

In the Matter of:

Information Security and Financial Institutions Workshop

July 13, 2020
First Version

Condensed Transcript with Word Index



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

1	3
1 FEDERAL TRADE COMMISSION	1 WELCOME AND OPENING REMARKS
2 INFORMATION SECURITY AND FINANCIAL INSTITUTIONS:	2 MR. LINCICUM: Good morning. I want to
3 FTC WORKSHOP TO EXAMINE SAFEGUARDS RULE	3 welcome everyone to the Information Security and
4	4 Financial Institutions Workshop by the FTC. My name
5	5 is David Lincicum. I am an attorney here at the
6	6 Division of Privacy and Identity Protection at the
7	7 FTC. Today's workshop is going to be looking at the
8	8 Safeguards Rule, which is a rule that requires
9	9 financial institutions to enact safeguards to protect
10	10 customer information.
11	11 We're going to start by looking at our
12 MONDAY, JULY 13, 2020	12 current rule and what it requires of financial
13 9:00 A.M.	13 institutions and then move on to some of the proposed
14	14 amendments that we issued. If -- and so, let's go
15	15 ahead and start the slides. Next slide, please.
16 VIRTUAL EVENT	16 Thank you. The Gramm-Leach-Bliley Act was
17	17 enacted in 1999, and, among other things, it required
18	18 several agencies to issue rules for financial
19	19 institutions in order to have them safeguard their
20	20 customer information.
21	21 In response to that, the Federal Trade
22	22 Commission enacted its safeguard in 2002 and it became
23	23 effective back in May of 2003. So over the next 17
24	24 years, no real changes -- well, no changes at all have
25	25 been made to the rule. We think that shows how
2	4
1 FEDERAL TRADE COMMISSION	1 flexible that rule has proven, and how robust. But we
2 I N D E X	2 do periodically review our rules to see if there needs
3 PAGE:	3 to be updates and we did so recently with the
4 Welcome and Opening Remarks 3	4 Safeguards Rule.
5	5 After that review, and seeking some comments
6 The Costs and Benefits of Information	6 from the public, we issued a notice of proposed
7 Security Programs 23	7 rulemaking in March of 2019. We got quite a few
8	8 comments back from proposed rulemaking, and this
9 Information Security Programs and Smaller	9 workshop is going to be looking at some of the issues
10 Businesses 71	10 raised both by the proposed amendments and by some of
11	11 those comments. Next slide.
12 Continuous Monitoring, Penetration, and	12 So let's start with the current rule so we
13 Vulnerability Testing 121	13 know where we're starting from, what the amendments
14	14 are -- would change and where they might expand upon
15 Accountability, Risk Management, and Governance	15 the current rule. So the current rule applies to
16 of Information Security Programs 172	16 customer information held by financial institutions.
17	17 Customer information is fairly self-explanatory.
18 Encryption and Multifactor Authentication 222	18 That's information that a financial institution may
19	19 hold that they received from a customer as part of
20	20 providing a financial service or product.
21	21 "Financial institution" needs a little more
22	22 explanation if you're not familiar with it. I think
23	23 most people when they hear "financial institution"
24	24 think banks, and while banks are certainly financial
25	25 institutions, they're not covered by our rule. Our

5	<p>1 rule -- those are handled by other agencies rules. 2 Our rule covers nonbank financial institutions and any 3 basically financial institutions that don't have 4 deposits. And there are a few others that are 5 excluded. 6 But generally speaking they're the other 7 kinds of financial institutions. And that's a fairly 8 broad definition compared to what many people have in 9 their mind. It goes anywhere from, say, payday 10 lenders, other online lenders, debt collectors. It 11 can -- it also applies to car dealerships, if they're 12 involved in helping customers obtain loans for their 13 -- or helping their customers obtain loans. It can 14 also apply to universities, if they are involved in 15 the financial aid process. 16 So the rule would apply to all -- it does 17 apply to all customer information that a financial 18 institution has, either their own customers or the 19 information of customers of other financial 20 institutions that give them that information. So it's 21 not just the information of that financial institution 22 or that that financial institution receives from its 23 own customers. 24 The rule is based on a requirement that the 25 financial institution have a comprehensive information</p>	7	<p>1 integrity of the customer information. 2 So the program needs to have looked at the 3 risks to customer information. It has to basically be 4 based on a risk assessment and it has to then assess 5 the security of the financial institution and the 6 safeguards it has in place to control those risks that 7 it's identified. 8 Also, the program must address employee 9 training, information systems, and detecting, 10 preventing and responding to attacks. So kind of a 11 full spectrum of information security issues. Next 12 slide, please. 13 The rule also requires financial 14 institutions to -- well, design those safeguards we 15 discussed, to control those risks, and to regularly 16 test those safeguards to make sure they are actually 17 working. 18 Also, it addresses service providers as many 19 financial institutions use service providers to handle 20 or process or store customer information they have. 21 And the rule requires a financial institution to 22 oversee those service providers by first selecting 23 ones that are actually capable of maintaining 24 appropriate safeguards and then requiring the company 25 to actually maintain those safeguards by contract.</p>
6	<p>1 security; so a plan that lays out all aspects of 2 security -- physical, electronic -- and is meant to 3 protect the integrity and security of the information 4 that they hold. Next slide, please. 5 So let's go over what the comprehensive 6 information security program needs to have under the 7 current rule. First, it has to be appropriate to the 8 financial institution size and complexity. So a 9 smaller financial institution, a simpler one, will 10 have different needs than a financial institution 11 that is very large with a complex network. 12 The nature and scope of activities. So that 13 -- you know, how the information is used, how it's 14 stored, that sort of thing. And finally the 15 sensitivity of the customer information at issue. So 16 a collection of emails has to be treated differently 17 than information that includes social security 18 members, account numbers, very sensitive information 19 like that. 20 The program has to designate an employee or 21 employees to coordinate the program. So there's 22 someone or some people in charge and making sure that 23 this happens. And the program has to identify the 24 reasonably foreseeable risks, both internal and 25 external, to the security, confidentiality and</p>	8	<p>1 It also requires financial institutions to 2 evaluate and adjust the information security plan 3 based on the results of testing. So if they do a test 4 and they find a problem, they have to actually adjust 5 their plan to address that problem: any material 6 changes to operations. So if the financial 7 institution changes its business model or the setup of 8 its network or anything basically that would impact 9 how the financial institution operates, they need to 10 reevaluate their information security plan. And 11 finally a sort of catch-all of any other circumstances 12 that they had reason to know would impact their 13 information security program. Next slide, please. 14 So the current rule -- that is where the 15 current rule lies. And like I said, it is a pretty 16 flexible rule that covers a lot of situations. And 17 with the proposed amendments, what we sought to do was 18 to maintain that flexibility of the current rule while 19 also providing more guidance about what the 20 information security program actually has to consist 21 of and what it needs to address. 22 Our plan is to have -- what we intended is 23 for it to provide clear requirements for the financial 24 institution so they understand what it needs to 25 address while still allowing them to create a program</p>

9

1 that is adapted to the needs of that financial
 2 institution.
 3 And I also want to give credit where credit
 4 is due, that our proposed amendments are based very
 5 largely on New York’s cyber security regulations,
 6 which they implemented in early 2017. Next slide,
 7 please.
 8 So the proposed rule has the same basic
 9 structure of the current rule; doesn’t change it
 10 fundamentally. It’s still based on the creation of a
 11 comprehensive information security program that is, in
 12 turn, based on a risk assessment that is suited to the
 13 size and complexity of that financial institution.
 14 So, again, it’s going to vary depending on exactly
 15 what your financial institution looks like, what
 16 information they maintain and how they use it.
 17 What the rule does, though, is require --
 18 put forth more detailed requirements for the plan,
 19 what it needs to address, the areas it needs to look
 20 at, without actually telling the financial institution
 21 what they need to about those areas. It just says
 22 this is the area you need to look at and make a plan
 23 for, such as access control. Who can -- how do you
 24 control information and make sure that only those who
 25 are authorized to use it can actually use it.

10

1 Almost all the requirements are process-
 2 based and adaptable. And so, again, it doesn’t say
 3 what you need to do exactly. It just gives you a
 4 process that you need to go through to make sure that
 5 all bases are covered.
 6 And, finally, it has an exception for
 7 companies that have less -- that maintain very little
 8 customer information and exempts them from some of the
 9 requirements, primarily the written -- some of the
 10 written reporting requirements. Next, please.
 11 All right. The proposed rule, let’s go into
 12 a little more detail here. Under the proposed rule,
 13 the financial institutions have to first designate one
 14 qualified individual to be responsible for overseeing
 15 the program.
 16 So the only change we made here
 17 substantively from the current rule is that we made it
 18 so rather than it being person or persons, it has to
 19 be one person. And that’s designed to increase
 20 accountability so that, you know, someone is in charge
 21 of the program but also in case of emergency or
 22 generally process, that it’s always clear who the
 23 person in charge is, where the directions are coming
 24 from and, you know, basically give direction to the
 25 program.

11

1 We also added the word “qualified” to it so
 2 that the person needs to be qualified. I think we
 3 would argue that the current rule presumes that, but
 4 we’re making it explicit here.
 5 We did use as a term of shorthand, the term
 6 CISO, or chief information security officer. We
 7 didn’t intend that to imply that a specific set of
 8 qualifications was required, but I think that was the
 9 effect it had. But that was not the intention. We
 10 think “qualified,” what that means will vary based on
 11 the size and complexity of the network. A very large,
 12 complex network may need something -- someone who is,
 13 you know, what is commonly known as a CISO, or as a
 14 simpler one maybe it will have someone with more
 15 modest qualifications and experience.
 16 So the program has to be based on a written
 17 risk assessment that lays out -- that includes certain
 18 criteria for determining risks and then address how
 19 the program is going to address those risks. So,
 20 again, the main change here is we give a little more
 21 flesh on the bones to what the risk assessment has to
 22 look at and also requires that it be in writing.
 23 Then you have to periodically perform
 24 additional risk assessments. And it’s just not
 25 something that you -- you can’t just do a risk

12

1 assessment in the beginning and never think about it
 2 again because, as discussed earlier, things change.
 3 Certainly everyone knows in the information security
 4 field that it’s constantly a moving target as new
 5 threats arise, as new vulnerabilities are discovered.
 6 And like the current rule, there -- it needs
 7 to be tested and monitored, but a little more
 8 specificity here in that you can either monitor it
 9 through continuous monitoring or instead by at least
 10 doing annual penetration testing and biannual
 11 vulnerability assessments. Certainly people may
 12 choose to do it more often than that, but that would
 13 be the minimum requirement under the rule. Next
 14 slide, please.
 15 So the proposed rule also addresses
 16 training. Under the proposed rule, financial
 17 institutions must provide security awareness training
 18 to personnel. So this is to all employees. I think
 19 most people who work in a company have had similar
 20 training that lays out the basics of security
 21 awareness, how to avoid phishing. You know, again, we
 22 don’t go into that in detail, but, you know, it does
 23 require that there be at least basic security
 24 awareness training for everyone.
 25 And then it says if you have information

13

1 security personnel, they need to be qualified. And
 2 you can do that either through your own employees or
 3 through a service provider, which I think is
 4 increasingly common. And then those security
 5 personnel have to be trained. And the financial
 6 institution has to verify they're taking steps to
 7 maintain current knowledge because, as I said, new
 8 threats arise all the time and security personnel
 9 really need to be up to speed on what they need to be
 10 doing to keep their program secure. Next slide,
 11 please.

12 The proposed rule, in addition to those plan
 13 requirements, would still require financial
 14 institutions to oversee service providers. This is
 15 pretty much the exact same requirement under the
 16 current rule. And just -- and also they need to
 17 periodically assess those providers. So that would
 18 require you to, again, occasionally check and make
 19 sure that things are actually being maintained
 20 properly and that they're still capable of providing
 21 the safeguards that are necessary.

22 Again, you have to evaluate and adjust your
 23 program just as under the current rule. One addition
 24 is the requirement for a written incident response
 25 plan. So this plan lays out what needs to be done,

14

1 who needs to be reported to in the event of a cyber
 2 security incident. So if there's a breach or
 3 something like that, they have a -- a plan is in place
 4 to begin with and how to respond to that and how to
 5 mitigate the harm; lessen the harm to consumers and
 6 customers and to your business.

7 And then it would also require that the
 8 person in charge of the program provide annual written
 9 reports to the board of directors, or if you don't
 10 have a board of directors or some equivalent governing
 11 body or management regarding the status of the
 12 information security program to basically lay out what
 13 the needs are, how things have been going, that sort
 14 of thing. Next slide, please.

15 All right. So the information security
 16 program, we need to address certain elements. As I
 17 said, we do lay out some areas it needs to address
 18 without saying how it needs to be addressed. I'm
 19 going to go through those quickly.

20 One is access controls. So these are
 21 controls that limit who can access the information to
 22 make sure only people who are supposed to give
 23 information are the ones who are able to access it.
 24 Another is information inventory. It's basically in
 25 order to program you really need to know what data you

15

1 have, who's going to be -- who has access to it; what
 2 devices there are, and where they're all located. You
 3 need to be able to do that to measure your risk and
 4 then protect it. If you don't know what you have,
 5 you're not able to protect it.

6 The secure development practices. So this
 7 is if your company develops its own applications, they
 8 need to do it -- the program needs to require that
 9 they do it in a secure fashion with security in mind
 10 so that they're not creating applications that are
 11 vulnerable to attack. And if you're using third party
 12 applications, you have to do some sort of evaluation
 13 to make sure they're secure. What that would mean
 14 would probably vary depending on exactly what software
 15 you're using and how widely accepted and widely known
 16 its security is. Next slide, please.

17 Your plan would also need to address audit
 18 trails and what information you need to record about
 19 transactions to allow you to detect security events.
 20 So you can see something strange is going on here, we
 21 have some record of this; we need to investigate it to
 22 see if it's a breach or something like that.

23 It also has to address disposal. And this
 24 is for information you have that you no longer need
 25 for a legitimate business purpose. There needs to be

16

1 a program in place to dispose of it in a secure
 2 fashion.

3 Change management. This is basically a plan
 4 in place for how you will handle changes to your
 5 system, including connecting up new servers, new
 6 computers, changing the structure of the network,
 7 adding databases and that sort of thing. That's often
 8 a place where vulnerabilities are introduced into a
 9 system, is during change. And so your plan needs to
 10 address how you're going to handle that when you do
 11 this sort of thing; how are you going to make sure
 12 that your security is maintained.

13 And you have to -- it has to look at how
 14 authorized users are using their information. Do you
 15 have employees who are misusing information? And this
 16 needs to track that so that you can detect problems
 17 early and deal with them. Next slide, please.

18 So as I've been saying, most of the elements
 19 of the information security plan are very process-
 20 based and up to the financial institution to determine
 21 exactly how it's implemented. There's two elements,
 22 though, that will require a little more specific
 23 action from the part -- on part of the financial
 24 institution. That's in encryption and multifactor
 25 authentication. We felt that both of those are just

17

1 an integral part of security for financial
 2 institutions handling customer financial information.
 3 Both of those requirements, though, allow
 4 alternatives if the person in charge of the program
 5 approves them. If, for whatever reason it's not the
 6 best solution for a financial institution or it's just
 7 not a viable solution. And both of them, while they
 8 require encryption or multifactor authentication,
 9 don't go into the details of exactly how that will be
 10 implemented. That is still up to the financial
 11 institution to decide what encryption solution or
 12 multifactor authentication solution is best for them.
 13 Next one, or next slide.
 14 All right. So let's look at the encryption
 15 requirement first. It would require that all customer
 16 information that is being held by the company or
 17 transmitted be encrypted while in transit if it's over
 18 external networks and while it's at rest.
 19 So points to note about this is it applies
 20 only to customer information. Other information
 21 handled by the financial institution would not
 22 necessarily need to be encrypted and it would be up to
 23 the financial institution. And for the transmitted
 24 information, it only applies to external networks. It
 25 does not apply to transmissions within the financial

18

1 institution's network.
 2 And as I said before, if encryption is not
 3 feasible for some way, then you can come up with
 4 alternative controls that have been reviewed and
 5 approved of by the person in charge of your
 6 information security program. Next slide, please.
 7 All right. The multifactor authentication
 8 requirement would require multifactor authentication
 9 for any individual accessing customer information. So
 10 if anyone is going to look at the customer
 11 information, they need to go through a multifactor
 12 authentication process. I think most people are at
 13 least basically familiar with multifactor
 14 authentication. Most of us use it in some fashion in
 15 our online life.
 16 But just to be clear, what we've defined
 17 multifactor authentication here is — is that it must
 18 include two of three possible factors that it's going
 19 to need. One is a knowledge factor, or things you
 20 know. So this is our passwords or biographical
 21 information such as mother's maiden name or older
 22 addresses, that sort of thing.
 23 Possession factor, things you have. So this
 24 might be an actual physical token that you have that
 25 gives you a code or something like that or it is

19

1 attached to your computer, or it may be a device that
 2 you have possession of, a particular phone or a
 3 particular computer that verifies that you have this
 4 factor. It can be satisfied that way.
 5 There's also the inherence factor, which is
 6 things you are. So this would be biometric
 7 characteristics. I think fingerprints are probably
 8 the most common still, but it also might include voice
 9 prints or face recognition, or to get a little less
 10 common and more sci-fi, retina prints, that sort of
 11 thing. I mean, it's meant to include anything that
 12 anyone comes up with that is things you are.
 13 And, again, if this doesn't work for
 14 whatever reason, the person in charge of the program
 15 can come up with a different solution. You just have
 16 to memorialize that decision in writing. Next,
 17 please.
 18 All right. A little more detail on the
 19 proposed exception to the written requirements. We
 20 decided that the best way to measure this was the
 21 amount of information that a financial institution
 22 maintains about consumers. Because a small company
 23 that is maybe small in size, so budget or customers,
 24 may still hold information of tens/hundreds of
 25 thousands of information of consumers in today's

20

1 environment. It's something that happens. And those
 2 companies, even if they're small, if they have access
 3 and responsibility for information of that many
 4 consumers, we feel they still need to meet these
 5 requirements.
 6 But if you're a company that really does not
 7 maintain much information, this would require --
 8 exempt you from most of the requirements that things
 9 be in writing and the written reports and things of
 10 that nature, just to make it a little easier to comply
 11 with. Although the basic requirements would still be
 12 very much in place for anyone handling customer
 13 information. Next slide, please.
 14 So that brings us to today's workshop.
 15 We're going to be speaking with people with direct
 16 experience providing information security to
 17 organizations, including financial institutions and
 18 other experts in the field, who, you know, have direct
 19 expertise in the information that we're talking about.
 20 What we're looking to do today is to gather
 21 some more concrete information on the cost and
 22 benefits of the practices that we set forth in the
 23 proposed rule and to address some of the comments,
 24 just to get more information on those comments.
 25 We are particularly interested in the costs

21

1 and scalability of these requirements to smaller
 2 businesses. What will the cost be to a small business
 3 and are there solutions that are -- that scale down to
 4 your size? Are there solutions that take into account
 5 your smaller size that will be cheaper and easier to
 6 implement. Next slide, please.
 7 All right. I believe the schedule should be
 8 on the page that you're all watching this from. But I
 9 hope you'll join us for the rest of the day. In just
 10 a few minutes after this, we'll start Panel 1. It's
 11 going to look at costs and benefits of information
 12 security programs. Then after a short break, we'll
 13 have a panel on information security programs and
 14 smaller businesses particularly.
 15 Then after lunch, at 1:00, we'll do a panel
 16 on continuous monitoring and penetration vulnerability
 17 testing. And after a short break at 2:15, we'll do
 18 one on accountability, risk management and governance
 19 of information security programs. And finally we'll
 20 finish up the day with a panel at 3:30 on encryption
 21 and multifactor authentication. Next, please.
 22 Throughout the day, we really hope that if
 23 you have any questions for our panelists that you'll
 24 send them to us. This being our first virtual panel,
 25 we're still -- virtual workshop, we're working out

22

1 details. Hopefully this will work well. If you send
 2 any questions to safeguardsworkshop2020@FTC.gov --
 3 there should be a link on the page you're viewing this
 4 on -- then we will try to ask as many of those as
 5 possible of our panelists.
 6 And then following the workshop, if you have
 7 any comments on the proposed amendments or anything
 8 that is said or presented in this workshop, go to
 9 regulations.gov and look at the Safeguards Rule entry
 10 and you can enter comments there for about a month
 11 after today.
 12 So thank you very much and I will see you
 13 all in a few minutes on the first panel. Have a good
 14 day.
 15 (Brief recess.)
 16
 17
 18
 19
 20
 21
 22
 23
 24
 25

23

1 THE COSTS AND BENEFITS OF INFORMATION SECURITY
 2 PROGRAMS
 3 MR. LINCICUM: Good morning and welcome to
 4 the first panel of the FTC Safeguards Workshop. I'm
 5 David Lincicum, an attorney with the Division of
 6 Privacy and Identity Protection here at the FTC. And
 7 we have four panelists who were gracious enough to
 8 join us this morning. I will go through and introduce
 9 them each, and I think they'll probably raise their
 10 hand or somehow gesture just so you know who I'm
 11 talking about.
 12 First we have Pablo Molina, who is the chief
 13 information security officer at Drexel University and
 14 a lecturer at Georgetown.
 15 Then we have Serge Jorgensen, who is the CTO
 16 and founding partner of the Syllint group.
 17 And then Chris Cronin, a partner at HALOCK
 18 Security Labs. And Sam Rubin, the vice president at
 19 the cybersecurity consulting firm, the Crypsis Group.
 20 So this panel is going to address the costs
 21 and benefits of information security programs of
 22 financial institutions. You saw in my introductory
 23 remarks, I mentioned that both the current rule and
 24 the new rule are really based on risk assessment. And
 25 in order to have risk assessment, really costs and

24

1 benefits of these programs are key to that.
 2 So let's start, and I'll ask Chris. What is
 3 a risk assessment in this context? What are people
 4 look at as far as costs and benefits and how do they
 5 start that process?
 6 MR. CRONIN: Yeah. Well, there's what
 7 people are doing and there's what they should be
 8 doing. So I'll just very quickly say that people are
 9 not generally doing what we would consider risk
 10 assessments. What they're doing is having an auditor
 11 come in and run an audit or they'll be engaged in a
 12 maturity model assessment. Am I a one, two, three,
 13 four or five? And if they're with a consultant who
 14 isn't really grappling with real security issues or
 15 risks, then they might even hear, well, go to a three.
 16 Everyone -- all of your peers are at a three out of
 17 five, whatever that means.
 18 That's actually commonly what's happening.
 19 What we understand the Federal Trade Commission,
 20 regulators, even litigators and information security
 21 people, are really going for is an evaluation of the
 22 likelihood and the magnitude of harm that can come
 23 from bad things that happen.
 24 Now, we all have really good information
 25 about the bad things that happen. There are some that

25

1 have yet to be invented, we know. But if we're doing
 2 an actual risk assessment, we're looking at the
 3 likelihood and impacts of things that could go wrong
 4 in environments like ours. And what you're also
 5 suggesting in the proposed updates is that there's a
 6 -- that you also evaluate the controls, which is super
 7 important. If we're going to have a good definition
 8 for reasonableness, we want a cost/benefit evaluation
 9 to say when you look at the likelihoods of impacts
 10 without the control I'm considering. Let me evaluate
 11 it with the controls I'm considering and let me see
 12 where the balance is. And as long as we've thought
 13 about the impacts to ourselves that could be harmed
 14 and the impacts to others who we're protecting, then
 15 we're actually -- we've got a good basis for
 16 reasonableness. We're just not hitting that yet.
 17 When you do look at stuff that comes from
 18 the federal regulators and three-letter agencies, the
 19 way you see attorneys talk about things, you know,
 20 when a breach case is going on, when you're talking to
 21 information security people, they all have the
 22 essential ingredients to have a definition for risk
 23 basis of reasonableness, but it's like we're at a --
 24 we're running a marathon; we've gotten 10 yards short
 25 of the finish line and we've stopped. And we looked

26

1 at each other and say now what do we do? Well, you
 2 cross the finish line; just do that risk assessment
 3 and compare the two and then you've got a good basis
 4 for reasonableness.
 5 So we're excited to see even stronger
 6 direction about what that risk analysis should be.
 7 But that -- we're -- the public just hasn't gotten
 8 there yet. And we're really encouraging them to move
 9 forward there.
 10 MR. JORGENSEN: Chris, one of the things you
 11 just mentioned there in terms of how that risk is
 12 calculated, you touched on that risk to the data that
 13 you're protecting and the risk to the consumer. And I
 14 think that's something that we see frequently missed
 15 in that risk analysis because there seems to be a
 16 preponderance of people that are saying, oh, okay, I
 17 can transfer the risk; I can buy insurance for this.
 18 And then the insurance will pay for all of that
 19 downstream impact of the risk.
 20 But you really haven't necessarily protected
 21 the data that you've -- you are supposed to be
 22 protecting. And so it's just an interesting look at
 23 that can I transfer this or is it something I do have
 24 to protect?
 25 MR. CRONIN: Right. Or consider the harm to

27

1 people directly. And when I'm doing litigation
 2 support, one of the first questions I ask whether
 3 among the defense or plaintiff's or regulator side is
 4 I ask when we look at the risk analysis, did we
 5 explicitly look at the kinds of harm that could come
 6 to people and did we make investments that were
 7 appropriate for protecting that harm?
 8 When I do see a risk assessment, it's
 9 usually what is the impact to business. That's
 10 important. But that's not the only thing you should
 11 be paying attention to. When we're talking about
 12 cost/benefit analysis for reasonableness, our cost is
 13 impact to business. Right? The benefit is what we
 14 need to actually be sure we're taking a look at when
 15 we're evaluating risk to the public. Because we're
 16 seeing that missing, a lot of people are going to have
 17 a hard time demonstrating reasonableness.
 18 MR. LINCICUM: All right. Here's a question
 19 I'll kind of ask the group, then. You talked about,
 20 you know, the bad things that can happen with a
 21 breach, and we certainly have all seen them in the
 22 news. Those are sort -- those tend to be the very bad
 23 situations.
 24 What information do people have about the
 25 more general risks to them? You know, what kinds of

28

1 attacks are they most likely to face; how bad are they
 2 going to be? Where do they get that information and
 3 how does a company start to come to terms with what
 4 their vulnerabilities are and where the risks are?
 5 MR. RUBIN: Yeah, this is Sam. I can speak
 6 to that. So my firm, Crypsis, does a tremendous
 7 amount of data breach incident response. So we're
 8 working with companies every day helping them respond
 9 to these types of incidents. And what I would say is
 10 that, you know, if companies kind of have their eyes
 11 and ears open, there is a tremendous amount of
 12 information whether it's threat intelligence,
 13 publications from firms like mine and other great
 14 infosec firms that are talking about the risks that
 15 are out there; the things that companies are facing.
 16 For example, right now based on our work,
 17 what we're seeing is that the two greatest threats
 18 facing financial institutions are business email
 19 compromise -- that's threat actors getting into your
 20 email and trying to perpetrate wire fraud or otherwise
 21 monetize that access -- and ransomware. So those are
 22 the two biggest threats that we're seeing impact
 23 organizations. But for -- to answer your question,
 24 you know, what companies can do is really just -- it
 25 just takes kind of a level of effort to look to see

29

1 what's out there and what your peers are facing, and
 2 just to have that awareness.
 3 MR. JORGENSEN: I think one of the
 4 challenges there, though, is that you have to
 5 understand what the risk is, because if you purely
 6 look at it from that perspective of here's the attack
 7 vector that the threat actors might be using, and you
 8 said business email compromise or ransomware -- and,
 9 Sam, I totally agree with you in terms of the type of
 10 attacks that we're seeing. But from a risk
 11 perspective, I think a lot of people miss the
 12 incentives of the threat actors, and these attackers
 13 out there have -- can get millions of dollars from a
 14 successful attack. So from their perspective, they
 15 look at it more like what's the easiest way to get to
 16 the data that I'm going after? And where right now it
 17 may be business email compromise, tomorrow it's going
 18 to be something different.
 19 And so if we go back to how do we do that
 20 risk analysis and that risk assessment, it's got to be
 21 around what kind of data do I have and then how do I
 22 protect that, yes, against the current threats but
 23 also how do I build out a program that appreciates
 24 that the sensitivity of that data, the risk of that
 25 data being compromised, and then how do I adjust my

30

1 protections based on the evolving threat?
 2 And that way, I'm not always chasing the
 3 most current one, but I'm planning for the future as
 4 well.
 5 MR. MOLINA: At Drexel University and other
 6 universities we're in the business of educating
 7 people. So we educate our community members, faculty
 8 and staff, students. I gave interviews with the
 9 regional media outlets to educate the community about
 10 some of the cyberthreats out there, some of them being
 11 business cyberthreats; others are personal.
 12 But to be honest, I would say that the
 13 number one source of information for most people is
 14 the regular media. And some media outlets are very
 15 good at reporting what's going on and how to take
 16 precautions in organizations and as individuals
 17 against some of these cyberthreats. But others have
 18 not. So it is our experience that many of our
 19 community members are sometimes ill-informed about the
 20 different threats. They may have heard time and time
 21 again that there are phishing scams out there, and yet
 22 they fall for them. They might have heard do not
 23 click on this link or else ransomware will be
 24 unleashed upon your organization's computers, and yet
 25 they click on the link.

31

1 So it's an interesting ongoing exercise that
 2 requires -- it takes a village to educate the entire
 3 society, but particularly our employees and our
 4 clients in order to understand those cybersecurity
 5 risks.
 6 MR. JORGENSEN: You know, one of the things
 7 that I know a few of us participated in the Sedona
 8 Working Group 11 on data security and privacy. And
 9 one of the things that that blend of legal and
 10 technological experts, one of the things that Sedona
 11 is looking at, and other organizations, is trying to
 12 find that line, that cost/benefit analysis of risk.
 13 And, Pablo, you must be facing this from a
 14 university perspective. Companies like to maintain
 15 historic data for whatever purposes -- reasons or
 16 purposes. And I know Sam and Chris, all of us out
 17 there face this information governance problem where
 18 after a breach has occurred, the threat actors got far
 19 more data than they could have. And, Pablo, my
 20 background or experience at universities anyway has
 21 been that they'll keep registration information for
 22 not just students, but, you know, possible students or
 23 applicants or people that you send scholarship
 24 information to, going back 20 years.
 25 And then we have to assess is that -- what's

32

1 the value of that information or should I -- could I
 2 get rid of it and reduce the risk to the organization?
 3 And I think that really comes, Chris, back full circle
 4 to what you were saying about risk analysis, risk
 5 assessment, is you can just say, okay, well, you've
 6 got antivirus, you've got these three controls,
 7 everything's protected. But where we're trying to
 8 encourage people to think about can I get rid of data,
 9 what's my information governance process, and then if
 10 I do have a business email compromise, if I do have a
 11 ransomware attack that exfiltrates data, as well, then
 12 if I can reduce the scope of that data that I'm
 13 holding, then I have a much smaller exposure, much
 14 smaller risk, and ultimately much smaller impact to
 15 consumers.
 16 MR. MOLINA: Well, in the case of
 17 universities, we hold records for Drexel over 100
 18 years; in the case of Georgetown where I teach, over
 19 220 years. So you're right about -- that's the
 20 policy, yeah.
 21 MR. LINCICUM: All right. I'm going to move
 22 on to the next topic, which is very tightly connected
 23 to what we've been talking about, and that is kind of
 24 the benefit side of the coin.
 25 After you've assessed the risk and the

33

1 magnitude of the risk, you then have to look at a
 2 solution. In one way, the costs of those solutions
 3 are fairly obvious. You'll know how much it costs to
 4 implement. But part of the equation is also how
 5 effective are they?
 6 Sam, you said you've been involved in a lot
 7 of, you know, common after incidents. How do
 8 companies determine which protection pays for itself,
 9 actually creates enough benefit to justify the cost?
 10 MR. RUBIN: Sure. Yeah, I mean, the
 11 unfortunate reality of what I see often is that it is
 12 that knee-jerk reaction in a post-breach scenario that
 13 makes it easy for leadership teams to see and
 14 understand what additional controls they need to
 15 implement because they're basically saying how can I
 16 make sure this never happens again?
 17 And so, you know, whether it's, you know,
 18 insecure remote access, multifactor authentication,
 19 poor identity and access management, whatever the
 20 control gaps were, maybe no continuous monitoring,
 21 that makes it easy to see what they need to add or
 22 implement.
 23 So that's one side of the coin. But where
 24 we want to get to is kind of for companies that
 25 haven't experienced a breach or incident in the recent

34

1 past, like, how -- to your question, how can they
 2 evaluate the benefit of implementing any given
 3 control. And, you know, I think an answer is some of
 4 the analysis that Chris was talking about where in a
 5 risk assessment, it allows you to demonstrate
 6 essentially the return on a control because a proper
 7 risk assessment, what it will do is it will take a
 8 probability of loss and a dollar impact and that
 9 allows you to essentially demonstrate how a change or
 10 implementation of control can kind of reduce the costs
 11 of a breach and relatedly kind of demonstrate the
 12 value or return on control.
 13 So that's kind of the rigorous risk
 14 assessment method way to assess the benefit. Not
 15 always as Chris indicated at, you know, the top of the
 16 hour what we're seeing companies do at this point, but
 17 I think it's a place that they can get to.
 18 Where we are right now, again, as companies
 19 have been kind of having this knee-jerk reaction,
 20 maybe the next layer of maturity is when they're using
 21 these risk matrices where you have, you know, a
 22 likelihood and an impact and the red and green and
 23 yellow.
 24 I had a matter recently where I was talking
 25 to a CEO and he said how can I get more green on my

35

1 chart? And that was his goal for, you know, reducing
 2 risk, which, you know, it's better than nothing, I
 3 would argue, but if we can get to that point where
 4 we're doing something a little bit more rigorous, we
 5 would all be better suited.
 6 MR. JORGENSEN: You know, that's a really
 7 interesting -- it's an interesting metric. And I
 8 think from a CEO's perspective, that may be "the"
 9 metric, is hey, what do I need to do to make this
 10 thing green? And if you tell me that it's get these
 11 business units in line with our security program, our
 12 risk analysis or whatever it is, then that may be what
 13 the CEO can do because ultimately they can't do it.
 14 Should they have to understand the
 15 intricacies of cybersecurity or do they know that all
 16 they really have to do is help Pablo get to the
 17 registrar's office and actually delete data that they
 18 don't actually need anymore and help implement this
 19 information governance program, and that will turn a
 20 whole bunch of other things green?
 21 So I think part of the challenge from
 22 identifying what those key performance indicators are,
 23 identifying what those metrics are, that can help
 24 leadership manage the risk for something that they
 25 really don't understand and maybe don't need to

36

1 understand, but rather just need to support the effort
 2 to implement those controls, but then appreciating the
 3 benefits of those controls becomes really hard.
 4 And I know, Sam, you're probably going to
 5 talk about this, too, of trying to understand
 6 something where the only benefit is something doesn't
 7 happen. And it's really hard to explain that of, hey,
 8 we won; there's been no incident.
 9 MR. RUBIN: Yes, right. Or companies really
 10 -- you don't get a bonus for not getting hacked,
 11 right? So, yeah, if that's your metric of success, it
 12 can be very hard. And, you know, when a CFO looks at
 13 that and they're looking at their profitability, you
 14 know, information security essentially just becomes a
 15 cost center. And so without a way to demonstrate the
 16 benefit, you know, we see things get cut or just a
 17 failure of, you know, whether it's a CISO or director
 18 of infosec to persuade his executive team to add those
 19 necessary controls.
 20 MR. MOLINA: And risk analysis is very
 21 industry- and context-sensitive. Even though we're
 22 here discussing these issues in the context of
 23 financial services and the Federal Trade Commission,
 24 the truth of the matter is that there are a great
 25 variety among different financial services

37

1 institutions.

2 We're considered one as a university because
3 of the disbursement of financial aid and other
4 transactions that we perform and accomplish for the
5 community. So for that it is very important for us to
6 curtail and manage the risk of economic losses, for
7 example. But even more important than that is to
8 protect the brand name of the institution. Those six
9 letters that read Drexel are worth more than the
10 regulatory fines or some of the financial losses that
11 I may experience.

12 Because, for example, we have really
13 outstanding cybersecurity programs. If we are hacked,
14 and it is reported that we're hacked as most
15 universities have been hacked in the past, then some
16 of the students or faculty members who were thinking
17 about joining our cybersecurity programs are going to
18 say I don't think that these guys, they have their act
19 together very well, so we might as well go to a
20 university that has yet to be hacked as opposed to one
21 that was hacked before.

22 And even within universities, we have very
23 different units. We have the financial aid units, but
24 we also have the ones that deal with patient data, DOD
25 data. So each one of those require a different risk

38

1 analysis. So sometimes the devil is in the details.

2 MR. LINCICUM: You all have sort of touched
3 on this in one way or another, but I'd like to ask the
4 group. With your experience in various ways looking
5 at company security, what's your general impression
6 either in certain fields or in certain areas that
7 you're familiar with or generally, where are
8 businesses with data security?

9 Are most companies where they need to be or
10 are you seeing a lag kind of universal or in
11 particular areas?

12 MR. JORGENSEN: You know, it's interesting
13 that I think most companies are aware of something
14 called cybersecurity at this point, as we're doing
15 incident response work, as we're doing proactive
16 security, whatever it may be. We're certainly not
17 having to explain that data exists in the cyber world
18 and that threat actors are trying to get it. I mean,
19 you'd have to be under a rock if you haven't read a
20 news story about that type of attack recently.

21 But one of the big challenges that we're
22 seeing, and maybe the next big challenge for industry,
23 is that it's more and more difficult for them to apply
24 that across the various business units. So somebody
25 -- the university goes, hey, I have a CISO and

39

1 therefore I'm okay. But not recognizing that maybe in
2 a university perspective, research and development is
3 off doing their own thing, or in a corporate
4 perspective sales can pretty much do anything they
5 want because that's a revenue source and if they say,
6 well, I didn't have multifactor authentication in
7 place because it lost a deal, or then I can't
8 communicate because I have this mail filter in place.

