.

We're in recess.

(Recess)

JUDGE CHAPPELL: Back on the record.

Go ahead.

MS. LASSACK: Your Honor, there was a pending question before we took a break. May I restate it?

JUDGE CHAPPELL: Would you like her to read the question?

MS. LASSACK: Sure.

(The record was read as follows:)

"QUESTION: So to come back from there to the higher level of risk assessment, are you saying that one

type of risk assessment can only address one type of risk?"

THE WITNESS: Yes.

BY MS. LASSACK:

Q. Professor Hill, what types of measures did LabMD use to assess risk on its network?

A. LabMD used logs from their firewalls. They used antivirus software. And in 2010, they did a penetration test.

Q. Why did you conclude that LabMD did not use an appropriate set of risk assessment measures?

A. First, the logs from the firewalls were very limited. And there's no evidence in the record of the actual log from the firewall. There's just a discussion in the transcripts that discusses reviewing the logs from the firewall. But the firewall logs are very limited. They could only collect a few days of data that had been transmitted into the network.

And with regards to the antivirus software, an antivirus application can only identify malicious software that it knows about, and so -- and its purpose is to detect the presence of malicious -- known malicious software, so it has a limited functionality when you begin to look at the full scope of risk assessment.

145

And...

Q. Are there any other reasons why you concluded that LabMD's antivirus software was not a sufficient risk assessment mechanism?

A. There were times that some of the antivirus software could not be updated and could not be run, and so there was then no -- those machines who were -- those machines that were running that particular antivirus software, no detection of viruses could occur on those machines because those machines were not able to update their virus signatures and actually run the antivirus software.

So that's one reason why I say that their use of antivirus software was not sufficient.

Q. Professor Hill, I'd like to draw your attention to CX 35 and page 2 in particular.

What is CX 35?

A. CX 35 is an APT service invoice.

Q. We talked earlier about APT.

What type of work did APT do for LabMD?

A. APT deployed some firewalls. They also helped with problems that were reported to them.

For example, in this particular case, they were looking at, you know, the anti- -- a particular server at LabMD and the inability to run the antivirus

146

software and the fact that the software hadn't been updated, the virus definitions hadn't been updated since 2005. And this particular service invoice is dated 2006.

Q. Okay. Professor Hill, are you referring to the first entry on page 2 of CX 35?

A. Yes, I am.

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

A. "Ran a complete virus scan on the server and found no issues after it had completed. The LabMD server however does still have an issue. It will not run a virus scan, nor will it go out and get updates for the virus definitions. It has not updated since July of 2005. Tried to run an online virus scanner, but since the server did not have Java and would not install it, I was not even able to do that. Suggested that we need to totally wipe and reload that server."

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

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

Q. Did you consider this entry when forming your opinion about the effectiveness of LabMD's antivirus applications?

A. Yes.

Q. What did you conclude from that entry?

147

A. I concluded that their use was not -- their use of antivirus software was not sufficient in order to protect critical servers within their infrastructure.

Q. Why did this entry support that conclusion?

A. Because the virus definitions had not been updated since July 2005, and this particular work order was for the day of May 3, 2006, and so that's approximately a year without new virus definitions. And as I previously stated, antivirus software can only detect malware that for which it has a data signature.

And a signature is, just think of it as the signature that we sign. And our signature is usually unique to us, and so a virus signature is unique to that specific virus.

So if the antivirus software can't update itself to get new signatures, then it cannot detect the new and emerging viruses that may be present on a system.

Q. Professor Hill, I'd like to turn your attention to page 3 of CX 35, particularly the entry dated June 21, 2006.

What does that entry say?

A. It says, "Did check on all of the servers. Each server was not updating antivirus definitions since May '06. Tried to run a manual update of the

148

definitions, but on every server it would start the live update process and then lock the program up. Suggested they upgrade their antivirus since they are running Symantec Corporate 7 which is not supported by Symantec."

Q. Did you review this entry in connection with reaching your conclusions about LabMD's antivirus applications?

A. Yes.

Q. What did you conclude from this entry?

A. I concluded that they were not running antivirus software that would protect their servers.

Q. Professor Hill, we've discussed antivirus software for LabMD's servers.

Did you reach any conclusions about LabMD's antivirus software for individual employee workstations?

A. Yes. The -- for some point in time during the relevant time period, the antivirus software on individual employees' computers were run and -- but the logs from those were not reviewed until there was a problem with the machine, a noticeable problem, so maybe there's a slowdown that prevented the employee from performing his or her duties.

So at that point the employee would report to

149

the IT staff that I'm having problems with my computer, and at that point in time is when those logs would be -- antivirus scanning logs would be reviewed.

And so this is a very reactive kind of approach, and it occurred -- to securing a system or assessing the risk in a system. And it often occurred in an ad hoc manner, so there wasn't scheduled, you know, reviews of these logs for some period of time during the relevant time period.

Q. You mentioned earlier why LabMD's firewalls were not sufficient risk assessment tools.

Why was that?

A. Because the main purpose of a firewall is to block unnecessary and unwanted traffic and unauthorized traffic from entering the network, and so unless it's a firewall that also has some intrusion detection functionality, it's not going to have the ability to capture large amounts of traffic in order to do some analysis on that traffic and alert IT staff of, you know, possible threats and suspicious activity within the network, and so their firewalls only had the capability of capturing a limited amount of traffic.

Q. Did LabMD's firewalls have intrusion detection functionality?

A. LabMD's -- one question. Which firewall are you

150

referring to?

Q. I'm referring to LabMD's gateway firewalls.

A. Okay. LabMD's gateway firewall, as I recall, it had intrusion detection capability, but it was not enabled.

Q. Do you recall if that's true for whether all LabMD gateway firewalls had that capability?

A. There was -- as I recall, there was one gateway firewall, and then the other firewalls were internal firewalls, and I don't recall them having that capability.

Q. Was any intrusion detection capability in operation on any LabMD firewalls during the relevant time period for your conclusions?

A. No.

Q. Did APT monitor LabMD firewalls in a proactive way?

A. No.

Q. Why do you conclude that?

A. Because there's evidence of APT only providing service in response to a request, and also there's testimony from APT -- an APT representative which said that it provided service in an ad hoc manner as a reaction to there being problems within the network.

Q. Professor Hill, I'd like to direct your

151

attention to CX 731.

What is CX 731?