9 And so the business unit pushback tends to
10 still win and that makes it hard to implement those
11 security controls even if you have this risk analysis
12 or risk assessment done. So that's one of the things
13 that we're seeing, is that businesses are starting to
14 understand security and starting to understand the
15 ideas, but implementing it across all the business
16 units is still difficult.

17 MR. CRONIN: Yeah. David, I'm going to
18 throw in there, too. Serge is exactly on point. And
19 organizations are behind, right? So at HALOCK, we're
20 going into organizations of all types and sizes, and
21 as a rule they're all behind.

22 Information security is a big challenge, and
23 financial services often try to drive things by a
24 dollar basis. So there's actually something working
25 actively against the Federal Trade Commission's

40

1 interest in getting to reasonable security, and it's
2 something to be very aware of as you move forward with
3 the next steps of the Safeguards Rule. And that's
4 that -- and most of us on the panel here are
5 consultants of one form or another, but there's a
6 brand of consultancy that's a real problem and it's
7 actually pushing against this definition of
8 reasonableness.

9 So we have consultancies that go out. I
10 mentioned maturity models before, where someone might
11 be graded one, two, three, four, five. Five is, you
12 know, you're innovating, and one is, oh, you're sort
13 of ad hoc. And we have organizations going in with
14 these maturity models telling their clients, get to
15 three, get to three. Because three is where your
16 peers are. And three basically means you've
17 implemented your controls, but you're not testing and
18 improving them, and you're not innovating in any way,
19 you're not taking care of root cause problems. You've
20 just got evidence you implemented your controls.

21 And when you talk to these consultants who
22 say get to three, you ask why do you say that? Well,
23 that's where their peers are. But their peers are
24 there because you tell everyone to get to three.
25 You're forcing a mediocre quality of information

41

1 security.

2 So there is an aspect of the business that's

3 pushed by a certain level of we've got to make the

4 clients happy. If we tell them they have to get to

5 five, they'll go find someone else who will tell them

6 to get to three. And this is a real economic driver

7 that pushes organizations away from thinking about

8 what is reasonable.

9 The irony here is that if you actually are

10 thinking about what's reasonable and you're taking

11 this risk-based approach, you've got the challenges

12 that we just described earlier. We've got the costs,

13 we know what those are; the invoices come in. Right?

14 The salespeople tell us what the number will be. The

15 benefits, that's hard to figure out. This is a big

16 problem.

17 So in order to help people get through these

18 economic drivers, away from thinking about what a

19 reasonable security control would be, HALOCK worked

20 with the Center for Internet Security and just

21 developed this document called Center for Internet

22 Security's Risk Assessment Method, CIS-RAM. It's

23 freely available for anybody. But it helps you do

24 this evaluation where you can say what are my

25 financial costs, what are the costs and benefits to my

42

1 mission, the reason why we engage in risk to begin

2 with? What are the costs and benefits to the

3 individuals who are at risk in my organization and to

4 get people to systematically think about this.

5 So what we're seeing as a real driver away

6 from the right behavior is just the economics of

7 trying to have a happy client in the field causing

8 people to do things other than think about reasonable,

9 because they haven't quite figured out what that

10 process is.

11 And I think the FTC has a real opportunity

12 here with this round of the Safeguards Rule to tell

13 people, by the way, what we mean by reasonable, this

14 is a cost/benefit analysis. So think about the costs

15 to your mission, your objectives, why you're in

16 business and your obligation to protect others with

17 and without the safeguard and we're going to figure

18 out whether the costs and benefits balance.

19 So that's part of what we're seeing as a

20 challenge that gets people away from doing the right

21 thing and something that I think the Safeguards Rule

22 could help people get back on the right track.

23 MR. MOLINA: One of the ways in which we

24 measure the progress we made in many aspects of

25 economic activity is we'll look at the investment

43

1 levels. Ardent (phonetic) reported late last year, on

2 average U.S. organizations are spending between 5

3 percent and 8 percent of their technology budgets in

4 information security; as low as 2 to 4 percent in

5 manufacturing businesses, and as high as 10 to 15

6 percent financial services, which is quite a wide

7 range between 10 and 15 percent.

8 What we don't get from those numbers is

9 whether we're making a good investment with that

10 money. Just because you're buying the most expensive

11 advanced firewall does not mean you're protecting, as

12 Serge mentioned before, the data that is critical to

13 your organization, or as Sam mentioned before, that

14 you're addressing the threats that are lingering out

15 there.

16 So we still don't have enough research and

17 enough actuarial information to understand the risks

18 very well but also to understand whether or not what

19 we're spending in cybersecurity is really taking us to

20 the level that we should be at. And the suspicion

21 that most of us have without hardcore research is that

22 we're really falling behind the bad guys. And proof

23 of this are the mounting losses that come from

24 cybercrime.

25 MR. RUBIN: Yeah, I agree with that.

44

1 MR. JORGENSEN: You know, it's interesting

2 -- go ahead, Sam.

3 MR. RUBIN: Okay, sure. Yeah, I agree with

4 those comments. And just, you know, based on what

5 I've seen out there often is sometimes you see strong

6 investment in tools, right? Like, you know, investing

7 in an endpoint detection and response or putting in a

8 SIM, but without consideration of the people that you

9 need to support those tools.

10 So, I mean, just equally important is the

11 cybersecurity team to support ongoing security

12 operations, to provide that continuous monitoring to

13 look at the telemetry coming from your endpoints, to

14 look at the logs.

15 And so just, you know, back to the question,

16 David, of what we're seeing out there, that's a huge

17 shortcoming that I'm seeing in the field. Another one

18 you know, along the lines of what you were saying,

19 Serge, is that divergence in business groups, I see

20 that also with organizations moving to the cloud and

21 to SaaS, you know, especially in this COVID time where

22 we're all working remotely, you know, from our

23 laptops. You know, some of us, you know, may be

24 engaging in a little bit of shadow IT when we

25 shouldn't be, looking for applications to help us get

45

1 our job done and organizations having this kind of
 2 legacy protection model of, you know, the firewall and
 3 I'm going to protect my employees kind of hiding
 4 behind the corporate local area network. And what
 5 they're not doing is kind of protecting the cloud
 6 applications, protecting the SaaS applications, like
 7 Office 365, and protecting the endpoints.
 8 So I think that that's a huge gap right now
 9 and area of focus. So, again, you know, cloud, SaaS,
 10 and then obviously having the right people.
 11 MR. JORGENSEN: And I think, Sam, you
 12 just touched on it, too, where companies are thinking
 13 they can leverage the risk assessment that's been
 14 done for their SaaS provider or their cloud solution.
 15 And I can't tell you how many times I've gotten the
 16 obligatory, well, everything's secure because I have
 17 it hosted in AWS and here's Amazon's SOC 2. And I'm
 18 looking at it going, I appreciate that their
 19 information is secure, but what about your
 20 information? How is that working for you?
 21 MR. RUBIN: That's right.
 22 MR. JORGENSEN: So it is one of those very
 23 big challenges, yeah.
 24 MR. LINCICUM: Let me go ahead and move on
 25 to the next question, something that came up I think

46

1 Chris was talking about how certain consultants will
 2 have a certain approach. And that's a question I have
 3 with a company that is starting this process of
 4 setting up a program or updating it based on a new
 5 rule or new standard. How do they determine what they
 6 should be doing? I mean, a consultant will come in.
 7 Are there standards that a consultant will be working
 8 towards? Are there qualifications that tell you, oh,
 9 this person is going to get you in the right place?
 10 Or are you just kind of doing it one at a time on
 11 people who come through your door? What standards are
 12 there out there?
 13 MR. JORGENSEN: I'll tell you one of the
 14 most powerful pieces that we've been able to use to
 15 address that question is your own FTC publication on
 16 cybersecurity basics and just putting that out there
 17 and saying, hey, here's a cybersecurity basic book; go
 18 through these scenarios in here of FTC actions and
 19 things that have happened already and make sure that
 20 your programs are addressing those areas, because I
 21 think something that that does is it really helps
 22 people understand that even if I have anti-virus and
 23 even if I have -- I'm being told that I have DLP --
 24 and going back to Chris' point of, it's a three,
 25 therefore it's implemented and I have a policy for it,

47

1 but it got turned way down and it's now ineffective
 2 because it started blocking all of my outbound mail
 3 because I use a nine-digit number that looks like a
 4 social security number, but it's not really. So I
 5 turned down that control or I didn't put that control
 6 in place.
 7 So in terms of being able to explain the
 8 impact and some of the considerations with a bunch of
 9 war stories, I think that cybersecurity basics manual
 10 is -- has been incredibly useful.
 11 MR. LINCICUM: Good to hear.
 12 MR. MOLINA: There are others. We all use
 13 the National Institute of Standards and Technology
 14 cyber controls. They have been very helpful. But
 15 also, for example, as I mentioned, many of these
 16 decisions are context- and industry-sensitive.
 17 So, for example, those of us in higher
 18 education, we get together through an organization
 19 called Educause. And many of us belong to the Higher
 20 Education Information Security Council. So there we
 21 develop the risk analysis and we develop frameworks
 22 that are very good for higher education. They map to
 23 the other controls, they map to the NIS controls and
 24 they map to the CIS controls and many of the other
 25 ones we discussed, but they have been tailored for our

48

1 own industries.
 2 So the interesting part would be to work
 3 with partners. I would suggest particularly for
 4 organizations that are not mature in this field to
 5 work with partners and vendors who have a certain
 6 specialization in the financial services industry
 7 because they can provide that nuanced approach to
 8 cybersecurity and risk analysis that are going to make
 9 them very, very effective in those efforts.
 10 MR. CRONIN: Yeah, Pablo's right that the
 11 industry-adjusted approach is an important thing to
 12 consider. Now, we don't have one information security
 13 control standard per industry, right? But there are a
 14 variety of security control documents like ISO 27002,
 15 NIST 800-53, which is more detailed, but also leaves a
 16 lot to the imagination of the reader. CIS controls
 17 can be very specific and practical. There are a lot
 18 of these control sets that people use.
 19 What's interesting is when you look at the
 20 instructions for each of these controls, they all tell
 21 you to do risk analysis. This is one of the really
 22 important things that FTC is doing with the proposed
 23 changes to the Safeguards Rule, by getting more
 24 specific about what this means, because no matter what
 25 control set you look at, you're going to see things

49

1 that just can't be applied.

2 We had a client, a hospital, that was --

3 they were fed up with their security team, their

4 internal security team, because the internal security

5 team was saying use multifactor authentication; you

6 must do it. Now, that sounds like of course you

7 would; you've got it in the proposed rules. It was

8 driving the physicians crazy because they would be in

9 emergency situations and they wouldn't have their

10 second factor with them, you know, where's my phone;

11 I've got to get in to get this patient's record; she's

12 having an allergic reaction; where's her file? It's

13 on the system, but I don't have the second factor;

14 what am I going to do?

15 The hospital has a mission, right, and the

16 mission is patient care outcomes. The patients have

17 to come out healthier than they were before or they

18 failed their mission. And physicians were pushing

19 back saying your security control of multifactor

20 authentication is hurting our mission. You're

21 creating -- in other words, you're creating a risk to

22 our mission.

23 So these control standards, when you look at

24 the NIS risk management framework and the

25 cybersecurity framework, and you look at CMMC, this

50

1 new pending standard that's coming out for suppliers

2 of the Department of Defense. You look at what's

3 coming out from the FTC since you've uttered a word

4 about this. You have to analyze the risk.

5 I say that you use whatever control standard

6 looks like what you can do with your business, what's

7 practical with your people and your technologies, you

8 have to have that standard of care. But then those

9 control standards are going to be hard to fit and hard

10 to negotiate unless you have a real clear

11 understanding of what that risk is.

12 MR. RUBIN: Yeah, I agree with that, Chris.

13 I would sum it up by saying these frameworks, you

14 know, there's a lot of them out there, obviously

15 different ones that apply to different industries.

16 You know, you pick the ones that are right for your

17 organization, your industry. Get the fundamentals as

18 you're saying but then leverage the risk assessment to

19 get -- to assess where you are in that gray area of

20 controls that you may not have, you know, economic

21 resources or time to implement all of them. And the

22 risk analysis helps with that gray area.

23 MR. CRONIN: And, David, just one quick

24 point on a draft commentary, on the recommended -- on

25 the proposed rule change is this concept of the CISO

51

1 signing off on an exception. So if I've got

2 multifactor authentication, unless the CISO signs off,

3 one real big problem we've got in the industry as well

4 is this concept of risk acceptance without someone

5 knowing what risk they're accepting.

6 We hear it a lot. Why did this breach

7 happen? Well, we didn't do X, Y or Z. Why? Well,

8 they accepted the risk. Was it your risk to accept or

9 was it someone else's?

10 One thing I'd recommend going into these

11 proposed rules is that, as you mentioned something

12 like encryption or multifactor authentication where

13 the CISO can sign off on an exception, that that

14 exception should be based on the risk evaluation and

15 to make that explicit. You can do it if you determine

16 that the likelihood and the impacts of the problem are

17 either acceptably low for all interested parties or

18 there's no safeguard that would be appropriately

19 burdensome given the risk.

20 So there's a way to inject that risk

21 reasonableness because there is an epidemic of CISOs

22 signing off on risks that isn't their risk to accept.

23 MR. JORGENSEN: One of the challenges also

24 is -- comes in under risk mitigation at the end of the

25 day, I think, but it's post-incident risk mitigation.

52

1 So when you use that example of multifactor

2 authentication, it's one thing if that access provides

3 that physician with access to a certain part of the

4 medical record or for a certain number of medical

5 records or something like that. And we still look at

6 this as very black and white. So when you look at

7 risk analysis, risk mitigation, I think the knee-jerk

8 way to do that is to prevent a threat actor from

9 breaching the edge, from getting into an environment

10 at all.

11 And one of the pieces that's in a lot of

12 standards that we're talking about, and certainly in

13 some of the FTC guidance, is that discussion about

14 post-incident impact. And so it's much, much

15 different if the impact is limited and I detect things

16 quicker versus if I have a threat actor running around

17 in my environment for days, months, years, and able to

18 access anything they want.

19 So that would be another piece that I think

20 could use some highlighting in any sort of

21 publications or new regulations.

22 MR. LINCICUM: I want to make sure that we

23 get to ask some questions from the audience. I'm

24 going to move on to that now and maybe we can finish

25 up with one last question after we do that.

53

1 We have one question. It's fairly lengthy,
 2 so I'm going to try to parse it out as best I can for
 3 us. It asks what role should a determination of
 4 substantial harm and inconvenience play in the
 5 determination of -- it says complaint requirements --
 6 I'm wondering if they mean compliance requirements --
 7 in the space, given that it's an integral part of the
 8 rule both currently and as proposed?
 9 So I guess it's asking, you know, how much
 10 should you be looking at the substantial harm and
 11 inconvenience and how much does that play a part? And
 12 how does that standard affect the nature of
 13 appropriate risk assessments, incident response and so
 14 forth. So anyone who think they got that, please
 15 answer.
 16 MR. MOLINA: I'd love to, but I think that,
 17 David, you are the lawyer here. Me, I have a doctoral
 18 degree, but it's not in law. But I think that we
 19 understand the issue of harm. I also serve on the
 20 board of the Electronic Privacy Information Center in
 21 Washington, D.C., and we work very closely at times as
 22 friends of the FTC, sometimes in a more controversial
 23 relationship trying to push on the boundaries on this.
 24 The issue of harm for any data breach is
 25 something that we have not solved. It's very, very

54

1 difficult to prove harm to consumers because you
 2 really don't know whether your data was exposed
 3 because of the breach today or the one two days ago
 4 from a different organization, or another one. There
 5 are no fingerprints to data that tells you what data
 6 caused the harm.
 7 Hence, when you cannot address the issue of
 8 harm. Of course, organizations, we don't want to harm
 9 our constituents. We want to protect them, we want to
 10 do business with them out of the goodness of our
 11 heart. We also don't want to get into trouble with
 12 the regulators, particularly not with the FTC or the
 13 state attorney generals of any -- or the GDPR data
 14 protection authorities in Europe. We just don't want
 15 to do any of these things.
 16 But the issue of harm is an almost -- a very
 17 difficult one to tackle. And to my knowledge, there
 18 have been no good solutions, not even on the other
 19 side of the Atlantic with a much more advanced privacy
 20 regulation and the GDPR.
 21 MR. CRONIN: Yeah, I've got a slightly
 22 different take on that. Pablo, I agree with you as we
 23 look back. It's certainly hard to figure that out.
 24 It's hard to sometimes use our imaginations, too.
 25 But what we can say is there are certain

55

1 risks that we're not going to take, whether I know
 2 what the subsequent harm will be or not. And I know
 3 that -- if I have a risk that could expose some number
 4 of a kind of sensitive record, that's something I'm
 5 not going to accept. And I might even equate that
 6 with some level of harm my organization might suffer.
 7 So even if we don't have a way to quantify that harm,
 8 there are ways for us to say qualitatively I would not
 9 want X amount of data of X type to go out, and I would
 10 equate it with this much harm that I could suffer,
 11 therefore, I'll put a control and that safeguards us
 12 both to some level.
 13 I think this is actually a good opportunity
 14 for us to think about qualitative ways to talk about
 15 risk, where quantitative methods are helpful for other
 16 questions like dollars.
 17 MR. LINCICUM: Okay. We have another
 18 question, and it is also a very lengthy one. I'll try
 19 my best to get to the meat of it so we can do
 20 multiple. Okay, I'll see if I can paraphrase.
 21 Basically, the question asks since the rule
 22 would only affect customer information, information
 23 that's actually connected to a financial transaction,
 24 does that change how a risk assessment would be done.
 25 And it gives an example of -- let's see, registration

56

1 of student information that's not related to financial
 2 aid may be held for a variety of purposes by a
 3 university. And doesn't that affect -- you know, if
 4 you only have to consider some of the information,
 5 does that affect how you do the risk assessment, I
 6 think is the meat of that question.
 7 MR. MOLINA: I think I can take it since
 8 student information, that seems to be under my
 9 purview. Those are the things that I see. So I would
 10 sign an exception for and accept the risk -- just
 11 kidding. I would never accept the risk for anything,
 12 thank you very much.
 13 MR. CRONIN: That's very funny.
 14 MR. MOLINA: But in academics, it's
 15 sensitive. It goes back to what Chris and Serge and
 16 some were saying that we have different business units
 17 and business processes and data elements, and we have
 18 to take a context-sensitive approach to those. So
 19 you're absolutely right.
 20 For example, student information is mostly
 21 regulated by FERPA, the Family Education Rights
 22 Privacy Act, whereas the financial aid transactions
 23 that we're discussing under the Safeguards Rule are
 24 mostly regulated by the Federal Trade Commission.
 25 And by the same token, you mentioned the

57

1 cybersecurity model maturity certification. A new one
 2 for those of us who are Research I institutions doing
 3 research with DOD, Department of Defense, funding. So
 4 the interesting part is that a CISO and also as
 5 executives of large, complex organizations, we have to
 6 be able to synchronize all of those different
 7 requirements and make sure that we came up with
 8 umbrella risk analysis processes that take into
 9 account all of those different regulatory
 10 requirements.

11 So the answer is, yes, it's different how
 12 you would protect the information for financial aid
 13 based on the Safeguards Rule and other FTC regulations
 14 than you would according to FERPA. Never do you want
 15 to expose your community members information to the
 16 outside world because it's not a good thing for
 17 reputation or economic or regulatory reasons. But
 18 it's true that this is different.

19 Now, there are some people that have tried a
 20 very difficult approach. Let's say they have a
 21 hospital and they say I'm going to make the entire
 22 university HIPAA-compliant. And those people right
 23 now are looking for a job because it is very difficult
 24 to do that without spending inordinate amounts of
 25 money and antagonizing everybody in the community. So

58

1 most of us are doing that fine-grained security
 2 approach where we're trying to fine-tune our approach
 3 to this.

4 MR. JORGENSEN: But one of the challenges
 5 there, I think, is that as you do that, that fine-
 6 grained approach is making sure that you are
 7 protecting the trusted to trusted edges there, because
 8 that's where you run into issues with PCI. So we're
 9 one of the 12 companies or so that does payment card
 10 forensic investigations. And most of the incidents
 11 that we see there start from -- at the trusted
 12 environment and the rest of the company, and then they
 13 move into the trusted environment in the cardholder
 14 data environment. And then from there, manage to get
 15 access to the data that the threat actors are looking
 16 for.

17 So when you start trying to be too
 18 dismissive -- and, Pablo, I completely understand that
 19 this is not where you were going, but I think it's
 20 something that is worth calling out because a lot of
 21 companies have the attitude of, oh, I don't need to
 22 protect it because it's not -- it doesn't fall into
 23 this particular area or this particular regulation.

24 So it's not covered by the Safeguards Rule
 25 or it's not covered by HIPAA or whatever, therefore

59

1 it's okay; I'll apply this no security rule to it.
 2 And then what happens is you end up with machines that
 3 are connected to both environments or a trusted person
 4 that's inside is then used to attack the area that's
 5 supposed to be protected.

6 In hospital environments, nurses'
 7 workstations or something that aren't supposed to have
 8 any PHI on the workstation, but they have direct
 9 access to everything that has PHI. So it's just --
 10 you've got to be really careful about where you try to
 11 draw those lines, and when you draw the lines,
 12 understand that you have to still then protect that
 13 barrier.

14 MR. LINCICUM: All right. Thank you very
 15 much. All right. Here's a more of-the-moment topical
 16 question for us. It's asking about the impact of
 17 COVID-19 on the resources and capacity of companies
 18 right now. It's asking should that be taken into
 19 account in the rule. But I think let's ask more of a
 20 -- as Pablo said, not an attorney, so let's get more
 21 into the world of, you know, actual risk assessment
 22 and data security.

23 How much is COVID-19 affecting companies'
 24 ability to protect things? Is the crunch on resources
 25 being felt so that it's harder to do the protection or

60

1 is the awareness increasing? What effect has COVID-19
 2 had?

3 MR. RUBIN: I can jump in here. So from my
 4 perspective, what we're seeing is that there's been a
 5 real strain on security operations teams that, again,
 6 they were set up in what's now looking like a legacy
 7 world where they're delivering their services to again
 8 an organization kind of inside an office, and then
 9 obviously that's having to shift to, you know, your
 10 entire workforce being remote and how do you maintain
 11 the right level of, you know, security operations,
 12 continuous monitoring, when your users are connecting
 13 to, you know, home networks as opposed to, you know,
 14 behind your firewall?

15 And so that's been a burden that we've seen
 16 companies struggle with is, you know, for example, we
 17 worked with an organization recently that knew they
 18 needed to upgrade their endpoint protection
 19 application and, you know, normally while they could
 20 have done that much more easily, you know, with
 21 everybody on the corporate network, it's been a
 22 struggle and a burden to try and touch employees
 23 wherever they reside. So things like that are a
 24 challenge from an operational perspective.

25 MR. CRONIN: Go ahead, Pablo.

61

1 MR. MOLINA: So I noticed sadly we were
 2 doing a little bit of a hybrid online learning, hybrid
 3 remote work, until we moved to 100 percent remote. A
 4 number of things happened. You know, first we went to
 5 all Zoom sessions. And guess what? Then we got into
 6 Zoom bombing incidents because the bad guys realized,
 7 hey, this could be fun. And some of them were not
 8 fun. Some of them were even illegal and required
 9 collaboration with the FBI to report the culprits and
 10 everything else.
 11 Then we realized that people working at home
 12 without peers on their side, multitasking, taking care
 13 of their children. Some of them I imagine they
 14 started drinking at 10:00 a.m. in the morning based on
 15 some of their reactions and the things they did of
 16 sending gift cards or small things like that. People
 17 were tired. They were afraid reading the news and
 18 everything else.
 19 So I would say that people who are known for
 20 good critical thinking, sometimes they were suspending
 21 their critical thinking. So they brought us more
 22 security incidents than we've seen before based on the
 23 human factor. And the bad guys will take advantage of
 24 the human factor because that has been done since the
 25 beginning of human beings getting together in a social

62

1 way, scamming each other out of food or tools or
 2 anything like that.
 3 So that is one part that we have seen right
 4 here. That human element that has resulted into added
 5 risk because well-trained people, people who once a
 6 year are taking our security awareness training, all
 7 of a sudden in the middle of the pandemic seem to have
 8 forgotten many of the things they had learned, many of
 9 the business practices that they have been following
 10 before.
 11 MR. CRONIN: Yeah, you're right. And I'll
 12 just cap it off quickly because there's a -- there's
 13 such a direct correlation between the way we behaved
 14 in the pandemic and the way information security has
 15 been happening.
 16 HALOCK's business has been just thrust upon
 17 with incident after incident after incident, taking on
 18 just an immense number of incidents, because of the
 19 stuff that we're talking about, people moving
 20 remotely. And they're spending less on preventive
 21 stuff. So we're not actually preventing the thing;
 22 we're paying at the end of it when we're actually
 23 getting infected. It's a very frustrating thing to
 24 have this problem happen both in your public life and
 25 in your professional life. But it's what we see

63

1 happening.
 2 Now, where it comes to organizations that
 3 just don't have the resources or organizations that
 4 must move for the sake of their consumers to do things
 5 that are more risky now, the one thing we tell people
 6 is if you cannot afford the security controls that you
 7 were affording before, you're going to have to tell
 8 people. And you may find that they're still going to
 9 engage in that risk with you.
 10 So if you're not able to meet a certain
 11 deadline and you miss a security certification because
 12 you've got -- be direct with your consumers and tell
 13 them this. And I think the Federal Trade Commission
 14 would be 100 percent behind this. You have to let the
 15 consumers know the nature of the risks they're engaged
 16 in when they're doing business with you. And it's not
 17 always an easy thing to be honest, but it's the right
 18 thing to be honest. And consumers are often very
 19 understanding when they see that something is not
 20 going right because, guess what, it's not going right
 21 everywhere.
 22 So our urge to our clients when they can't
 23 afford the preventive measure is to say just be frank
 24 with your consumers and business partners, let them
 25 know what's happening or you're going to just make

64

1 things worse for everybody.
 2 MR. JORGENSEN: We have seen a driver
 3 towards implementing solutions, though, that have been
 4 on the table for a long time, too. And I think
 5 everyone here has touched on some of those solutions.
 6 And recently, though, I think the driver to implement
 7 those solutions has gone up, and it's really raised
 8 the level of awareness up to leadership, because where
 9 you used to have to argue about multifactor
 10 authentication and somebody would say, well, you know,
 11 it's only 10 percent of our users are accessing
 12 remotely, therefore, the risk is small.
 13 Now with 100 percent of users accessing an
 14 environment remotely, they're coming back and going,
 15 oh, okay, well, I've accepted that risk for years
 16 because I thought the risk was small. Now, I
 17 understand that it really is large and I need you to
 18 implement it in the next 15 days. And suddenly
 19 they're willing to have that workforce impact and
 20 willing to deal with some of those controls that I've
 21 talked about, information governance and limiting
 22 access to data and testing those choke points and
 23 making sure that if people are accessing things
 24 remotely, what do they have access to, and making sure
 25 that they can't get to the entirety of the data set.

65

1 And adding those controls in has, I think, increased
 2 because of the pandemic response.
 3 MR. LINCICUM: Great. We are just about out
 4 of time, but I wanted to ask one last question. And
 5 if you all could take about a minute answering a
 6 fairly big question, but, you know, as best you can.
 7 We've talked about how information security
 8 is very particular for each company. It's going to
 9 have different needs. But are there some information
 10 security practices that are just so universal and so
 11 easy to implement that they should be just considered
 12 absolutely required if you were handling sensitive
 13 information like financial information?
 14 MR. CRONIN: Go ahead, Pablo.
 15 MR. MOLINA: Chris, after you, please.
 16 MR. CRONIN: Okay. Because I'm probably
 17 going to say what you were saying because you've been
 18 saying these things, too. I'm going to take a step
 19 back and say let's not talk about each control that
 20 should be expected because our risk analysis is going
 21 to show us how to apply those things differently, in
 22 different ways.
 23 What I will say is you find the security
 24 control standard that looks like it addresses the risk
 25 that you've got in your organization and apply those

66

1 controls the best you can. And where they're
 2 difficult to apply, you do a risk analysis to see
 3 whether you can accept the risk or whether there are
 4 alternative controls that provide you the security
 5 safeguards you need.
 6 So those are the two things I say are
 7 universal, a standard of care and a risk analysis
 8 where you think of yourself and others and put the
 9 risks in balance.
 10 MR. MOLINA: So I believe that cybersecurity
 11 is a little bit like human behavior in general. It
 12 works better when you follow principles. So if you do
 13 a principle-based information security, you know the
 14 old standards we've been proposing from the OECD and
 15 many other forums for many years: privacy by design,
 16 security by design, something the FTC is very strong
 17 about in enforcement, which I call hon-tegrity,
 18 honesty and integrity, meaning do as you say, say as
 19 you do so that you'll be transparent and consequential
 20 in your actions. Things like encrypt in motion,
 21 Encrypt at rest.
 22 You know, things like encrypt in motion,
 23 encrypt at rest, always there are general things. And
 24 then from there you can draw into the specific
 25 controls that tells you, you know, security awareness

67

1 for your workers and your constituents and, sure,
 2 firewalls and protect the credentials with multifactor
 3 authentication. There's a plethora of different
 4 controls. But if you act with a few guiding
 5 principles, it's going to help you align all of your
 6 efforts into some really impactful measures.
 7 MR. JORGENSEN: I think one of the
 8 challenges as we try to answer that question is -- it
 9 was embodied by Chris and Pablo's response of, hey,
 10 you have to look at the big picture. And certainly it
 11 would be easy to say, yes, multifactor authentication;
 12 yes, change your password.
 13 Something I saw as early as two weeks ago,
 14 one-two-three is not an acceptable password in 2020.
 15 But if you really scale it up for a moment and said,
 16 okay, how am I going to look at identity and access
 17 management, and so then access to what, and the data
 18 privacy and the implications of the data security and
 19 data privacy around that access becomes a focal point.
 20 So are there controls that are so basic that
 21 you should have in place? Yes, I think we've covered
 22 them here. But the problem is that those controls may
 23 change over time and it's the controls that give
 24 access to what then becomes part of that challenge.
 25 So if I have remote access into the keys to the

68

1 kingdom, then those controls that are so basic and you
 2 have to appreciate that I can't have an open cloud
 3 storage bucket or a database that's public-facing. So
 4 those are those really basic controls and security
 5 that should be in place. But it's hard to say
 6 specific for what without that risk analysis that
 7 Pablo and Chris were just talking about.
 8 MR. RUBIN: Yeah. And I agree with
 9 everything that's been said here, and that is the
 10 driving kind of basis for risk assessment. So I think
 11 instead of, like, prescriptive controls, you know,
 12 because of the changing threat landscape and all the
 13 variation in organizations, it's helpful to think of
 14 things a little bit more conceptually, which in a way
 15 -- not to kind of plug this too much, but in a way
 16 it's what the -- it seems like the FTC Safeguards Rule
 17 is trying to do when it's saying things like you have
 18 to have governance. Like, that's just a fundamental
 19 part of an information security program which, believe
 20 it or not, a lot of organizations don't do.
 21 You have to have a program, which is, again
 22 -- it sounds like basics but that's what we're talking
 23 about. You need some people that are experts to help
 24 you out, whether it's to perform the risk assessment
 25 or to perform the technical, you know, security

69

1 operations. You need to protect your sensitive
 2 information, which means you need to know where it is,
 3 what it is; you need to have identity and access
 4 management around it; you need to educate your people
 5 about what the risks are and what the threats are that
 6 your organization is facing. You need to protect your
 7 organization in an ongoing basis with ongoing
 8 monitoring, and you need to be cognizant of your
 9 third-party risk.
 10 I think those things aren't prescriptive
 11 controls and are more kind of just baseline
 12 fundamentals that will change depending on time and
 13 threats.
 14 MR. LINCICUM: It looks like maybe we lost
 15 Sam, or maybe everyone. Hopefully not. I want to --
 16 oh, everyone else seems to be there. Well, that was
 17 unfortunate for Sam but fairly well timed in that we
 18 are out of time.
 19 I really want to thank everyone for your
 20 time in both being on this panel and helping us
 21 prepare for it. It was immensely valuable. And I
 22 want to thank everyone for giving us some time
 23 watching it.
 24 We'll be taking a short break now and the
 25 next panel will be at 10:45, about information

70

1 security and smaller businesses. Thanks, very much.
 2 Have a good one.
 3 MR. JORGENSEN: Thank you.
 4 MR. CRONIN: Thank you.
 5 (Whereupon, a recess was taken from 10:32
 6 a.m. to 10:47 a.m.)
 7
 8
 9
 10
 11
 12
 13
 14
 15
 16
 17
 18
 19
 20
 21
 22
 23
 24
 25

71

1 INFORMATION SECURITY PROGRAMS AND SMALLER BUSINESSES
 2 MS. MCCARRON: Good morning. Welcome to the
 3 second panel of the GLB Safeguards Rule Workshop.
 4 This morning, we're going to be talking with five
 5 experts about information security programs and
 6 smaller businesses.
 7 I would like to introduce the five panelists
 8 who will join me this morning. If you could all
 9 please just wave or acknowledge when I introduce you.
 10 I would like to begin by introducing Rocío Baeza. She
 11 is the CEO of CyberSecurityBase. She's joining us
 12 this morning from Chicago.
 13 Next, James Crifasi. He's the COO and CTO
 14 of Redzone Technologies here in the D.C. area.
 15 Brian McManamon is the president of TECH
 16 LOCK, and he's joining us this morning from Troy,
 17 Michigan.
 18 Kiersten Todt is the managing director of
 19 the Cyber Readiness [microphone feedback].
 20 And, finally, I'd like to introduce Lee
 21 Waters, who's the IT manager of McCloskey Motors,
 22 joining us from Colorado Springs, Colorado.
 23 My name is Katherine McCarron. I'm an
 24 attorney in the Division of Privacy and Identity
 25 Protection at the Federal Trade Commission, and thank

72

1 you very much for joining us.
 2 I'd like to begin by picking up from where
 3 we left off on Panel 1, where we talked about the
 4 costs and benefits of information security programs.
 5 As part of its public comment, in the first round of
 6 the GLB Safeguards Rule's proposed -- comments about
 7 the proposed amendments, the National Automobile
 8 Dealers Association provided a technical cost study as
 9 part of its comment. It was entitled the Average Cost
 10 per U.S. Franchise Dealership, because as we discussed
 11 earlier, auto dealerships are financial institutions
 12 under the GLB Safeguards Rule and must comply with the
 13 Safeguards Rule itself.
 14 I'd like to begin with speaking with James
 15 Crifasi. James, you're an IT service provider and you
 16 did some work on this cost study. What can you tell
 17 us about the requirements the study assumed and its
 18 conclusions about the costs of those requirements?
 19 MR. CRIFASI: Sure. So Redzone Technologies
 20 helped NADA with portions of the study. NADA looked
 21 for really costs across a number of different shapes
 22 and sizes of dealerships. They also got real vendor
 23 quotes from those specific dealerships to figure out
 24 what is it currently costing them to do these
 25 safeguards; what would it cost for a new provider to

73	<p>1 do them, or for their existing provider to add the 2 level of service required.</p> <p>3 We can see from the numbers that they're 4 really quite large. And what we're noticing here is 5 that from a small/mid-sized business point of view, 6 they start becoming a little bit unaffordable here. 7 The cost structure that was used is actually quite 8 conservative. There's a couple of things that aren't 9 even considered within the study.</p> <p>10 So, for example, the need for additional 11 staff is not part of this study. In our experience, 12 in working with small businesses, there's a great deal 13 of bringing systems to a current level of operation 14 required before you could even make use of these 15 safeguards or the technologies required to adhere to 16 them.</p> <p>17 So those auxiliary costs are really not 18 within the study at all. Our belief is that based on 19 this study, really it will be probably double or 20 triple those costs to really get the value out of 21 implementing the different safeguards. I mean, it's 22 one thing to be able to say, you know, we've checked 23 the box, we put the system in place. It's another 24 thing to actually get the value out of it. 25 I know in Panel 1 that was something that</p>	75	<p>1 one of the other panelists. You know, that kind of 2 team effort is what's really important to have the 3 smaller businesses able to do that kind of qualified 4 individual task list.</p> <p>5 There's one level where, you know, there's 6 advice needed that is coming from someone experienced 7 in security, but there's another requirement for 8 enforcement. And that enforcement is really where we 9 need a team effort.</p> <p>10 What we've definitely found is that if the 11 business is not involved and this is considered an IT 12 project, the effectiveness is going to go way down. 13 And so really all of the business needs to be on board 14 with implementing these safeguards.</p> <p>15 MS. MCCARRON: Thank you very much. 16 I would like to pivot now to asking Lee 17 Waters. Lee is an IT manager at an automobile 18 dealership in Colorado Springs and he has implemented 19 the existing GLB Safeguards Rule in his business.</p> <p>20 Lee, I'd like to ask you how much would it 21 cost your dealership to implement the proposed 22 amendments to the GLB Safeguards Rule? 23 MR. WATERS: Well, we started by looking at 24 the costs for hiring outside help, the CISO and the 25 cybersecurity analyst. And we'd be looking at on</p>
74	<p>1 was talked about a lot is not just have an expensive 2 firewall or not just have an expensive audit system, 3 but actually use it and make sure it's effective and 4 useful on a daily basis.</p> <p>5 MS. MCCARRON: As a follow up, James, where 6 did you see -- when you were doing this study, where 7 did you see existing security in financial 8 institutions falling short of the proposed amendments? 9 And where were there already resources in place?</p> <p>10 For example, the current rule, the current 11 Safeguards Rule, which the automobile dealerships 12 comply with, requires financial institutions to have 13 people in charge of their programs. And so can 14 businesses use existing personnel as the qualified 15 individual responsible for the program?</p> <p>16 MR. CRIFASI: I think from what we've seen, 17 they definitely can. What is important, though, is it 18 needs to be a team effort. So not so much a specific, 19 single individual, but when we're talking about a 20 small and medium business and, you know, there might 21 be a very small IT staff or potentially almost no IT 22 staff for the business, we really need to see that 23 "qualified individual" be a mix of folks. Sometimes, 24 it's going to be someone on the operations or finance 25 side; possibly outsourced consultants such as us or</p>	76	<p>1 average in our area about \$180,000 for a chief 2 information security officer; another \$76,000 for a 3 cybersecurity analyst. If we outsourced the work that 4 these two people would do, we would still be looking 5 between \$120,000 and \$240,000 a year.</p> <p>6 On top of that, we'd have to implement 7 multifactor authentication; looking at about \$50 per 8 computer to implement something like that, or we could 9 go with an outside resource like Duo, which would cost 10 us about -- between \$3 and \$9 per user per year. And 11 with our dealership, that's about 55 users.</p> <p>12 So we also have to implement annual 13 penetration testing. If you do a search on Google, it 14 says average cost is about \$4,800. I called a local 15 cybersecurity company that I've dealt with in the 16 past. For their external test, we'd be looking at 17 \$2,160. For an internal test, which is based on the 18 number of computers we actually have, we would be 19 looking at \$7,360 per test.</p> <p>20 We would also have to update our physical 21 security. We'd be looking at about \$215,000 for extra 22 construction to enclose existing cubicles and build 23 offices for desks that are out on the showroom floor.</p> <p>24 MS. MCCARRON: Thank you, Lee, for providing 25 this detailed information.</p>

77

1 I'd like to talk about the qualified
 2 individual requirement of the proposed Safeguards
 3 Rule. Several of you have mentioned the costs of the
 4 requirement in the proposed amendment to
 5 "designate a qualified individual responsible for
 6 overseeing and implementing your information security
 7 program." That is the language of the proposed
 8 amendment. This person may be employed by you, by an
 9 affiliate or by a service provider.

10 So the intention of that proposed language,
 11 as my colleague David Lincicum mentioned earlier, was
 12 to increase accountability and to lesson the
 13 possibility that there would be gaps in responsibility
 14 between individuals.

15 So, Brian, I'd like to ask you your opinion
 16 of the costs versus the benefits of hiring a "single
 17 qualified individual" to coordinate the information
 18 security program at a small business.

19 MR. MCMANAMON: Sure, Katherine. In TECH
 20 LOCK's experience, I think first and foremost it
 21 depends on what the definition is of a qualified
 22 individual. That individual would have to go through
 23 the proper security training in order to help lead and
 24 develop a security program within the organization.
 25 In TECH LOCK's experience, most companies do

78

1 not have that qualified individual. And the reason
 2 for that is they're often -- they have a small IT
 3 staff; they're often wearing multiple hats. You know,
 4 you could be looking at an IT system administrator or
 5 an IT director or a CIO that's basically serving as
 6 that lead security person.

7 So what TECH LOCK has found that what works
 8 best is a combination of outsourcing to a managed
 9 services company. What that company can provide is
 10 that security skill set and expertise, especially in
 11 terms of potentially providing a virtual CISO role.

12 CISOs, as you heard, the average salary
 13 that's out there can range anywhere from 180K; it
 14 could be upwards of 400K. So providing that help and
 15 assistance on a strategic basis, I think, is what
 16 works best in transferring that knowledge internally.
 17 What a virtual CISO can help do is develop that
 18 security strategy and then help to implement that over
 19 time.

20 MS. MCCARRON: Lee, can I follow up with you
 21 then and ask what is the difference between what a
 22 qualified individual means for a smaller, less complex
 23 business? For example, can a small auto dealership
 24 have a less experienced person in charge of a program
 25 than a business with, say, a more complex network?

79

1 MR. WATERS: Definitely. If the dealership
 2 has any IT staff at all, they can take one of their
 3 more experienced people and they would have to do some
 4 research, maybe even call in a little bit of outside
 5 help, but somebody could definitely handle that.

6 With some of the smaller dealerships that
 7 only have, you know, maybe five people working the
 8 lot, they may not have anybody with IT experience. So
 9 they would have to go outside for help.

10 MS. MCCARRON: Thank you.

11 James, can I ask for your opinion as well?
 12 What do you see in terms of what a "single qualified
 13 individual" would mean in a small business versus a
 14 business with a larger, more complex network?

15 MR. CRIFASI: Sure. In the small financial
 16 institutions that we deal with, often the only IT
 17 staff onsite is maybe PC support or end-user support
 18 and there really is no IT management or upper level
 19 IT.

20 In those cases, we typically are working
 21 with the executive team. And what we found is that
 22 that executive team can really be the qualified
 23 person. Because at the end of the day if they have
 24 the proper advice and support or an MSSP or a virtual
 25 CISO, you know, that team is really who's going to

80

1 enforce everything and make sure that the business is
 2 adhering to the rules and the standards. Otherwise,
 3 it's just something that someone external has told
 4 them to do and no one really believes it or feels it
 5 or lives it.

6 So, in our experience, if we really involve
 7 it less as a find a single person and more as let's
 8 involve the head of finance, the head of business
 9 development, the head of operations and make that part
 10 of the team, it's a lot more effective for the smaller
 11 businesses.

12 MS. MCCARRON: Thank you.

13 Now, the proposed amendments to the
 14 Safeguards Rule permit a financial institution to
 15 bring that talent in-house and have an in-house
 16 qualified person, or that role could be filled by an
 17 affiliate or a third-party service provider.

18 Rocio Baeza and Brian McManamon are both in
 19 the business of offering information security services
 20 to smaller businesses. So I would like to begin,
 21 please, with Rocio. What can you tell us about the
 22 costs to small businesses of retaining vendors that
 23 outsource those qualified individual services? Rocio?
 24 You're on mute.

25 MS. BAEZA: All right. Can you hear me now?

81

1 MS. MCCARRON: Thank you, yeah.
 2 MS. BAEZA: Awesome. Well, first of all, I
 3 just want to say thank you so much for having me on
 4 the panel. So there are two slides that I want to
 5 share. If we can go to the first slide.
 6 So when I think of cost models being
 7 available to small businesses, so these are the three
 8 models that I see. And for context, so
 9 CyberSecurityBase is in the business of serving
 10 chief compliance officers in the fintech space, and we
 11 are specialists in the online payday lending space, so
 12 my perspective is coming from that direction. So as
 13 we're thinking about, all right, how are small
 14 businesses that don't have -- don't currently have a
 15 CISO in-house and they're not expecting to appoint one
 16 in the next two to five years, how can they possibly
 17 conform with the proposed changes?
 18 So there are three models that I would want
 19 to point these individuals to. The first model is one
 20 where an existing member of the team is wearing the
 21 CISO hat. Now, I would expect that this individual
 22 sits in the compliance space of the organization and
 23 they're bringing in internal teams. So, for example,
 24 technology teams to supplement and to help develop and
 25 implement the program. And for any areas where there

82

1 may be skill gaps, that can be supplemented with
 2 either certifications or some type of education.
 3 For the outsource model, so think of the
 4 situation where a small business is going to engage as
 5 a risk provider like CyberSecurityBase to wear the
 6 CISO hat.
 7 And the third one is going to be a hybrid
 8 approach. And I think this is going to be the best
 9 fit for small businesses. So think of the case where
 10 someone internally is accountable and is wearing the
 11 CISO hat and they are pulling in internal resources
 12 and external resources as needed. And these
 13 researchers are going to be pulled based on the
 14 preferences of the organization. Access to talent,
 15 timelines, any specific projects that have a specific
 16 deadline, and, of course, budget.
 17 So if we move on to the next slide, so we
 18 have some sample pricing for what some of these
 19 options might look like. And I've got to say, so when
 20 we're working with our clients, so they tell us that
 21 they love being able to to have a mixed and matched
 22 approach, having a hybrid approach where they may
 23 engage with us to provide say, for example, strategic
 24 direction, implementation support or outside
 25 assurance.

83

1 So what we're looking at here is this is a
 2 table that has sample pricing for service providers
 3 that are in the market today that small businesses,
 4 that fintechs can tap into and comply with the
 5 proposed changes.
 6 So we have company A, they are app sec
 7 focused. They have a security-in-the-box solution,
 8 and they have a number of offerings depending on the
 9 level of support that the organization may need. We
 10 have an MSSP that, based on the size of the
 11 organization, they have different price points.
 12 And CyberSecurityBase, so we offer the CISO
 13 service as a professional service, and we also have
 14 pricing available to fit part-time virtual CISO
 15 support. So as you can see here, we have a range of
 16 \$200 a month estimate to \$15,000 a month. And, to me,
 17 this paints a positive picture that there are
 18 different options in the marketplace today. And I
 19 expect there to be more once the proposed changes are
 20 finalized.
 21 MS. MCCARRON: Thank you very much, Rocio.
 22 Brian, I would like to ask you as well. Can
 23 you talk us through your understanding of what the
 24 different options are for smaller businesses?
 25 MR. MCMANAMON: Sure. And I think there was

84

1 a slide that I'd like to show that represents those
 2 costs. Coming from what we've just heard, TECH LOCK
 3 provides these services from both an in- and outsource
 4 prospective as well as a hybrid prospective. We do
 5 need that -- or we think it's important to have that
 6 internal skilled security resource that can help
 7 implement a lot of the elements of a security program.
 8 So what you see here is sample pricing that
 9 TECH LOCK provides to our small/medium-sized business
 10 customers, all the way from -- if you see, the range
 11 there is starting with small at 25 to 250 endpoints
 12 for \$2K to \$5K per month. A medium-sized business we
 13 would designate as 250 to 750 endpoints for a \$5K to
 14 \$15K a month; a large, 750 to 1,000 endpoints at \$15K
 15 to \$30K; and then finally a very large organization
 16 can be anywhere up to 2,500 endpoints and up to \$50K
 17 per month.
 18 The type of services that TECH LOCK
 19 provides, and if you look at the revisions to the
 20 Safeguards Rule, some of the key elements of that rule
 21 is really around continuous monitoring, being more
 22 proactive with potential threats. So some of the
 23 services that we provide that address those issues are
 24 related to vulnerability management, endpoint
 25 detection and response, network and firewall

85

1 management, log-in SIM. And what's key there is all
 2 on the back end we're providing 24/7/365 monitoring.
 3 So it's that continuous monitoring to make sure that
 4 you can not only detect those threats but also respond
 5 to them very quickly.
 6 And what TECH LOCK feels is this provides
 7 really a holistic and comprehensive view of satisfying
 8 the key elements of a strategic security program. And
 9 if you compare those costs that I just showed to the
 10 cost that a small/medium-sized business would have to
 11 pay, they brought that technology in-house, those
 12 resources and staffing in-house, you'd be looking at
 13 multiple six figures, I think, as you saw earlier in
 14 this panel.
 15 MS. MCCARRON: Thank you. Now, one of the
 16 questions that the Commission has sought feedback and
 17 comment about is the definition of a small business.
 18 And in the proposed amendments to the
 19 Safeguards Rule, the Commission has suggested that in
 20 order to reduce the burden on smaller financial
 21 institutions, the proposed amendment would contain a
 22 new section that would exempt smaller businesses from
 23 certain requirements.
 24 The exemptions would apply to financial
 25 institutions that maintain customer information

86

1 concerning fewer than 5,000 customers. Such financial
 2 institutions would not be required to have a written
 3 risk assessment. They would not be required to
 4 conduct continuous monitoring or annual penetration
 5 testing and biannual vulnerability assessment. They
 6 would not have to have a written incident response
 7 plan in place, or have a written annual report by the
 8 CISO.
 9 So, Kiersten, as a threshold matter, the
 10 Commission seeks comment on whether the use of the
 11 number of customers about whom a financial institution
 12 retains customer information is the most effective way
 13 to determine whether financial institutions should be
 14 exempted, and, if so, whether 5,000 customers is the
 15 appropriate number. So would you share with us your
 16 thoughts about the definition of a small business?
 17 MS. TODT: Sure, Katherine. Thanks very
 18 much. And thanks also for the opportunity to
 19 participate.
 20 Just to understand the position from which
 21 I'm coming, I run a nonprofit called the Cyber
 22 Readiness Institute, which works with small businesses
 23 in helping them improve their cybersecurity by
 24 focusing on human behavior.
 25 So I think there are really two questions at

87

1 play here. The first is what you asked around what
 2 the definition of a small business is for this
 3 purpose, and what that definition fails to acknowledge
 4 is that regardless of size, every small business is
 5 part of a global value chain/supply chain under the
 6 safeguard rules that we're talking about.
 7 So to make that demarcation, I think, is
 8 not actually appropriate because it doesn't allow or
 9 account for the fact that every business has a role.
 10 The challenge there, however, is that you cannot put
 11 -- if you focus so much on the technology, I'd like to
 12 go back to a couple of the points that James made,
 13 which is particularly for small businesses you have to
 14 focus on the culture. And when you don't have the
 15 resources to allocate and bring in a CISO, and I think
 16 Rocio had walked through a lot of the different
 17 versions that we can use and I think that's important,
 18 it's recognizing that small businesses have to do the
 19 basics, and a lot of that really focuses on human
 20 behavior. That ability to do the basics and to do
 21 cyber hygiene should -- no business should be -- not
 22 be accountable for doing that. Every small business
 23 should have to do that.
 24 But we also have to make sure that in
 25 providing guidelines, while we may be able to provide

88

1 very rigid guidelines for security, if small
 2 businesses are then forced to do workarounds and don't
 3 actually have the ability to follow them, that creates
 4 an -- even more of an unsafe environment.
 5 So to answer your initial question, I don't
 6 think there should be a number on this. All small
 7 businesses should be responsible for doing the basics,
 8 but we have to really focus on the culture of security
 9 and the human behavior element, particularly for small
 10 businesses that don't have the resources to allocate
 11 to some of these more technological requirements.
 12 MS. MCCARRON: So, in your opinion, is such
 13 an exemption appropriate at all, or should all
 14 financial institutions regardless of size be required
 15 to comply with all of the proposed amendments?
 16 MS. TODT: I don't think size should be a
 17 matter, but I don't think that the required amendments
 18 really are appropriate for all small businesses. So I
 19 think that all small businesses need to be held
 20 accountable, but we need to work with small businesses
 21 to help them and to provide resources that focus on
 22 human behavior.
 23 So I'll answer it in two ways that we should
 24 not -- no small businesses should be exonerated. But
 25 the rules need to be more flexible to address the

89

1 cover and the range of small businesses.
 2 MS. MCCARRON: Okay, thank you.
 3 Brian, a follow up question: How does the
 4 size of a financial institution and amount and nature
 5 of the information that they hold factor into an
 6 appropriate information security program?
 7 MR. MCMANAMON: Yeah, I would agree that,
 8 you know, just to chime in on the last question, I
 9 think there are a minimum set of standards that need
 10 to be adhered to by small businesses. The way TECH
 11 LOCK views businesses and the way we scope the work
 12 that we do is based on number of users, number of
 13 endpoints, and then also number of sites and what
 14 their processing environment looks like.
 15 So if you think about, you know, servers,
 16 workstations, laptops, the network footprint, any of
 17 those elements in an organization's environment may
 18 introduce a threat into that environment. So you have
 19 to look at that total threat landscape.
 20 From a data prospective, you know, when we
 21 do audits on, for example, PCI or high trust, we
 22 follow that data, right, all the way from the -- where
 23 it comes into the environment and to how it's
 24 protected at each step, whether it's storage or
 25 processing all the way through to the back end. So

90

1 data does come into play in terms of size.
 2 And if you were to compare, for example, to
 3 how PCI judges the size of an organization, you know,
 4 they do it based on level of transactions that a PCI
 5 data processor would process annually. So, you know,
 6 for example, over 6 million transactions, it would be
 7 designated that they would need to have an audit by an
 8 external auditor. Very small businesses would just
 9 have to go through what they call a self-assessment.
 10 But the issue that TECH LOCK has seen with those self-
 11 assessments, it's more of checking the box. Right?
 12 And that's what we're trying to avoid here. We want
 13 businesses to really go through that internal risk
 14 assessment and make sure that they are implementing
 15 the appropriate security controls for their
 16 environment.
 17 MS. MCCARRON: Lee, I'd like to follow up
 18 with you about the issue of the size of a financial
 19 institution and the nature of the information that
 20 that financial institution holds, as a factor, into
 21 the appropriate data security program that they put
 22 into place.
 23 Can you tell us from your experience whether
 24 it's the number of employees or the number of
 25 customers that you keep data about that's relevant to

91

1 to your business?
 2 MR. WATERS: Well, I don't think the type of
 3 data really makes much difference as an attacker is
 4 just going to go for something easy that he's going to
 5 get a lot of information from. So the amount of data
 6 would definitely have an influence on whether a
 7 business is even going to be attacked or not.
 8 The number of employees can also introduce
 9 other risks. The more employees you have, the greater
 10 you are at risk for either inside attacks or just
 11 social engineering. So you have to be prepared for
 12 pretty much everything from all sides.
 13 MS. MCCARRON: James, how do you view the
 14 risks of how cybersecurity events change based on the
 15 size of a financial institution?
 16 MR. CRIFASI: From our point of view, it's
 17 the point of view of the risk that changes, but we
 18 consider it pretty much equal risk. We have some
 19 small businesses we deal with that just have an
 20 enormous amount of consumer records, and so they might
 21 have a few number of employees or a few number of
 22 endpoints, but the amount of data available there is
 23 just quite vast. And so from that point of view, we
 24 would say, okay, they need to follow all of the
 25 safeguards, right? Because they just have such a

92

1 massive amount of data, they can't get away with just
 2 doing the basics.
 3 On the flip side of that, we see small
 4 businesses where really they just need to focus on the
 5 basics. I know in Panel 1 they talked a lot about
 6 doing risk assessments and assessing what data is
 7 there, where it is and how it is. And there's a point
 8 of view for a small business that says if they get
 9 hacked at all, it doesn't matter if they lose employee
 10 data, financial data, consumer data, they're probably
 11 going to go out of business.
 12 So there's a shift to me that says that when
 13 we look at a small business and we look at something
 14 like the safeguards, that doing the basics, or as
 15 Kiersten mentioned, changing the culture and making
 16 sure people are getting educated and understand
 17 security becomes more important, because really they
 18 can assume the level of risk, they can assume that at
 19 some point they will get an intrusion or malware or
 20 ransomware. And there's a lot of money that can be
 21 spent better doing proactive security against these
 22 types of attacks or cyber hygiene versus measuring a
 23 risk when really we can just assume it in most
 24 businesses, especially on the small/medium size.
 25 MS. MCCARRON: Thank you.

93

1 Kiersten, what is your view about how risks
 2 of cybersecurity events change based on the size of
 3 the financial institution?
 4 You're on mute.
 5 MS. TODT: You still do this after three
 6 months of Zoom. I still think that the smaller the
 7 business, the more impact it can have. So one of the
 8 things that one of our member organizations,
 9 Mastercard, has researched is that 56 percent of
 10 organizations can suffer a breach by a third party,
 11 meaning that there is a greater attack surface.
 12 Sixty-seven percent of small businesses fail to
 13 survive a cyber breach.
 14 And so when we look at these numbers, we
 15 understand that there is a much smaller, if any,
 16 safety net for small businesses. So the impact of a
 17 breach, the impact of an event, can be much more
 18 devastating. And that's why when we talk about
 19 prevention, we're also talking about resilience.
 20 Because what is so important -- and this is going back
 21 to your other question, why every business needs to
 22 have basic protocols in place, because you don't want
 23 a breach to be devastating and to actually take down
 24 the business.
 25 By focusing on resilience, what we're doing

94

1 then is minimizing the impact of an event, containing
 2 it, and ensuring that it causes the least amount of
 3 disruption to that small business. And so as we look
 4 at overall cybersecurity protocols, it's really
 5 critical that we both focus for small businesses on
 6 prevention and what they can do, but also helping them
 7 to respond and react, which is why instant response
 8 plans and those others elements are the basics for all
 9 small businesses to be engaged in.
 10 MS. MCCARRON: Thank you.
 11 Rocio, do you have thoughts on the risks of
 12 cybersecurity events, how that changes based on the
 13 size of the financial institution?
 14 MS. BAEZA: Sure. So I think size of a
 15 financial institution is a factor, but I don't think
 16 it's the one that we should be paying attention to. I
 17 think the ones that are better indicators for
 18 cybersecurity risk are going to be two things: the
 19 volume of consumer records that a financial
 20 institution holds and also the rate of change.
 21 So in the fintech space, it's awesome.
 22 They're using technology and data to disrupt the
 23 industry and provide services that haven't been
 24 feasible in the past. And so there's a number of
 25 integration points, right? So take the case of an

95

1 online payday lender, we should expect them to have an
 2 LMS to process loan applications, connections with
 3 data vendors, and maybe an outsourced consumer
 4 function, payment collection processing activities.
 5 And then there's also services and IT systems that the
 6 corporate teams are using to leverage the data and the
 7 technology to better serve the consumer.
 8 So, to me, because we have this web of
 9 applications and systems both managed in-house and
 10 outsourced, every time there is a change to any of
 11 these environments, that is creating additional risk.
 12 And that's elevated as we're seeing if the institution
 13 is processing large volumes of consumer data.
 14 So I think size of the financial institution
 15 is a factor. I think the more critical ones are the
 16 volume of consumer data that they hold and the rate of
 17 change within their data processing environment.
 18 MS. MCCARRON: Okay, thank you.
 19 I'd like to move to a new topic, which is
 20 the requirement in the proposed amendment that there
 21 be reporting to the board of directors. And I'd like
 22 to talk about this from the lens of a smaller
 23 business.
 24 The proposed amendment would require the
 25 CISO or the qualified individual to record in writing

96

1 at least annually to the financial institution's board
 2 of directors or the equivalent governing body
 3 regarding the following information: the overall
 4 status of the information security program and the
 5 financial institution's compliance with the Safeguards
 6 Rule and material matters related to the information
 7 security program addressing such risks such as risk
 8 assessment, risk management and control decisions,
 9 service provider arrangements, results of testing,
 10 security events or violations, and management's
 11 responses thereto, and recommendations for changes to
 12 the information security program.
 13 So for for financial institutions that do
 14 not have a board of directors or equivalent, the CISO
 15 must make the report to a senior official responsible
 16 for the financial institution's information security
 17 program.
 18 Kiersten, the Commission requests comment on
 19 whether the burden of this risk reporting requirement
 20 outweighs the benefits of, number one, having the
 21 governing body engaged in and informed about the state
 22 of the financial institution's information
 23 security program, and, two, creating accountability
 24 for the CISO. So can you comment on that? And, also,
 25 if you think the written requirement should have other

97

1 requirements, please let us know.
 2 MS. TODT: So I certainly think engagement
 3 with any sort of senior leadership, whether it's a
 4 governing body like a board or a senior executive on
 5 security, is critical because this is not, as was
 6 mentioned earlier, security, cybersecurity, should not
 7 be restricted to one individual, to an IT department,
 8 to an IT person. It really is now the responsibility
 9 and accountability of every individual within an
 10 organization to have an understanding of his or her
 11 role in security.
 12 So creating that culture, again, and having
 13 that reporting requirement makes sense. But I would
 14 like to adjust that word around reporting. It should
 15 be a conversation. It should be a discussion and
 16 ongoing -- I would argue that it should happen more
 17 than once a year because this -- while there is an
 18 accountability within an individual, again, the
 19 organization has accountability.
 20 So we're discussing this with a senior
 21 executive. That senior executive has accountability
 22 for the security of the organization. We've seen a
 23 lot at the senior level where -- we saw it in the
 24 Federal Government with the OPM breach where the
 25 director at the time said it was no one's

98

1 responsibility.
 2 What we have to get to in changing that
 3 culture is that it's actually everybody's
 4 responsibility. And so having requirements to update
 5 on what's going on on the number of breaches, on how
 6 things are being responded to, where the challenges
 7 are, that should be an ongoing discussion. And if the
 8 catalyst for that is a reporting requirement, I think
 9 there could be value in that, but it is not just
 10 a static written report.
 11 I would assert that it has to be a
 12 discussion. And it's not a one-way discussion; that
 13 it is about getting leadership involved and that
 14 hopefully there is a relationship between the CISO and
 15 the board or -- and the senior executive that allows
 16 for improvement, that allows for adjustment and
 17 evolution, because with cyber risk management, the key
 18 here and the priority
 19 should always be agility and flexibility to evolve
 20 with the threat.
 21 So the concern sometimes is when you have
 22 compliance -- most of the time when you have
 23 compliance requirements, they often can't keep up with
 24 where the threat is going. And that's why risk
 25 management, when it comes to an organization of any

99

1 size, is critical.
 2 MS. MCCARRON: I'd like to ask a followup to
 3 Rocio on this one, which is speaking of the
 4 communication between the CISO and the board, should
 5 the board have to certify compliance with the rule?
 6 MS. BAEZA: So I think that an annual report
 7 to the board and then having the board report or
 8 perform some type of certification, that can be used
 9 as a way to ensure organizational accountability and
 10 also accountability for the CISO. But I think that if
 11 either of these two items, the annual report or the
 12 certification, if they don't have the proper
 13 guardrails I can see it quickly turning into a
 14 burdensome administrative test that outweighs the
 15 benefit of what we're trying to accomplish here.
 16 So I think that in order to have effective
 17 mechanisms, let's talk about the annual report first.
 18 So if we're setting expectations for a 40-page
 19 document to be presented to the board on an annual
 20 basis, that's not going to be effective. Instead, if
 21 we consider using a one-pager that summarizes the
 22 items that are in the proposed changes, things like
 23 the status of the program, identified high risks,
 24 previous management decisions to identify the high
 25 risks, and using that to funnel information up to the

100

1 board so that they can say, yes, we're comfortable
 2 with the program or, no, we're not comfortable and
 3 being able to articulate between the board and the
 4 CISO what that comfort level is, what that risk
 5 tolerance is, I think that can be a great way of
 6 raising organizational accountability and also
 7 accountability for the CISO.
 8 Now, if you think about the certification, I
 9 think that if the certification piece isn't worded
 10 carefully, it's going to be an administrative
 11 burdensome task. So if the question -- if it's one
 12 question that someone from the organization has to
 13 submit so you can comply with the Safeguards Rule, do
 14 you comply with the privacy rule, that's a very
 15 generic question. So we have to be very specific.
 16 Some examples are instead of asking a very
 17 broad, generic question, let's get into specifics. So
 18 on the risk assessment side, the question -- so these
 19 would be yes-or-no questions. Do you have a written
 20 risk assessment, yes or no; when was it last
 21 completed; what's that date; when is the next
 22 scheduled risk assessment scheduled for; very good
 23 specifics.
 24 The thing about the case of a third-party
 25 vendor, there's an expectation to oversee service

101	<p>1 providers, making sure that they can develop and</p> <p>2 maintain safeguards. Well, there's going to be very</p> <p>3 concrete questions. Do you have third-party data</p> <p>4 inventory? When was it last reviewed? When are you</p> <p>5 going to review it next?</p> <p>6 And by having a different structure around</p> <p>7 the certification and also the annual report</p> <p>8 requirement, they can set up guardrails so that the</p> <p>9 organization is providing meaningful information.</p> <p>10 It's very specific. And I think that that will be a</p> <p>11 more effective approach of raising organizational and</p> <p>12 CISO accountability.</p> <p>13 MS. MCCARRON: Thank you very much.</p> <p>14 I'd now like to turn to two of the</p> <p>15 requirements of the proposed Safeguards Rule that are</p> <p>16 specific to the technologies or the types of</p> <p>17 information security protocols that are put in place.</p> <p>18 The first one is multifactor authentication.</p> <p>19 The proposed amendment would require financial</p> <p>20 institutions to implement multifactor authentication</p> <p>21 for any individual accessing customer information.</p> <p>22 Multifactor authentication, according to the proposed</p> <p>23 amendment, shall be utilized for any individual access</p> <p>24 in your internal networks that contain customer</p> <p>25 information unless your qualified individual or CISO</p>	103	<p>1 application policy enforcements. And then you can</p> <p>2 implement single sign-on for some, their access to</p> <p>3 internal corporate resources.</p> <p>4 MS. MCCARRON: Thank you very much for that</p> <p>5 information.</p> <p>6 James, I'd like to ask you as well for your</p> <p>7 thoughts on the proposed amendments requirement that</p> <p>8 financial institutions shall use multifactor</p> <p>9 authentication.</p> <p>10 MR. CRIFASI: Our point of view is we fully</p> <p>11 support multifactor as well. When we're pulled into</p> <p>12 an environment that has had some kind of security</p> <p>13 incident or data loss or ACH wire transfer fraud, so</p> <p>14 far in the last, say, 12 to 18 months every single one</p> <p>15 would have been stopped by having basic multifactor</p> <p>16 authentication.</p> <p>17 So from our point of view, it's a good basic</p> <p>18 business practice at this point regardless of the</p> <p>19 Safeguard Rules or PCI or any other requirement. It's</p> <p>20 just a good business practice to have, just to protect</p> <p>21 the internal information as much as it is to protect</p> <p>22 the company's own internal information as much as it</p> <p>23 is to protect their consumer information.</p> <p>24 I think the one thing that we see that</p> <p>25 becomes an issue is, you now, simply buying a</p>
102	<p>1 has approved in writing the use of a reasonably</p> <p>2 equivalent or more secure access control.</p> <p>3 Brian, I'd like to ask you for your comments</p> <p>4 on this approach to requiring MFA for any individual</p> <p>5 accessing customer information in an internal network.</p> <p>6 MR. MCMANAMON: Sure. Number one, you know,</p> <p>7 TECH LOCK fully supports this requirement. It is</p> <p>8 absolutely critical that organizations have</p> <p>9 multifactor authentication in place for accessing</p> <p>10 their systems or any of their applications.</p> <p>11 To support that, TECH LOCK has implemented</p> <p>12 MFA for a number of our small/medium-sized business</p> <p>13 customers. The product that we normally use and we</p> <p>14 resell is Duo. So what I've done is pulled some</p> <p>15 pricing from Duo's website just to get an idea of what</p> <p>16 it would cost a SMB to implement.</p> <p>17 As you can see there, there's four different</p> <p>18 categories of cost all the way from free for up to 10</p> <p>19 users to \$3 per month. And what that adds is some</p> <p>20 additional security policy checks. \$6 per user per</p> <p>21 month is the most recommended that has more robust</p> <p>22 device trust checks in place; more robust policy</p> <p>23 enforcement, and then all the way to \$9 per use per</p> <p>24 month. That's their premium subscription that has the</p> <p>25 most robust device trust checks. It also provides</p>	104	<p>1 multifactor doesn't really give you a solution there</p> <p>2 because you have outsourced dealer management systems</p> <p>3 or loan management systems and you need to make sure</p> <p>4 the multifactor will actually take care of all of the</p> <p>5 service providers as well as remote access into your</p> <p>6 environment.</p> <p>7 So I think flexibility there is really</p> <p>8 important. But at the same time, the definition</p> <p>9 really needs to encompass all of those kind of</p> <p>10 auxiliary and external providers, some of which we</p> <p>11 know from helping a lot of customers, they won't</p> <p>12 support it. You know, the dealer management system or</p> <p>13 associate management system, or core banking system,</p> <p>14 they won't support the multifactor.</p> <p>15 And so we, as security technologists, we</p> <p>16 have to come up with an alternative method to secure</p> <p>17 that high-risk area. And it is available, it is</p> <p>18 possible, it's things that can easily be done. Those</p> <p>19 service providers don't always like it, but it's a lot</p> <p>20 cheaper than, let's say, telling a small business go</p> <p>21 change out the dealer management system that you've</p> <p>22 used for the last 20 years. The cost on that is going</p> <p>23 to be much more than that business can, you know,</p> <p>24 adapt to.</p> <p>25 So I think multifactor is great, but we need</p>

105

1 to really consider those third parties and service
 2 providers in scope of that requirement.
 3 MS. MCCARRON: A good point, thank you.
 4 Now I'd like to turn to encryption, which is
 5 the other specific callout in the proposed Safeguards
 6 Rule -- amendment to the proposed Safeguards Rule.
 7 The proposed amendment would require
 8 financial institutions to protect by encryption all
 9 customer information held or transmitted by you both
 10 in transit, over external networks and at rest.
 11 To the extent that a financial institution
 12 determines that encryption of customer information
 13 either in transit, over external networks or at rest
 14 is infeasible, the financial institution may instead
 15 secure such customer information using effective
 16 alternative compensating controls reviewed and
 17 approved by the qualified individual or CISO.
 18 So, Rocio, I'd like to begin with you,
 19 please. Could you please share with us your thoughts
 20 about this requirement of encryption both in transit
 21 or at rest.
 22 MS. BAEZA: So, I'm a big fan of this
 23 specification. So as a data privacy advocate, as a
 24 provider of information security services, I welcome
 25 the changes. I think that there is room for

106

1 misinterpretation by an untrained professional that
 2 might be tasked with implementing this.
 3 So, take, for example, if I were to ask a
 4 CEO or a chief compliance officer, does your company
 5 encrypt consumer data, they'll probably say yes. If
 6 you ask that question to a system administrator or a
 7 software developer, they're going to be asking -- they
 8 should ask -- what environment are you referring to,
 9 what systems are we talking about, and then are we
 10 talking about data in transit or data at rest. Data
 11 in transit, the encryption of data in transit has been
 12 standard. There's no -- there's no pushback with
 13 that.
 14 The pushback that I tend to see from service
 15 providers and partners is when we're talking about
 16 encrypting data at rest. And I think that the
 17 specificity is important so that whenever we're having
 18 conversations about encryption, regardless of what our
 19 technical background is and what our idea is around
 20 encryption -- the encryption of data that we can't
 21 see, I think we're going to get to a path where
 22 there's more consistent application and understanding
 23 of the requirements, and that's what will ultimately
 24 lead to comprehensive application of IT security
 25 controls in the environment.

107

1 In the online payday lending space, so we
 2 have a number of players, right, a number of systems.
 3 And the question around encryption, it really applies
 4 to every single path that you can think of where a
 5 system is talking to another system, where data is
 6 going back and forth from one vendor to another or
 7 where data is going back and forth from a human to a
 8 human.
 9 So the only way that this proposed change
 10 can be effective is if there's particular language
 11 to make sure that we're expecting this to be
 12 comprehensive; not just the critical application that
 13 the organization relies on but the whole data
 14 processing environment.
 15 MS. MCCARRON: Thank you.
 16 James, I'd also like to ask for your view on
 17 the encryption requirement.
 18 MR. CRIFASI: So I think specificity is
 19 really the key there of what data are we talking
 20 about, where, and how you want to encrypt it. So as
 21 an example, there was a study that said three-quarters
 22 of all phishing sites operate under SSL. So that's
 23 encryption in motion.
 24 And in doing that, they all hide from all
 25 the great security stuff that we like to give people

108

1 and that everyone thinks is good, basic cyber hygiene.
 2 So it's a good example of how encryption in motion can
 3 be completely misused.
 4 We have a small insurance company we're
 5 working with right now who their service provider
 6 misunderstood that and they're now trying to over-
 7 encrypt, I would say, the communication between their
 8 servers and their computers that are all sitting right
 9 next to each other. As a result of what they're
 10 trying to do, though, it is now invalidating three or
 11 four different levels of security that used to be able
 12 to see and do something about the data, and now it
 13 can't because it's hidden in this encryption tunnel.
 14 And so for us, while we like the idea of
 15 encryption at rest and in motion, it really has to be
 16 well defined and it needs to be defined to the point
 17 where, you know, folks like us don't have to explain
 18 to people what does it mean, how does it work and what
 19 does it look like. It needs to be very, very detail-
 20 oriented in terms of we're talking about information
 21 that's perhaps not in a secure environment, or to
 22 Rocio's point, the system interaction is really a key
 23 place. But we have to keep in mind, the more we
 24 encrypt, the more we rob visibility and purview from
 25 our security systems that might actually reach out and

109

1 take action.
 2 So at one point we're encrypting it, but at
 3 the other point we're potentially stopping our DLP
 4 from blocking that from getting out of the
 5 environment. And I think that's a key point of
 6 contention there between a desire for encryption and a
 7 desire to actually have proactive security that's able
 8 to do something useful. So specificity, to me, is
 9 really required in that rule before it should be
 10 really applicable.
 11 MS. MCCARRON: Okay, thank you. So we have
 12 about 10 minutes left. We have a question that has
 13 come in from the audience which I'd like to pose, and
 14 then whoever would like to answer this just please
 15 raise your hand and go for it. And then after that, I
 16 would like to have some wrap-up thoughts from all five
 17 of you.
 18 Okay. So the question from the audience is
 19 small- to medium-sized entities have diverse
 20 management structures and often take a team approach
 21 to security management. Are there alternatives to
 22 naming a single responsible individual and/or annual
 23 reporting to the Board that would help establish clear
 24 lines of responsibility and accountability among the
 25 team required to lead security?