A. CX 731 is the deposition transcript of Allen Truett.

Q. Who an Allen Truett?

A. Allen Truett was the owner of APT.

Q. Is he the representative you were referring to earlier?

A. Yes.

Q. I'd like to direct your attention to page 69 of Mr. Truett's deposition transcript.

Lines 1 through 16 in particular.

Is this the testimony that you were referring to earlier?

A. Yes.

Q. What did you conclude from this testimony?

A. That APT did not do any active monitoring of LabMD's firewalls.

Q. Did LabMD conduct manual inspections?

A. Yes.

Q. What did you conclude about LabMD's manual inspections as effective risk assessment mechanisms?

A. I concluded that LabMD's manual inspections were not effective.

Q. Why did you conclude that?

152

A. I concluded that for two main reasons.

The manual inspections were performed in an ad hoc manner for some period during the relevant time period, meaning that it was usually in response to an employee noting a problem was occurring with their machines.

And another reason that I concluded that the manual inspections were not effective was because it's virtually impossible for a human to inspect every aspect of a computer and determine that there has been a change in integrity of the system, basically that there's been a change that would compromise the security of a system.

So a computer may have over a thousand files. There are configurations that are in multiple places, configuration of shared folders and other types, the configuration of the firewall, so there are many aspects of the computer that would need to be inspected, including antivirus logs, any logs that the operating system may generate.

So there's so many places that you would have to look in order to do an assessment of the system, there's -- it's virtually impossible for it to be effective as a risk assessment tool.

Q. Earlier you talked about LimeWire being

153

installed on the billing manager's computer.

Did LabMD's manual inspections detect LimeWire on the billing manager's computer?

A. No, it did not.

MS. LASSACK: May I ask the witness -- may the witness approach CXD 1 again?

JUDGE CHAPPELL: Go ahead.

BY MS. LASSACK:

Q. Professor Hill, will you note on CXD 1 when LimeWire was installed on the billing manager's computer.

A. Okay. LimeWire was installed on the billings manager's computer between 2005 and 2006 (indicating).

Q. Will you note when LimeWire was removed from the billing manager's computer.

A. LimeWire was removed from the billings manager's computer in 2008.

Q. When was that in 2008?

A. May of 2008.

Q. Will you note that, please, on CXD 1.

A. (Witness complies.)

MS. LASSACK: May the witness return to the witness stand?

JUDGE CHAPPELL: Sure.

BY MS. LASSACK:

Q. Professor Hill, how long then was LimeWire installed on the billing manager's computer without being detected by LabMD's manual inspections?

154

A. From two to three years.

Q. Earlier you testified that LabMD's manual inspections were conducted in an ad hoc way; is that correct?

A. Yes.

Q. What did you base that conclusion on?

A. I based that conclusion on testimonies that were provided through the deposition.

Q. I'd like to draw your attention to CX 734.

Professor Hill, what is CX 734?

A. It is the deposition transcript of Alison Simmons.

Q. Did you review Ms. Simmons' testimony in connection with reaching your conclusion about LabMD's manual inspections?

A. Yes, I did.

MR. SHERMAN: Your Honor, if I could object, I don't think this is a deposition transcript. It's a CID hearing transcript.

JUDGE CHAPPELL: You need to stand up to object.

MR. SHERMAN: I'm sorry, Your Honor.

Yes, I believe this is a CID hearing

155

transcript, and I would just like that corrected for the record.

MS. LASSACK: That is correct, Your Honor. We will note for the record that that is -- CX 734 is Alison Simmons' investigational hearing transcript.

JUDGE CHAPPELL: You're questioning the witness. Why don't you let the witness handle that.

MS. LASSACK: Okay. I apologize.

JUDGE CHAPPELL: Did the witness give you the wrong answer?

MS. LASSACK: I believe so, Your Honor.

JUDGE CHAPPELL: Then why don't you have her correct it.

MS. LASSACK: Okay.

BY MS. LASSACK:

Q. Professor Hill, what is CX 734?

A. CX 734 is Alison Simmons' investigational hearing testimony.

Q. Did you consider CX 734 in connection with forming your conclusions about LabMD's manual inspections?

A. Yes, I did.

Q. I'd like to draw your attention to pages 78 through 80 of Ms. Simmons' investigational hearing transcript.

156

What did you conclude from this testimony?

A. I concluded that the manual inspections were performed in an ad hoc manner.

Q. I'd now like to direct your attention to page 14 lines 8 through 12 of Ms. Simmons' investigational hearing transcript.

What did Ms. Simmons testify about when she worked at LabMD?

A. She testified that her starting date was late August 2006 -- October 2006 and through August 2009.

Q. So is it correct that she testified that she was at LabMD from October 2006 through August 2009?

A. Yes.

Q. Professor Hill, you testified that manual inspections are not a sufficient risk assessment tool.

Before May 2010, did LabMD use any automated risk assessment measures?

A. No.

Q. Would that be other than antivirus software?

A. Other than antivirus software, that was the only one that was an actual electronic.

Q. So I can clarify the record then, your testimony is that Lab- -- other than antivirus software, LabMD did not use any automated risk assessment mechanisms prior to May 2010.

157

A. Yes, that's true.

Q. And Professor Hill, you testified that LabMD first conducted penetration testing in May 2010; is that correct?

A. Yes.

Q. What types of risks did LabMD's May 2010 penetration testing identify?

A. The -- one of the risks that was identified was that of the anonymous FTP server.

Q. Professor Hill, I'd like to direct your attention to CX 70.

JUDGE CHAPPELL: I want to point out something for the record here because of things I've seen in posttrial briefing in the past.

This is an expert witness, and a lot of these questions are very factual based, for example, when LabMD first conducted penetration testing. And as I understand it, this is based on -- this is her opinion based on what she's read in the record. She doesn't know for a fact when it began. Am I correct?

MS. LASSACK: You are correct, Your Honor. It's her conclusions based on the record.

JUDGE CHAPPELL: Right. I just want to make that clear. I have seen, for example, that question and answer type cited in a brief for a factual assertion.

158

I'm just letting everyone know that that's not correct to do that.

BY MS. LASSACK:

Q. Professor Hill, I'd like to direct your attention to CX 70.

What is CX 70?

A. CX 70 is the ProviDyn report.

Q. What is the ProviDyn report?

A. The ProviDyn report is the report that was generated by the company ProviDyn, and it was -- ProviDyn had been engaged by LabMD to perform an external vulnerability scan of LabMD's network.