110

1 So they're looking for your thoughts. And,
 2 Kiersten, I'd like to have your thoughts, please.
 3 What are the alternatives to a single responsible
 4 individual and/or reporting to the board that would
 5 achieve the goals of responsibility and
 6 accountability.
 7 MS. TODT: I think it's a great question
 8 because it really gets at this issue of, in a perfect
 9 world it would be wonderful to be able to identify a
 10 CISO for every small business to say all of the
 11 responsibility for cybersecurity rests within this
 12 individual and everyone can go about and do what
 13 they've been doing. But that's not really the reality
 14 that we live in anymore. The idea, again, that every
 15 employee has this responsibility. And I think a team
 16 approach particularly for smaller businesses is what
 17 is more viable.
 18 Again, we don't want to create rules and
 19 regulations that do not respect or recognize the
 20 challenges of these small business environments. So
 21 we're not actually helping the small businesses but
 22 we're challenging them to do more with limited
 23 resources.
 24 And so by creating a team, it's where you
 25 have to then identify and articulate specific

111

1 responsibilities to individuals that come together.
 2 And I think one of the key advantages to this type of
 3 approach is it does create that culture of everybody
 4 has a role within the organization, whether it's
 5 toward the Safeguard Rules, but I would argue it
 6 should just be for the basics in cybersecurity first.
 7 Then you are creating that culture because you have
 8 the responsibilities distributed across the
 9 organization.
 10 And as far as the accounting requirements,
 11 you always want to make sure that you are exchanging
 12 with your leadership, whomever that is. And
 13 oftentimes in small businesses we see that a leader
 14 can have multiple responsibilities. But the idea here
 15 is to have that exchange of information so that there
 16 is an evolving sense and growth toward a more cyber-
 17 secure environment.
 18 MS. MCCARRON: Okay, thank you.
 19 And then one last question from the
 20 audience. How does it, or should it, change the
 21 analysis of the cost and benefits of a vendor
 22 relationship if the financial institution must address
 23 multiple legal and regulatory regimes?
 24 Rocio?
 25 MS. BAEZA: The way we do that is by

112

1 harmonizing. And it's going to take work and it's
 2 going to take resources and manpower. So many
 3 fintechs have this challenge. They operate in
 4 different states. They are subject to state-specific
 5 law that are a lot industry-specific expectations
 6 around security. For example, PCI DSS.
 7 MS. MCCARRON: Mm-hmm.
 8 MS. BAEZA: The only way that you can be
 9 comprehensive in meeting your security requirements
 10 across the board is through a process of harmonizing
 11 what all the requirements are. And that takes work
 12 and effort and resources. And it's an important job
 13 that has to be carried out. That's the only way that
 14 you can do that.
 15 MS. MCCARRON: Okay, thank you.
 16 So now I'd like to go to the final question.
 17 I'd like to do a speed round of your thoughts on the
 18 proposed amendments to the Safeguards Rule from the
 19 perspective of a small business.
 20 So let me start with James. James, could
 21 you tell us what -- from the perspective of someone
 22 who works with small businesses, what do you like
 23 about the proposed amendments and what do you think
 24 you don't like or that have too many costs? Thank
 25 you.

113

1 MR. CRIFASI: So, obviously multifactor
 2 authentication. We like the fact that it's in there
 3 and it's universal. We strongly believe in that. I
 4 think from the point of view of things we don't like
 5 about it, the written requirements, what we don't like
 6 about that isn't that there are written requirements.
 7 What we don't like about it is that it robs people of
 8 the ability to interact.
 9 And so as an example when we talk about
 10 having one individual that's responsible, it kind of
 11 implies that everybody else is no longer responsible
 12 because you found one person who is now the scapegoat.
 13 And so what we find in the small businesses if we go
 14 in and we read someone's board report and it's 40
 15 pages of gobbledeygook about how they compare against
 16 all of these different things that they need to do for
 17 different states and we look it, it's very bloodless.
 18 It's very political. There's no material in there to
 19 actually effect change.
 20 What we find works a lot better is to have
 21 that be an interactive discussion and actually open it
 22 to be able to talk about what are people doing well,
 23 what are they doing poorly, and how can we change
 24 that. And I think that brings them more into a
 25 culture of effecting change from a security point of

114

1 view. It gets everybody enlisted with it. And so
 2 from the safeguards statement, you know, I wish it was
 3 a little bit more oriented in that manner.
 4 MS. MCCARRON: Okay, thank you.
 5 Brian, may I turn to you next for your --
 6 speed round of your thoughts?
 7 MR. MCMANAMON: Sure. Yeah, and I'm going
 8 to talk more about, you know, what I like versus what
 9 I dislike. I think the proposed changes are the
 10 minimum necessary to have an effective security
 11 program in place. And really starting with the annual
 12 risk assessment, I think that's a great place to start
 13 for small/medium-sized business, really understand the
 14 risks. And we've heard about that in these panels
 15 around people, process and technology and really
 16 understanding what that threat environment looks like
 17 for that particular business.
 18 We need to get beyond the traditional
 19 checklists that are out there and really create a
 20 flexible and adaptive security program. And the
 21 reason for that is because the hackers aren't
 22 sleeping. Right? They're constantly changing their
 23 methods and businesses, and their security controls
 24 need to change with those hackers' methods.
 25 More specifically, I'm in agreement with the

115

1 implementation of controls around continuous
 2 monitoring and penetration testing. I think being
 3 proactive to those threats is critical. And then
 4 moving towards more of a maturity model is important
 5 for SMBs. That's what we're seeing from some of the
 6 scams that are out there from PCI to HITRUST, the
 7 upcoming Department of Defense cybersecurity maturity
 8 model. So really starting with that basic security
 9 strategy and then continuing to mature that over time
 10 is what will make SMBs more secure.
 11 MS. MCCARRON: Thank you, Brian.
 12 Rocio, I'd like to turn to you next for your
 13 concluding thoughts on the proposed amendment.
 14 MS. BAEZA: Absolutely. So there's -- my
 15 favorite part is the requirement for a risk
 16 assessment. So the expectation that it's written and
 17 that it serves as a foundation for the information
 18 security program.
 19 Two things that I don't like, I'm not a big
 20 fan of, one, I think it's missing -- the proposed
 21 changes are missing foundational elements that need
 22 to be in place in order to be able to build an
 23 effective information security program.
 24 And I think James and Kiersten alluded to
 25 this with the importance of having basics and being

116

1 specific of what data we're talking about and where.
 2 So the basics that I'm referring to are expectations
 3 around having data asset inventory, a data inventory,
 4 a third-party vendor inventory, a data flow diagram.
 5 Like, we have to be very specific with what we're
 6 talking about. What data do we hold, where is it
 7 coming, where is it going? And I would love to see
 8 that be integrated either as part of the risk
 9 assessment requirements or as a foundational step that
 10 is -- that the risk assessment points to.
 11 The other item that I'm not a fan of is the
 12 weak position that small businesses have as it relates
 13 to engaging service providers. So fintechs are able
 14 to move very fast because they're able to partner up
 15 with different third-party vendors to fulfill very
 16 specific options. But these third-party vendors have
 17 very canned terms of use. We're seeing less and less
 18 negotiations of agreements and more of this is our
 19 canned agreement, take it or leave it.
 20 And, like, if you look at the liability
 21 limitations sections, it's right there. They're
 22 wanting not to accept responsibility, share
 23 responsibility for any security events that happen in
 24 the environment that they're making available. And,
 25 to me, that's a concern.

117

1 MS. MCCARRON: Thank you very much.
 2 Kiersten, may I have your concluding
 3 thoughts?
 4 MS. TODT: Thank you. So I think some of
 5 the key points that are positive are focusing on
 6 things like multifactor authentication. I believe
 7 that right now multifactor authentication should be a
 8 default. And my hope for something like the Safeguard
 9 Rule that mandates multifactor is that it now starts
 10 to encourage those companies that can offer it and
 11 make it a default but don't and leave it up to the
 12 user to choose to do MFA that you start to see
 13 incentives in the actual workspace and across industry
 14 for doing so. And I think that could be a very
 15 positive output from something like this.
 16 The debate and the discussion we had on MFA
 17 versus encryption, I think, highlights why those two
 18 are not the same. And so mandating both of those is a
 19 very different -- it's apples and oranges. And so I
 20 don't need to repeat the conversation around
 21 encryption, but I think it is not -- they can't really
 22 be bucketed together and so we really have to look
 23 more closely at what we're asking small businesses to
 24 do.
 25 The other piece is that a lot of what we've

118

1 talked about requires an outsourcing. And when we do
 2 that, then we have to really be able to help small
 3 businesses monitor and work with third-party vendors
 4 and outsourcing requirements to know what they should
 5 be looking for and what's required of those third-
 6 party -- those third-party vendors.
 7 I mentioned earlier that 56 percent of our
 8 organizations suffer breaches caused by third-party
 9 vendors. So it's just enough to say, okay, if you
 10 can't do it in-house, then you should outsource it.
 11 We have to really provide that guidance and that
 12 specificity.
 13 Now, to what I don't like, I think this is
 14 -- it's an interesting conversation that we've had
 15 because I know there's been support for this is great
 16 because it starts with a baseline set of requirements.
 17 I would assert, however, that I think that baseline is
 18 still very high for small businesses. I don't think
 19 it's actually at the ground level. I think that we're
 20 assuming that small businesses have a lot more
 21 resources than they have. And my concern there is
 22 that we then get into a checklist, and then you start
 23 to see noncompliance and you start to see costs for
 24 small businesses being driven very high in order to
 25 comply to all these requirements. And that affects

119

1 their competition.
 2 And if we ask small businesses to do too
 3 many things, we run the risk of doing a lot of things
 4 not great and not really doing the basics right. And
 5 so I think going, again, to the drum that I've been
 6 beating in all of this is we really have to focus on
 7 the human behavior of the whole organization,
 8 getting those basics integrated and ensuring that by
 9 having a qualified individual that does not delegate
 10 and distribute and then relegate all authority and
 11 responsibility for cybersecurity.
 12 We have to get out of the mindset that there
 13 is an individual responsible for security within an
 14 organization and get to that place while there might
 15 be somebody who's responsible for overseeing it, every
 16 individual within an organization has that
 17 responsibility.
 18 MS. MCCARRON: Thank you very much.
 19 Lee, I would like to give you the last word.
 20 Can we have your thoughts, please, on the proposed
 21 amendment?
 22 MR. WATERS: I like the fact that we are
 23 addressing the security. But we need to also be
 24 careful not to overregulate it. Now, the smaller
 25 businesses, they can do a lot with the resources they

120

1 have, but when you start piling on too much and they
 2 have to start hiring outside businesses, third-party
 3 vendors or hiring overpaid security experts to handle
 4 something that's been regulated, it starts affecting
 5 consumer prices; it starts affecting the small
 6 business profit margins, and it's just not good for
 7 anybody. So we just need to find a balance here.
 8 MS. MCCARRON: Very good. Well, thank you.
 9 It looks like we are out of time. I want to thank all
 10 of you for our time this morning. And thank you for
 11 sharing your perspectives and your expertise. We're
 12 going to take a break now and we'll be back with Panel
 13 3 in a moment.
 14 (Whereupon, a recess was taken from 11:49
 15 a.m. to 1:01 p.m.)
 16
 17
 18
 19
 20
 21
 22
 23
 24
 25

121

1 CONTINUOUS MONITORING, PENETRATION, AND VULNERABILITY
 2 TESTING
 3 MR. IGLESIAS: Good afternoon and welcome
 4 back to the FTC's workshop on the GLB rule. My name
 5 is Alex Iglesias and I'm an IT specialist at the FTC,
 6 and I will be moderating this panel on continuous
 7 monitoring, penetration testing and vulnerability
 8 testing.
 9 Joining me on this panel are Thomas Dugas,
 10 who is the assistant vice president and chief
 11 information security officer and an adjunct faculty
 12 member at Duquesne University; Fredrick Lee, who goes
 13 by Flee, who is the chief information security officer
 14 at Gusto; Scott Wallace, who is a penetration tester
 15 at the Department of Homeland Security; and Nicholas
 16 Weaver, who is a researcher at the International
 17 Computer Science Institute and a lecturer in computer
 18 science at UC Berkeley.
 19 This panel is going to discuss the proposed
 20 changes to the GLB Safeguards Rule related to
 21 continuous monitoring, vulnerability testing,
 22 penetration testing.
 23 As David discussed earlier, the proposed
 24 rule would require information systems to include
 25 audit trails, to detect and respond to security

122

1 events. Second, the proposed rule would require
 2 policies and procedures to monitor the activities of
 3 authorized users and to detect unauthorized access,
 4 use of or tampering with customer information.
 5 Lastly, the proposed rule are continuous monitoring or
 6 periodic penetration testing and vulnerability
 7 assessment, whereas penetration testing would be
 8 conducted annually and vulnerability testing would be
 9 biannual.
 10 I would note if you have any questions
 11 during this panel, please feel free to email them to
 12 safeguardsworkshop2020@FTC.gov.
 13 To get us started, I'll ask Tom, what is
 14 continuous monitoring and can businesses and other
 15 institutions big and small reasonably be expected to
 16 implement continuous monitoring.
 17 MR. DUGAS: Thanks, Alex. And thanks for
 18 having me as part of the workshop and on the panel.
 19 So continuous monitoring is the ability to see and
 20 react to activity within your computing environment
 21 based on logging and log aggregation. The analysis of
 22 those logs provides us the ability to take a look at
 23 what we need to do to react or protect our computing
 24 environments to reduce risks related to incidents and
 25 breaches.

123

1 That continuous monitoring could be done
 2 with systems and services or polls, or it can be done
 3 manually. While these services are also very
 4 valuable, part of the challenge is that it can also be
 5 very costly. For example, you know, one of the
 6 sessions this morning talked a little bit about the
 7 fact that for, you know, a 3,000-plus endpoint
 8 environment, it would be about \$50,000 a month for a
 9 university like Duquesne, for example, which is kind
 10 of a small/mid-sized university. It would be about
 11 \$600,000 a year in expense in that consideration.
 12 Universities are so expensive in these
 13 considerations because we have a lot of data.
 14 Duquesne itself has about 9,000 students. And we act
 15 as both an ISP to those students who live and work
 16 here on campus and also basically serve our
 17 institution in the businesses that we actually run.
 18 We almost have, you know, 1,800 employees as well that
 19 are working to support our institution and our
 20 mission.
 21 So being able to continuously monitor that
 22 entire network can cost hundreds and hundreds of
 23 thousands of dollars. And we need to make sure
 24 because those are based on ingestion costs in a lot of
 25 cases.

124

1 Just as a quick analysis based on retail
 2 costs for a tool like Splunk, for example, we have
 3 about 200-gig-plus in ingestion a day. And that would
 4 probably cost us about, you know, \$600 per gigabyte
 5 annually. So that can be quite expensive when you get
 6 to that consideration when you look at something like
 7 that. It would be about \$120,000-plus for a
 8 university like ours.
 9 So we need to continue to keep an eye on
 10 those costs and certainly need to make sure that we
 11 have the dedicated security staff to manage them. So
 12 it's certainly important. I think it's very valuable,
 13 but it's also something we need to keep an eye on to
 14 make affordable as well.
 15 MR. IGLESIAS: Great. Thanks, Tom.
 16 Nick, do you have anything to add on the
 17 costs, benefits or implementation of continuous
 18 monitoring?
 19 MR. WEAVER: Yes. So when things go wrong,
 20 you want to know what happened. And the whole point
 21 of continuous monitoring of systems and logging all
 22 that information is so that when something does go
 23 wrong, you can ask what happened; what got
 24 compromised; what did not. And there are -- there's
 25 an unfortunate tradeoff here. There's a lot of tools

125	<p>1 that are actually really cheap for this.</p> <p>2 So for network monitoring, there's the Zeek</p> <p>3 network monitor. For monitoring end hosts, per se,</p> <p>4 you've got Syslog, Linux and Sysmon on Windows, and</p> <p>5 these both support remote log-in. You've got Nessus</p> <p>6 to inventory your network and know what's on it.</p> <p>7 But to use those tools, you need experienced</p> <p>8 personnel. So you've got basically a tradeoff here.</p> <p>9 If you're outsourcing the work, you're spending a</p> <p>10 fortune. If you're insourcing the work, you aren't</p> <p>11 necessarily spending a fortune because if you're the</p> <p>12 system administrator, you want this information</p> <p>13 anyway. You want to know what's on your network. You</p> <p>14 want to be able to check that everything is working</p> <p>15 right. And the logging facilities are just as useful</p> <p>16 for debugging incident response. But there's a</p> <p>17 general shortage of good personnel in this space and</p> <p>18 they aren't cheap.</p> <p>19 MR. IGLESIAS: Nick, do you think those are</p> <p>20 accessible to smaller businesses and smaller</p> <p>21 institutions?</p> <p>22 MR. WEAVER: It depends. So if you're a</p> <p>23 small institution but have one or two good experts,</p> <p>24 you're in good shape. So like at ICSI, we're a small</p> <p>25 outfit but we have a really good system administration</p>	127	<p>1 staff, either outsource or in-house, or even in some</p> <p>2 cases automated tools act like an actual attacker.</p> <p>3 Obviously these are meant to be somewhat benign</p> <p>4 attacks. But the goal is to actually really see how</p> <p>5 severe a vulnerability could be if exploited, to help</p> <p>6 give a group an understanding about, you know, what</p> <p>7 are the issues to fix and also what are the priorities</p> <p>8 of the issues.</p> <p>9 So, you know, when you do a pen test, you</p> <p>10 also are not only classifying the potential exploits</p> <p>11 or potential defects there but essentially also how</p> <p>12 severe those things are.</p> <p>13 With regards to, like, how and where that</p> <p>14 actually fits into the ecosystem, it really is meant</p> <p>15 to be almost like a sanity check of what the system</p> <p>16 looks like from an attacker's perspective. Something</p> <p>17 to actually keep in mind, though, is that a pen test</p> <p>18 is not, like, completely comprehensive. And that's</p> <p>19 actually one of the weaknesses of a penetration test,</p> <p>20 is kind of like this notion of coverage. How many</p> <p>21 different parts of the system were you able to test;</p> <p>22 how effective were your tests?</p> <p>23 So just because a pen test doesn't have a</p> <p>24 lot of issues, per se, does not necessarily mean that</p> <p>25 a system is secure but it does give some confidence of</p>
126	<p>1 team of two and a network security incident response</p> <p>2 team that consists of multiple researchers who</p> <p>3 specialize in this.</p> <p>4 But that's -- we're able to do that because</p> <p>5 we have the personnel already in place. And so it's</p> <p>6 how good and creative and motivated is your system</p> <p>7 administration staff.</p> <p>8 MR. IGLESIAS: Great. Thanks, Nick. Moving</p> <p>9 on to another topic, what is penetration testing and</p> <p>10 what role does that have in an information security</p> <p>11 program? How often should an organization conduct</p> <p>12 these tests and what factors should go into</p> <p>13 determining the frequency of these tests? And I would</p> <p>14 ask that to Flee.</p> <p>15 MR. LEE: Yeah. So penetration testing is</p> <p>16 effectively just attack simulation, with the goal</p> <p>17 being to try to actually just go across the entire</p> <p>18 gamut of potential vulnerabilities that a</p> <p>19 system/infrastructure may contain, and then actively</p> <p>20 try to, you know, truly exploit those systems.</p> <p>21 So, you know, we're going to talk a little</p> <p>22 bit more later about vulnerability scanning, but think</p> <p>23 about, like, pen testing as being not only finding</p> <p>24 vulnerabilities but trying to determine which</p> <p>25 vulnerabilities are true by essentially having your</p>	128	<p>1 saying, like, hey, at least these types of issues were</p> <p>2 tested for; we did not find these issues in these</p> <p>3 particular areas, but it doesn't mean that something</p> <p>4 is explicitly secure or insecure. The other thing to</p> <p>5 actually take into account is that a pen test is</p> <p>6 literally just an assessment at a specific point in</p> <p>7 time. So just because a pen test was actually done</p> <p>8 six months ago does not mean, and most likely is not</p> <p>9 meaning, that the system that was tested is in the</p> <p>10 same condition. More than likely, software has been</p> <p>11 updated; patches were applied; the network itself may</p> <p>12 have changed.</p> <p>13 So that's actually part of the reason to</p> <p>14 think about, you know, how you do pen testing to</p> <p>15 really be a check against significant changes that</p> <p>16 actually were made to a system. Ideally you're doing</p> <p>17 a penetration test at least annually. However, a lot</p> <p>18 of people would recommend that you also do a</p> <p>19 penetration test with any kind of significant change</p> <p>20 to the system. So if you've actually added new</p> <p>21 features to the software that you're building, if</p> <p>22 you've changed the network topology, et cetera, you</p> <p>23 probably want to do a penetration test again.</p> <p>24 But, once again, that really is part of a</p> <p>25 broader holistic security program. Penetration tests</p>

129

1 in and of themselves are not sufficient. It's meant
 2 to actually just really be yet another tool to help
 3 identify security weaknesses in a proactive manner so
 4 that you're able to actually fix things prior to an
 5 attacker exploiting them.
 6 MR. IGLESIAS: Thanks, Flee. And what would
 7 those typically cost a business and what is the range
 8 for that?
 9 MR. LEE: And so this is where it gets
 10 really interesting. For the penetration test -- and I
 11 love that Nick kind of already got onto this. You're
 12 always paying some kind of cost when it comes to
 13 resourcing, right? Obviously you can have in-house
 14 talent that can actually do that penetration test.
 15 Security engineers in general are not cheap. So, you
 16 know, there's no such thing as a security engineer
 17 that's making less than six figures. And obviously
 18 this is going to generally be at the higher end of
 19 that. So in-house is going to be expensive for you.
 20 Going externally definitely is an option.
 21 That kind of goes across the gamut. But to some
 22 extent you are kind of getting what you pay for. So
 23 it's not uncommon for kind of like an 80-hour
 24 penetration test to start at at least \$40K, but that
 25 can actually quickly go up to six figures depending on

130

1 the complexity of the system, the specific vendor that
 2 you pick, and also how much you want to have tested.
 3 So if you want to have somebody doing
 4 testing on something that is actually fairly nuanced,
 5 so, for example, you built an embedded system of some
 6 sorts or, you know, kind of like an IOT-type device,
 7 that expertise is way more expensive than somebody
 8 just doing a penetration test for a "basic website."
 9 So that definitely is one of those things to take into
 10 consideration.
 11 There are some new novel type alternatives.
 12 Because when you think of a penetration test, if you
 13 think of it from the lens of what you really want the
 14 outcome to be, the outcome should be trying to find
 15 vulnerabilities or security weaknesses in the system
 16 proactively. And so there are other mechanisms like
 17 things such as bug bounties, which can make that cost
 18 a little bit less. But it's also one of those areas
 19 where as an industry we haven't really solidified on
 20 that being adopted. And particularly around things
 21 like regulations, to get regulations to start
 22 accepting bug bounty reports as being at least
 23 comparable to a "classic penetration test."
 24 MR. IGLESIAS: Thanks, Flee.
 25 Nick, did you want to respond to that?

131

1 MR. WEAVER: I just want to add one other
 2 real valuable thing from the penetration test, is it
 3 basically gives you a dry run on all your response.
 4 So whether or not the pen testers succeed, you should
 5 go back and see in your logging infrastructure, your
 6 monitoring infrastructure, did you record this. Did
 7 you catch this either before or even after you find
 8 out.
 9 MR. IGLESIAS: Great.
 10 Scott, did you have anything to add, and
 11 specifically are there any limitations with
 12 penetration testing at large?
 13 MR. WALLACE: Yeah, so sure, I'll just kind
 14 of talk about what it's like on a typical pen test for
 15 us. So we get all of the IP addresses that we're
 16 allowed to operate in on both the external and the
 17 internal network. We also get a list of emails for a
 18 phishing campaign. And so the pen tests that we
 19 normally do are one week externally and then one week
 20 internally.
 21 So on the external week, the first thing we
 22 do on Monday is we prepare for the phishing campaign.
 23 We have a template and a payload that we run by the
 24 point of contact. And then once that's all been
 25 approved, we send that out to the email list. And we

132

1 generally get beacons off of that. We have a
 2 surprisingly high click rate. Other things that we do
 3 on the external network are do host discovery and
 4 vulnerability scans on the hosts that are open and
 5 have ports available.
 6 There's generally not much that is directly
 7 exploitable on the external network, although there
 8 are some crazy things that we've seen. So, like, my
 9 favorite one was there was an entity that had default
 10 credentials on the external network. And so we just
 11 looked up the default credentials, logged on to the
 12 server and there was all of this crypto mining
 13 software that was running on the server and calling
 14 back to Europe. So he was using them as a server
 15 farm, whoever was doing that over in Europe.
 16 But generally we'll get a couple beacons off
 17 of the phishing campaign, and from there it gets more
 18 interesting because people are a little more lax on
 19 their internal network than their external network.
 20 So the kind of joke is that in cybersecurity, that
 21 it's hard and crunchy on the outside and soft and
 22 chewy on the inside.
 23 And so we'll do things like -- Responder is
 24 a popular technique to use on the internal network
 25 whereby there's all sorts of folks requesting services

133	<p>1 on the internal network. So, for example, if somebody 2 is searching for a printer, we'll just say, hey, yeah, 3 on that printer, here's a handshake, talk to me. And 4 then so we can possibly get some hashes from that. 5 And weak passwords is definitely one of the most 6 common vulnerabilities that we find on the internal 7 network. So we could get hashes from Responder, we 8 could get hashes from a technique called 9 Kerberoasting. On a traditional Microsoft network, 10 you have a ticket graining system called Kerberos, 11 which is authentication on the internal network, and 12 you can request hashes from Kerberos. And so that is 13 another way that you can possibly crack some hashes. 14 And then patching is another big 15 vulnerability that people don't keep up with as well 16 as they should. And another one is network 17 segmentation. And this has especially been important 18 as we've been working throughout the 2020 elections 19 because states and counties interact with each other 20 for the voting process. 21 And so when it comes to network segmentation 22 at a county level, for example, you could have the 23 sheriff and the emergency medical services and the 24 board of elections and the, you know, garbage all on 25 the same county network but not properly segmented.</p>	135	<p>1 system, and then patches. Some of these like 2 EternalBlue and some of these things that came out 3 even years ago people have still not patched. So 4 that's traditionally what you'll see on a pen test, 5 especially on the internal network. 6 MR. IGLESIAS: Flee, did you have something 7 to add? 8 MR. LEE: Yeah. I actually wanted to 9 piggyback on several of Scott's comments because 10 actually they were great. And, also, Scott's comments 11 give some insight into some of the challenges of these 12 kind of rules, and pen testing in particular, how it 13 will impact a small/medium-sized business or 14 organization. 15 Everything Scott said was true. But I can 16 imagine that probably half the people actually 17 watching this audience didn't understand a word that 18 he said. And not because the people in the audience 19 aren't, you know, intelligent, but because it's 20 actually really technically, you know, complex. 21 And on the side of a business or somebody 22 else, a small organization needing to have a 23 penetration test done, one of the important things is 24 actually understanding the scoping, this concept of 25 what should we test but also how the test should be</p>
134	<p>1 So, in other words, you could exploit the landfill's 2 network or the sheriff's network and be able to find 3 your way to the elections side of the county. And so, 4 yeah, Nick, I see his comment here. But Mimikatz is 5 very popular. So when we're spreading around a 6 Microsoft network, there's a tool called Mimikatz that 7 actually allows you to pull credentials out of memory 8 if that person is logged on to the box. 9 So traditionally what we'll do once we get 10 that initial beacon from the phishing, there's a 11 really, really effective tool called BloodHound. And 12 the guys that wrote it are very smart. We used to 13 work with them. And basically what it does is it maps 14 out active directory in the Microsoft domain. And so 15 you can see where the domain admins are logged in to. 16 And what you want to do is navigate to those 17 boxes that they're logged in to so that you can scrape 18 the DA's creds out of memory and then you control the 19 network. 20 So that's sort of a summary of kind of what 21 it's like in the real world on a test. We generally 22 use some form of phishing to get beacons and then 23 running BloodHound to navigate to where the admins 24 are. Responder is another one. Kerberoasting, like I 25 said, to get more hashing from the ticket graining</p>	136	<p>1 conducted. 2 So, like, Scott spoke a lot about, you know, 3 what it's like actually doing a bunch of pen tests, in 4 particular like, hey, should it be a network 5 penetration test; should it be a penetration test of 6 just, say, like a web application. But even moreso, 7 he was mentioning tests that were for things that are 8 actually, like, in a Windows environment. 9 So if you are a small business or a small 10 organization that doesn't have internal security 11 experts or really, really intelligent maybe network 12 engineers, you may be at a disadvantage for actually 13 figuring out how to actually properly test. So you 14 can actually have a pen test done, but the true value 15 that we're driving for here is incentivizing and 16 encouraging businesses to proactively find security 17 defects and get those defects fixed. 18 It also requires that they have either some 19 in-house knowledge or some assistance in actually 20 trying to figure out how to properly test their 21 business. So a traditional like OWASP top ten or like 22 a web-type penetration test, if I'm a manufacturer of, 23 you know, like, embedded devices, that test isn't 24 relevant to me. But if I don't have the necessary in- 25 house expertise, I wouldn't know which test I'm</p>

137

1 buying, if I'm buying the right services or not.
 2 And that actually is one of the things that
 3 we have to worry about when we consider these kinds of
 4 rules and regulations and how they're going to impact
 5 people that may not have a Scott on their team. So if
 6 you have a Scott in your organization, you're fine.
 7 If you don't have a Scott in your organization, you're
 8 going to be at a disadvantage. And we need to make
 9 sure that whatever rules and guidance we push down
 10 still allow for people to actually figure out and
 11 actually learn that process as it goes along.
 12 MR. IGLESIAS: Thanks, Flee.
 13 Tom, did you want to add anything on this
 14 topic?
 15 MR. DUGAS: And, Flee, I think that's
 16 spot on. One of the challenges that I think is really
 17 important to make sure we cover in part of the
 18 Safeguards Rule change is the fact that the scope of
 19 the rules must really fit the information that's
 20 covered.
 21 What are we defining as customer
 22 information; how does it apply? I mean, the perfect
 23 example is what we have the -- you know, why we are
 24 part of the FTC Safeguards Rule in the first place for
 25 higher education is because we handle financial aid

138

1 data. Financial aid data is really just a very small
 2 subset of what we do here at the institution. But it
 3 obviously, you know, could have major implications for
 4 us in terms of what we need to do to, you know, fund
 5 and staff a cybersecurity program.
 6 So we need to make sure that as we're
 7 thinking about what we need to cover in terms of the
 8 rule, we need to be very explicit about what that GLBA
 9 Safeguards Rule defines as customer information and
 10 how it fits in institution because arguably, when
 11 we're doing a pen test, if I had called Scott and
 12 said, Scott, I want you to do a pen test but I only
 13 need you to pen test that financial aid data, but the
 14 reality of it is that, you know, he could easily
 15 maybe get the financial aid data as, you know, Flee
 16 was talking about from somewhere else, you know, or I
 17 think Scott was talking about by going in a different
 18 way, from a different subsystem. Maybe it's not my
 19 financial aid system; maybe it's my admission system.
 20 Maybe it's something else that actually would provide
 21 that beacon that allows them to look in and see what's
 22 there.
 23 And so those kind of considerations are very
 24 important as we look at this information to make sure
 25 we're counting for it correctly.

139

1 MR. IGLESIAS: Great. Thanks, Tom.
 2 Moving along to vulnerability testing, how
 3 often should an organization conduct vulnerability
 4 testing and what factors should they determine -- what
 5 factors should they consider in determining the
 6 frequency? Should testing be done, performed when
 7 there's been a change in the system or an intrusion
 8 attempt? Can it be automated and what does it cost?
 9 And I would call to Flee to answer.
 10 MR. LEE: Yes. So, you know, the TLDR here
 11 is that at a super, super high level, you can just
 12 think about vulnerability testing and vulnerability
 13 scanning as trying to just do a really, really broad
 14 sweep of the entire ecosystem and identifying things
 15 that could, under certain circumstances, reduce the
 16 security controls. Right? So making something
 17 weaker.
 18 Oftentimes when we think about this in
 19 practice, what does it look like? It's scanning your
 20 environment for the software that's installed and
 21 comparing and checking to see if that software has any
 22 known published security vulnerabilities.
 23 This is often done via automated means. In
 24 fact, I don't know of anybody that currently does
 25 vulnerability scanning manually anymore. It really is

140

1 now at a point where we can actually automate the
 2 majority of it. And that automation can be
 3 extraordinarily cheap because there's actually a lot
 4 of free tools that actually can help with that. But
 5 there's also a lot of commercial tools out there.
 6 Some of those differences could be the
 7 frequency with which they update some of the "rules/
 8 signatures," the things that they actually look for in
 9 the environment, all the way to the ease of actually
 10 using the platform. So, you know, like a tool like
 11 Qualys, et cetera, is actually highly polished, made
 12 to make it really, really easy for somebody that can
 13 utilize it. There's also open source tools such as
 14 OpenVAS that kind of, you know, puts the -- you know,
 15 essentially the operational burden onto the
 16 organizations that's utilizing it.
 17 But because it's so cheap and because it is
 18 automated, most places should try to have
 19 vulnerability scanning operating as frequently as
 20 possible. So I know that the rules are actually
 21 looking for, you know, these vulnerability scans to
 22 occur probably like, I guess, twice a year. But I
 23 would argue to say that it's actually one of those
 24 things that is achievable more frequently.
 25 Some of the things to actually watch out for

141

1 is how vulnerability scans actually work. So because
 2 they are doing some active things on the network,
 3 there could be network performance issues even inside
 4 of a, you know, test environment. There could be
 5 issues where a vulnerability scan could potentially
 6 impact those systems and the uptime itself. So that
 7 actually is something to watch out for, and part of
 8 the reason why it's good to actually have an expert on
 9 staff that can actually detect those nuances and also
 10 correct any errors that actually may be caused by the
 11 vuln scanning.
 12 One of the other issues also to worry about
 13 with vulnerability scanning is, once again, kind of
 14 like this nature of scope, like how much of your
 15 ecosystem are you seeing and can you see. So in a
 16 really, really well segregated network, doing a
 17 vulnerability scan can be complex. You have to figure
 18 out where do you actually deploy the tools so you can
 19 actually see all of the network.
 20 The other thing to actually also think about
 21 is how do you actually aggregate all that data. And,
 22 also, finally because of the nature of vulnerability
 23 scans, you also have to worry about this concept of
 24 false positives, meaning that you're going to find
 25 things that will show up on a report that in your

142

1 current environment or how things are actually
 2 deployed are not actually truly exploitable or not
 3 really, really security weaknesses.
 4 So sometimes that will appear when maybe
 5 you're running custom software, like a custom version
 6 of a Linux package, for example, and that package
 7 itself is not vulnerable but it has a signature that
 8 looks similar to something else, which can introduce
 9 some overhead with regards to that key work effort.
 10 But to actually kind of, like, summarize, it
 11 can be automated. And because it can be automated,
 12 teams should actually drive towards doing those vuln
 13 scans as frequently as possible, and definitely there
 14 should be a vulnerability scan after any significant
 15 network or application change, and always there should
 16 be a vulnerability scan after a intrusion exercise,
 17 whether it's a true, you know, intrusion attempt or
 18 just an alert that was actually being investigated.
 19 You're muted, Alex.
 20 MR. IGLESIAS: Sorry about that. Thanks,
 21 Flee. Tom, related to this topic, do you have
 22 anything to add? That would be great. And then
 23 specifically how much do these type of things
 24 typically cost an organization?
 25 MR. DUGAS: Well, certainly. I

143

1 couldn't agree more with Flee. Vulnerabilities
 2 account for the vast majority of cyber breaches in the
 3 world today. In fact, you know, it's probably up
 4 there, you know, with the number one reason why, you
 5 know, information is being targeted, is because of a
 6 breach. People have the automated scanners, they're
 7 out there doing it maliciously. If you're not doing
 8 it yourself, somebody else is doing it for you and you
 9 just don't know if they're just doing it with ill
 10 intent.
 11 So we're trying to protect our critical
 12 assets, our PII intellectual property, and I think
 13 that the scanning of this needs to happen at -- you
 14 know, we try to do it quarterly and at least annually.
 15 But we realized that there's -- it's hard to manage
 16 this because every time you find a vulnerability, you
 17 have to assess whether that vulnerability really
 18 impacts your university or not, or your organization.
 19 Because in that case, it could have mitigating
 20 controls that you've already implemented just to, you
 21 know, keep that vulnerability at bay; to hide it from
 22 the attacker.
 23 And in some cases, you can actually keep
 24 that, you know, system from being exploitable for a
 25 period of time and keeping other mitigating controls,

144

1 defense and debt, microsegmentation, firewalls, you
 2 know, intrusion detection, intrusion prevention
 3 system. There's a whole bunch of things that can
 4 happen to allow that to occur.
 5 But you've got to keep a mind that when you
 6 find all these things, you know, whether it's a free
 7 toll or an automated toll, or a per-fee toll, you get
 8 this, you know, big, huge report with dozens and
 9 dozens of pages of things that someone has to take
 10 action off. You need to have expertise on staff to
 11 understand what those vulnerabilities mean, how to
 12 manage them, how to actually fix them, because that's
 13 not something you can just do. I can run a toll tool,
 14 you know, forever, but if the tool doesn't have
 15 somebody behind it to analyze and understand whether
 16 or not it impacts your organization and you have to do
 17 something with it, and what you have to do, that's the
 18 hard part.
 19 And for -- we're kind of a mid-sized
 20 organization. We're right on the cusp of where we
 21 have that expertise. But I've got to tell you, of the
 22 25 universities we partner with in Pennsylvania, we're
 23 one of the minorities who have that level of expertise
 24 that could run this continuously. Most of them can't.
 25 They can't sustain that operation, even though it is a

145

1 best practice, something I recommend. It's costly to
 2 them from a staffing perspective, resource perspective
 3 and the tool set, too.
 4 MR. WEAVER: Agreed. One other reason,
 5 though, why you want to do this and when you have
 6 automation, you want to basically -- if you have your
 7 system automated, you basically want it, like, every
 8 day, is that a side consequence is this also gives you
 9 an inventory. It tells you what is actually on your
 10 network. So when the CTO's son logs in a gaming rig,
 11 you actually find it.
 12 MR. DUGAS: And, Nick, that's an important
 13 characteristic. I mean, I don't know about Berkeley,
 14 but I have 30,000 connected devices. I've got to
 15 imagine you're a lot greater than that. So trying to
 16 find that gaming system is a needle in a haystack
 17 sometimes when you're thinking about unlimited amount
 18 of resources in most IT organizations. We have
 19 unlimited demand for limited resources.
 20 And certainly we're going to talk, you know,
 21 probably more about what this means for how
 22 organizations are revolving around COVID. But, I
 23 mean, we're even more struggling now with the way
 24 we're managing our IT resources than we ever did
 25 because we're trying to find a new way to help meet

146

1 demand that's increasing, and at least in our case in
 2 terms of IT needs. So, 30,000 devices, yeah, it's
 3 easy to inventory it, but trying to, you know, manage
 4 30,000 systems and all of the vulnerabilities that
 5 come around with that is pretty intense.
 6 MR. IGLESIAS: Thanks. Tom.
 7 Scott, did you have anything you'd like to
 8 add to this topic?
 9 MR. WALLACE: Well, I can just kind of
 10 piggyback off of it and jump into topic four if we're
 11 ready and kind of describe some of the other services
 12 that we have related to continuous monitoring and a
 13 couple other services. Does that sounds good, Alex?
 14 MR. IGLESIAS: Go for it, Scott.
 15 MR. WALLACE: All right. So what I
 16 described earlier was a risk and vulnerability
 17 assessment that we do, which is sort of the full pen
 18 test. If you want just a phishing campaign, we have
 19 that as well, if you just want to do the phishing
 20 test. We also have just the remote campaign.
 21 Probably our most popular product, though,
 22 is called cyber hygiene. And before I was on the pen
 23 testing team, I was on the software development team
 24 with a couple of smart and great guys that wrote this.
 25 And basically what it is is it's a PDF that you get

147

1 every Monday that details your entire external
 2 network. And so it's a very simple sign-up process
 3 and anyone can sign up. You just contact our mailbox
 4 and give us your IP space. We go ahead and end map
 5 that, figure out where the hosts and ports are, and
 6 then run the vulnerability scan on that.
 7 And the report we deliver every Monday
 8 will kind of have an initial report card at the top.
 9 And so you'll see mitigated vulnerabilities,
 10 vulnerabilities that have remained and new
 11 vulnerabilities that have popped up. They'll all be
 12 color-coded based on their severity.
 13 And then once you go deeper into the report,
 14 you'll get details on the IP and what specific
 15 vulnerability it is and additional detail. And so
 16 that is called cyber hygiene. It's pretty effective
 17 because the scanning is based on the severity of the
 18 vulnerabilities. So when we pick up critical
 19 vulnerabilities, the scanner comes back and rescans
 20 that every 12 hours. And highs are every 24, mediums
 21 are three days and lows are six days.
 22 And so when you get it on Monday, your more
 23 intense vulnerabilities have been scanned very
 24 recently. And so when you get it on Monday, you have
 25 a general picture. And like somebody said, you know,

148

1 people doing things over the weekend -- we had a
 2 customer who did some configuration changes on their
 3 network one weekend and accidentally dumped the whole
 4 internal network on the internet. And so there was a
 5 massive spike in the report card that they saw when
 6 they got it at 6:00 a.m. on Monday morning. So they
 7 knew that they had made a mistake so they were able to
 8 tackle it quickly. And that's totally, you know, free
 9 at the point of signing up for anybody that would like
 10 to sign up.
 11 MR. IGLESIAS: And, Scott, what would an
 12 organization need to sign up for that program?
 13 MR. WALLACE: Well, there's not many
 14 requirements. We just -- you know, we might have an
 15 interaction with you and then all you need to do is
 16 send -- you'll sign the legal contract and then you'll
 17 give us your IPs. And then as soon as the next
 18 Monday, you'll start getting your reports. It's
 19 pretty straightforward and simple.
 20 MR. IGLESIAS: And it would just scan the
 21 external network or would it also scan the internal
 22 network? How does that work?
 23 MR. WALLACE: Yeah. It's just the external
 24 network.
 25 MR. IGLESIAS: Great. Thanks, Scott.

149

1 Nick, are there any other products and
 2 services available to institutions for continuous
 3 monitoring and/or testing and what would these
 4 normally cost?
 5 MR. WEAVER: There's a lot. And the cost is
 6 often a -- basically it's a product of how much you're
 7 willing to spend and how much local expertise you
 8 have. So for network monitoring, you have free high
 9 quality network monitoring in the form of Zeek and
 10 Snort and Suricata and all those that are really good
 11 at logging everything that happens.
 12 But if you're running them yourself, you've
 13 got to have an expert on staff, or you can go with one
 14 of the companies that's outsourcing the skill. And so
 15 you don't need necessarily as much skill on staff, but
 16 now you have a big dollar line item. In terms of
 17 collecting on end host, it's the same thing. Sysmon
 18 is free; Corelight costs a fortune. But Sysmon means
 19 you have to have experts on staff who are able to set
 20 up a server to ingest the logs, to analyze the logs.
 21 Similarly for log analysis, you can spend a
 22 fortune and go with Splunk, or you can go, these are
 23 logs I'm rarely going to read and so it's
 24 column/delimited text and you're using grep and
 25 Python, or you might be splitting the difference and

150

1 tossing it in the PostgreSQL database.
 2 And so basically what it comes down to is
 3 you have your questions. What's on the network?
 4 What's happening on the network? What's happening on
 5 the end host? And you basically then have to decide
 6 where in the internal expertise versus external cost
 7 tradeoff you are as an institution. And that
 8 basically tells you what approach you have to take.
 9 MR. IGLESIAS: Thanks, Nick.
 10 Tom, did you have something to add?
 11 MR. DUGAS: I did. And, you know, certainly
 12 there are a lot of tools in this space and a lot of
 13 services. In fact, this morning's sessions
 14 demonstrated a number of them and what those costs
 15 are. They're well documented. They can be tens of
 16 thousands or hundreds of thousands of dollars
 17 annually.
 18 In order to get around that, at least in
 19 higher education, we've done so by building
 20 consortiums to try to stem the tide of the cost
 21 because it's very hard to come up with that kind of
 22 money when we know it directly ties back with, you
 23 know, student tuition dollars, for example.
 24 So the University of Texas at Austin, for
 25 example, built a system called Dorkbot, which does a

151

1 lot of the same things that the hygiene service at,
 2 you know, the Department of Homeland Security does but
 3 specifically for government and higher education to
 4 actually analyze that external web content.
 5 And then a number of Big Ten schools and
 6 other research institutions built something called the
 7 OmniSOC, which is a centralized security operations
 8 center for universities to collaborate collectively
 9 together and then normalize data and talent, because
 10 it is a really hard thing to do even if you gather all
 11 the great tools that Nick talked about, which are free
 12 and available for a lot of people, somebody still has
 13 to sit there and watch them 24/7, 365 days a year and
 14 make sure that we're protecting, you know, our assets,
 15 our digital assets from attackers. And trying to
 16 maintain that kind of operation without a partner who
 17 can help you do that certainly can be a lot.
 18 So, you know, for big organizations, they're
 19 tackling it well. I'm sure there's a high expense to
 20 it for small organizations. Some of them haven't even
 21 figured how to even start. So we need to just balance
 22 out the fact that there's both big and small between
 23 them.
 24 The other thing that I think is becoming
 25 increasingly challenging, Alex, is the fact that at

152

1 least in a lot of cases the data is not even at my
 2 location in a data center anymore. It's in a cloud
 3 service or offers a service somewhere else that's
 4 being managed, you know, by another organization or
 5 multiple organizations.
 6 So I may have, you know, several different
 7 enterprise relationship planning software solutions
 8 that are actually managing data. So we need to be
 9 cognizant of the fact that data is being distributed
 10 in ways that it's never been before. In a lot of
 11 places, people have done a lot of paper abatement to
 12 meet COVID restrictions and needs because of the way
 13 we're working and they've moved a lot of things to
 14 cloud-based services because of that in order to make
 15 that accommodation happen.
 16 So we've got to remember the fact that even
 17 if we run penetration tests and vulnerability tests,
 18 that's for our systems and services. And we heard
 19 from this morning's sessions, what if that's at
 20 Amazon, and what if it's with Microsoft or whether
 21 it's with Google or Oracle or some other cloud
 22 platform where it's not here? Because then I need to
 23 ask them to do the same thing and they need to run the
 24 same test and they need to give me the validations and
 25 results, not just myself.

153

1 And now we're independently validating all
 2 of their controls and all of their things that they're
 3 doing to protect my data that they own or they're
 4 controlling. They don't own it, of course, but
 5 they're actually controlling on our behalf. So
 6 there's a lot that goes into that.
 7 MR. IGLESIAS: Great. Thanks, Tom.
 8 Moving on to the next topic, what is the
 9 purpose of security logs and audit trails? How are
 10 these beneficial to organizations and are there any
 11 limitations doing this? And I would ask that to Nick.
 12 MR. WEAVER: So logs and audit trails are
 13 really important. You notice actually a lot of the
 14 tools that I've been talking about are really logging.
 15 So you can theoretically do proactive defense on the
 16 network and the like. But the greater value is
 17 actually the logging itself. You got compromised.
 18 What did the attackers get? What did they not get?
 19 Because if they did not get your financial disclosure
 20 stuff or stuff like that, not only is that good for
 21 you, or good news, but that might save you a fortune
 22 because now you don't have to deal with the State of
 23 California's notification business.
 24 And basically what it comes down to is the
 25 pen testing and the vulnerability scanning, and stuff

154

1 like that is all about preventing attacks. The
 2 logging is all about recovery: being able to do a true
 3 damage assessment and a true recovery. And that's why
 4 logging is so important, is because it does enable
 5 this damage assessment and recovery that in the end
 6 might save your corporation hundreds of thousands of
 7 dollars.
 8 MR. DUGAS: And to add what Nick was talking
 9 about, I mean, it's like a crime scene. Right? So
 10 that -- you're logging all this data and you're
 11 gathering it all, and if you ever have to do an
 12 incident or a breach investigation, you're going and
 13 pouring through those logs in order to, you know,
 14 build a case against that perpetrator or to ascertain
 15 what they did, how they did it and what they got
 16 access to.
 17 If you didn't have those logs, you would
 18 have a real hard time being able to find that
 19 information you need to figure out what happened and
 20 why it happened or how it happened. And so the
 21 challenge is that you can -- you gather a lot of these
 22 logs and logs consumes data and storage, and that data
 23 and storage consumes a lot of costs. And so you have
 24 to make sure you understand how much data you need to
 25 retain for logs and how long you're going to keep

155

1 them, and more importantly those logs have to be
 2 protected as if it's a case file and an investigation.
 3 They need to be protected and secure to make sure that
 4 it can't be altered; to make sure they're not being,
 5 you know, changed by somebody who doesn't have
 6 permission to do so.
 7 So certainly it's something that is really
 8 critical for what we do. But it's also a lot of
 9 things we do after the fact. We're not -- we're not
 10 -- we've got to still prevent people from getting in
 11 and doing it, but after the fact if you don't have
 12 them, you don't really have the necessary means to
 13 actually do anything to investigate correctly.
 14 MR. WEAVER: And there's one other problem
 15 of you don't know until after you're trying to
 16 investigate what you wish you logged. And so as a
 17 consequence, when in doubt, error on more aggressive
 18 and error on basically right only.
 19 So a big blob of disk that just gets stuff
 20 because, like, for example, Lawrence Berkeley Labs
 21 does very aggressive logging of the network. And they
 22 have used decade-old logs of connectivity in
 23 investigations. And a properly run network monitor
 24 would embarrass the NSA with how aggressive you do it.
 25 So, for example, the NSA did bulk recording

156

1 of network data for five days, and they were oh-so-
 2 proud. Lawrence Berkeley Labs does bulk reporting of
 3 network data and keeps it for months. Raw packets,
 4 just because it might be useful in an analysis.
 5 MR. LEE: I like one of the things that you
 6 called out there, Nick. And particularly you said
 7 this phrase, a well architected network logging
 8 system. And I 100 percent actually agree with you,
 9 and I think one of the challenges, though, is like how
 10 many people have the expertise to actually do that.
 11 And that's where, you know, some of this
 12 guidance and things like that that the FTC is putting
 13 together really needs to be considerate, also,
 14 especially of the capabilities of the institutions
 15 doing this. You know, because, yes, we can definitely
 16 actually set up monitoring, et cetera, et cetera. But
 17 envision a scenario where it's like a 200-person
 18 company or like a 400-person contractor or that kind
 19 of scenario. Do they have the people on staff that
 20 can actually put monitoring in place so you're
 21 actually effectively grabbing the correct logs?
 22 I 100 percent agree with you. Like, you
 23 want as much security telemetry as possible. Some
 24 telemetry is actually more useful and more important
 25 than others. And you do need trained personnel that

157

1 can actually help make that useful. You know, it's
 2 definitely great to just have kind of, like, all of
 3 the logs, but then you also get into the scenario that
 4 I think you, Nick and Scott, have already, you know,
 5 touched on. Well, now you also need the expertise to
 6 actually go through that data. Right? So, like,
 7 having the forensics is great and there are definitely
 8 third parties that can come in post-incident that can
 9 study the logs that you have. But it's also useful
 10 internally that you have somebody that can actually go
 11 through that data and see if it actually is useful or
 12 relevant.

13 And when it comes to what some of those
 14 tools and expertise looks like, it can get really
 15 expensive. You've already mentioned Splunk.
 16 Everybody is very well aware of Splunk. I don't think
 17 there's anybody that is happy with their bill from
 18 Splunk. But it is, it's one of those tools where
 19 there just aren't a lot better. I mean, there's
 20 QRadar, there's SomaLogic, there are tools that are
 21 still bringing that price down. But it is, for --
 22 especially for small companies, it's cost-prohibitive,
 23 in particular if they only have a really small budget
 24 for security.

25 And, once again, there are open source tools

158

1 that are really, really great, you know, like, you
 2 know, ELK, the stuff that, you know, Cisco released
 3 Garseki SOX (phonetic), et cetera. But it comes back
 4 to, oh, well, now you're trading expertise time for
 5 money. At the end of the day, you always are paying
 6 for this really, really small set of experts; those
 7 either experts you hired in-house or experts in
 8 somebody else's company. You know, if you're going
 9 like the managed security service provider route,
 10 you're still paying somebody else and still kind of
 11 beholden to that.

12 So I think it's actually one of the things
 13 to always be considerate of when we talk about
 14 logging. We definitely want to encourage companies to
 15 do that, but we should be realistic about what their
 16 capabilities will be around that and what value they
 17 can get out of having those logs.

18 MR. DUGAS: And, Flee, along those lines, I
 19 mean, Ponemon Institute said it takes 197 days to find
 20 an incident this year, right? One hundred and ninety-
 21 seven days. And you've got to remember how many days
 22 that actually people keep logs for and do they keep
 23 197 days, enough of it to be able to go back.

24 Many organizations don't, and that's
 25 unfortunate because it takes a hard time to see it.

159

1 Even if we have all the monitoring, and Scott can
 2 maybe talk to this, how many of even -- when you do a
 3 penetration test, how many of them actually see you
 4 doing that, Scott? I mean, we can invest a lot of
 5 money and time, but I don't know how many actually see
 6 those attacks happening and those tests? Maybe a lot,
 7 maybe a little. But I know the smaller ones are
 8 probably less prepared to do so.

9 MR. WALLACE: Yeah. Or with a two-week
 10 assessment frame, we're generally a little noisier
 11 than a normal attacker would be that would be much
 12 slower with packets going back and forth, you know?

13 Another one of the paradigms that's emerging
 14 now is to just assume that you're going to get
 15 phished. This is difficult for many people to accept
 16 because we want to believe that if we show people
 17 training videos that they won't click on anything.
 18 But that's not proving to be reality.

19 So basically with some endpoint protection
 20 and network segmentation like I described earlier,
 21 that's kind of a new paradigm that organizations are
 22 moving towards and just trying to assume breach and
 23 then contain it once it's inside.

24 MR. WEAVER: And I'd just like to add, it's
 25 slightly off topic on phishing, but how many have

160

1 received emails about mandatory security training that
 2 are indistinguishable from a phishing attack?

3 MR. WALLACE: Yeah.

4 MR. WEAVER: The other thing is, is if your
 5 infrastructure and setup allows it, security keys are
 6 great because this cannot be phished.

7 MR. IGLESIAS: All right. Moving along, we
 8 have a question from the audience for Tom. In a
 9 university environment for GLB Safeguard purposes, are
 10 you concentrating primarily on student information
 11 systems? What about the data, customer info, that has
 12 legs outside of financial aid?

13 MR. DUGAS: So at least in my perspective --
 14 and I can't speak on behalf of a lot of other
 15 universities -- I try to treat all the data that is
 16 sensitive in a restricted data format in the same way.
 17 And I try to protect it to the same degree following
 18 as closely as I can to NIST 800-171 compliance
 19 regulations in order to protect it.

20 Obviously it's quite cumbersome to try to
 21 find all the data we have everywhere. But we do try
 22 to make sure we cover it as much as possible and
 23 protect it whether it's in a student information
 24 system or whether it's in a research, you know, study
 25 somewhere else on campus that has something that's

161

1 very sensitive as well.
 2 MR. IGLESIAS: Great. We have another
 3 question that's asking, the Safeguards Rule is
 4 intended to set development of the comprehensive
 5 information security program in the context of what's
 6 appropriate to an organization size and type as well
 7 as nature and sensitivity of the data the organization
 8 handles.
 9 With that in mind, how should the FTC work
 10 with different stakeholders, communities, covered by
 11 the rule to identify for organizations what the
 12 relevant standards for their industry may be in
 13 relation to these issues?
 14 MR. LEE: I can chime in on that at a high
 15 level. I mean, there are tons of, you know, like
 16 essentially business organizations and
 17 representatives. I do think it's useful to
 18 distinguish between the size of these companies.
 19 What's appropriate and realistic from a security
 20 posture standpoint and security programs standpoint
 21 for a large financial institution, you know, such as
 22 Goldman Sachs or Bank of America, is very different
 23 than what it is for a 200-person company. And it's
 24 important that the FTC recognize that and really start
 25 to hyper-focus on particular behaviors that they want

162

1 to see and the outcomes of those behaviors.
 2 And what that means is being open to
 3 examining the new guidance to determine if it's
 4 really, really truly outcome-based, meaning that not
 5 being overly prescriptive and saying that, hey, you
 6 have to have penetration testing, thinking more along
 7 the lines what you really want out of penetration
 8 testing.
 9 The assumption is that you want penetration
 10 testing because you want to see businesses have ways
 11 that they can proactively find security weaknesses,
 12 and then once finding those security weaknesses,
 13 properly prioritize those and then finally remediate
 14 those weaknesses in a repeatable way, with the
 15 expectation that software and information technology
 16 is always going to have new vulnerabilities.
 17 There are always going to be classes of
 18 things that we're not taking into account today that
 19 may, you know, in the future end up being vulnerable.
 20 Like, obviously we're all aware of things like, you
 21 know, the Hartley vulnerability that was in open SSL a
 22 while back, or the, you know, SSE/secure enclave
 23 issues that Intel has had, or all of these other kind
 24 of classes of vulnerabilities.
 25 So it's important that we really actually

163

1 focus on do companies have the ability to find
 2 security defects, and do they have the ability to
 3 actually fix those in repeatable fashion. And what
 4 that looks like at a large company should be different
 5 than what that looks like at a small company. And
 6 what that means is a small company may need to rely on
 7 just one individual who doesn't have certain
 8 certifications or doesn't have security in their title
 9 but is still capable of actually doing the job versus
 10 a large organization that, yeah, probably has, you
 11 know, hundreds of people in their security department.
 12 MR. DUGAS: So I want to tag a little bit
 13 onto that. Because as we have guidance in the GLBA
 14 Safeguards Rule specifically towards organizations of
 15 different sizes, we need to make sure they're
 16 expansive enough that we -- and detailed enough that
 17 they're applying to the different organizations the
 18 way that they're intended to.
 19 So going back to a small liberal arts
 20 college versus Berkeley, are they going to be applied
 21 the same? If not, we need to define what that's going
 22 to look like and how we're going to apply it to those
 23 different institutions based on their Carnegie class,
 24 for example, in research institutions. Applying on
 25 some financial institution status and basically how

164

1 they're being, you know, grouped, I guess, in their
 2 categorization is not necessarily the same. We're not
 3 -- we can't go based on the size of a bank, for
 4 example. We need to go based on the size of an
 5 institution, how we're actually deemed in our
 6 industry.
 7 But when we have all of these different
 8 considerations and things that are being applied for
 9 the changes in the rules, we've got to take into
 10 account that putting these things into place for some
 11 organizations isn't just going to be something we can
 12 do quickly.
 13 I think the proposal said something like,
 14 you know, it should apply six months after go live.
 15 I'd be hard-pressed to think it's going to be a year.
 16 It would likely be two years where people are really
 17 getting to it where they need to finish all the
 18 components that they need to to get compliant.
 19 So we need to take that into consideration,
 20 too. I just don't think six months is going to be
 21 enough. We're going to have to give enough time and
 22 effort into this to allow those smaller organizations
 23 to get up to speed with the things they need to, to
 24 find the partner they need to, get the tools in place
 25 they need, to find the services they need to get

165

1 involved with and actually get the things in place
 2 that are going to be necessary.
 3 So comprehensive, yes, we need to keep that
 4 all in consideration. But the specifics here, we need
 5 to be very particular about what we need to do and
 6 make sure we need to provide some institutional
 7 discretion about what that looks like as well.
 8 MR. LEE: Yeah. And I want to piggyback
 9 also on your response again, Tom, because I think
 10 there's one other aspect to home in on. I feel like
 11 we may just be dancing around -- and not
 12 intentionally, but it's like we're right on the tip of
 13 our tongues, which is really right-sizing these
 14 controls and what we actually want to see out of these
 15 safeguards to the amount of data that's potentially
 16 impacted. Right?
 17 So if you're a small college, yeah, you have
 18 a small student population. What you should be
 19 looking for from that security program is going to be
 20 different from a university that has 200,000 students.
 21 Right? And that 200,000 students represents a larger
 22 amount of data. And that's a larger impacted
 23 population. It's not meaning to say that anybody
 24 should necessarily be off the hook, but the rules that
 25 apply for somebody that's carrying a million, you

166

1 know, records of sensitive data is probably going to
 2 look different than somebody that's only carrying
 3 2,000.
 4 And even moreso that some of these
 5 businesses that are going to be subjected to this
 6 regulation may not actually even host the data
 7 themselves. And are we doing a good job where we're
 8 actually maybe calling that out? We want them to be,
 9 you know, responsible and knowledgeable about where
 10 data flows in their ecosystem. But if they are
 11 relying upon third-party SaaS providers for various
 12 things, including, like, data storage, how much leeway
 13 do we give them to leverage, you know, these security
 14 protections that they're getting from these third
 15 parties, et cetera.
 16 So those are all things to actually
 17 definitely take into account because the nature of the
 18 data is going to look different, the nature of that
 19 impact or potential data custodianship is going to
 20 look different.
 21 MR. IGLESIAS: I think this dovetails nicely
 22 into our last question to finish up this panel. Based
 23 on the discussion we've had, what impact do you think
 24 the proposed amendment would have? Are these things
 25 organizations should be doing or are there any other

167

1 recommendations you have for the FTC? And we'll go
 2 ahead and start with Tom.
 3 MR. DUGAS: Sure. I think I talked quite a
 4 bit about this. But I think all of the monitoring of
 5 testing is absolutely critical for securing our
 6 computing resources. We need to make sure we have
 7 those in place. There are numerous threats and
 8 attacks daily, and without proper controls such as
 9 penetrating tests, vulnerability scans, continuous
 10 monitoring, we're susceptible to them.
 11 But we also need to understand that there's
 12 a cost associated with it, whether it's personnel or
 13 whether it's technology. And no matter how we do
 14 that, in some ways we're only going to be able to do
 15 that through collaboration and partnership with other
 16 people like us. In higher education, we are very
 17 collaborative and we do find ways to find innovative
 18 ways to solve these complex problems. But it takes
 19 time to get that going as well.
 20 So just keep in mind that, again, the
 21 Safeguards Rule only applies to that very small
 22 portion of the data that we are actually responsible
 23 for managing and protecting. But we need to make sure
 24 we also protect our academic and research data as well
 25 just as importantly. Our students and our researchers

168

1 and things they produce are just as critical to us.
 2 MR. IGLESIAS: Thanks, Tom.
 3 Flee?
 4 MR. LEE: Yeah. You'll probably hear me
 5 duplicating a lot of Tom's answers. But, you know,
 6 like I said, I believe these rules are decent, but
 7 there's definitely some additional areas of concern
 8 and things for the FTC to actually be aware of.
 9 I love the fact that this is actually trying
 10 to push to be a little bit more prescriptive, but we
 11 have to make sure that people really understand the
 12 actual motivation here and the overall objective. The
 13 objective should be to incentivize, to encourage and
 14 hold companies accountable for having good, repeatable
 15 and understandable security programs.
 16 And fundamental towards that is having the
 17 ability to, you know, quickly, proactively find
 18 security weaknesses and defects via, you know,
 19 vulnerability scanning, penetration testing, et
 20 cetera, to actually quickly contextualize those so we
 21 can actually, know, properly, you know, classify them,
 22 apply the proper resources, and actually get them
 23 fixed. But that should allow for people to actually
 24 have a fairly broad agreement with regards to, like,
 25 how they accomplish those things.

169	<p>1 In particular, because these companies are</p> <p>2 going to look different, a small business of 200</p> <p>3 people is definitely different than a company of</p> <p>4 2,000, a company of 20,000, et cetera. And their</p> <p>5 security capabilities, their ability to implement</p> <p>6 these controls, are going to look different. But we</p> <p>7 should be more concerned with the outcome that we want</p> <p>8 from those controls rather than how those controls are</p> <p>9 actually implemented.</p> <p>10 I do think it's great that the FTC is, you</p> <p>11 know, looking at guidance for things like the NYDFS,</p> <p>12 et cetera, but it's also important to note that things</p> <p>13 like some of the policy requirements or documentation</p> <p>14 requirements are going to look different at these</p> <p>15 companies, and we need to make sure that when we're</p> <p>16 holding companies accountable for it that we really</p> <p>17 hyper-focus more on the outcome that we want as</p> <p>18 opposed to if they, you know, dotted every I/crossed</p> <p>19 every T, and if their policies look exactly like a</p> <p>20 large bank's policies because that's really not the</p> <p>21 reality. And then recognizing that the cost of</p> <p>22 implementing this is going to be burdensome for small</p> <p>23 companies in a way that it's not for a large company.</p> <p>24 So that's definitely something we need to take into</p> <p>25 account.</p>	171	<p>1 want to thank each of you for your time today and for</p> <p>2 a very informative discussion.</p> <p>3 (Whereupon, a recess was taken from 2:02</p> <p>4 p.m. to 2:16 p.m.)</p> <p>5</p> <p>6</p> <p>7</p> <p>8</p> <p>9</p> <p>10</p> <p>11</p> <p>12</p> <p>13</p> <p>14</p> <p>15</p> <p>16</p> <p>17</p> <p>18</p> <p>19</p> <p>20</p> <p>21</p> <p>22</p> <p>23</p> <p>24</p> <p>25</p>
170	<p>1 MR. IGLESIAS: Thanks, Flee.</p> <p>2 Nick?</p> <p>3 MR. WEAVER: Second or third, everybody.</p> <p>4 But I'd like to add one little thing that Tom touched</p> <p>5 on, that we should in some ways have number and type</p> <p>6 of data at risk as part of the calculation, because a</p> <p>7 small business that nonetheless has detailed financial</p> <p>8 records on everybody in the U.S. would be a huge risk</p> <p>9 in practice and really doesn't justify sort of light</p> <p>10 small business controls.</p> <p>11 While a used car dealer, the number of</p> <p>12 financial records at issue might be a few hundred or a</p> <p>13 few thousand, and so the damage in case of a failure</p> <p>14 is so much less in that case.</p> <p>15 MR. DUGAS: You're muted, Alex.</p> <p>16 MR. IGLESIAS: Sorry about that. Scott, for</p> <p>17 the final word?</p> <p>18 MR. WALLACE: Yeah, not much to add. Just</p> <p>19 segment your network and don't click on anything weird</p> <p>20 and you'll be in relatively good shape.</p> <p>21 MR. WEAVER: And get security keys.</p> <p>22 Security keys and password managers.</p> <p>23 MR. WALLACE: Amen, Nick.</p> <p>24 MR. IGLESIAS: All right. Thanks,</p> <p>25 everybody. We're out of time for this panel, but I</p>	172	<p>1 ACCOUNTABILITY, RISK MANAGEMENT, AND GOVERNANCE OF</p> <p>2 INFORMATION SECURITY PROGRAMS</p> <p>3 MS. WETHERILL: Welcome back. Thanks for</p> <p>4 joining us at today's FTC Safeguards Rule workshop.</p> <p>5 Our next panel will address accountability, risk</p> <p>6 management and governance. My name is Robin</p> <p>7 Wetherill. I am an attorney with the Division of</p> <p>8 Privacy and Identity Protection here at the FTC.</p> <p>9 And with me today are Adrienne Allen,</p> <p>10 director of security, governance, risk and compliance</p> <p>11 at Coinbase; Michele Norin, senior vice president and</p> <p>12 chief information officer at Rutgers, the State</p> <p>13 University of New Jersey; and Karthik Rangarajan, head</p> <p>14 of security at Robinhood. So thanks to all of you for</p> <p>15 being with me today; looking forward to this</p> <p>16 discussion.</p> <p>17 So I wanted to just start by asking each of</p> <p>18 you to briefly introduce yourself and tell us a bit</p> <p>19 about your experiences working in and around</p> <p>20 information security programs and in particular the</p> <p>21 aspects of those programs that touch on accountability</p> <p>22 and governance.</p> <p>23 So, Adrienne, would you like to start us</p> <p>24 off?</p> <p>25 MS. ALLEN: Sure. And, first of all, thanks</p>

173

1 for having me, Robin. I've been at Coinbase now for
 2 about two and a half years. And I should mention our
 3 current program also includes third-party security
 4 where we're assessing the vendor risk of the parties
 5 that we work with, and we are also performing the due
 6 diligence requests for partners where we are their
 7 third party. So we do get to see both sides of due
 8 diligence. There's a lot of accountability and
 9 governance that goes into that. I look forward to
 10 touching on that later.

11 And before joining Coinbase, I spent most of
 12 my career as a consultant on information and security
 13 and risk assessments for both federal sector clients
 14 as well as private sector between DC and the Bay area;
 15 primarily information security assessments again and
 16 then later on with the implementation of a NIST
 17 Cybersecurity Framework. And a lot of my private
 18 sector clients have been in high-tech, energy, finance
 19 and retail.

20 I'd say most of my work has actually
 21 centered around accountability and governance over the
 22 last several years in some form, primarily on two
 23 fronts: the first really around incident response
 24 planning, including designing operating models for
 25 decision-making and keeping others informed, and the

174

1 second around rolling out compliance and risk
 2 assessment frameworks. That includes reporting up and
 3 out over risk maturity, operating effectiveness of
 4 controls over time. And I've also worked with a few
 5 collaborative groups, including some statewide
 6 initiatives on future-looking information security
 7 projects and public/private partnerships, and
 8 accountability roles and responsibilities have been
 9 really critical to success there.

10 So, overall, I'm really happy to be here and
 11 looking forward to the chat.

12 MS. WETHERILL: Thanks, Adrienne.
 13 Michele, would you like to go next?

14 MS. NORIN: Sure. I'm glad to be here as
 15 well. I have been, as Robin indicated, I'm the CIO at
 16 Rutgers University. I've been at Rutgers for -- I'm
 17 rounding out my fifth year as their CIO.

18 Prior to Rutgers, I was at the University of
 19 Arizona for almost 30 years. And all of my career has
 20 been within the central IT division. Leaving U of A,
 21 I was CIO there for seven years before coming to
 22 Rutgers.

23 You know, the CIO role is broader than
 24 information security. So I have responsibility for a
 25 variety of tools and services and support programs for

175

1 the institutions. Part of that portfolio includes an
 2 information security program in both of my roles here
 3 and at the U of A. And so that responsibility comes
 4 with, you know, setting up the program, making sure
 5 we've got the right leadership, understanding the
 6 aspects of that program, representing information
 7 security and the program to the institution,
 8 understanding the risks. You know, sort of all of the
 9 strategic and decision-making components to a program
 10 such as information security has been within my
 11 portfolio as the CIO.

12 And I think in a little bit we're going to
 13 talk about accountabilities, and with that comes, you
 14 know, sometimes the CIO is the one on the hot seat for
 15 things that come up. So I share in that
 16 responsibility, but it is a component of a much
 17 broader portfolio that I deal with in my role.

18 MS. WETHERILL: Great. Thanks, Michele.
 19 Karthik?

20 MR. RANGARAJAN: Sure. Thanks, Robin, for
 21 having me here. I'm Karthik Rangarajan. I manage
 22 security and privacy at Robinhood. I've been with
 23 Robinhood for a little over three years. I started
 24 March 2017 as the security lead, and I have built out
 25 the security and privacy teams here.

176

1 The last seven years of my life have been
 2 working for startups. I've worked in other financial
 3 technology companies before this. And a lot of
 4 working in startups like Robinhood and my previous
 5 company is setting up a program that people can trust
 6 and can rely on for making the right risk decisions.
 7 So whether -- right now I've worked for a consumer
 8 company; in the past I've worked for NetEnterprise,
 9 a financial software company. And in situations like
 10 that, when you are selling to banks and you're
 11 selling to funds and other highly regulated
 12 institutions, they look to make sure that your
 13 security guarantees are at least as high as theirs, if
 14 not more.

15 Now working for a consumer company regulated
 16 by various authorities, we have to make sure that
 17 whatever governance structure, whatever security
 18 structure we have meets and goes beyond the
 19 requirements that are placed on us and making sure
 20 that our customers feel safe and all of the security
 21 decisions are made in the same, consistent current way
 22 so that everyone in the company has visibility into
 23 how risk-based decisions work.