Q. What is an external vulnerability scan?

A. So an external vulnerability scan is one -- is a risk assessment scan. I say "external" because it's performed from outside of an organization's network, and it uses various risk assessment techniques like penetration testing and, in addition to penetration testing, looking for vulnerabilities in the software that is run on specific machines for which it is probing.

Q. On page 1 of CX 70, what is shown about the overall security posture in connection with the external vulnerability scan conducted?

A. That the overall security posture was poor.

159

Q. What does that mean?

A. That means that the system is not secure and it's vulnerable to risks that would actually compromise the system, compromise data that's stored on the system and even possibly take control of the system.

Q. I'd like to direct your attention to page 19 of CX 70, the top entry in particular.

What does the top entry on page 19 of CX 70 show?

A. It shows that there is an anonymous FTP writeable root directory vulnerability.

Q. Is that the vulnerability you were referring to earlier?

A. Yes.

Q. Please describe for the court what that vulnerability is.

A. It is possible to write on the root directory of this remote anonymous FTP server. And a root directory is the administrative directory within a computer, so if you have access and write access to the root directory, you can control and reconfigure the machine, so this allows an attacker to upload arbitrary files which could be used in other attacks or to turn the FTP server into a software distribution point.

Q. What would be the consequence of that?

160

A. The consequence of that is that malicious software can be loaded on this computer that would then distribute any data that is on the computer to outside of the network.

So this notion of a software distribution point means that now I -- if I'm a malicious entity, I now control that computer, and any data on that computer, I can distribute it to any computer on the Internet.

Q. What computer was this vulnerability found on?

A. On mapper.

Q. And can you remind us what the mapper is?

A. The mapper server was the machine that collected the data from the doctors' offices, so doctors' offices would write, do bulk transfers into the mapper server.

Q. What types of information were stored on the mapper server?

A. Sensitive data information like consumer names, their Social Security numbers, their addresses, their date of birth, insurance information, banking and credit card information.

Q. When was the anonymous FTP problem first reported?

A. I would need to consult my expert witness document for that detail.

161

Q. I'd like you to turn then to CX 740.

Does paragraph 72 of CX 740 refresh your recollection?

A. Yes.

Q. When was the anonymous FTP problem first reported?

A. July 14, 1993.

Q. How long was that before it was identified by LabMD's penetration tests?

A. 17 years.

Q. What is secure FTP?

A. Secure FTP is an extension of the file transfer protocol that transmits data over an encrypted channel.

So unlike FTP, secure FTP encrypts the data as it's being transmitted from one point to the next.

Q. Did LabMD use secure FTP?

A. No.

Q. How do you know that?

A. Because the port that's open on mapper is one for the file transfer protocol. There's no port open on mapper during the relevant time period for secure FTP. That's a different port.

Q. Could LabMD have corrected its failure to use an appropriate set of risk assessment measures at relatively low cost?

162

A. Yes.

Q. How could LabMD have done that?

A. LabMD could have used some of the freely available tools for risk assessment, some of the same ones that were used by ProviDyn.

Q. What's an example of one of those tools?

A. One example is NMAP, is one example.

The Nessus tool was free up until a period of time.

Q. Do you recall how long Nessus was free?

A. I would need to consult -- free until 2008.

Q. How much did the May 2010 penetration test that LabMD conducted cost?

A. $450.

Q. Were there other risk assessment measures besides the ones you discussed that were available at relatively low cost?

A. Yes. Wireshark is another risk assessment measure, and it was available since 1998.

Q. Will you remind the court what Wireshark is.

A. Wireshark is a data traffic analysis tool, so it allows you to capture data off of your -- that is coming into your network and do what I call deep packet inspection of the data, look at -- look beyond the headers of the data and look explicitly at the data

163

itself to determine what information is flowing into and flowing out of your network.

Q. How much did Wireshark cost?

A. Wireshark is also freely available.

Q. Professor Hill, I'd like to direct your attention to the section of your report that begins with paragraph 78.

Did complaint counsel ask you to provide an opinion on whether LabMD maintained more personal information than necessary on its network?

A. Yes.

Q. What did you conclude?

A. I concluded that LabMD maintained information about approximately a hundred thousand consumers that it never performed lab tests for.

Q. Did you conclude that LabMD needed that information to conduct its business?

A. I concluded that they did not need that information to conduct their business.

Q. Why did you reach that conclusion?

A. Because lab tests were never performed by LabMD or any of its associated lab testing organizations.

Q. How long did LabMD maintain that information?

A. They maintained it throughout the relevant time period.

164

Q. Did LabMD ever delete that information?

A. No.

Q. Why is maintaining more information than necessary problematic?

A. This goes back to the -- one of the seven principles of don't keep what you don't need, because if there's a compromise with this data, you have an increased scope of harm for individuals for which were never your consumers, for which you never provided services for.

So -- and also it adds an additional burden for maintaining and protecting that information.

Q. Could LabMD have deleted the approximately hundred thousand records that you concluded it didn't need to conduct its business?

A. Yes.

Q. How could LabMD have done that?

A. They could have done -- they could have removed it from their database.

Q. How so?

A. By deleting those records.

Q. What would that have cost?

A. That would have cost only the time of the IT professional who was responsible for managing their database.

165

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

A. Yes.

Q. What did you conclude?

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

Q. Why did you reach that conclusion?

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

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

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

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

166

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

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

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

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

A. Yes.

Q. How would LabMD have done that?

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

Q. How much would that have cost?

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

167

to limit access to data.

Q. Would there have been any additional monetary cost?

A. No.

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

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

A. Yes.

Q. What did you conclude?

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

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

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

Q. Let's start with information technology employees.

Why is proper information security training for information technology employees important?

168

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

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

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

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

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

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

So it's too late to wait until the system is running so slowly that you can't perform your job.

And they also need to understand the risk of changing configurations on their system, downloading an application, and those types of things.

Q. Earlier you testified that LabMD had given administrative access to at least some employees during the relevant time period.

How does that relate to the importance of training for non-IT employees?

A. So when you have administrative access on your machine, you have complete control of that machine. You can reconfigure anything on the machine.

And so if you have that amount of power, you need to not -- you need to understand and have the knowledge of the consequences of making such changes, like, for example, disabling your firewall, what would that actually mean, downloading some unauthorized software and the possibilities of compromise that go along with that.

So that's why they need to have training, especially when they have full control of their machines.