24 That's kind of the role I play here. And I
 25 ultimately believe that accountability and governance

177	<p>1 really starts with the first line of defense, security 2 teams sort of making the right calls and setting the 3 framework for making the right calls. 4 MS. WETHERILL: Great. So to dive right in, 5 you know, as a few of you have noted, one of the 6 themes of this panel is accountability. So I thought 7 it would be useful to just start by talking about this 8 word, accountability, which has become, you know, kind 9 of a buzzword or often comes up in discussions around 10 information security. 11 And so just to set a baseline, you know, 12 what do we mean by accountability in the information 13 security context and how important is it as an element 14 of an information security program? 15 So, Karthik, would you like to start us off? 16 MR. RANGARAJAN: Yes. I guess we'll start 17 with what accountability is. For me, accountability 18 is who's responsible for identifying and managing 19 risk as well as mitigating who is responsible for the 20 many controls, who is responsible for making sure 21 things are safe and things are accounted for, who 22 testifies when something goes wrong? These are sort 23 of the parameters I think about when I think about 24 accountability. 25 And in most organizations, at least in</p>	179	<p>1 CIO, your lead IT person, also bears a good deal of 2 accountability for protecting information assets. 3 I would submit that your organization 4 generally, the leadership, also plays a role in 5 accountability. I think any organization has a 6 responsibility for protecting your information assets 7 and protecting, you know, people's identities and 8 protecting, you know, your services and what you do as 9 a company. And in today's world, you know, 10 information security and the threats that come with 11 that and how we protect, it's a pretty big deal. 12 And so leadership bears some level of responsibility 13 and accountability for that as well. 14 We also take a shared approach. We like to 15 remind members of our community, depending upon the 16 role they play or the job that they do, that they have 17 a role to play as well in protecting our assets. Not 18 clicking on links and phishing messages, you know, 19 making sure they're not sharing their password. You 20 know, some of those general awareness tips and 21 reminders also plays to the fact that, you know, 22 everyone is responsible and has some level of 23 accountability for playing their part in making sure 24 we're protecting our assets. 25 And so depending upon your role and where</p>
178	<p>1 companies that are fairly small, you may have a small 2 security team, you may have somebody that is the head 3 of engineering or head of IT playing the security hat. 4 And, to me, accountability is about who makes the 5 security decisions and, when something goes wrong, who 6 is going to show up to resolve the incident or respond 7 to the incident, and, afterwards, when you're being 8 questioned by the regulators, who is in the hot seat 9 answering those questions. 10 MS. WETHERILL: Thanks. 11 Michele, did you want to add something to 12 that response? 13 MS. NORIN: Sure. And I touched on this a 14 little bit. I completely agree with my colleague 15 Karthik. You know, there are certainly roles that are 16 automatically accountable for what goes on in the 17 information security space. 18 I will add to that, as well -- and we 19 operate this way with our program -- we like to remind 20 our community that there are varying levels of 21 accountability. Certainly the CIO plays a big part in 22 accountability. You mentioned the hot seat. You 23 know, it's usually the CIO who, along with the CISO, 24 the CIO is also there, you know, taking the heat for 25 what went wrong; why'd this go wrong. So clearly the</p>	180	<p>1 you sit in the organization, clearly the leadership, 2 the senior levels, they're going to be the ones -- me, 3 you know, who I report to, will be the more visible 4 ones when it comes to an incident or a situation. 5 But, you know, at a very broad level it is shared to 6 some degree as everyone, you know, could be a 7 vulnerability in certain circumstances. 8 MS. WETHERILL: Great. 9 Adrienne? 10 MS. ALLEN: Yeah, I agree with what both 11 other panelists have shared. I think, you know, I 12 agree that accountability ultimately is about 13 ownership and being able to represent the successes, 14 mistakes, needs of whatever is in your purview to 15 leadership. And in a lot of ways that ends up looking 16 like speaking truth to power. These people, the 17 CISOs, the CIOs, you are really partnering with the 18 business to understand what those business goals are 19 and helping the business to then understand what are 20 the risk outcomes of making those decisions. There 21 may be security consequences or other technological 22 consequences that just aren't necessarily thought of 23 when the business is framing its objectives for the 24 year, for the quarter or whatever the time frame is. 25 So the CISO, the head of security, whatever</p>

181	<p>1 that role looks like, is really partnering with the</p> <p>2 business to understand those goals, developing,</p> <p>3 recommending some options, maybe even a couple</p> <p>4 different options for how to implement controls to</p> <p>5 help the business achieve those goals within the risk</p> <p>6 appetite, getting that buy-in and then moving forward</p> <p>7 on that control implementation.</p> <p>8 So I definitely see it as a highly</p> <p>9 integrated, highly partnering type of role, but</p> <p>10 ultimately, yes, it is the person in the hot seat and</p> <p>11 it's also the person that is supposed to understand</p> <p>12 the business goals, how that impacts security and</p> <p>13 making sure the business is fully informed before</p> <p>14 moving forward on something.</p> <p>15 MS. WETHERILL: Great. So to switch gears,</p> <p>16 you know, while the FTC's current Safeguards Rule</p> <p>17 requires financial institutions to designate "an</p> <p>18 employee or employees" to oversee their information</p> <p>19 security programs, the proposed rule would require</p> <p>20 that they designate a single point person who's</p> <p>21 responsible for implementing and maintaining the</p> <p>22 program.</p> <p>23 So I have three related questions about this</p> <p>24 change in the requirements. First, to what extent is</p> <p>25 a single point person already typical of what</p>	183	<p>1 it's also -- it can be very difficult to understand</p> <p>2 what the staffing and resourcing costs are when you</p> <p>3 have a distributed view. It's not coming out of a</p> <p>4 single line item. And you can sometimes have analysis</p> <p>5 paralysis. Without that single ownership, the</p> <p>6 accountability piece that we just mentioned, you can</p> <p>7 fall into traps of each relying on someone else to</p> <p>8 make a hard call. And there are hard calls in</p> <p>9 security. So with that model issues can sometimes</p> <p>10 fall through the cracks.</p> <p>11 And I'd also like to put on my third-party</p> <p>12 security hat for a second. From the standpoint of</p> <p>13 reviewing another vendor's third-party risk, before</p> <p>14 integrating them into your environment -- and, again,</p> <p>15 I'll speak from the fintech point of view where we're</p> <p>16 talking about a lot of SaaS vendors, you know, very</p> <p>17 technical integrations that can be complex in nature.</p> <p>18 You really do need to understand who oversees security</p> <p>19 specifically within that vendor organization for a</p> <p>20 couple of reasons. One, it might be during an</p> <p>21 incident. God forbid you need to know who to reach</p> <p>22 out to or even share threat intelligence with.</p> <p>23 On the first point, every once in a while a</p> <p>24 questioner or an issue will come up with a vendor.</p> <p>25 Attackers may even try to compromise a vendor on their</p>
182	<p>1 financial institutions are doing to consolidate</p> <p>2 responsibility?</p> <p>3 And, question number two, what are the</p> <p>4 benefits, if any, of that as a choice for how to</p> <p>5 organize responsibility in your institution?</p> <p>6 And, question number three, what are the</p> <p>7 costs of that as a strategy?</p> <p>8 And, Adrienne, would you like to go first on</p> <p>9 this one?</p> <p>10 MS. ALLEN: Sure. I'm happy to start with</p> <p>11 the first question. You know, I think to the extent</p> <p>12 to which this is already happening, there is a similar</p> <p>13 requirement in other financial services regulations.</p> <p>14 So, for example, the New York Department of Financial</p> <p>15 Services already has a similar ask for someone to</p> <p>16 oversee and implement the cybersecurity program.</p> <p>17 So for any company doing business in the</p> <p>18 State of New York, fintechs, for example, this isn't</p> <p>19 that new. And I think the pros of having this model</p> <p>20 is that it does or can make decisions better and</p> <p>21 faster.</p> <p>22 I think when decision-making is distributed</p> <p>23 you can run into a diffusion of information. It's</p> <p>24 harder to pull together a single view of how an</p> <p>25 information security program is running. Frankly,</p>	184	<p>1 way to trying to get at a primary target. So it's</p> <p>2 important for the sake of the incident response</p> <p>3 planning process to be able to have a single point of</p> <p>4 contact, or at least a single channel to reach someone</p> <p>5 to work with within a short amount of time.</p> <p>6 I think secondly, it doesn't need to be a</p> <p>7 CISO but it should be someone who can make that type</p> <p>8 of informed decision or quickly and appropriately</p> <p>9 escalate to leadership so you meet regulatory</p> <p>10 reporting notifications if you have any.</p> <p>11 I think sometimes, to the last question, the</p> <p>12 cost of doing this with one person, you know, for</p> <p>13 smaller companies is obviously the cost of that</p> <p>14 resource. You might not be resourced to bring in</p> <p>15 someone to focus solely on security.</p> <p>16 I think another cost is that sometimes even</p> <p>17 if you have someone, security can get relegated to a</p> <p>18 side issue. So it's really important that that person</p> <p>19 is senior or influential enough to direct and equip</p> <p>20 program resources and to be able to influence</p> <p>21 decision-making.</p> <p>22 MS. WETHERILL: Great. Thanks, Adrienne.</p> <p>23 Michele, did you want to followup on that?</p> <p>24 MS. NORIN: Sure. I completely agree with</p> <p>25 Adrienne. I think it's extremely important to have a</p>

185

1 person in front of the information security program.
 2 I think that there are so many components to
 3 understand, to manage, to keep an eye on. I think
 4 it's difficult to do that if it's part of someone
 5 else's job. And so I found that it's extremely
 6 helpful to have a person in charge of that program
 7 just from a pure basic management perspective and
 8 understanding perspective.
 9 That gets difficult when you're smaller. I
 10 get it. You know, it's hard to, you know, carve out
 11 one person to do everything, you know, or one specific
 12 thing. We don't always have the luxury of having
 13 that. But if you've got one person who you know, this
 14 is, you know -- this is it, you need to keep your eye
 15 on this, I think it's extremely important to have
 16 that.
 17 When you're bigger, it makes it even more
 18 important that you have that, that person who is just
 19 every day constantly thinking about and managing this
 20 kind of a program, and to raise those issues and
 21 situations, you know, to their leadership, to the
 22 institution or organization's leadership
 23 appropriately. And so it takes having someone who is
 24 dedicated in that way to serving as the lead of a
 25 program, a CISO or otherwise, that, you know, they're

186

1 responsible for the management and the progression of
 2 the program.
 3 MS. WETHERILL: Great.
 4 Karthik, did you have anything to add?
 5 MR. RANGARAJAN: Yeah. Adrienne and Michele
 6 said some excellent things, and I won't say the same
 7 thing. I will add that one benefit of having a single
 8 person or team that is responsible for this is you
 9 remove the conflict of interest, potentially.
 10 Let's say I'm managing the engineering
 11 organization and I'm also managing security. And the
 12 product organization is telling me that they need this
 13 shipped tomorrow, and I see there are security risks,
 14 I'm probably going to listen to the product
 15 organization and ship it and then take a look at the
 16 security risks and figure out what needs to happen
 17 there.
 18 But if there was an independent point of
 19 contact, if there was somebody who does not have that
 20 conflict of interest, they can play those checks and
 21 balances. They can say, okay, I hear what the
 22 business wants, I hear what you're trying to do, but
 23 these are the risks that are coming up.
 24 The second component to this is certain
 25 financial companies have the three-layer defense model

187

1 where there is the security teams who play the first
 2 line of defense, and then there is the enterprise risk
 3 and the audit teams.
 4 Even in those models, I think it's
 5 especially important that the why's of security, the
 6 simplified decision-making, lies on the security team
 7 or on the single person that is the designated head of
 8 security.
 9 For a really small company, for somebody
 10 that may have outsourced all of their business -- all
 11 technologies, it might be hard to hire somebody or
 12 justify the cost of hiring a point person that plays
 13 head of security. And I think in those situations,
 14 the way I look at it is you don't need to hire
 15 somebody that is 20 years a CISO or something like
 16 that. You can find somebody that is experienced, that
 17 knows about the subject matter.
 18 Most of the regulations that I'm familiar
 19 with don't require you to hire a CISO but require you
 20 to designate somebody as head of security. So find
 21 somebody that can provide value for you, that can help
 22 you manage risk and make security decisions in a smart
 23 way, and designate them as your point person. And
 24 then you get two things for the cost of one.
 25 MS. WETHERILL: Great. Thank you for your

188

1 answers on that.
 2 So the development and implementation of an
 3 information security program, as Karthik just
 4 referenced, can implicate not only IT personnel but
 5 also employees who work in other areas like
 6 compliance. So does it make it more difficult, you
 7 know, given that kind of diversity of involved
 8 personnel, to have a single point person and why or
 9 why not?
 10 And, Karthik, I can go back to you to start
 11 us off on this one.
 12 MR. RANGARAJAN: Yeah. I think in reference
 13 to my last answer, I think it depends on what the
 14 organization is doing. Let's say all of your
 15 technology providers are fully outsourced, you don't
 16 build in-house software, you don't have engineers in-
 17 house, and it's just putting things together to serve
 18 your customers. In those cases, I think you could
 19 outsource your security responsibilities, too, as long
 20 as you're outsourcing to a firm, as long as -- I would
 21 say you need a named person that you are working with,
 22 but you can outsource it. You don't have to have this
 23 person in-house.
 24 However, if you are building anything in-
 25 house, even if it is the smallest thing, if you're

189

1 serving products to a customer that you built in-
 2 house, then I would say having a point security person
 3 in-house is unavoidable. Because it's going to be
 4 really hard for an external personnel to handle all of
 5 the contacts of the business, understand everything
 6 that is happening, and be in the the rooms where the
 7 decisions are being made, and do it consistently so
 8 that the business' interests are put ahead and risks
 9 are managed appropriately.
 10 So if you are building in-house products, if
 11 you're building in-house services, you absolutely need
 12 a point security person. But if you're completely
 13 outsourcing it, then I would say you could consider an
 14 outsource model for security.
 15 MS. WETHERILL: Great.
 16 Adrienne, did you have anything to add to
 17 that response?
 18 MS. ALLEN: Yeah. I think just maybe a
 19 quick analogy. One of the studies I think the
 20 Corporate Executive Board recently did was actually
 21 how software decisions are made when you're purchasing
 22 a new piece of software, potentially something that is
 23 a large system; it extends across the environment.
 24 They said that while there is a single decision-maker,
 25 there's actually an average of seven people that are

190

1 involved in forming that decision.
 2 And I think, you know, when we talk about
 3 other teams being involved in security and ultimately
 4 kind of rolling up to a single person, that model is
 5 actually fairly consistent here, too. You know, it's
 6 very unlikely that a single point person for security
 7 would be making decisions in a vacuum. They're going
 8 to have to cooperate with teams, like with risk and
 9 compliance, the three lines of the defense model that
 10 Karthik mentioned earlier. And that's great.
 11 You know, I think to the extent that it does
 12 make decisions take longer sometimes, that's
 13 absolutely true. I think you can do it efficiently,
 14 but they're still taking new factors into
 15 consideration before making calls.
 16 But at the end of the day, you know, again,
 17 I'll unpack an example that Karthik mentioned. If
 18 you're following the three lines of defense where you
 19 have, you know, the first line security, conducting
 20 operations, making these choices; you have a second
 21 line risk management that's noticing the risk about
 22 the program; third line internal audit that's checking
 23 on what the others are doing, you know, it very well
 24 may be that you have another team that's asking the
 25 security program to put segregation of duties in

191

1 place. That will take time to implement. It's the
 2 new requirement being handed to the security team, to
 3 include in a building and a designing of that program.
 4 But at the end of the day, you -- while it
 5 may have taken you a little bit longer to design roles
 6 and responsibilities a little bit differently, to
 7 identify maybe you need to bring someone else new into
 8 the team to distribute those responsibilities
 9 differently, they're still taking the time to decrease
 10 your chance of insider threat down the road.
 11 So while the overall program might take
 12 longer in some ways because you are working with other
 13 teams, by virtue of working with those other teams
 14 you're building a model that can grow with the
 15 company; you're building a model that is more
 16 resilient to the types of risks that security programs
 17 face.
 18 So I think the short answer is, yes, it can
 19 take longer and it does make it more complex to work
 20 with these other teams, but at the end of the day,
 21 their bottom-tier model, you're altogether working on
 22 a common success criteria, and then you have the
 23 single head that can more easily report out on how all
 24 of those needs are being met.
 25 MS. WETHERILL: Great. Thank you.

192

1 Michele?
 2 MS. NORIN: Yes. I will reinforce that. I
 3 think it's critical to have a program, a set of
 4 processes and a governance model that accounts for
 5 multiple units. In my view, I don't think there's any
 6 one unit that can do all -- you know, that can address
 7 all of the components of what would need to be done.
 8 So it's important to have the partnerships.
 9 I know for us as an institution, we have a
 10 couple of different working groups and committees that
 11 are responsible for, you know, the process around
 12 evaluating the software that we buy, or for responding
 13 to an incident. And those -- that group is made up of
 14 representatives from all of these other areas: IT,
 15 our risk and compliance office, our general counsel's
 16 office, our information security, IT, audit, internal
 17 audit sometimes is on there depending upon the focus.
 18 So, you know, we set that up intentionally
 19 in that way so that they are all responsible for the
 20 process and a program that's well-rounded and, you
 21 know, will address all of the aspects of the
 22 institution as best we can. Right? If we need to add
 23 people in the moment depending on what we're dealing
 24 with, we can do that.
 25 But it's not just information security.

193

1 It's not just, you know, the risk and compliance.
 2 They have to work together. And so we've worked
 3 really hard to set up those components, those
 4 partnerships, working arrangements, in that way
 5 specifically so that each area of that -- of the
 6 institution is represented.
 7 And you're right. It takes longer, but in
 8 the end, it's better, it's stronger, because we took
 9 the extra time to really -- to really make sure we had
 10 all the right perspectives represented in the process.
 11 So I just throw my advocacy for, you know, making
 12 sure that happens with those kinds of pieces in place
 13 as well.
 14 MS. WETHERILL: Great. So, another change
 15 that the proposed rule would make, compared to the
 16 current rule, is that this single designated point
 17 person would be required to report to the
 18 organization's board of directors or whatever the
 19 equivalent of that is, in an organization that doesn't
 20 have a board at least annually, and that the report
 21 would have to be in writing.
 22 So, you know, we're wondering about the pros
 23 and cons of that kind of direct communication between
 24 the individuals who are tasked with overseeing
 25 information security and the board or senior officers

194

1 of financial institutions.
 2 So, Michele, did you want to go first on
 3 this one?
 4 MS. NORIN: Sure. A couple of thoughts
 5 here. So one is, I think it's important for
 6 information security as a topic be at the board -- at
 7 the senior leadership level of whatever organization
 8 you are a part of. For me, it's Rutgers or higher ed,
 9 as well as the board. I think it's important that
 10 they understand what that concept is, what it means,
 11 what comes with it. It's not a one-and-done
 12 conversation.
 13 I know for the boards that I've worked with
 14 with in higher ed, it's a progression of information.
 15 It's a way to build awareness about what we do, how we
 16 protect, where we see risks. And I think for their
 17 level of responsibility, they need to be aware of
 18 those subjects, those topics.
 19 So I think that topic should be present at
 20 those tables on some regular basis, at a minimum once
 21 a year. It depends on your structure, your board
 22 cadence. You know, I think your board has to be
 23 brought into that kind of topic. I know for us that
 24 topic lives at the audit committee, which is a
 25 committee of our board. So I think -- so I think the

195

1 topic needs to be there.
 2 The second thought, the second item here for
 3 me is I think who is the voice of that program can
 4 depend upon your culture, your circumstances as
 5 leadership. I think it takes a certain perspective to
 6 share that messaging in a way that's effective and
 7 clear for the audience. If your CISO can do that, I
 8 think it's great. I think the CISO should have a
 9 voice there. I think they should -- at a fundamental
 10 level, if they have to raise an issue that might be a
 11 little sensitive, they have got to have avenues to do
 12 that, right? I mean, no question.
 13 But in terms of regular awareness, I think
 14 that, you know, you've got to have the right voice to
 15 demonstrate that. Sometimes that's a CISO, sometimes
 16 it's the CIO, sometimes it might be some other
 17 leadership, your risk management officer, possibly.
 18 Somebody -- and maybe it's all of those voices that
 19 share in that messaging with leadership.
 20 And so I think that just depends on, you
 21 know, who the person is, how well they can talk about
 22 the subject matter, you know, what's the interest of
 23 the leadership and the board, and then, you know, how
 24 do you formulate that right -- the right voice around
 25 that, around the topic.

196

1 MS. WETHERILL: Thank you.
 2 Karthik?
 3 MR. RANGARAJAN: Yeah. You know, from my
 4 perspective, when you're reporting to the board of
 5 directors, one issue that can come up is the
 6 familiarity of the board with the topics that you're
 7 talking about, so the familiarity of the Board with
 8 security.
 9 One -- a potential risky scenario is you go
 10 to the board and say, hey, these are our high-,
 11 medium-, low-risk items, and they get concerned that
 12 there are so many risks that you are managing. And
 13 the question that gets asked might be why are there so
 14 many risks? Why haven't they gone away or something
 15 like that?
 16 And it's -- with qualitative risk management
 17 mechanisms, it might be hard to say, well, this is a
 18 high risk but it may not actually come to fruition
 19 because of these following factors or things like
 20 that. It gets -- it becomes a really technical,
 21 really difficult conversation.
 22 One mechanism that I've been experimenting
 23 with that is gaining traction in the security industry
 24 as a whole is this quantification frameworks, which is
 25 instead of qualitative mechanisms that talk about here

197	<p>1 are the myriad of risks you need to worry about, you 2 present to the board here's how much of a loss over 3 the next X number of years that you're potentially 4 looking at based on our existing control framework and 5 the existing security program, and here's why we need 6 we need the budget that we need in order to reduce the 7 risk, and having, say, X million dollars to reduce the 8 security risk by Y million dollars or something like 9 that.</p> <p>10 And the numbers don't have to be absolute. 11 The dollar amounts are more of a high watermark for me 12 than actual numbers. There's no way that I can 13 guarantee that the firm will only lose X million or Y 14 million a year. But it is a watermark that we can use 15 to measure the progress that the team is making when 16 it comes to building out the program.</p> <p>17 If quarter over quarter, year over year, 18 this watermark isn't reducing, then board of directors 19 should be able to challenge us and say maybe you're 20 not mapping your risks correctly, or vice versa if 21 it's reducing but we're seeing more incidents, we're 22 seeing potential breaches, things like that, then the 23 board of directors should be able to say maybe you 24 don't have the right risk quantification framework or 25 the right risk management framework.</p>	199	<p>1 that a lot of the financial services industry protects 2 very sensitive customer data, knowing where those 3 critical assets are, being able to report out on the 4 overall effectiveness of the security program and 5 protecting those is really key.</p> <p>6 I think what you end up with if you're doing 7 this on an annual basis is sort of a point-in-time 8 look at where the program has been over the last year. 9 And so it kind of depends, again, on the goals of 10 bringing the board in. You know, is it that we 11 actually want meaningful feedback on a regular basis? 12 Do we want to clue them in to the types of risks that 13 we're seeing, help them understand the risk landscape 14 so that they can make different products or services 15 decisions, maybe reallocate or reprioritize funding? 16 A lot of security is going to have downstream effects 17 on other teams. If there are major risks in one area, 18 maybe IT or even customer service, that needs to go 19 fix something.</p> <p>20 So providing, you know, even shorter, more 21 iterative types of feedback potentially with that 22 quantification, I think will ultimately be more 23 successful in helping to educate the board on the type 24 of pace that the company operates within. If that 25 pace is not super fast, then annual may be perfect.</p>
198	<p>1 So presenting to them in such a way that 2 they're actually able to use that to make decisions 3 and provide input is something I would strongly 4 recommend. It's something that we have been trying 5 out.</p> <p>6 MS. WETHERILL: Thanks, Karthik. 7 Adrienne, did you want to jump in? 8 MS. ALLEN: Sure. I just have one or two 9 things to add. I definitely agree with both of the 10 prior comments. First, quantification is likewise 11 something that we're starting to experiment with as 12 well, and it can be a very helpful kind of neutral way 13 of characterizing some of the risks.</p> <p>14 I do think it's worthwhile to call out that, 15 you know, security landscape, the threat and 16 vulnerability environment, the risk landscape, changes 17 so quickly. For most businesses that do any kind of 18 business online, you know, they may see risks on a 19 daily basis that emerge. So having an annual 20 reporting cadence is -- you know, I agree with 21 Michele, probably the bare minimum for a lot of the 22 financial institutions, and especially the ones that 23 do have an online presence to be able to report out on 24 progress over time.</p> <p>25 I think that, you know, especially given</p>	200	<p>1 And I think as a requirement, annual makes sense.</p> <p>2 I think, you know, in order to kind of take 3 a look at your model for reporting to the board, 4 decide on the right cadence, that may be a more risk- 5 adjusted decision based on the type of financial 6 services company that you are. And if you do have 7 that online presence, then you might want to identify 8 opportunities to provide greater visibility throughout 9 the year than just one long report at the end, which, 10 you know, again, kind of comes back to the business 11 visibility to produce that type of report, make it 12 meaningful, get the meaningful feedback in return.</p> <p>13 MS. WETHERILL: Great. Thank you. So that 14 requirement that we were just discussing is an example 15 of a kind of trend in the new rule to generally 16 increase the amount of decision-making that financial 17 institutions have to put into writing. So that report 18 to the board is one example. Another example is that 19 while the current rule requires that financial 20 institutions engage in a risk assessment, under the 21 proposed rule, you know, that assessment would have to 22 be also in writing.</p> <p>23 So we are curious what you think about, you 24 know, that kind of requirement, whether putting 25 decision-making into writing fosters accountability</p>

201	<p>1 within institutions or what are the benefits or costs 2 of that as, you know, a procedural requirement. 3 So, Adrienne, do you want to comment on 4 that? 5 MS. ALLEN: Sure, yeah. So I think my 6 answer is similar to what I just mentioned, is it 7 depends mostly on how it is used and revisited over 8 time. So I think, yes, you know, first as financial 9 institutions, most requirements that I'm familiar with 10 ask for some form of a risk assessment. So financial 11 institutions, a lot of which are most likely doing 12 this anyway, I think it's a natural step for asking 13 that they should be written. 14 So let me talk first about the benefits and 15 then the costs. I think on principal reporting 16 decisions it's helpful when you're taking a risk-based 17 approach. You want to be able to revisit decisions in 18 light of technical changes, resourcing changes, 19 additions to the environment, or, frankly, just the 20 passage of time. 21 I think it helps you understand how long ago 22 a decision was made, whether things have changed. It 23 minimizes individual interpretation of that decision. 24 So people might hear something and then go off with 25 their separate marching orders, each thinking that</p>	203	<p>1 them to that joint commitment that you both made 2 earlier, and provide the rationale for the exception 3 and why, you know, they may or may not see it extended 4 if they haven't been able to do that. So, yes a lot 5 of value to being able to track these decisions over 6 time, come back to the specific rationale. 7 I think on the cost side, you know, 8 formalized documentation can be a huge time cost to 9 the business when it's too heavy-handed. So I do want 10 to caveat that a little bit. I think when it comes to 11 evidencing decision-making there should be more 12 flexibility. 13 For example, in some of the examples I just 14 gave, we might be making risk-based decisions in 15 different mediums and different ways: IT service 16 management tickets, code reviews, project design 17 documents, to name a few examples. So I think it's 18 important to note that businesses should have the 19 flexibility to record decisions in different ways. I 20 think it's perfectly realistic that the sum of a lot 21 of those small decisions might rise up to the level of 22 going into more formalized risk assessment, and 23 that's perfectly effective as well. 24 So, again, there may be a formalized risk 25 assessment. There may be a set of other decisions</p>
202	<p>1 they've heard a version of that. And it does create 2 clarity over company policy. 3 I think there have been many instances, 4 especially in environments where decisions are being 5 made quickly all day throughout the day where 6 something comes up, it rings a bell, you then have 7 your prior analysis to go look back on. You can then 8 either reinforce that prior decision that was made or 9 adjust it based on the changes in the risk appetite or 10 resourcing. 11 I think two examples here stick out to me. 12 First, we see this all the time in the third party 13 landscape, memorializing decisions about why you chose 14 to accept or reject a given vendor comes up a lot. 15 You might be a year later choosing to integrate that 16 vendor with three of your critical systems. So you 17 really do need to be able to rely on the earlier 18 detail and some of the tradeoffs that you made when 19 onboarding them in the first place. 20 And then, second, it also helps with 21 exception management. I think security often holds 22 other teams accountable for their own work. You may 23 grant a team an exception to go fix something and in 24 three months time you can come back, followup with 25 them, identify whether or not they've fixed it, hold</p>	204	<p>1 that are made outside of that. I think as long as you 2 have a consistent method of deciding when and what is 3 appropriate for what, then it shouldn't all need to be 4 in a single place where you can go back and look at 5 all of that. 6 So, overall, yes, writing things down is a 7 great step, but there are many ways of doing it. As 8 long as everyone is aligned on how you are providing 9 visibility then it's great. That's what I would say. 10 MS. WETHERILL: Thanks, Adrienne. 11 Karthik, do you have any comments on written 12 decision-making? 13 MR. RANGARAJAN: Yeah. I agree with 14 everything Adrienne just said. Going back to the 15 three layers of defense model where the security team 16 is the first layer and then you have the risk 17 management and audit teams as second and third layers, 18 whenever the security team makes a decision that 19 impacts the business in meaningful ways, maybe it's to 20 choose a major vendor or other vendor, whether it is 21 an outsourcing model or anything that people may 22 disagree with, there may be multiple stakeholders. 23 It's important to have clarity on how that decision is 24 made and why that decision is made. 25 And especially now in the current remote</p>

205

1 world that we live in, written documents have gone
 2 much farther than they used to before. You can't just
 3 get into a meeting room and hash it out. And so
 4 writing a one-pager or writing a message on Slack has
 5 had more impact than multiple sets of meetings would
 6 have.
 7 So purely from an efficiency standpoint, I
 8 have actually come to believe that writing things down
 9 is more helpful than not writing things down. Even
 10 though it might seem as overhead, even though it might
 11 seem as undue process, writing things out for major
 12 decisions -- and that's the qualifier I want to add,
 13 major decisions. You don't want to write a one-pager
 14 for why you chose to reject this code review over that
 15 code review. That doesn't -- that doesn't really rise
 16 to the level everyone is speaking. Well, maybe tying
 17 it to a risk score, tying it to the -- tying to the
 18 overall risk management framework and saying for all
 19 higher or critical risk decisions, we want to have a
 20 written documentation for why certain decisions were
 21 made.
 22 If risk is accepted for our higher -- major
 23 risk is accepted, people have written documentation as
 24 to how we accepted this risk, what controls we looked
 25 at, what controls we are going to build and how we

206

1 attained that consensus across the company, so that
 2 the next time you have to make a similar decision you
 3 can follow the precedent that was set.
 4 And this doesn't just happen for third-party
 5 vendors. This doesn't have to be just for product
 6 decisions. This could even be for actions you take in
 7 the case of a security incident or something like
 8 that. Let's say you have a security incident but you
 9 don't notice or you don't find evidence of breach or
 10 don't find evidence of any malicious activity, you
 11 could write that down, memorialize it in the company
 12 so that the next time something like this happens you
 13 don't have to have this discussion all over again.
 14 You can look back at your previous precedent and say,
 15 okay, this is what we followed, let's stay consistent
 16 with our decisions so that not only do you now have an
 17 easier way to make decisions in the future, you also
 18 have defensibility for your legal and audit partners
 19 in the future.
 20 MS. WETHERILL: Great.
 21 Michele, I'd love to know if you have any
 22 comments on this issue, in particular, and I invite
 23 other panelists to chime back in. But I'm interested
 24 if anyone thinks there are costs associated with these
 25 kinds of requirements that the FTC should take into

207

1 consideration in deciding whether to press forward
 2 with some of these changes.
 3 MS. NORIN: So I don't have a whole lot to
 4 add to my -- to what my colleagues have said. I
 5 think, you know, it is generally good practice to
 6 document. And as Karthik said, not every little
 7 nitty-gritty thing, but, you know, certainly major
 8 reports, major decisions, processes, steps that have
 9 been taken, incidents, all of those things.
 10 I mean, I think that if anything, you know,
 11 in a year or two years after that particular moment in
 12 time, you need to remind yourself, why did we decide
 13 that? You know, why did we decide that? What were we
 14 thinking? And you can go back and look at the
 15 documentation. So I just think it's generally good
 16 practice to document.
 17 In terms of costs, you know, I think it's
 18 just the time factor. I think if you go overboard,
 19 yes, it can be overly disruptive and it depends on
 20 sort of, you know, your organization, your size, how
 21 generally you operate, you know, how much process and
 22 procedure you have generally. I mean, you know, that
 23 factor -- those pieces can shape, you know, how much
 24 you do and then thus the time factor which then leads
 25 to the costs.

208

1 I mean, if you're spending all day
 2 documenting and you can't get anything else done, that
 3 might be an issue and you might -- there might be
 4 questions about that.
 5 So, to me, the cost is really the time
 6 factor and the tradeoff of, you know, who is it that's
 7 doing the documentation, and then what are they not
 8 doing because you're doing documentation? And is
 9 there value add there and what's that balance?
 10 So to me it's really time and effort in
 11 terms of what it takes to actually do the
 12 documentation. If you're getting an assessment by an
 13 external party and it's a formal process, yeah, I want
 14 to see the report. You're paying them to assess you
 15 and produce a report that's actionable. And so there
 16 is a cost factor, and that -- in that specific
 17 instance where I'm paying somebody to come in and do
 18 this for us.
 19 But I know that up front and I have a
 20 decision to make about, you know, the fact that I'm
 21 going to spend money on that kind of an exercise. So
 22 it seems to me the biggest cost internally is just
 23 really the time factor, and maybe the tradeoff if you
 24 don't document and something happens and then you have
 25 to go back and take the time to think about what you

209

1 did a year ago because you should have documented and
 2 you didn't. So there is kind of the reverse cost
 3 effect as well if you aren't documenting at the right
 4 level.
 5 MS. WETHERILL: Yeah, thank you for your
 6 comments on that. So you brought up third parties,
 7 which makes a great segue because the next topic I
 8 would like to ask about relates to the way that third
 9 parties operate under the proposed rule.
 10 So the proposed rule would specifically
 11 state that it's permissible for a financial
 12 institution to hire a third party to basically fulfill
 13 that designated point person role as long as the
 14 institution maintains kind of ultimate responsibility
 15 for overseeing that third-party vendor.
 16 So I'm wondering if that provision makes it
 17 easier or financial institutions, particularly those
 18 who may be sensitive to costs, like smaller
 19 institutions, to comply with the rule's requirements
 20 and, you know, whether on the other hand there are
 21 disadvantages to allowing third parties in that kind
 22 of a role.
 23 So, Michele, I'm going to turn it back over
 24 to you to start us off on this question.
 25 MS. NORIN: So I think, you know, third

210

1 parties can be -- can be helpful to fill that role,
 2 particularly given the size of your organization. I
 3 think it's an interesting balance to consider. I'm an
 4 advocate for even if you have a third-party who
 5 manages your program, I think it's important to have
 6 someone inside the organization who is managing that
 7 relationship.
 8 We work with a lot of third-party entities
 9 in all aspects of our operation. And as much as, you
 10 know, we put a lot of trust in what they do and
 11 they're really good partners and they do really good
 12 work for us, we need to be managing that. Sometimes
 13 you just have to manage those relationships. And I
 14 think the same would be true for an information
 15 security program. You still need someone who is
 16 ultimately the voice inside your organization
 17 responsible for that program, whether you're doing it
 18 with your own team or you're managing an external
 19 team. I think it's important.
 20 I also think that the idea of having a
 21 third-party serve in that capacity, particularly
 22 around information security, I think there's things to
 23 consider there in terms of what is your culture,
 24 what's the culture of your organization. Is that --
 25 you want -- I advocate for having an organization who

211

1 knows you as an entity. They know your organization,
 2 your culture, how you operate, your risk tolerance.
 3 That might be hard to do from a third-party
 4 perspective, especially if they have a portfolio of
 5 entities that they support. You know, they've got --
 6 they have to know your nuances to know, okay, well,
 7 you know, what things are relevant here and, you know,
 8 what are the aspects of their level of tolerance
 9 around risk that we have to account for in the
 10 program.
 11 So I think it can fill a role if you don't
 12 want to stand up your own internal resources. But
 13 maybe it's a split role, at a minimum, with
 14 management, but maybe even your team itself where you
 15 still have some internal resource as well as being
 16 supplemented or bolstered by a third-party entity.
 17 I just think in these cases, it's helpful to
 18 have ownership within and that true commitment to
 19 protecting, you know, the assets from within the
 20 organization.
 21 MS. WETHERILL: Great. Thanks, Michele.
 22 Karthik, did you have anything to add on
 23 that topic?
 24 MR. RANGARAJAN: Yeah. I think I mentioned
 25 this earlier, but if you -- if you're building

212

1 products and services in-house, then it becomes key
 2 that you have somebody internally managing the
 3 program, even if you depend entirely on third parties
 4 to manage the program. But it's key that you have
 5 somebody present the what-if's of security in-house
 6 that's not completely outsourced.
 7 Third parties, there are a lot of good
 8 services you can get from third parties if you want
 9 penetration testing, vulnerability assessment, even
 10 risk management. You don't have to become an expert
 11 in risk assessment technologies. You can hire people
 12 to do that for you. But you need somebody in-house
 13 that can translate that and that can convert that into
 14 something that is meaningful for your business.
 15 So if you hire a third-party to do all of
 16 it, they don't live and breathe with your business.
 17 They don't work with your business all the time. So
 18 they are only going to give you the perspective, the
 19 outside perspective. But to get an inside
 20 perspective, you might want to have somebody in-house.
 21 From my perspective, is it imperative to
 22 have somebody in-house? I think that's kind of where
 23 the qualifier comes in, where if you're building in-
 24 house systems, then, yes, it becomes imperative that
 25 you have somebody in-house, even if that is not a

213	<p>1 designated security person, even if it is somebody on 2 engineering that's managing these -- or some engineer 3 in IT that's managing these folks. But it is 4 imperative that there is some person, there is a 5 person whose job it is to think about security for the 6 firm. 7 If you're not managing in-house systems, if 8 everything is external, as I said, everything is 9 outsourced, then there is more flexibility, I believe, 10 for these in terms of getting these third parties to 11 understand how these outsourced systems work. You can 12 get guarantees from our outsourcing providers, too, 13 where if you're -- at least if you're doing vendor 14 security assessments and things like that at the 15 outset, you can get guarantees from these outsource 16 providers that they are doing the right things from a 17 security perspective. 18 So that's where this is. It depends on how 19 your business works. There is obviously a cost 20 associated with having somebody in house that is 21 managing security for you. Security is almost always 22 seen as a cost sector, even though that is the 23 function everybody looks for when there is the biggest 24 incident that happens. 25 But I think it comes down to the fact that</p>	215	<p>1 be at odds. 2 I think there's also the question of 3 knowledge transfer, too. If you are relying solely on 4 third parties then turnover may be more of a risk. 5 You just have less insight into some of the external 6 factors that might impact the third party that you're 7 working with. So if you've been working with a 8 dedicated partner for a while and they leave or 9 something else happens, then you might be at risk of 10 losing some of that knowledge, that institutional 11 knowledge, that they've built up. 12 So, again, I think, you know, maybe this is 13 where some of the documentation and just process comes 14 into play. Not that you're paying for them to do 15 that, but in order to have effective knowledge 16 transfer when you have some kind of a handoff. That 17 becomes even more important with third parties. 18 And then I think briefly, Robin, just to go 19 back to the prior question on documentation, and 20 actually really tier two is that there may be an 21 element of privilege that comes up when documenting 22 part of an information security program or specific 23 risk decisions that may have been made in response to 24 a particular regulatory requirement. 25 We see this a lot on the privacy side, for</p>
214	<p>1 you have to make the call that is right for your 2 business and how your business operates. And no 3 matter which way you go, there's going to be a cost. 4 Whether you hire a person or whether you outsource, 5 there's going to be a cost and it's figuring out which 6 cost you're more willing to accept. 7 MS. WETHERILL: Great. Thanks, Karthik. 8 Adrienne, did you have any comments about 9 the costs or benefits of using a third-party? 10 MS. ALLEN: I agree with what's been said 11 before. I think there is, again, a time and a place, 12 and it very well may be along the maturity curve that 13 you start with a third-party and eventually move 14 towards someone coming in-house. 15 I agree that, you know, they actually are 16 going to have less insight into some of the business 17 drivers. It's going to take more work to get there. 18 And I do think it's worth noting, too, that at the end 19 of the day they still do have that split mission and 20 even cost incentive between their employer and the 21 company that they're supporting. And that is not 22 nothing. You know, they're going to be incentivized 23 to bring in money for their employer and they're also 24 incentivized to provide the best quality work for you. 25 But sometimes -- and on occasion those two things may</p>	216	<p>1 example, where the laws are still emerging in some 2 places and there may be room for a particular opinion 3 about the company's decision to implement something or 4 not implement something. So I think that partnership 5 between legal and security also becomes more important 6 when deciding, you know, what are the major things 7 that we want to document; when do we want to retain 8 attorney/client privilege in some of those things. 9 And then same thing here with third parties 10 as well. You know, I think one of the drawbacks of 11 working with third parties is that you can't really 12 allow for their own training and development. There 13 are employment laws around that. And so, you know, I 14 think ultimately building into a workforce that knows 15 your services, your technology, enabling them to 16 invest in their own career path and learning 17 development is something that you can't do with a 18 third-party. You basically take them as they come. 19 So I think that's another drawback as well. But it's 20 more important to consider the long run, not 21 necessarily right away when using a third party but 22 certainly as you work with one over time. 23 MS. WETHERILL: Okay. Thank you, Adrienne. 24 We just have a few minutes left, so I want 25 to very quickly try to address some of the audience</p>

217

1 questions that we received. And here's one that I
 2 think we haven't discussed, and I think this really --
 3 I'm going to direct this to Michele, but if others
 4 have comments, feel free to weigh in. But I think
 5 this is an interesting issue.
 6 So the question says, please address the
 7 issues that may be presented at public institutions
 8 subject to open records requests. And if the annual
 9 written report is detailed as to vulnerabilities,
 10 could that create a roadmap for bad actors?
 11 And so I'm interested to hear if this is an
 12 issue that has come up in any of your work and how you
 13 have kind of worked around that.
 14 MS. NORIN: It has absolutely come up.
 15 Having served, you know, in public institution
 16 settings, we are subject to overt type circumstances.
 17 And so we try to balance that as best we can. We
 18 don't -- you know, there are ways that we can get to
 19 the details that would be considered sort of under the
 20 purview of our general counsel that would give us some
 21 layer of at least internal-eyes-only type of
 22 perspective. But it is an issue.
 23 And, you know, we were talking about
 24 documentation earlier. Everything that is as a record
 25 of our operation is subject to being requested by

218

1 outside entities. And so it is what it is. We
 2 operate around that and we do the best we can in, you
 3 know, just trying to create documentation and enough
 4 information that we can take action on. But it
 5 doesn't give away or create an even bigger
 6 vulnerability for us in terms of, you know, how we
 7 produce those kinds of reports.
 8 I know, for example, in dealing when I give
 9 reports to our board sometimes, I will give reports
 10 that are oral, not always on a piece of paper.
 11 Depending upon the certain circumstances, that may be
 12 an approach that, you know, would work in a particular
 13 incident or something that I need to convey.
 14 But, you know, I think that's where it's
 15 important to have a really good relationship and
 16 operating procedure with the legal counsel or general
 17 counsel's office so that, you know, we are following,
 18 you know, the essence of the requirement of those
 19 kinds of requests, but yet also, you know, making sure
 20 that we're not creating a different kind of liability
 21 internally.
 22 MS. WETHERILL: Okay, great. So we have one
 23 minute left. So as a lightning round, if everyone
 24 could just very quickly go around and say, you know,
 25 if you had to pick kind of one strategy or feature of

219

1 an information security program that for you is the
 2 best or most effective way to build accountability
 3 into the program, what would that feature be? And I'm
 4 going to start with Adrienne.
 5 MS. ALLEN: I think if I had to pick one, it
 6 would be going back to that idea of a single person
 7 who's accountable and making sure that they have
 8 enough influence to make security management an issue.
 9 I think, you know, as long as security is going to be
 10 a second-class topic to some of these other management
 11 issues, then it's much less likely to get integrated
 12 with the rhythm of the business.
 13 MS. WETHERILL: Great, thanks.
 14 Michele?
 15 MS. NORIN: So we like to work with carrots
 16 and not always sticks, but sometimes if we need a
 17 stick a couple things we've done in the past is cost
 18 sharing in incident response situations with the unit
 19 that has caused an issue. So if we've had a breach,
 20 for example, and we figure out that it was something
 21 that we've been trying to work with a particular
 22 department around and it just hasn't quite stuck, then
 23 sometimes having to pay to remediate builds a little
 24 bit of a different level of awareness.
 25 MS. WETHERILL: Great. All right.