Q. Turning back to training for IT employees, how is that an important part of a defense in depth strategy?

A. It's an important part of defense in depth because, as I stated, if they don't have the knowledge that they need, they won't be able to specify a comprehensive security program that applies mechanisms in a defense in depth way.

And so you can -- even with the best training, there's still a possibility of human error. But with no training, you can't expect for there to be proper security measures in place, put in place, and that they will be configured properly and that they will achieve the goal that they're set to achieve. You can't even expect that there will actually -- that the proper goals will be identified.

Q. Professor Hill, why did you conclude that LabMD did not provide proper training for its IT employees?

A. I concluded that they didn't provide proper training for their IT employees because there were -- there was testimony that stated that there was -- that IT employees did not receive training.

Q. I'd like to turn back to CX 734, which was Ms. Simmons' investigational hearing transcript. And I'd like to draw your attention to page 1 of her testimony -- I'm sorry -- page 61 of her testimony, lines 6 through 14.

Did you consider this testimony in connection with reaching your conclusion about LabMD's lack of IT staff training?

A. Yes.

Q. Is this one of the examples that you were referring to earlier?

A. Yes.

Q. Now turning to non-IT employees or regular employees as you called them, why did you conclude that those employees did not receive proper information security training?

A. I concluded that they didn't receive proper information security training because there was no evidence in the record that supported that they received proper IT security training.

Q. I'd like to turn back to page 61 of Ms. Simmons' testimony, investigational hearing testimony at CX 734. I'd like to turn to line 15 of page 61 through line 6 of page 62.

Did you consider this testimony when reaching your conclusion about LabMD's lack of information security training for non-IT employees?

A. Yes.

Q. How did LabMD's lack of information security training affect how LabMD performed security?

A. Basically the lack of knowledge about, you know, how to create a comprehensive security program in a defense in depth manner rendered them -- rendered their whole approach to one -- or relegated their whole approach to one that was ad hoc and reactive.

Q. Was there any written documentation in the record of information security training for LabMD employees?

A. No.

Q. You just testified how LabMD performed security in an ad hoc manner as a result of not having proper information security training.

Could you provide the court some examples of that.

A. Can you repeat the question. I'm sorry.

Q. Sorry.

Can you -- I believe you testified earlier that LabMD performed information security in an ad hoc manner due to its lack of information security training. Is that correct?

A. Yes.

Q. Will you please provide the court some examples of that.

A. If -- there's evidence about, you know, IT staff addressing issues once they've been told that there is a problem, and so this actually occurred --

and the problem would be my computer is running so slowly that I can't perform my job. And this not only happened, you know, with their internal employees but also with the machines that were placed in the doctors' offices.

Q. Are there any things that with respect to security that LabMD should have done but didn't do because of improper information security training?

A. Things that they should have done.

Q. Such as a security practice that should have been implemented?

A. They should have -- they should have done risk assessment, and that risk assessment should have been done periodically. And if they had had proper training, they would have done risk assessment periodically.

Q. Are there any other examples of those types of things?

A. They would have had strong passwords.

They would have applied patches in a timely manner, so updating their operating systems, updating their applications to address vulnerabilities.

And there's evidence in the record that show that that wasn't being done.

Q. Could LabMD have provided training, proper

information security training, for its IT employees at relatively low cost?

A. Yes.

Q. How could LabMD have done that?

A. There were low-cost and no-cost options for training.

There was I think -- I recall -- I would have to look back at my report, but I think it's the National Research Alliance that would provide training, security training for small businesses, businesses with 25 employees or less, at no cost.

There were online training modules that were provided by the Computer Emergency Response Team at no cost. And there were some low-cost options for IT training at $850 -- for $850.

So there were some basic -- there were some free options for training and there were low-cost options also.

Q. You mentioned the Consumer Emergency Response Team.

What is that?

A. The Computer Emergency Response Team, CERT. CERT is an organization that is at Carnegie-Mellon, and it was created in response to the first Internet vulnerability. And it includes participation of

government, academic and industry professionals. They all come together to create guidelines and information that helps to secure computing systems.

Q. Are these guidelines easily found?

A. Yes.

Q. How so?

A. The guidelines are available online. If there's anything that you are specifically looking for, you can usually go to their main -- CERT's main Web site and, you know, they're available. Or you can do something as simple as a Google search for specific terms. If you're looking at confidentiality policies for small businesses, you would find some of these guidelines.

Q. Could LabMD have provided proper information security training for its non-IT employees at relatively low cost?

A. Yes.

Q. How could LabMD have done that?

A. Some of these same guidelines, they also provide some basic training not just for IT professionals but for people to understand the emerging risks that are out there so that non-IT employees, you know, have a better understanding of the consequences of, you know, their actions when they are

using a computing infrastructure.

Q. Professor Hill, I'd like to direct your attention to the section of your report that begins with paragraph 93.

Did complaint counsel ask you to provide an opinion on whether LabMD required employees or others with remote access to its network to use common authentication measures?

A. Yes.

Q. Will you remind the court what an authentication measure is.

A. An authentication measure is a way of verifying the identity of users on your network.

So a common way to do that is with a user name, which becomes your identity, and a password, which is proof of your identity.

Q. What did you conclude about LabMD's authentication measures?

A. I concluded that LabMD's authentication mechanisms were not reasonable and appropriate for securing LabMD's network.

Q. Why is it important to use effective authentication measures?

A. If you don't use effective authentication measures, you increase the risk of unauthorized access

177

to your system.

For example, if you use weak passwords, it's likely that an attacker will be able to guess a password and gain access to your system.

Q. What is a weak password?

A. A weak password is a password that is short in length, less than eight characters, one that uses either all alphabets or all numbers, no special characters.

So if you are not varying those characters and you don't have a long length, you actually reduce the uncertainty in the password, and so basically that deals with information entropy, and so what you want is there to be a lot of uncertainty, which creates a large search space for an attacker.

So if I use alphabets of uppercase and lowercase, that increases the search space. If I don't use dictionary words, that also increases the search space. If I introduce numbers and special characters, like punctuation characters, that also increases the search space.

So it makes it more difficult for an attacker to actually brute-force your authentication mechanism -- and when I say "brute-force," I mean try all possibilities -- because that attacker will have to

178

search a large space in order to determine what the actual password is.

Q. You've discussed the length and required characters in connection with passwords.

How does the history of a password relate to its strength?

A. A history of the password has to be taken under consideration in order to have strong passwords, because if you maintain the history, you can ensure that individuals don't reuse passwords.

And so that's why you would want to maintain a history of passwords and require users to create unique new passwords.

Q. How often should a password be changed?

A. That should be determined by the role of the user, the types of information that the user will have access to, the sensitivity of that information.

So if you have access to highly sensitive information, you would want to change your password more frequently.

So it's a process for determining that, the frequency of changing passwords and the history you'd want to maintain.

Q. How should passwords be stored within a network?

179

A. Passwords should be stored in a way that is not readable in the network, so it's best to store the passwords in encrypted form. And usually a hash of a password is taken and the password is stored with that hash. And in addition to that hash, you add some randomness to the password before you create that cryptographic hash of a password.

Q. I'm going to ask you some more about that to make sure I understand the technical terms here.

What is -- a cryptographic hash you said?

A. Yes. A cryptographic hash is a transformation of a piece of information into a fixed-size information.

And so what you have that's used is a function that would create a one-way mapping of your password to a numeric value that is not in alphabetic form, so it translates your password to some numeric value. And so an attacker, even if they saw it, they wouldn't understand what that value was.

Q. Why did you conclude that LabMD failed to use effective authentication measures?

A. I concluded that they failed to use effective authentication measures because they had no policy for strong passwords. And there was evidence in the record to show that individuals used very weak passwords that

180

included dictionary words, parts of the names of the individuals for which the password was used, and so this makes it easy for these passwords to be guessed.

And they also -- there's also evidence that some users used these passwords for years and that they were never changed.

Q. Professor Hill, I'd like to direct your attention to CX 167.

What is CX 167?

A. CX 167 is -- it's a small database of passwords that were being used within the relevant time period.

Q. Did you consider CX 167 in reaching your conclusion about the effectiveness of LabMD's authentication measures?

A. Yes.

Q. What did you conclude from CX 167?

A. I concluded that LabMD didn't have a strong -- a policy for strong passwords and that they had no mechanism in place to enforce strong passwords, so you had passwords like "LabMD."

So meaning that there's some users that actually used the password "LabMD" as their password.

Q. Why is a LabMD employee using "LabMD" as a password problematic?

A. It's problematic because it would be very easy to guess. An attacker -- that would be one of the first things that an attacker would choose, is the name of the company, as a potential password.

It also -- if you see here, "labmd" is all lowercase. "LabMD" also contains a dictionary word, which is, when an attacker is trying to crack a password or determine a password, they will often use dictionary words in that approach.

The password is actually less than eight characters. "LabMD" is only five characters long, which is a small search space to begin to look or to try to brute-force a password.

Q. When you say "brute-force a password," what do you mean?

A. When I say "brute-force," I mean I'm going to try all possible combinations to determine what the password is.

So here, I only have to try the alphabet, the letters in the alphabet. I'm only -- an attacker would only have to try lowercased alphabets, and so that -- and only five characters.

So that defines my search space, and so in order to brute-force this, you know, I would -- as an attacker, I would actually look for five characters and change those five characters in order to search for

possible passwords.

Q. When you say "search space," what do you mean?

A. Search space is basically the different combinations of characters and -- that I would have to search across in order to possibly find this particular password.

So that constitutes a search space. And the length, the number of characters I would have to consider, the alphabet that I would have to consider where I'm dealing with lowercase and uppercase, if I now, you know, add numbers to that, I've increased that search space.

Q. So what is the consequence of a smaller search space?

A. The consequence of a smaller space is that it takes less time to determine the actual password in a brute force attack.

Q. Professor Hill, I'd like to direct your attention to CX 706.

What is CX 706?

A. CX 706 is the transcript for Sandra Brown.

Q. Who is Sandra Brown?

A. Sandra Brown -- I think that Sandra Brown is the billings manager.

Q. Is she the same billing manager who had the

1718 File installed on her computer?

A. No. She's not the same one that had the 1718 File on her computer.

Q. Did you consider Ms. Brown's testimony when reaching your conclusions about LabMD's password practices?

A. Yes.

Q. I'd like to draw your attention to page 13 of Ms. Brown's testimony, lines 4 through 20 in particular.

What did you conclude from this testimony?

A. I concluded that she used the same password for the duration of the time that she was there from 2006 to 2013.

Q. Is this one of the examples you were referring to earlier?

A. Yes.

Q. Did you consider her using the same password from 2006 to 2013 problematic?

A. Yes, I did.

Q. Why?

A. There are a couple of reasons. She's using the same password. She has a weak password that was only five characters long, all lowercase letters, so that increases the chances that an attacker could compromise

that password.

She's also logging in remotely, so if her password is compromised and she's using this weak password, there is no two-factor authentication in place for remote users.

And so if I had a different way of auth- -- an additional way of authenticating myself for remote users, it would make it harder for an attacker to gain unauthorized access.

Q. Okay. I'd like a unpack that a little bit.

What is two-factor authentication?

A. Two-factor authentication is that I have two ways, two sources of proof that I am who I claim to be.

So with regard to the user name, I present an identity to the computer and the infrastructure in order to log in.

So with a one-factor authentication mechanism, I only present one source of proof, and usually that is a password. With a two-factor mechanism, in addition to presenting you some -- with something that I know, like my password, I also have to present you with something that maybe I have, like a biometric or a token that generates a random number.

Q. Did LabMD use two-factor authentication for any of its remote users?

A. No.

Q. How would using two-factor authentication for remote access have implemented a defense in depth strategy?

A. Because it requires two different types of proofs of identity, so even if the password is compromised, an attacker would also have to gain access to the thing, for instance, that you know -- I mean, that you have, like a biometric or a token that's generating a random number for you to enter.

So it decreases the likelihood of a compromised access for remote users.

Q. I'd like to turn now from employee passwords to passwords that LabMD used for accounts in its doctor -- the offices of its doctor or physician clients.

What types of passwords did LabMD use for accounts that its physician clients' offices had?

A. I would also characterize those passwords as weak passwords. They used nurses' initials as passwords, nurses' initials with a couple of numbers, so these were short passwords. They included information about the users themselves, and they also had a small search space.

Q. When you say "information about the users themselves," what do you mean?

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

Q. Should passwords be limited to one user?

A. Yes.

Q. Why?

A. If you share passwords, you also increase the chance and likelihood of compromise.

Q. Why is that?

A. Because now I need to -- as I explained what an authentication mechanism is, I present to you an identity and I give you then proof of that identity, which is the password. Now I have one identity, but then I have multiple people with the proof for that identity, so how then do you verify, you know, which individual is actually associated with that user name credential.