220

1 And, Karthik, I'll let you kind of have the
 2 last word, so go ahead.
 3 MR. RANGARAJAN: Yeah. I'd say the biggest
 4 thing -- I think I would say two things. One is
 5 having the central point person that we've talked
 6 about, having security be represented at management
 7 and having this person write these risk quantification
 8 reports I spoke about earlier, having that will give a
 9 way to keep accountability for this person and for the
 10 company as a whole.
 11 The second thing is measure why security
 12 matters for this company. Like, how does it impact
 13 your customers; how does having this person make your
 14 product better or worse for customers, and how can
 15 this work well for the business and the company in the
 16 long term, having some sort of mechanism to metrics
 17 along that can help the business make these decisions
 18 in a much better way. And it will make it easier for
 19 us to have the carrots and sticks we need to do our
 20 jobs well.
 21 MS. WETHERILL: Great. Well, thank you so
 22 much again to all the panelists for joining us. It's
 23 been a great discussion. We really appreciate your
 24 help and your input today. And thanks to everyone
 25 who's tuning in. We will now take a 15-minute break

221	<p>1 and then be back with our final panel of the day. So 2 thanks again and have a great afternoon, everyone. 3 (Whereupon, a recess was taken from 3:18 4 p.m. to 3:31 p.m.) 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25</p>	223	<p>1 bilinear map-based cryptography. 2 Randy Marchany, who is joining us from 3 Virginia Tech, he is the CISO of Virginia Tech and has 4 been there since -- has been acting as CISO since 5 2010. He has 30 years of experience in cybersecurity 6 and has been a senior SANS Institute instructor since 7 1992. 8 Finally, Wendy Nather is joining us from 9 Austin, Texas. She is the head of advisory CISO team 10 at Duo Security, now part of Cisco. Wendy has led 11 security at a Swiss bank and in Texas state 12 government. She has served as research director for 13 the security practice at 451 Research, and was 14 research director for Retail Hospitality ISAC. 15 So, welcome Matthew, Randy and Wendy. Thank 16 you very much for participating in the panel today. 17 Now, as we've been discussing throughout the 18 day, these proposed amendments to the Safeguards Rule 19 are process-based. However, there are two instances 20 where they would require financial institutions to 21 adopt specific security safeguards. And that would be 22 in encryption and multifactor authentication. However, 23 the proposed Safeguards Rule allows flexibility and 24 implementation and alternative controls if approved by 25 a person in charge of the program.</p>
222	<p>1 ENCRYPTION AND MULTIFACTOR AUTHENTICATION 2 MS. MCCARRON: Hi. Good afternoon and 3 welcome to the fifth and final panel of the GLB 4 Safeguards Rule workshop. My name is Katherine 5 McCarron. I'm an attorney at the Division of Privacy 6 and Identity Protection of the Federal Trade 7 Commission. 8 This afternoon, I am joined by three experts 9 who will address the issues of encryption and 10 multifactor authentication. I'd like to take a moment 11 to introduce them, please, before we dive into the 12 substance of our panel. 13 I would also like to say that if anybody 14 listening in the audience has questions for our 15 panelists, please feel free to email those questions 16 to the email address safeguardsworkshop2020@FTC.gov. 17 Thank you very much for participating in the workshop 18 today. 19 First I would like to introduce Matthew 20 Green. Matt is a cryptographer and associate 21 professor at the Johns Hopkins Information Security 22 Institute, where he teaches cryptography. His 23 research focus is in the area of applied cryptography 24 and includes techniques for privacy enhanced 25 information storage, anonymous payment systems and</p>	224	<p>1 So, first of all, I'd like to start with 2 encryption. The proposed encryption requirement would 3 require that all customer information held or 4 transmitted be encrypted both in transit over external 5 networks and at rest. 6 Some points to note about the proposed 7 amendment's language. First, the encryption 8 requirement would apply only to customer information, 9 and it would apply only to transmitted information 10 when it's transmitted over external networks. 11 The proposed rule does not require any 12 particular technology or technique. Finally, if a 13 financial institution determines that encryption is 14 infeasible, it may use effective alternative 15 compensating controls that -- as long as they're 16 reviewed and approved by the person in charge of the 17 program. 18 So I'd like to, first of all, start by 19 asking Matthew whether encryption has become 20 sufficiently inexpensive and simple to adopt that it 21 should be required for all financial institutions when 22 handling sensitive data? 23 MR. GREEN: Okay. Well, first off, there 24 are, as you just mentioned, different kinds of 25 encryption. There's encryption for data in motion and</p>

225

1 there's encryption for data at rest. In the data-in-
 2 motion setting, we have some types of encryption, for
 3 example, SSL and now called TLS, which have become
 4 extremely efficient over the last few years and
 5 efficient to the point that they're almost universally
 6 adopted. I think website usage is above 80 percent
 7 and other types of services are using them at similar
 8 rates.

9 So overall the efficiency of these
 10 technologies has gotten to the point where the
 11 computational cost is just a few percent in addition
 12 to what you already have to deal with in most cases
 13 using normal data transmission.

14 The biggest cost really is certificate
 15 management. People have to install and maintain
 16 certificates. But even that has become much easier
 17 thanks to things like Let's Encrypt where you can get
 18 free TLS certificates and install them on your
 19 machine. So essentially the costs have gone down to
 20 the point where I think if you're not using TLS
 21 encryption for data in motion, then, you know, you're
 22 making a sort of unusual decision that's outside of
 23 the norm, at least outside of your network.

24 Data at rest is a much more complicated
 25 point because there are many different ways to do

226

1 that. So I won't sort of go into all of that right
 2 now. But certainly data in motion is much more
 3 feasible to do.

4 MS. MCCARRON: Okay. Thank you very much.
 5 Randy, I'd like to followup with you. Can
 6 you provide your perspective on encryption and whether
 7 it has become sufficiently simple or inexpensive to
 8 adopt that it should be required by all financial
 9 institutions?

10 MR. MARCHANY: Yeah. I mean, I agree, you
 11 know, entirely with what Matt said. For in motion,
 12 especially through doing any type of web-based
 13 traffic, it is a no-brainer. I mean, in fact,
 14 most people don't even know it's being done for them
 15 because it's been set up by the web server users.

16 Web-based traffic is one way that sensitive
 17 data is transmitted. Another way that sensitive data
 18 is transmitted is the crazy standard email attachment.
 19 I'm sending you a financial form. I'm encrypting that
 20 form as an attachment and I'm sending that to you.

21 And as Matt alluded to at the end, that's
 22 where it gets a little crazy in terms of what type of
 23 encryption methods are you going to use, you know, in
 24 making sure -- there's two cases. One is when you're
 25 all inside your organization's umbrella; Virginia Tech

227

1 to Virginia Tech, for instance. But if I'm sending
 2 something from Virginia Tech to, say, Matt at Johns
 3 Hopkins or Wendy at Cisco, we have to make sure that
 4 they can decrypt whatever it is that I'm sending to
 5 them and vice versa. So there's got to be a lot more
 6 coordination done that way.

7 For us at Virginia Tech, we start off with
 8 the data classification. We say any high-risk data
 9 has to be encrypted at rest or in transit. And high-
 10 risk data is any data that's covered by regulations.

11 The one curious thing about the proposed
 12 safeguards is they don't -- I believe they need to be
 13 delayed before they come out because they're not
 14 taking into account the new environment that we're in
 15 right now. We have cloud infrastructure. We're
 16 working from home. And while that does make
 17 encryption still not that difficult, but the way the
 18 Safeguard Rules are worded, that needs to be
 19 addressed. And so from the safeguard standard, there
 20 needs to be some change done; from the user standard,
 21 not that much.

22 MS. MCCARRON: A followup question for you
 23 when you were talking about data that you received
 24 from other parties: how frequently do you have data
 25 that should have been encrypted and was not?

228

1 MR. MARCHANY: Well, I mean, it happens.
 2 You know, a lot of times, especially in the case of
 3 financial aid where parents, you know, are using their
 4 Gmail system or whatever, they put something in the
 5 clear and send it to us, and we can't really do
 6 anything about that. That's outside of our bubble, so
 7 to speak. But the moment it comes into our control,
 8 then our encryption standard kicks in.

9 MS. MCCARRON: Do you have particular tools
 10 that you can use to try to find the sensitive data so
 11 you know where it is so you can protect it on
 12 university systems?

13 MR. MARCHANY: Yeah. And this is -- this is
 14 something that everybody does. There is one -- I'm
 15 not connected with this company in any way, shape or
 16 form. But there's a company called Spirion, and Palo
 17 Alto and a number of other ones have features like
 18 this. But basically they have tools that do search
 19 for what we would call PCI, you know, or PII data,
 20 personally identifiable data; social security numbers,
 21 credit card numbers, driver's license numbers,
 22 passport numbers.

23 You know, it's not a perfect tool. It
 24 doesn't have complete functionality across all the
 25 major platforms, but it certainly covers Windows well.

229

1 And that's -- you bring up a great point because
 2 before you can encrypt it, you have to find it. And
 3 we're all digital pack rats. We have folders from,
 4 you know, 15, 20 years ago that may have Social
 5 Security numbers in them.
 6 So, yes, we have to find it first; decide do
 7 we still need it. If the answer is no, get rid of the
 8 file. If the answer is yes, then encrypt it.
 9 MS. MCCARRON: And then a final followup for
 10 you, Randy. I wanted to ask, you know, the Commission
 11 is interested in the costs of these proposed
 12 amendments to the Safeguards Rule. So as a financial
 13 institution scales up, how much does it increase the
 14 cost to encrypt data, and just using Virginia Tech as
 15 an example?
 16 MR. MARCHANY: Well, if you're going to use
 17 a vendor product, you need to look at their licensing
 18 structure. They may have a charge per license, per
 19 user. It may be a blanket thing. A common
 20 denominator might be to use Microsoft Office file
 21 encryption. It meets the AES standards. It's
 22 password, you know, based. But you can, you know,
 23 deal with that situation. But if I'm sending
 24 something to Matt or to Wendy at their respective
 25 things, I could use Office encryption and then out of

230

1 band send them the password and they can open it up
 2 and do whatever they need to and store it using their
 3 own local encryption systems.
 4 So it's going to depend on the costs. But
 5 if I were looking at uber-cheap enterprise-wide, we're
 6 already paying for Microsoft licenses and encryption
 7 is already built into the Office environment. So
 8 spreadsheets, .xls, DocX, PowerPoint and a number of
 9 other Microsoft Office products all support that
 10 encryption feature.
 11 MS. MCCARRON: Thank you. That's very
 12 informative. I'd like to turn to multifactor
 13 authentication and talk about the requirement that
 14 would be in the proposed amendments to the Safeguard
 15 Rule.
 16 The proposed amendment would require
 17 financial institutions to implement multifactor
 18 authentication for any individual accessing internal
 19 networks that contain customer information. And as
 20 all of you know very well, multifactor authentication
 21 must include two of three factors. The first is the
 22 knowledge factor, which is things that you know such
 23 as passwords or biographical information.
 24 The second factor is the possession factor,
 25 things that you have. That could be tokens or

231

1 possession of devices.
 2 The third factor is the inherence factor,
 3 things that you are, such as biometric
 4 characteristics, fingerprints or voice.
 5 The text of the proposed amendment lays out
 6 these items, but what it doesn't say is whether or not
 7 you can use SMS as an appropriate factor for
 8 multifactor authentication.
 9 So, Wendy, I'd like to turn to you first and
 10 ask, what is your view on whether SMS is an
 11 appropriate factor for multifactor authentication?
 12 MS. NATHER: Well, there are certain risks
 13 with SMS that are very well known by now. Sort of the
 14 implied possession factor for SMS is that you possess
 15 the phone. But what it really turns out to be is that
 16 you possess the phone number and attackers do have
 17 ways of stealing that phone number out from under you,
 18 which is NIST had announced that they wanted to
 19 deprecate the use of SMS.
 20 But when they made that announcement, there
 21 were a lot of objections, including from me, for a
 22 number of reasons. First of all, it's the cheapest
 23 and most widely available method for sending a code
 24 out. And in most of the world, people do not
 25 necessarily have smartphones. They have to use SMS.

232

1 So for financial institutions who cannot
 2 control the devices that their partners or their
 3 customers or even their employees are using, they're
 4 stuck with what's available. So there are plenty of
 5 times when you have to fall back to SMS.
 6 Now, as far as the phone number or the SIM
 7 jacking problem, I have talked to telco companies that
 8 are trying to address that issue. They realize that
 9 it's a problem. And I think a big challenge will be
 10 to get telco providers around the world to get
 11 together to address that threat.
 12 So is SMS the best solution? No, it isn't.
 13 But we don't necessarily tell people that they have to
 14 use, you know, bank-level security on their front
 15 doors, either. It may be practical and usable for a
 16 certain number of risk cases. And so there's no way
 17 to bar them from using SMS.
 18 MS. MCCARRON: Okay. As a followup
 19 question, Wendy, I wanted to ask you, how do financial
 20 institutions make that risk-to-cost decision? So when
 21 they're trying to decide do we invest in bank grade
 22 security or something else, how do they make that
 23 decision?
 24 MS. NATHER: In a lot of different ways.
 25 And as Randy intimated, some of it depends on

233

1 licensing, how things are bundled together. When I
 2 was working for the Texas Education Agency, for
 3 example, we could not afford to send people, staff, in
 4 the districts hard tokens. We simply couldn't afford
 5 it. And the other problem was that interacting with
 6 our systems was more of a role than it was an
 7 individually assigned account. So we were never able
 8 to be sure exactly who was going to be using an
 9 account to log in and do the state-mandated reporting.
 10 So that's an example.

11 Another one is that even if MFA is provided
 12 for free. For example, Duo offers up to 10 licenses
 13 for free. There are organizations that don't
 14 necessarily have the expertise or the people who can
 15 even set it up. If you're looking at a CPA firm that
 16 has, you know, three members and none of them are
 17 technical people, then even if they have free MFA,
 18 they may have trouble using it. That's what I refer
 19 to as the security poverty line.

20 And then finally what you want to do -- and
 21 financial institutions want this as much as anybody --
 22 is to be able to use factors that are easiest to use
 23 at the point of authentication.

24 Now, I have a slide that I think we can
 25 bring up here from -- thank you -- from a Duo industry

234

1 report. And I have to say, I have to caveat this by
 2 saying that we looked at data based on people who were
 3 using the Duo product and looking at which factors
 4 they tended to use the most often.

5 So you can see in this chart we picked four
 6 really popular industry sectors. We picked healthcare
 7 and financial services, higher education and the
 8 federal government. And you can see the different
 9 factors that a user has to be involved with, you know,
 10 that the user has to actually touch or use or interact
 11 with. There are many other factors that are available
 12 that are kind of hidden to the user, but this is the
 13 one that involves the users.

14 And you can see that simply clicking a
 15 button, what we call the Duo push, and saying, yes, I
 16 really do want to log in, clicking that on an app is
 17 the most popular. But they will also use the option
 18 of a phone call to a landline where they pick up the
 19 phone and say -- you know, and they hear press 1 to be
 20 connected, and they press 1 and then they can hang up
 21 again. And that's very popular. Twenty percent of
 22 healthcare uses that for one reason or another. It
 23 may be easier for the doctors and the nurses and so
 24 on.

25 You can see here that SMS passcodes are

235

1 already falling out of favor in general among the
 2 users. Where they have a better alternative, they do
 3 tend to use it. So despite the fact that SMS is still
 4 necessary sometimes, it's a good sign that
 5 organizations are using it less and less.

6 And then, of course, hardware tokens are
 7 very popular in the federal government. We don't see
 8 that going away anytime soon.

9 So I hope this gives us a good picture of
 10 what organizations are using today, not just for
 11 reasons of cost but for reasons of usability for their
 12 users.

13 MS. MCCARRON: Thank you. Yes, that is very
 14 informative.

15 Randy, I'd like to turn to you next and ask
 16 the same question in terms of how financial
 17 institutions make the risk-to-cost decision. And if
 18 you could, you know, just let us know about how
 19 Virginia Tech made those decisions when it was
 20 implementing multifactor authentication. And you're
 21 on mute.

22 MR. MARCHANY: When it comes down to this,
 23 it basically is, again, high-risk data versus low-risk
 24 data. And so the big risk is are there financial
 25 penalties if there's a breach. Is there -- you know,

236

1 Virginia has a data breach notification law. What's
 2 that going to cost us if there is a data breach. You
 3 know, if a high-risk data breach happens, it's not
 4 only my office, the security office, that gets
 5 involved; the data owners, the CFO, for instance, gets
 6 involved.

7 But the public relations wing of the
 8 university gets involved because we have to set up,
 9 you know, press releases. You know, things like
 10 what's a hidden cost. The institution pays for a
 11 year's worth of credit monitoring for however many
 12 people -- however many records are, you know, exposed.
 13 Right now I think that price is somewhere around 15
 14 bucks a record. So you get a 6,000 record, you know,
 15 breach and multiply that by 15, and that gives you the
 16 cost just for credit monitoring.

17 Now, again, maybe 5 to 10 percent of the
 18 people who are offered credit monitoring take that.
 19 But you have to reserve that amount of money in case
 20 everybody does. So there is a financial risk, you
 21 know, involved with that.

22 We moved to two-factor authentication in
 23 2016 as a result of a recommendation from a task force
 24 that I chaired back after we had a breach in 2013.
 25 And multifactor was -- two-factor authentication was

237

1 one of the recommendations. Our CIO basically gave
 2 our team, the central IT staff, a year to implement
 3 it. And, you know, we ripped the band-aid off, so to
 4 speak. July of 16, all faculty, staff and students
 5 were two-factor.
 6 Now, we had a six-month transition period
 7 where we could get the early adopters and we worked
 8 out most of the bugs before the final date. But, you
 9 know, right now we have over 156,000 users at Virginia
 10 Tech.
 11 Again, with regard to the Safeguards Rule,
 12 universities and colleges are in an interesting spot
 13 with regard to the regulations because we handle, you
 14 know, financial aid. So that says, yes, we're a
 15 financial institution under the GLBA definition. But
 16 that's not our primary business. So our primary
 17 business is not financial. It's a much more open
 18 model.
 19 And so under the current standards, we have
 20 that flexibility to -- where they leave it up to us to
 21 adjust to our model. I bring this up because, as
 22 Wendy mentioned about with the phones, you know, we've
 23 -- BYOD, every student at Virginia Tech is required to
 24 own a personal computer. 33,000 students. You know,
 25 we have 6,000 of them, or somewhere between 5,000 and

238

1 6,000 come every year. They own their own devices.
 2 We don't control those devices. Some of the students
 3 have text-only plans. Some of them don't have -- more
 4 than I thought don't have smartphones. They use flip
 5 phones. They may have their phone or text plans
 6 charge them for text messages, and so they incur a
 7 cost if they're using SMS.
 8 And so, you know, how do you -- you have to
 9 address that type of stuff. BYOD for us is not a big
 10 deal. We've been doing it since 1984. But a lot of
 11 the rest of the world is now, you know, how do we deal
 12 with this with work from home? You know, are you
 13 using an institution, you know, owned device or are
 14 you using your home computer? So there's lots of
 15 things you have to take into account that way.
 16 MS. MCCARRON: Thank you very much.
 17 Now, one of the questions that is raised by
 18 the proposed amendments to the Safeguards Rule are
 19 whether there are instances where multifactor
 20 authentication is not appropriate for users accessing
 21 sensitive information, or put another way are there
 22 circumstances where it may be more difficult within a
 23 common infrastructure for financial institutions
 24 affected by the rule to use MFA?
 25 In those circumstances, I want to talk about

239

1 what would be -- what are reasonably equivalent or
 2 more secure access controls that could be approved by
 3 a CISO?
 4 So, Matt, can I start with you, please?
 5 MR. GREEN: So, you know, there are a lot of
 6 different ways to do this, to provide alternative
 7 access controls. A lot of them really do kind of fall
 8 under the general category of MFA because MFA is just
 9 such a broad term.
 10 But leaving that aside, I mean, nowadays one
 11 of the things that most people think about when they
 12 think about MFA and 2FA is these little key fobs that
 13 you carry around. This is kind of the classical
 14 version of what 2FA is. But nowadays we carry phones
 15 with us basically everywhere. Your phone can be your
 16 car key. It can be sort of everything that you use.
 17 And phones nowadays have modern secure hardware
 18 processors inside them. They have biometric sensors
 19 and readers. So we can increasingly get a lot of the
 20 security we need just through these devices that we
 21 already have by storing cryptographic authentication
 22 keys on the devices and then using the phone to
 23 actually activate those.
 24 It is MFA but I think it's a more practical
 25 version of MFA that's maybe a little bit more, you

240

1 know, friendly for people to use. And then there are
 2 other techniques that people can use. For example,
 3 there are these behavioral systems that look for
 4 patterns of behavior in the way that people access
 5 systems and try to identify fraud. I don't know if
 6 they're particularly effective in all cases but
 7 certainly people do deploy systems like that. So
 8 there are some options.
 9 MS. MCCARRON: Thank you.
 10 Wendy, I wanted to ask the same question to
 11 you. Are there other circumstances where you think
 12 that a financial institution would need to use
 13 something other than MFA that would be reasonably
 14 equivalent or more secure access controls?
 15 MS. NATHER: Where it might be difficult is,
 16 again, for smaller financial institutions that are
 17 below the security poverty line where they're very
 18 heavily dependent on the third-party software that
 19 they're using.
 20 For example, I have seen tax preparation
 21 companies that are using cloud-based services that use
 22 email as a poor man's multifactor authentication. In
 23 other words, you log in with your password and then it
 24 sends you an email back to your address of record with
 25 a code that you then have to type in. That's the

241

1 cheapest and slowest and, you know, kind of least
 2 reliable method there.
 3 But, again, it's what the smaller
 4 organizations are stuck with. Because the level of
 5 influence that a company has may determine whether
 6 those companies can make their third parties use
 7 multifactor authentication.
 8 In cases where state governments, for
 9 example, have to contract to very small firms, this
 10 may not be possible at all for the very small firms
 11 that they're contracting with. It can be difficult
 12 for mid-sized companies to force those third parties,
 13 especially with certain software that can't be
 14 replaced.
 15 You asked about whether there are any times
 16 when it's inappropriate to use MFA. And the only
 17 thing that really comes to mind is if availability is
 18 much more important than confidentiality, when you
 19 have to get access to something because of public
 20 safety.
 21 For example, a healthcare provider once
 22 said, I would rather not see my patient dying on the
 23 gurney with their privacy intact because I couldn't
 24 get into the equipment that I need to save them. So
 25 that kind of thing could be a very good reason when

242

1 MFA is not -- either not practical, not appropriate or
 2 it needs to fail open if there's any question about
 3 whether, you know, people can get access.
 4 Sometimes MFA may not be necessary because
 5 the risk is being mitigated by other factors. For
 6 example, I had a healthcare provider ask me how to use
 7 MFA in a sterile operating theater where you cannot
 8 sanitize any of the things that we would normally
 9 bring in for multifactor authentication. But if
 10 you're looking at the real risk scenario around that,
 11 if it's a sterile operating theater, it's probably
 12 physically secured. If you locked down the account so
 13 that it could only be accessed from the equipment
 14 inside of that operating theater, you might not
 15 actually need MFA. So there are a lot of different
 16 ways where you could put in alternatives if it really
 17 becomes too impractical.
 18 MS. MCCARRON: And, Randy, may I ask you,
 19 can you think of any circumstances of where a
 20 financial institution would need to put a reasonably
 21 equivalent or more secure access control in place?
 22 MR. MARCHANY: Well, the business process is
 23 always going to trump the security process. That's
 24 been my experience with this. But I think in the
 25 beginning a lot of financial services sort of shield

243

1 away from MFA because they thought it was, you know,
 2 too difficult or people wouldn't use it. And it's the
 3 seat belt problem. You know, in the '60s when seat
 4 belts were being mandated by the federal government,
 5 automakers rebelled. They said customers will never
 6 buy this. And then an automaker -- if I remember
 7 right, it was American Motors -- they started
 8 marketing it as a safety feature. And then all of a
 9 sudden they noticed a little uptick in their sales
 10 because, oh, it's a safety feature; I'm going to buy
 11 that.
 12 And we've seen sort of something similar
 13 happen with financial institutions that now they're
 14 marketing this as a safety factor. This is one more
 15 piece of our security portfolio to, you know, help
 16 ensure the security of your financial data that you're
 17 entrusting with us.
 18 So I think you're seeing that shift. Where
 19 it goes south is -- as Wendy said, is a lot of
 20 vendors, software vendors, still aren't -- haven't
 21 gotten it yet to at least provide APIs or some sort
 22 of, you know, mechanisms to allow us to hook an
 23 authentication system, two-factor or not, into their
 24 software. And so, you know, that needs to be
 25 addressed.

244

1 I think shared assessments, you know, if
 2 everybody in the industry says, hey, these vendors,
 3 their software packages support 2FA or MFA, these guys
 4 don't, I think that's a way that we can apply pressure
 5 on the vendors to kind of move into the MFA
 6 requirement with the shared assessment process.
 7 But as Wendy said, public safety. You know,
 8 if you're a first aid, first responder, you're there,
 9 you're dealing with an accident victim or whatever,
 10 you don't have time to just say let me get my fob and,
 11 you know, jam it in there. In some cases, you don't
 12 even have time to log in. So public safety certainly
 13 would be the one time when I would be, you know,
 14 really considerate of the fact that it might not work
 15 in that environment.
 16 MS. MCCARRON: All right. But no financial
 17 institution situations come to mind?
 18 MR. MARCHANY: I can't think of one that
 19 would want to do that because their competitors would
 20 immediately say our version is safer. You know, and
 21 sooner or later, you know, that's going to hit their
 22 bottom line.
 23 MS. MCCARRON: So I'd like to ask, then,
 24 about what possible alternatives there are to
 25 encryption and multifactor authentication.

245

1 So let me just start, Wendy, I'd like to ask
 2 you first. Starting with MFA, what is your view about
 3 whether IP address restrictions are a reasonable
 4 equivalent to MFA? Yes, go ahead.
 5 MS. NATHER: Yeah. I was going to say, no,
 6 please! IP addresses, we know, are not practical as
 7 -- especially as a single authentication factor. We
 8 know they can be spoofed. And, in fact, the entire
 9 zero trust security movement these days is in reaction
 10 to our realization that you cannot trust something
 11 just because it comes from a certain IP address.
 12 Now, it used to be that IP addresses were
 13 used as proxies for geolocation. We would assume that
 14 if you came from this IP address, you must be inside
 15 the office building and therefore you were safer
 16 because you came through physical security and there
 17 were other things that happened in the background to
 18 authenticate you. But we know now that that's not
 19 safe.
 20 And, in fact, relying on IP addresses for
 21 authentication and for trust has resulted in some
 22 really large famous breaches, including in the 2000s
 23 when government-backed attackers attacked a lot of
 24 high-tech companies including Google and took
 25 advantage of the fact that users were being trusted if

246

1 it looked like they came from inside the internal
 2 network.
 3 So I don't recommend that at all anymore.
 4 Sometimes you still need to use geolocation as part of
 5 your authentication or access restriction because of
 6 data privacy laws based on country or that sort of
 7 thing. But we have much better technology to do that
 8 now. We have GPS-based access control that works
 9 better.
 10 MS. MCCARRON: Okay, thank you.
 11 Matthew, I'd like to ask you the same
 12 question. Can you share with us your view about
 13 whether IP address restrictions are a reasonable
 14 equivalent to MFA?
 15 MR. GREEN: Yeah, I absolutely agree with
 16 Wendy. I mean, IP addresses are, you know, the burner
 17 phone numbers of the internet. Right? Anyone can
 18 just VPN to another location, use different IP
 19 addresses. It's a terrible way to try to actually
 20 authenticate people. You know, there are more
 21 sophisticated network-based attacks where you can
 22 actually, you know, pretend to be from a specific IP
 23 address, and those are more complicated to execute.
 24 But just moving around to different parts of the
 25 internet is something that's available to really the

247

1 lowest common denominator of attackers, I think, at
 2 this point.
 3 MS. MCCARRON: And what about device or
 4 account restrictions like behavioral fingerprinting as
 5 an alternative?
 6 MR. GREEN: You know, this is not my area of
 7 expertise, but part of the reason that I work in
 8 encryption is because there's a certain amount of
 9 certainty around encryption. If you encrypt something
 10 and you secure the keys well, it stays protected.
 11 It's sort of like putting it in a bank vault. Whereas
 12 with behavioral type of technologies where you're
 13 looking for patterns of misbehavior, you don't get
 14 that certainty. There's no mathematical theorem that
 15 says, hey, I can detect this attacker who's in your
 16 system. There is some hopeful probability it works,
 17 but I guess from my perspective the difference between
 18 that possibility it might detect somebody and the
 19 certainty that information will stay protected,
 20 there's just such a big delta between those two
 21 things, I don't feel comfortable with the probability.
 22 MS. MCCARRON: Okay. The proposed
 23 amendments to the Safeguards Rule would permit a
 24 financial institution to use something other than
 25 encryption or multifactor authentication as long as

248

1 the CISO had approved it in writing.
 2 So, Randy, I wanted to ask you, as the CISO
 3 of Virginia Tech, to walk us through what that would
 4 be like for a CISO to have to write a justification to
 5 approve an alternative method other than encryption or
 6 multifactor authentication.
 7 MR. MARCHANY: Well, as Mr. T would say, I
 8 pity the fool that has to sign that paper. It's
 9 really -- I would not want to be the person to do it.
 10 In fact, if I was asked to do that, this would be my
 11 terms and conditions, is that it has to come from the
 12 board. The board is the one that has to tell me that
 13 we are willing to -- the institution is willing to
 14 accept this risk of not using it. We're going to
 15 accept it. Go ahead and you figure out a way to make
 16 this work and then sign -- you know, create that
 17 document.
 18 But this is not a bottom-up thing. This has
 19 to come from the board down to the CEO or president or
 20 whoever and then down to us. I just would not -- I
 21 would stay away from that as far as possible.
 22 MS. MCCARRON: Okay. And so what is the --
 23 what would the burden be like on the CISO to have to
 24 write such a justification? What would that look
 25 like?

249

1 MR. MARCHANY: Well, we would be the
 2 scapegoat. I mean, the moment there was a breach,
 3 then all the fingers would point to us and they'd say,
 4 hey, you said this was the way to work. And I said,
 5 no, what I said was the probability is, you know, much
 6 different. But, you know, you'd have to do other
 7 types of analysis. Maybe -- you were talking about,
 8 you know, behavioral analysis, looking at certain log-
 9 in times for certain user IDs. And you can sort of do
 10 that with sort of a continuous monitoring model.
 11 There's a lot of research going on in machine learning
 12 and AI in that type of area of behavioral
 13 characteristics. But, I mean, that is so far away
 14 from where I would go. I'm not sure I'd have an
 15 alternative plan to do that.
 16 MS. MCCARRON: Okay.
 17 Wendy, I'd like to ask you the same
 18 question. Could you provide us with your perspective
 19 on the possible burden to CISOs of having to write
 20 justifications for using methods other than encryption
 21 or multifactor authentication? Whether this -- does
 22 this carve out -- does it help CISOs or does it help
 23 financial institutions?
 24 MS. NATHER: There are two justifications I
 25 can think of here for why you would want the CISO to

250

1 do this writing. And one justification is presumably
 2 the CISO can attest that from a technology point of
 3 view what they're suggesting is equivalent, you know,
 4 functionally, whether it would work.
 5 However, as Randy was alluding to, the
 6 probability, the risk measurement of whether this
 7 really is good enough is something that often is --
 8 this decision is not made at the CISO level. It's
 9 made at the board level in terms of whether they're
 10 going to fund MFA or whether they're going to fund
 11 encryption and say, no, this is just too expensive;
 12 we're just going to accept the risk but make up
 13 something that sounds good and write it down.
 14 So I personally, also as a former CISO,
 15 would much rather see -- for purposes of
 16 accountability to see that landing at the board level.
 17 Now, the other burden that would be on the CISO would
 18 be to argue the sufficiency of the exception with
 19 auditors. And in my experience that's never a good
 20 conversation because what you end up doing is not
 21 talking about whether functionally or technologically
 22 this is equivalent, an equivalent control. You're
 23 talking about whether you're really addressing risk
 24 that neither of you really agrees on.
 25 And so a risk discussion with an auditor as

251

1 opposed to, you know, a checklist or compliance
 2 discussion, is not good. And at the end of the day,
 3 it doesn't even matter what the auditor thinks because
 4 if a breach results from this alternative use, then,
 5 again, the accountability has to go back to the board.
 6 MS. MCCARRON: Thank you. We have a lot of
 7 questions coming in from the audience. So I will take
 8 the first one. And if you would like to answer it,
 9 just please raise your hand and I will call on you.
 10 The first question is we've had cloud
 11 infrastructure and people working remotely from home
 12 for a long time now, relatively speaking. Why do we
 13 need to delay implementation of the Safeguards Rule to
 14 account for that?
 15 Okay, Wendy? Or Matthew. Why don't you go
 16 first. Sorry.
 17 MR. GREEN: Well, actually, you know, I
 18 think Wendy is the right person to answer this
 19 question. I can actually -- I think she --
 20 MS. MCCARRON: Okay. All right. You first,
 21 Matthew, then I'll go to Wendy.
 22 MR. GREEN: Okay. Well, I mean, you know,
 23 so the question is why should we delay. I mean,
 24 personally, you know, I'm an academic and my view is
 25 we should not delay. We should get these things out

252

1 there immediately and there should be none whatsoever.
 2 However, I do know that, you know, at least
 3 from my perspective, a lot of the people that I work
 4 with are having a difficult time rolling out entirely
 5 new systems and, you know, making major changes in
 6 systems that are already stressed by the fact that
 7 we're in this situation that is -- right now seems a
 8 little dangerous to me; things can break.
 9 But I'm not sure, you know, if that's
 10 exactly the best answer. So I will turn it over to
 11 Wendy for that.
 12 MS. MCCARRON: Okay. Wendy, what are your
 13 thoughts?
 14 MS. NATHER: My thought is that, first of
 15 all, you know, this crisis hit us pretty suddenly and
 16 there were a lot of organizations that had to scramble
 17 either to implement remote access that they didn't
 18 have before or to scale up what they had.
 19 And I suspect that in many cases they put in
 20 the cheapest and quickest thing that they could with
 21 the expectation that this would only be lasting for a
 22 few months and then they could go back to normal. So
 23 there was probably not a lot of planning for the long-
 24 term.
 25 Where companies are now facing the prospect

253

1 of, you know, this being long-term or perhaps
 2 permanent to a greater or lesser extent, they may need
 3 to think long-term about more permanent
 4 infrastructure. They may need to rearchitect what
 5 they currently have. They may need to negotiate with
 6 the cloud providers that they had to sign up with in a
 7 hurry who, again, you know, for reasons of influence
 8 may or may not be able to give them what they really
 9 need in order to comply with the Safeguards Rule.
 10 So I think all of those argue for giving them a little
 11 more time.
 12 MS. MCCARRON: Okay. As a followup --
 13 MR. MARCHANY: I have one thing to add to
 14 that, though.
 15 MS. MCCARRON: Yes, please.
 16 MR. MARCHANY: The biggest problem with the
 17 proposed regulations is that they don't take into
 18 account the limitations that an organization may have
 19 when dealing with the cloud vendor. They assume that
 20 we have complete control of logs, access and things
 21 like that which a lot of cloud vendor providers do not
 22 provide to the organization. It's our world. You
 23 want to get logs of how, you know, things are used,
 24 you have to go through our process.
 25 And so there's a lot of things -- I mean, I

254

1 agree with Matt. We should do this. But as a CISO,
 2 I'm the one that's going to have to enforce it. And
 3 there's -- it's not clear. We don't -- continuous
 4 monitoring, for instance. You know, the proposed
 5 regulations say you have to be able to do a
 6 vulnerability scan on your end points. Well, in work
 7 from home, your vulnerability scan packets are not
 8 going to be going just through your network. They're
 9 going to be going to your home ISP network. And your
 10 ISP network may interpret that scan as an attack and
 11 block it or cut you off at the home because you're the
 12 one that initiated the scan.
 13 So a lot of these things are not under the
 14 control of the institution, and that's where the
 15 weakness is in the proposed safeguards. You know,
 16 take work from home out of that picture. You still
 17 have to deal with, you know, try and to get logs from
 18 Amazon or Gmail or even Office 365 when, you know, you
 19 have to have all that stuff contractually agreed upon
 20 before you set it up.
 21 And as Wendy said, if you did something in a
 22 hurry, you weren't thinking about, oh, I need to get
 23 access to email logs or stuff like that. So that's
 24 the reason why I say, you know, they need -- it needs
 25 to be delayed to address these new models. Because

255

1 while we may not be coming back -- you know, we may
 2 not be dropping work from home 100 percent, I think
 3 that percentage is going to stay pretty high for a
 4 long time, especially when we're still in this -- you
 5 know, is the pandemic going to affect our health
 6 thing.
 7 Cloud-based services, you know, how does
 8 your organization get information it needs? You know,
 9 email abuse. Somebody is threatening you with email.
 10 But your email goes through Office 365 that you don't
 11 control, or Gmail, for instance. How do you get that
 12 information you need?
 13 So that's the part that I think is a
 14 weakness in the proposed regs. The current
 15 regulations give us that flexibility. It's not as
 16 hard and concrete and set.
 17 MS. MCCARRON: Thank you for that. There is
 18 another question coming in about alternatives to
 19 requiring encryption. The question is, would
 20 dedicated leased lines be considered an accepted
 21 alternative to requiring encryption?
 22 So I'd like to ask the panel for their
 23 thoughts on dedicated leased lines as an acceptable
 24 alternative to encryption.
 25 MR. GREEN: Sure, an expensive alternative.