And so this becomes problematic. You don't know which user -- it's -- let me back up a little bit.

It's giving the user the ability to impersonate someone else, and so that's the first problem, so I've destroyed that link between identity and proof of identity. Okay?

And so now I'm sharing the password among multiple individuals, and what prevents that individual from additionally sharing it to more people, so this could lead to compromise or an individual exposing that

password in some way by, for example, writing it down on a sticky note or something like that.

So the more people who touch that password, the more likely it is to compromise.

Q. Are there instances where LabMD allowed passwords to be shared during the relevant time period for your report?

A. Yes.

Q. How do you know that?

A. There is testimony that discusses the sharing of passwords and how that was a major issue at LabMD.

Q. Was that throughout the relevant time period for your report?

A. That was at least up until 2009.

Q. Professor Hill, I'd like to draw your attention to CX 719.

What is CX 719?

A. CX 719 is the transcript of Robert Hyer.

Q. Who is Robert Hyer?

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

Q. I'd like to draw your attention to page 26 of the transcript of Mr. Hyer's deposition, lines 9 through 25 in particular.

Is this an example of the testimony you were

referring to earlier about LabMD having instances of employees sharing passwords?

A. Yes.

Q. Could LabMD have corrected its failure to use common effective authentication measures at relatively low cost?

A. Yes.

Q. How could LabMD have done that?

A. They could have used mechanisms that are provided by the Windows server in order to implement strong password policies.

Q. What would that have cost?

A. That -- there would be no additional cost because those mechanisms were provided.

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

A. There would be a cost in the form of employee time, the IT staff.

Q. Would there be any monetary cost?

A. There would be no monetary cost.

Q. Professor Hill, I'd like to draw your attention to the section of your report that begins with paragraph 97.

Did complaint counsel ask you to offer an opinion on whether LabMD maintained and updated operating systems and applications on its network?

189

A. Yes.

Q. What did you conclude?

A. I concluded that LabMD did not update its operating systems and other applications in a timely manner to address risk and vulnerabilities in those software applications.

Q. I believe you testified about this earlier, but will you remind the court why it's important to maintain and update operating systems and applications.

A. It's important, and I'll repeat the example that I gave. For every ten lines of software, there is on average one vulnerability.

So in something like Windows operating system, which has 50 million lines of code, there are at least on average five million coding mistakes and flaws in that code. And it's virtually impossible for a vendor to identify and fix all of those vulnerabilities before they are released to consumers.

Q. Why is it not possible to fix those vulnerabilities before the software is released to consumers?

A. One of the reasons that it's impossible is because in order to identify some of those vulnerabilities, you would need a large user base to get a large coverage of all of the functionality within that piece of software.

So if -- some of those problems won't be discovered until they're released to the consumer.

Q. And is there another reason?

A. Is there another reason?

Q. Why all of the flaws couldn't be fixed before the software is released.

A. That even -- even with automated testing, they won't get, you know, the type of coverage.

And also, usually the time from completion of a project to the release date is preset, and companies are going to release their data to -- release their products to consumers, so that may also have an effect, that window from coding completion to testing completion.

Q. Professor Hill, will you please provide the court an example of why you concluded that LabMD did not adequately update and maintain its operating systems.

A. LabMD -- one example would be that in 2006, LabMD was still using the Windows NT server on some of -- server operating system on some of its servers, and Microsoft had discontinued support for Windows NT in 2004.

Q. Will you please provide the court an example of why you concluded that LabMD did not adequately maintain and update its applications.

A. There -- after the -- the ProviDyn vulnerability scan identified applications with vulnerabilities. And one of those applications was the Veritas backup software. And this software had a Level 5 risk, which meant that that risk gave an attacker administrative access and control over the machine that was actually running that software. And it was a default password vulnerability.

So that was one of the vulnerabilities with that software. And the second vulnerability with that software was a buffer overflow vulnerability, which allowed an attacker to execute code remotely and gave them partial access to the data on the machine.

Q. Professor Hill, I'd like to direct your attention to CX 67.

What is CX 67?

A. CX 67 is the ProviDyn report.

Q. Is this a different ProviDyn report from the one we looked at earlier at CX 70?

A. No. It is the same ProviDyn.

Q. The company is the same; is that what you're saying?

A. Yes.

192

Q. What computer does CX 67 cover, if you recall?

A. I am --

Q. Do you not recall?

A. I don't recall the --

Q. I'd like to show a document -- split the screen. I'd like to show you CX 51 page 4.

And I'd like to turn to CX 67 page 22.

Professor Hill, do these two excerpts --

A. Yes.

Q. -- refresh your memory as to which computer?

A. Yes, it does.

Q. Which computer?

A. It was the LabNet computer.

Q. Is the LabNet computer a server?

A. Yes, it was.

Q. What did the LabNet server do?

A. The LabNet server maintained sensitive information that was used for the collection and the processing of test results.

Q. What types of information were on the LabNet server?

A. The LabNet server contained consumer names, Social Security numbers, insurance information, types of tests, test results, date of birth, those types of information.

Q. So I'd like to draw your attention to the bottom entry on page 22 of CX 67.

Is this the buffer flow vulnerability that you -- buffer overflow vulnerability that you discussed earlier?

A. Yes.

Q. What could happen if that vulnerability were exploited?

A. That vulnerability gave an attacker the ability to execute code remotely, so an attacker could execute -- exploit this vulnerability and execute code that could then take over partial control of that computer.

Q. When did LabMD first identify this vulnerability?

A. LabMD first identified this vulnerability in 2010.

Q. When was the risk first identified within the IT community?

A. I would have to consult my expert witness document to determine that.

(Pause in the proceedings.)

The problem was detected and a solution was available in July of 2007.

Q. How do you know that?

A. I know that because there was an alert and an announcement made by the vendor, Symantec, regarding this vulnerability. And that announcement provided information about when a solution was available.

Q. Could LabMD have corrected its failure to update operating systems and applications at relatively low cost?

A. Yes.

Q. How could LabMD have done that?

A. They could have just downloaded the update from the vendor.

Q. What would that have cost?

A. There would not have been any cost.

Q. So I'd just like to turn back to page 1 of CX 67 for a moment.

What was the overall security posture from the ProviDyn scan of the LabNet server?

A. It was poor.

Q. Professor Hill, I'd like you to turn to the next section of your report, which begins with paragraph 102.

Did complaint counsel ask you to provide an opinion on whether LabMD used readily available measures to prevent or detect unauthorized access to personal information on its network?

A. Yes.

Q. What did you conclude?

A. I concluded that LabMD did not use readily available measures to prevent and detect unauthorized access to their personal information.

Q. Why are measures to prevent and detect unauthorized access to personal information an important part of a defense in depth strategy?

A. It's important because there are a variety of ways that an attacker may try to gain access to a system, and so it's part of any defense in depth strategy to try to prevent and then to detect that unauthorized access. Detecting it allows you to know that it is occurring and would help you to remediate the problem.

Q. Professor Hill, I'd like to turn to paragraph 104 of your expert report.

What does this paragraph discuss?

A. This paragraph discusses the various measures that can be put in place to prevent the unauthorized sharing of personal information.

Q. Paragraph 104(a) discusses that employees should be given nonadministrative accounts on workstations.

A. Yes.

Q. You talked about this earlier this afternoon.

Can you just summarize why it's important for employees to have nonadministrative accounts.

A. It's important for employees to have nonadministrative accounts because giving them limited control of their machine prevents the inadvertent downloading of software that could compromise not only their system but compromise the entire network.

Employees often don't understand the consequences of reconfiguring or changing things on their system, and so by limiting the power that they have over their system, you can help prevent inadvertent compromise.

Q. You testified earlier today that there are instances where LabMD gave employees administrative accounts.

Was one of those instances the billing manager whose computer had LimeWire installed?

A. Yes.

Q. I'd like to turn to paragraph 104(b), which discusses backups of personal information.

Why is it important to store backups of personal information on devices that are separate from other employee activities?

A. Because employees, they use their computers in a variety of ways, especially those who are given full

197

power over those devices, the power to download software and to change security settings.

So because these are multiuse environments where they're reading their e-mail, they may inadvertently open an attachment that has malicious software embedded in it, any of those things put that computer, any information that's stored on that computer, at risk for exposure, so you would want to store backups on a machine where those types of activities are not occurring.

Q. Did LabMD store backups on devices that were not isolated from other employee activities?

A. Yes.

Q. Paragraph 104(e) of your report.

It says that a firewall should be configured to block all unwanted traffic from entering the network.

Why is that important?

A. That is important because if you restrict communication that's initiated from outside for unauthorized applications, then that would block that traffic from entering your network.

Q. What did you conclude about the configuration of LabMD's firewalls?

A. I concluded that LabMD's firewalls were not configured to block all traffic that wasn't necessary for LabMD to conduct its business.

198

Q. Why did you reach that conclusion?

A. I reached that conclusion because the Veritas backup software had a port open, port 10,000, and the Veritas backup software also had a vulnerability that was a Level 5 vulnerability that gave an attacker administrative access to that software and to the machine that was running that software. There was no business need for that port to be open. Backups were done within the local area network and not across the Internet.

Q. Professor Hill, I'd like to turn back to CX 67, page 22, and the top entry.

Is this the vulnerability that you were just referring to?

A. Yes.

Q. In your opinion, if LabMD's firewalls had been properly configured, would that have prevented the LimeWire application on the billing manager's computer from sharing files?

A. No.

Q. Why not?

A. Because LimeWire can still share files even if the request for files is not initiated from outside of an organization's network.

199

If a computer that's using LimeWire within the organization initiates a connection with the LimeWire network, then data can be transferred to that computer through that already-established communication channel.

Q. How does the fact that a properly configured firewall would not have prevented the LimeWire application from sharing files relate to the importance of a proper defense in depth strategy?

A. It's a great example of why you need to use defense in depth, because, as I stated earlier, it's an arms race and applications become more and more stealthy. If there's a mechanism in place, they try to determine -- application -- malicious application developers try to determine ways to circumvent that mechanism to achieve its goal, and its goal is to gain unauthorized access to a system.

So that's why you would need to deploy mechanisms, heterogeneous mechanisms, in a layered manner to combat that.

Q. How did LabMD allowing the billing manager to have an administrative account on her machine relate to the LimeWire application being present on her computer?

A. Given that the billings manager had administrative access, the billings manager was able to download and install applications onto the machine.

200

Q. How long was the LimeWire application on the billing manager's computer?

A. The application was installed somewhere between 2005 and 2006. It was not removed until 2008.

Q. Are there security measures that LabMD could have used to detect the application sooner?

A. Can you repeat the question, please.

Q. Are there automated security measures that LabMD could have used that would have detected -- could have detected LimeWire before May 2008?

A. Yes.

Q. Can you give us and the court an example?

A. They could have used a file integrity monitor to detect the presence of the application.

Q. What is a file integrity monitor?

A. A file integrity monitor is an application that first creates a base profile for your computer. And the assumption when you create the base profile is that that system is in a trustworthy state, so it actually creates a list of all the files that's stored on your computer, and periodically you can use it to check the integrity of the computer.

And what I mean by "integrity" is determine whether files have been added, the size of files have changed, and those types of things.

201

And so when you -- when you do this integrity check, by comparing the current state of the computer, the current list of files, to the list of files that's in your base profile, you can detect that there has been a change.

A change doesn't necessarily mean that it is malicious, but a change will help you to identify that, you know, there's -- further investigation is needed, and so you can further investigate those changes to determine whether, for example, an unauthorized file-sharing application has been downloaded.

JUDGE CHAPPELL: We're about at 5:30. What's your status?

MS. LASSACK: I think that we could finish in ten minutes or so, so...

JUDGE CHAPPELL: What do you think, Bailiff?

MR. MITCHELL: It's your call, sir.

JUDGE CHAPPELL: Press on.

BY MS. LASSACK:

Q. Professor Hill, did LabMD use file integrity monitoring?

A. No.

Q. Could LabMD have corrected its failure to use readily available measures to prevent or detect unauthorized access to personal information on its

202

network at relatively low cost?

A. Yes.

Q. How could LabMD have done that?

A. LabMD could have enforced a policy that prevented employees from having administrative access.

They could have used file integrity monitoring software that was freely available.

Q. How much would it have cost to prevent employees from having administrative accounts?

A. Nothing. It would only cost people time, so no additional monetary cost.

Q. How much would it have cost to store backups of personal information on machines that weren't used for other employee purposes?

A. There were other machines like servers available, so no additional machines would need to be purchased.

Q. Professor Hill, earlier this afternoon, you said no -- there's no such thing as perfect security. And His Honor asked whether this means that there is always the likelihood of a security problem. Do you recall that testimony?

A. Yes.

Q. If a company that maintains personal information cannot achieve perfect security, what, in

203

your opinion, should be a company's goal with regard to its security?

A. The company's goal is to do what is reasonable and appropriate and to apply strategies that would limit the probability of compromise.

Q. Professor Hill, now that we've discussed all of your specific opinions about LabMD's security practices, I'd like to turn back to your overall conclusion about LabMD's security practices.

What is your overall conclusion about the reasonableness and appropriateness of LabMD's security practices?

A. My overall conclusion is that LabMD did not practice reasonable and appropriate security to ensure the protection of its infrastructure and its data.

Q. What time period does that conclusion cover?

A. January 2005 until July 2010.

Q. Do you offer any opinion about the reasonableness of LabMD's security practices after July 2010?

A. No, I do not.

Q. Could LabMD have corrected its security failures at little or no cost?

A. Yes.

MS. LASSACK: Your Honor, that's my final

204

question.

JUDGE CHAPPELL: All right. Thank you.

MS. LASSACK: I would like to move admission of CDX 01, which is the version of the IT employee timeline that was not discussed with Professor Hill. And I'd also like to move the admission of CDX 02.

JUDGE CHAPPELL: Any objection?

MR. SHERMAN: Yes. I was informed that this was a demonstrative exhibit and not something that was going to be admitted into evidence, so I would object on that basis. I thought this was a demonstrative.

MS. LASSACK: Well, it's also a summary without Professor Hill's markup, which is what I would move first, CDX -- sorry -- CXD 01, which is a summary exhibit of testimony, which I believe we established the foundation for with Professor Hill's testimony.

I also have here binders with testimony that supports the summary exhibit that is CXD 1, the LabMD IT employee timeline.

And I'd also like to move a third exhibit, which is the LabMD IT employee timeline with Professor Hill's markup, which we'll give a new --

JUDGE CHAPPELL: Okay. What's the first exhibit you're offering?

MS. LASSACK: So the first exhibit would be

CDX 01, which would be the -- what we'll call the clean version.

JUDGE CHAPPELL: What's the next exhibit?

MS. LASSACK: CDX 02 is the -- Professor Hill's network diagram.

MR. SHERMAN: Isn't that in her report?

MS. LASSACK: It's the additional description with when the animation is shown through the PowerPoint slide.

JUDGE CHAPPELL: All right. You are objecting to the marked-up poster board?

MR. SHERMAN: I'm objecting to all three. They represented to us that these were demonstrative exhibits and that they weren't going -- well, they didn't say they weren't going to move them for admission, but they're demonstrative. I think they've served their purpose in assisting the witness in testifying today, and I will object to them being admitted as exhibits.

JUDGE CHAPPELL: Right.

Are you offering them as demonstrative and not for evidence?

MS. LASSACK: We're using them as demonstrative exhibits today, and I believe we've established the foundation necessary.

JUDGE CHAPPELL: I don't believe you have, so those are not going to be admitted into evidence over objection. If you want them to be merely demonstrative, I'll allow that, but not for evidence.

MS. LASSACK: Then at present we will leave them as merely demonstrative exhibits.

JUDGE CHAPPELL: I didn't understand you.

MS. LASSACK: Then we will leave them as merely demonstrative exhibits.

JUDGE CHAPPELL: Any objection for them as demonstrative?

MR. SHERMAN: No objection, Your Honor.

JUDGE CHAPPELL: Okay. That will be allowed. They will be admitted as demonstrative.

And just so you know, I don't believe you laid a proper foundation for all those time periods that are on that chart, just for your own personal knowledge there.

Any cross?

MR. SHERMAN: Yes, Your Honor.

JUDGE CHAPPELL: I just want to get that on the record. We won't do it today.

Anything further from you?

MS. LASSACK: Not at this time.

JUDGE CHAPPELL: Do you pass the witness now?

MS. LASSACK: Yes.

JUDGE CHAPPELL: All right.

We will reconvene tomorrow at 0930.

MR. SHERMAN: Your Honor, one housekeeping.

JUDGE CHAPPELL: Okay. Go ahead.

MR. SHERMAN: I've had discussions with complaint counsel regarding calling Mr. Eric Johnson in their case. Well, they're going to allow me to call him as if in my case but on Friday. And I believe we anticipate that Mr. Van Dyke will be testifying on Friday?

MS. VANDRUFF: Yes, that's correct, Your Honor. Respondent's counsel reached out yesterday to ask for our consent to call Mr. Johnson in our case, if you will, on Friday because of his scheduling constraints.

Mr. Van Dyke, our expert, likewise has scheduling constraints, and as long as we can conclude Mr. Van Dyke's examination, we have no objection to respondent calling Mr. Johnson on Friday, even if our case hasn't concluded.

MR. SHERMAN: The reason I bring it up is because Friday may be one of the days where we request additional time. We may go overtime, if that's -- if we can arrange that with the court and the court personnel.

JUDGE CHAPPELL: Nobody is going to be driving on freeways around here Friday anyway in the afternoon because they actually start on Thursday morning to get out of town, so we're stuck here anyway basically, so as long as it's okay with the -- everyone else involved, we can go late on Friday.

MR. SHERMAN: And we're not saying we have --

JUDGE CHAPPELL: What do you think there, Officer Proctor? Is it okay with you?

OFFICER PROCTOR: It sounds good to me, Your Honor.

JUDGE CHAPPELL: Why don't we -- we'll plan to do that and -- so in other words, you're going to direct-examine this witness.

MR. SHERMAN: Yes, sir.

JUDGE CHAPPELL: And without a jury, it's no big deal to take somebody out of time, so that's not a problem.

All right. Anything further?

MR. SHERMAN: Nothing further, Your Honor.

JUDGE CHAPPELL: All right. Until 9:30 in the morning we're in recess.

(Whereupon, the foregoing hearing was adjourned at 5:38 p.m.)

CERTIFICATION OF REPORTER

DOCKET/FILE NUMBER: 9357
CASE TITLE: LabMD, Inc.
HEARING DATE: May 20, 2014

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

DATED: MAY 24, 2014

JOSETT F. WHALEN, RMR

CERTIFICATION OF PROOFREADER

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

ELIZABETH M. FARRELL