256

1 Yeah, I mean, it seems like -- I mean, if your concern
 2 is the price of encryption, I mean, maybe you have a
 3 very good deal on dedicated leased lines that, you
 4 know, I don't know about. But they're not cheap. I
 5 used to work at AT&T so I have some insight into this.
 6 I guess my biggest thinking about this is it
 7 really depends who your attacker is. If you're, you
 8 know, worried about the National Security Agency or
 9 foreign intelligence agency, the answer is, no,
 10 absolutely not because we learned a few years ago that
 11 those are not in any way immune to those kind of
 12 attackers. But even sophisticated nongovernmental
 13 attackers have in some cases shown that they have the
 14 ability to sometimes be able to access these kinds of
 15 systems. So it's risky. It depends on what the data
 16 is. If it's financial data that has value, I'd be
 17 very nervous about that.
 18 MS. MCCARRON: Okay.
 19 MR. MARCHANY: It could be really expensive
 20 especially if your customer base is the public. You
 21 know, how do you deal with that? I'm not going to set
 22 up a leased line to work from home or from my phone.
 23 So, you know, unless as Matt said, unless that company
 24 has got a lot of money, I wouldn't say that it would
 25 be an alternative.

257

1 MS. MCCARRON: Okay.
 2 Wendy?
 3 MS. NATHER: Yeah, just to pile on what all
 4 was said. Yeah, leased lines worked great in the
 5 '90s. I spent a lot of time doing disaster recovery
 6 with leased lines. Believe me, encryption is a lot
 7 cheaper today. It's a lot more flexible. It's a lot
 8 easier. Just, you know -- I can't think of a good
 9 reason to go with leased lines instead.
 10 MS. MCCARRON: Okay. To followup on the
 11 question of the cost of encryption, there's a question
 12 from the audience that says Randy was just asked about
 13 the cost of encryption and his answer was technology-
 14 specific.
 15 I would like the panel to consider the total
 16 cost of an encryption deployment: staffing to
 17 support, training of end-users and, of course,
 18 software and associated licenses. I'd like to open
 19 that up to the panel.
 20 MS. NATHER: I would say five. The cost is
 21 going to be five. Five what? I don't know. That is
 22 one of the big problems with security, is that it is
 23 very difficult for us to price an entire solution like
 24 this. And I've tried several times as a research
 25 analyst. It depends so much on the geographical

258

1 distribution of the organization. It depends upon
 2 what kind of technology they have, whether they're
 3 cloud forward or not, what kind of data that they have
 4 and so on. That's one of the big problems, is we
 5 can't tell you how much it's going to cost.
 6 What we can say is here's a large selection
 7 of acceptable alternatives, try to pick the ones that
 8 work best for you. And in the case of pricing out
 9 what it will take for personnel who have the expertise
 10 and the time to be able to manage these solutions,
 11 again, for smaller organizations they're probably
 12 going to have to rely on vendors and cloud-based
 13 solutions where those things are built in. Just try
 14 to use the built-in versions wherever you can. But
 15 there's no escaping that somebody in the firm is going
 16 to have to at least be able to talk to that vendor
 17 about the technology and get it set up.
 18 MS. MCCARRON: Okay, thank you.
 19 MR. MARCHANY: Yeah, I mean, and you're
 20 right. Now, if you're talking about a support
 21 structure for your identity for authentication, you
 22 have an identity management group. You have -- for
 23 instance, we use Duo. So there's a group that
 24 supports the Duo stuff. You know, my office looks at
 25 Duo logs but so does the help desk. You've got a lot

259

1 of people that are involved on the support side if
 2 you're doing authentication for identity. If you're
 3 doing encryption for, you know, files or data streams,
 4 it can be as much, but, you know, again, it depends on
 5 what your target is.
 6 I mentioned the Office encryption. That's
 7 the lowest common denominator. You know, it comes
 8 built in, but it's a vendor thing. You can certainly
 9 get vendor products that do the exact same type of
 10 stuff.
 11 MS. MCCARRON: Anyone else?
 12 (No response.)
 13 MS. MCCARRON: I'll move on to the next
 14 question that I have. This is a question about
 15 ransomware attacks, which as we heard earlier this
 16 morning is one of the top two types of security risks
 17 for companies right now.
 18 The questioner has asked the panel, should
 19 the proposed GLB Safeguards Rule go farther and also
 20 require secure air-gapped backups of information to
 21 minimize the impact of a ransomware attack? To me,
 22 this seems as important as multifactor authentication
 23 and encryption.
 24 MR. MARCHANY: I'm going to jump into this
 25 one first.

260

1 MS. MCCARRON: Please do.
 2 MR. MARCHANY: The best defense against a
 3 ransomware attack is your backup system. If you get
 4 hit with a backup -- with a ransomware attack, blow
 5 away your -- the affected machines and restore it from
 6 your most recent backups. That's the most effective
 7 means to do so. You may lose a day's worth of work
 8 but I'd rather lose a day's worth of work than
 9 the entire, you know, cake. So our infrastructure,
 10 you know, for ransomware is very, very specific.
 11 Another thing is when you look at a lot of
 12 ransomware attacks that hit organizations, what gets
 13 encrypted in the ransomware attack is not just a file
 14 structure on my computer. It's a file share that I
 15 had with someone else. And we typically leave that
 16 file share open, the permissions open, to anybody that
 17 has access to that.
 18 If you manipulate the permission so that
 19 only this working group has access to these files and
 20 this big common file share, that does limit -- I mean,
 21 you're not going to prevent the damage but you're
 22 going to limit the damage that can be done. That's
 23 why we say use a separate account if you're using your
 24 home computer because most ransomware these days that
 25 we've seen does not require administrative privilege

261

1 to do its damage. It just operates on that.
 2 So if Wendy and I have an account, and Matt,
 3 the three of us have accounts on my computer and Wendy
 4 gets hit with ransomware, there's a good chance it's
 5 only going to encrypt her files and leave our files
 6 alone. So you can do some proactive stuff to limit
 7 the damage. But the number one thing is backups.
 8 MR. GREEN: Yeah. So, I mean, certainly the
 9 question is whether we should require this. I mean, I
 10 guess one of the nice things about ransomware today is
 11 that if you don't protect yourself against ransomware
 12 the way that Randy said, the consequences are you're
 13 in big trouble and, you know, maybe your users are in
 14 big trouble only in the sense that you can't service
 15 them anymore. But at least their data isn't spread
 16 across the internet. Right? It's lost.
 17 If ransomware evolves into the kind of thing
 18 people have been concerned about where it's actually
 19 exfiltration where information is not simply encrypted
 20 but is actually stolen, it's much more challenging to
 21 do. But if that were to happen, I guess maybe the
 22 calculation would change.
 23 Right now I guess, you know, the calculation
 24 that people are making is do businesses -- should we
 25 require that businesses protect their own operations,

262

1 or do we want to have rules in place to just require
 2 them to keep confidentiality of user data? And so
 3 these are really two things. I believe in protecting
 4 the confidentiality of user data and I also think
 5 people should voluntarily protect their data so it
 6 doesn't get destroyed. But I don't know personally
 7 whether we need to mandate that.
 8 MS. NATHER: Yeah. The question of
 9 ransomware is, as Matt just said, you know, partially
 10 a confidentiality issue, especially if that data is
 11 exfiltrated and the attacker is threatening to expose
 12 it. But it's also an availability issue. And, of
 13 course, we saw that with NotPetya and other, you know,
 14 more recent ransomware attacks.
 15 And the problem is that simply having
 16 available an air-gapped backup is not necessarily
 17 going to solve the whole problem. There are some
 18 problems that are much more difficult to solve like
 19 the level of connectivity needed amongst healthcare
 20 providers who have to be able -- again, for safety
 21 reasons, for health reasons, have to be able to share
 22 data widely and allow connectivity that, you know, is
 23 based on software that they do not control; that they
 24 can't rewrite; that they can't say stop using SMBv1.
 25 You know, so, again, when we get into what

263

1 can we realistically enforce, we can enforce some
 2 solutions but not all of them that we would need to
 3 address ransomware. Is enforcing some of it better
 4 than -- you know, better than nothing? Possibly. It
 5 depends on how the regulations are crafted. And I
 6 leave that to wiser heads.
 7 MR. MARCHANY: Well, and I think we just
 8 sort of all agreed that, you know, this is not
 9 enforceable. I mean, the primary vector that triggers
 10 the ransomware attacks is the end-user. You know,
 11 they click on something. So I don't know how they
 12 would -- how you would word a requirement in the
 13 regulations to prevent a ransomware attack.
 14 MS. MCCARRON: Right. We have another
 15 question from the audience. In an earlier
 16 presentation today, it was mentioned that CISOs
 17 perhaps shouldn't be risk acceptors but they should be
 18 those who say yes or no; that a risk is mitigated as
 19 to the process or as a technical change.
 20 So does that seem like something that is
 21 likely to be incorporated into the updated rule, that
 22 the board of directors or executives are the level of
 23 risk accepters?
 24 MR. MARCHANY: Well, that would be nice.
 25 No, I've never accepted -- the only thing I accept

264

1 risk for is the data that I'm the data owner of. My
 2 job -- and this is from my predecessor; he set this
 3 standard. My job is to provide technical advice as to
 4 whether the risk that, for instance, Wendy as CEO
 5 wants to accept. I would give her technical advice
 6 saying, yes, the method that you want to address the
 7 risk looks good from a technical standpoint, but I'm
 8 not the one that's going to say you shouldn't accept
 9 the risk or you should accept the risk based on
 10 anything else other than the technical stuff.
 11 MS. MCCARRON: Okay.
 12 MS. NATHER: Yeah, I would say that the
 13 level of risk is a long ongoing discussion between the
 14 CISO and their management. And a lot of it has to do
 15 with probability. And with financial institutions,
 16 the ones who are very, very good at quantifying risk
 17 on a financial level can sometimes approach a level of
 18 quantifiable risk in security that makes everybody
 19 happy at that institution.
 20 But looking at it from the outside, it can
 21 be difficult to say, well, I believe that
 22 technologically speaking this will mitigate 48.5
 23 percent of the risk that we just agreed on. You know,
 24 that is very, very hard to do.
 25 And the decision as to whether to accept the

265

1 risk, I believe, is ultimately a business one because
 2 mitigating that risk can cost money, effort, time. It
 3 can be an opportunity cost where the business is not
 4 moving forward on something else because they're
 5 having to remediate something. And those sorts of
 6 decisions, including reputational risk, are not the
 7 sorts of things that the CISO can or should be making
 8 in my opinion.
 9 MS. MCCARRON: Okay. Thank you.
 10 So those are the rest of the questions from
 11 the audience. So I would like to wrap up by asking
 12 you all to just do a quick speed round, your lightning
 13 last thoughts on encryption and multifactor
 14 authentication that is in the proposed amendments to
 15 the Safeguards Rule. I would like to give everybody
 16 just about one minute to summarize or provide any
 17 additional thoughts. I'd like to start with Matthew,
 18 please.
 19 MR. GREEN: Well, I mean, first of all, I
 20 think that we're in a great time when we've reached
 21 the point where we can actually mandate that
 22 encryption be used. I mean, years ago -- I've been in
 23 this field for 15, you know, 20 years now, I guess.
 24 And, you know, encryption used to be this exotic thing
 25 that was very, very difficult to use, very expensive

266

1 and not really feasible for securing information
 2 security systems. And we've reached the point where
 3 now it is something that's come to be and we can
 4 actually build well. So I'm really happy about that.
 5 And the same thing goes for MFA. We've
 6 reached the point now where we know that passwords do
 7 not work well. They are just simply not by themselves
 8 enough of an authentication feature. And fortunately
 9 there are a whole bunch of companies and inventors
 10 that come up with ways to make this better. And we're
 11 actually winning. I would say if you look at the
 12 overall progress of attackers versus defenders, the
 13 defenders -- when these systems are used and deployed,
 14 the defenders can win.
 15 And now having those systems deployed is
 16 really the last final challenge. And I think that's,
 17 you know, what's great about these rules, is they
 18 start to make that happen. So that's it.
 19 MS. MCCARRON: Thank you.
 20 Randy, may I ask you for your final thoughts
 21 on encryption and multifactor authentication for
 22 today?
 23 MR. MARCHANY: Yeah. I mean, certainly with
 24 encryption, as Matt said, it's become more
 25 commoditized, you know, now that it's not a big deal

267

1 from a financial standpoint.
 2 As far as MFA goes, I always tell people, I
 3 say, look, when people push back, I said, you've been
 4 using two-factor for at least 15 years now. It's
 5 called an ATM card. And so when they -- when you hit
 6 them with that, they go, oh, okay, I got you. And so
 7 we've been doing this type of stuff over time, as Matt
 8 said. And I think it's finally gotten into the public
 9 psyche that these are good things to do. So it makes
 10 perfect sense to have these requirements in the
 11 Safeguards.
 12 MS. MCCARRON: Thank you.
 13 And, Wendy, may I please give you the last
 14 word?
 15 MS. NATHER: Please, thank you. Yes, as
 16 Matt and Randy have both pointed out, we have a lot
 17 more options, a lot more technologies today than we
 18 did before that are making both of these solutions,
 19 both encryption and MFA, easier to use, more flexible,
 20 in some cases cheaper, and we should be encouraging
 21 their adoption wherever possible.
 22 Having said that, we need to maintain the
 23 flexibility in the enforcement to allow for situations
 24 and environments where the organization can't
 25 necessarily rebuild everything from scratch. They

268

1 have to work with what they've got.
 2 And, also, at the same time, we can't be
 3 absolutists about finding the perfect solution and
 4 enforcing the perfect solution because that may not
 5 necessarily be practical. We just have to make sure
 6 that organizations are not using the equivalent of a
 7 decoder ring from a cereal box to solve -- you know,
 8 to mitigate their risk problems. But I believe we can
 9 do that today.
 10 MS. MCCARRON: Thank you very much. I want
 11 to thank Matthew and Wendy and Randy so much for your
 12 time and for your expertise. Thank you very much for
 13 a very informative discussion. We appreciate it.
 14 So this concludes the GLB Safeguards Rule
 15 workshop. I wanted to thank everyone for tuning in
 16 and for listening and for all of your excellent
 17 questions during the course of the workshop today.
 18 If you have additional questions or any
 19 written comments, they may be submitted online at
 20 regulations.gov, any written comments related to the
 21 agenda topics or any of the issues discussed by the
 22 panelists of the workshop today. So please file any
 23 written comments that you have by August 12th so they
 24 can be considered as part of this rulemaking.
 25 Again, thank you all very much for your time and

269

1 your attention today, and the workshop is concluded.
2 Have a nice afternoon.
3 (Hearing concluded at 4:31 p.m.)

4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

270

1 CERTIFICATE OF COURT REPORTER

2
3 I, George Quade, do hereby certify that the
4 foregoing transcription was reduced to typewriting via
5 audio recorded by me; that I am neither counsel for,
6 nor related to, nor employed by any of the parties to
7 the case in which these proceedings were transcribed;
8 that I am not a relative or employee of any attorney
9 or counsel employed by the parties hereto, nor
10 financially or otherwise interested in the outcome of
11 the action.

12
13
14
15 s/George Quade
16 GEORGE QUADE, CERT
17
18
19
20
21
22
23
24
25

A				
a.m 1:13 61:14 70:6 70:6 120:15 148:6	264:25	260:23 261:2	activity 42:25 122:20 206:10	238:9 240:24 245:3,11,14 246:13,23 254:25 263:3 264:6
abatement 152:11	acceptable 67:14 255:23 258:7	accountabilities 175:13	actor 52:8,16	addressed 14:18 227:19 243:25
ability 59:24 87:20 88:3 113:8 122:19 122:22 163:1,2 168:17 169:5 256:14	acceptably 51:17	accountability 2:15 10:20 21:18 77:12 96:23 97:9,18,19 97:21 99:9,10 100:6,7 101:12 109:24 110:6 172:1,5,21 173:8 173:21 174:8 176:25 177:6,8,12 177:17,17,24 178:4,21,22 179:2 179:5,13,23 180:12 183:6 200:25 219:2 220:9 250:16 251:5	actors 28:19 29:7,12 31:18 38:18 58:15 217:10	addresses 7:18 12:15 18:22 65:24 131:15 245:6,12 245:20 246:16,19
able 14:23 15:3,5 46:14 47:7 52:17 57:6 63:10 73:22 75:3 82:21 87:25 100:3 108:11 109:7 110:9 113:22 115:22 116:13,14 118:2 123:21 125:14 126:4 127:21 129:4 134:2 148:7 149:19 154:2,18 158:23 167:14 180:13 184:3,20 197:19,23 198:2 198:23 199:3 201:17 202:17 203:4,5 233:7,22 253:8 254:5 256:14 258:10,16 262:20,21	accepted 15:15 51:8 64:15 205:22,23 205:24 255:20 263:25	accountable 82:10 87:22 88:20 168:14 169:16 178:16 202:22 219:7	actual 18:24 25:2 59:21 117:13 127:2 168:12 197:12	addressing 43:14 46:20 96:7 119:23 250:23
absolute 197:10	accepters 263:23	accounted 177:21	ad 40:13	adds 102:19
absolutely 56:19 65:12 102:8 115:14 167:5 189:11 190:13 217:14 246:15 256:10	accepting 51:5 130:22	accounting 111:10	adapt 104:24	adhere 73:15
absolutists 268:3	acceptors 263:17	accounts 192:4 261:3	adaptable 10:2	adhered 89:10
abuse 255:9	access 9:23 14:20,21 14:23 15:1 20:2 28:21 33:18,19 52:2,3,18 58:15 59:9 64:22,24 67:16,17,19,24,25 69:3 82:14 101:23 102:2 103:2 104:5 122:3 154:16 239:2,7 240:4,14 241:19 242:3,21 246:5,8 252:17 253:20 254:23 256:14 260:17,19	ACH 103:13	adapted 9:1	adhering 80:2
academic 167:24 251:24	accessed 242:13	achievable 140:24	adapting 114:20	adjunct 121:11
academics 56:14	accessible 125:20	achieve 110:5 181:5	add 33:21 36:18 73:1 124:16 131:1 131:10 135:7 137:13 142:22 146:8 150:10 154:8 159:24 170:4,18 178:11 178:18 186:4,7 189:16 192:22 198:9 205:12 207:4 208:9 211:22 253:13	adjust 8:2,4 13:22 29:25 97:14 202:9 237:21
accept 51:8,22 55:5 56:10,11 66:3 116:22 159:15 202:14 214:6 248:14,15 250:12 263:25 264:5,8,9	accessing 18:9 64:11 64:13,23 101:21 102:5,9 230:18 238:20	acknowledge 71:9 87:3	added 11:1 62:4 128:20	adjustment 98:16
	accident 244:9	act 3:16 37:18 56:22 67:4 123:14 127:2	adding 16:7 65:1	administration 125:25 126:7
	accidentally 148:3	acting 223:4	addition 13:12,23 225:11	administrative 99:14 100:10 260:25
	accommodation 152:15	action 16:23 109:1 144:10 218:4 270:11	additional 11:24 33:14 73:10 95:11 102:20 147:15 168:7 265:17 268:18	administrator 78:4 106:6 125:12
	accomplish 37:4 99:15 168:25	actionable 208:15	additions 201:19	admins 134:15,23
	account 6:18 21:4 57:9 59:19 87:9 128:5 143:2 162:18 164:10 166:17 169:25 211:9 227:14 233:7,9 238:15 242:12 247:4 251:14 253:18	actions 46:18 66:20 206:6	address 7:8 8:5,21 8:25 9:19 11:18,19 14:16,17 15:17,23 16:10 20:23 23:20 46:15 54:7 84:23 88:25 111:22 172:5 192:6,21 216:25 217:6 222:9,16 232:8,11	admission 138:19 adopt 223:21 224:20 226:8
		activate 239:23		adopted 130:20 225:6
		active 134:14 141:2		adopters 237:7
		actively 39:25 126:19		adoption 267:21
		activities 6:12 95:4 122:2		Adrienne 172:9,23 174:12 180:9 182:8 184:22,25 186:5 189:16 198:7 201:3 204:10,14 214:8 216:23 219:4
				advanced 43:11 54:19
				advantage 61:23

245:25	agrees 250:24	239:6 247:5 248:5	48:8,21 50:22 52:7	152:2 246:3
advantages 111:2	ahead 3:15 44:2	249:15 251:4	57:8 65:20 66:2,7	261:15
advice 75:6 79:24	45:24 60:25 65:14	255:21,24,25	68:6 111:21	anytime 235:8
264:3,5	147:4 167:2 189:8	256:25	122:21 124:1	anyway 31:20
advisory 223:9	220:2 245:4	alternatives 17:4	149:21 156:4	125:13 201:12
advocate 105:23	248:15	109:21 110:3	183:4 202:7 249:7	APIs 243:21
210:4,25	AI 249:12	130:11 242:16	249:8	app 83:6 234:16
advocation 193:11	aid 5:15 37:3,23	244:24 255:18	analyst 75:25 76:3	appear 142:4
AES 229:21	56:2,22 57:12	258:7	257:25	appetite 181:6 202:9
affect 53:12 55:22	137:25 138:1,13	Alto 228:17	analyze 50:4 144:15	apples 117:19
56:3,5 255:5	138:15,19 160:12	altogether 191:21	149:20 151:4	applicable 109:10
affiliate 77:9 80:17	228:3 237:14	Amazon 152:20	and/or 109:22 110:4	applicants 31:23
afford 63:6,23 233:3	244:8	254:18	149:3	application 60:19
233:4	air-gapped 259:20	Amazon's 45:17	announced 231:18	103:1 106:22,24
affordable 124:14	262:16	Amen 170:23	announcement	107:12 136:6
affording 63:7	alert 142:18	amendment 77:4,8	231:20	142:15
afraid 61:17	Alex 121:5 122:17	85:21 95:20,24	annual 12:10 14:8	applications 15:7,10
afternoon 121:3	142:19 146:13	101:19,23 105:6,7	76:12 86:4,7 99:6	15:12 44:25 45:6,6
221:2 222:2,8	151:25 170:15	115:13 119:21	99:11,17,19 101:7	95:2,9 102:10
269:2	align 67:5	166:24 230:16	109:22 114:11	applied 49:1 128:11
agencies 3:18 5:1	aligned 204:8	231:5	198:19 199:7,25	163:20 164:8
25:18	Allen 172:9,25	amendment's 224:7	200:1 217:8	222:23
agency 233:2 256:8	180:10 182:10	amendments 3:14	annually 90:5 96:1	applies 4:15 5:11
256:9	189:18 198:8	4:10,13 8:17 9:4	122:8 124:5	17:19,24 107:3
agenda 268:21	201:5 214:10	22:7 72:7 74:8	128:17 143:14	167:21
aggregate 141:21	219:5	75:22 80:13 85:18	150:17 193:20	apply 5:14,16,17
aggregation 122:21	allergic 49:12	88:15,17 103:7	anonymous 222:25	17:25 38:23 50:15
aggressive 155:17	allocate 87:15 88:10	112:18,23 223:18	answer 28:23 34:3	59:1 65:21,25 66:2
155:21,24	allow 15:19 17:3	229:12 230:14	53:15 57:11 67:8	85:24 137:22
agility 98:19	87:8 137:10 144:4	238:18 247:23	88:5,23 109:14	163:22 164:14
ago 54:3 67:13	164:22 168:23	265:14	139:9 188:13	165:25 168:22
128:8 135:3	216:12 243:22	America 161:22	191:18 201:6	224:8,9 244:4
201:21 209:1	262:22 267:23	American 243:7	229:7,8 251:8,18	applying 163:17,24
229:4 256:10	allowed 131:16	amount 19:21 28:7	252:10 256:9	appoint 81:15
265:22	allowing 8:25	28:11 55:9 89:4	257:13	appreciate 45:18
agree 29:9 43:25	209:21	91:5,20,22 92:1	answering 65:5	68:2 220:23
44:3 50:12 54:22	allows 34:5,9 98:15	94:2 145:17	178:9	268:13
68:8 89:7 143:1	98:16 134:7	165:15,22 184:5	answers 168:5 188:1	appreciates 29:23
156:8,22 178:14	138:21 160:5	200:16 236:19	antagonizing 57:25	appreciating 36:2
180:10,12 184:24	223:23	247:8	anti-virus 46:22	approach 41:11
198:9,20 204:13	alluded 115:24	amounts 57:24	antivirus 32:6	46:2 48:7,11 56:18
214:10,15 226:10	226:21	197:11	anybody 41:23 79:8	57:20 58:2,2,6
246:15 254:1	alluding 250:5	analogy 189:19	120:7 139:24	82:8,22,22 101:11
agreed 145:4 254:19	altered 155:4	analysis 26:6,15	148:9 157:17	102:4 109:20
263:8 264:23	alternative 18:4	27:4,12 29:20	165:23 222:13	110:16 111:3
agreement 114:25	66:4 104:16	31:12 32:4 34:4	233:21 260:16	150:8 179:14
116:19 168:24	105:16 223:24	35:12 36:20 38:1	anymore 35:18	201:17 218:12
agreements 116:18	224:14 235:2	39:11 42:14 47:21	110:14 139:25	264:17

appropriate 6:7 7:24 27:7 53:13 86:15 87:8 88:13 88:18 89:6 90:15 90:21 161:6,19 204:3 231:7,11 238:20 242:1	257:12 259:18 asking 53:9 59:16 59:18 75:16 100:16 106:7 117:23 161:3 172:17 190:24 201:12 224:19 265:11	assigned 233:7 assistance 78:15 136:19 assistant 121:10 associate 104:13 222:20 associated 167:12 206:24 213:20 257:18 Association 72:8 assume 92:18,18,23 159:14,22 245:13 253:19 assumed 72:17 assuming 118:20 assumption 162:9 assurance 82:25 AT&T 256:5 Atlantic 54:19 ATM 267:5 attached 19:1 attachment 226:18 226:20 attack 15:11 29:6,14 32:11 38:20 59:4 93:11 126:16 160:2 254:10 259:21 260:3,4,13 263:13 attacked 91:7 245:23 attacker 91:3 127:2 129:5 143:22 159:11 247:15 256:7 262:11 attacker's 127:16 attackers 29:12 151:15 153:18 183:25 231:16 245:23 247:1 256:12,13 266:12 attacks 7:10 28:1 29:10 91:10 92:22 127:4 154:1 159:6 167:8 246:21 259:15 260:12 262:14 263:10 attained 206:1	attempt 139:8 142:17 attention 27:11 94:16 269:1 attest 250:2 attitude 58:21 attorney 3:5 23:5 54:13 59:20 71:24 172:7 222:5 270:8 attorney/client 216:8 attorneys 25:19 audience 52:23 109:13,18 111:20 135:17,18 160:8 195:7 216:25 222:14 251:7 257:12 263:15 265:11 audio 270:5 audit 15:17 24:11 74:2 90:7 121:25 153:9,12 187:3 190:22 192:16,17 194:24 204:17 206:18 auditor 24:10 90:8 250:25 251:3 auditors 250:19 audits 89:21 August 268:23 Austin 150:24 223:9 authenticate 245:18 246:20 authentication 2:18 16:25 17:8,12 18:7 18:8,12,14,17 21:21 33:18 39:6 49:5,20 51:2,12 52:2 64:10 67:3,11 76:7 101:18,20,22 102:9 103:9,16 113:2 117:6,7 133:11 222:1,10 223:22 230:13,18 230:20 231:8,11 233:23 235:20 236:22,25 238:20	239:21 240:22 241:7 242:9 243:23 244:25 245:7,21 246:5 247:25 248:6 249:21 258:21 259:2,22 265:14 266:8,21 authorities 54:14 176:16 authority 119:10 authorized 9:25 16:14 122:3 auto 72:11 78:23 automaker 243:6 automakers 243:5 automate 140:1 automated 127:2 139:8,23 140:18 142:11,11 143:6 144:7 145:7 automatically 178:16 automation 140:2 145:6 automobile 72:7 74:11 75:17 auxiliary 73:17 104:10 availability 241:17 262:12 available 41:23 81:7 83:14 91:22 104:17 116:24 132:5 149:2 151:12 231:23 232:4 234:11 246:25 262:16 avenues 195:11 average 43:2 72:9 76:1,14 78:12 189:25 avoid 12:21 90:12 aware 38:13 40:2 157:16 162:20 168:8 194:17 awareness 12:17,21 12:24 29:2 60:1
---	--	--	---	--

62:6 64:8 66:25 179:20 194:15 195:13 219:24 awesome 81:2 94:21 AWS 45:17	band 230:1 band-aid 237:3 bank 161:22 164:3 223:11 232:21 247:11 bank's 169:20 bank-level 232:14 banking 104:13 banks 4:24,24 176:10 bar 232:17 bare 198:21 barrier 59:13 base 256:20 based 5:24 7:4 8:3 9:4,10,12 10:2 11:10,16 16:20 23:24 28:16 30:1 44:4 46:4 51:14 57:13 61:14,22 73:18 76:17 82:13 83:10 89:12 90:4 91:14 93:2 94:12 122:21 123:24 124:1 147:12,17 163:23 164:3,4 166:22 197:4 200:5 202:9 229:22 234:2 246:6 262:23 264:9 baseline 69:11 118:16,17 177:11 bases 10:5 basic 9:8 12:23 20:11 46:17 67:20 68:1,4 93:22 103:15,17 108:1 115:8 130:8 185:7 basically 5:3 7:3 8:8 10:24 14:12,24 16:3 18:13 33:15 40:16 55:21 78:5 123:16 125:8 131:3 134:13 145:6,7 146:25 149:6 150:2,5,8 153:24 155:18	159:19 163:25 209:12 216:18 228:18 235:23 237:1 239:15 basics 12:20 46:16 47:9 68:22 87:19 87:20 88:7 92:2,5 92:14 94:8 111:6 115:25 116:2 119:4,8 basis 25:15,23 26:3 39:24 68:10 69:7 74:4 78:15 99:20 194:20 198:19 199:7,11 bay 143:21 173:14 beacon 134:10 138:21 beacons 132:1,16 134:22 bears 179:1,12 beating 119:6 becoming 73:6 151:24 beginning 12:1 61:25 242:25 behalf 153:5 160:14 behaved 62:13 behavior 42:6 66:11 86:24 87:20 88:9 88:22 119:7 240:4 behavioral 240:3 247:4,12 249:8,12 behaviors 161:25 162:1 beholden 158:11 beings 61:25 belief 73:18 believe 21:7 66:10 68:19 113:3 117:6 159:16 168:6 176:25 205:8 213:9 227:12 257:6 262:3 264:21 265:1 268:8 believes 80:4 bell 202:6	belong 47:19 belt 243:3 belts 243:4 beneficial 153:10 benefit 27:13 32:24 33:9 34:2,14 36:6 36:16 99:15 186:7 benefits 2:6 20:22 21:11 23:1,21 24:1 24:4 36:3 41:15,25 42:2,18 72:4 77:16 96:20 111:21 124:17 182:4 201:1,14 214:9 benign 127:3 Berkeley 121:18 145:13 155:20 156:2 163:20 best 17:6,12 19:20 53:2 55:19 65:6 66:1 78:8,16 82:8 145:1 192:22 214:24 217:17 218:2 219:2 232:12 252:10 258:8 260:2 better 35:2,5 66:12 92:21 94:17 95:7 113:20 157:19 182:20 193:8 220:14,18 235:2 246:7,9 263:3,4 266:10 beyond 114:18 176:18 biannual 12:10 86:5 122:9 big 38:21,22 39:22 41:15 45:23 51:3 65:6 67:10 105:22 115:19 122:15 133:14 144:8 149:16 151:5,18 151:22 155:19 178:21 179:11 232:9 235:24 238:9 247:20 257:22 258:4	260:20 261:13,14 266:25 bigger 185:17 218:5 biggest 28:22 208:22 213:23 220:3 225:14 253:16 256:6 bilinear 223:1 bill 157:17 biographical 18:20 230:23 biometric 19:6 231:3 239:18 bit 35:4 44:24 61:2 66:11 68:14 73:6 79:4 114:3 123:6 126:22 130:18 163:12 167:4 168:10 172:18 175:12 178:14 191:5,6 203:10 219:24 239:25 black 52:6 blanket 229:19 blend 31:9 blob 155:19 block 254:11 blocking 47:2 109:4 BloodHound 134:11 134:23 bloodless 113:17 blow 260:4 board 14:9,10 53:20 75:13 95:21 96:1 96:14 97:4 98:15 99:4,5,7,7,19 100:1,3 109:23 110:4 112:10 113:14 133:24 189:20 193:18,20 193:25 194:6,9,21 194:22,25 195:23 196:4,6,7,10 197:2 197:18,23 199:10 199:23 200:3,18 218:9 248:12,12 248:19 250:9,16 251:5 263:22
--	---	--	--	--

boards 194:13	242:9	99:14 100:11	89:10,11 90:8,13	campaign 131:18,22
body 14:11 96:2,21 97:4	bringing 73:13 81:23 157:21 199:10	169:22	91:19 92:4,24	132:17 146:18,20
bolstered 211:16	brings 20:14 113:24	burner 246:16	93:12,16 94:5,9	campus 123:16
bombing 61:6	broad 5:8 100:17	business 8:7 14:6	110:16,21 111:13	160:25
bones 11:21	139:13 168:24	15:25 21:2 27:9,13	112:22 113:13	can't 11:25 35:13
bonus 36:10	180:5 239:9	28:18 29:8,17 30:6	114:23 116:12	39:7 45:15 49:1
book 46:17	broader 128:25	30:11 32:10 35:11	117:23 118:3,18	92:1 98:23 106:20
bottom 244:22	174:23 175:17	38:24 39:9,15 41:2	118:20,24 119:2	108:13 117:21
bottom-tier 191:21	brought 61:21 85:11	42:16 44:19 50:6	119:25 120:2	155:4 216:11,17
bottom-up 248:18	194:23 209:6	54:10 56:16,17	122:14 123:17	262:24 268:2
boundaries 53:23	bubble 228:6	62:9,16 63:16,24	125:20 136:16	canned 116:17,19
bounties 130:17	bucket 68:3	73:5 74:20,22	162:10 166:5	cap 62:12
bounty 130:22	bucketed 117:22	75:11,13,19 77:18	198:17 203:18	capabilities 156:14
box 73:23 90:11	bucks 236:14	78:23,25 79:13,14	261:24,25	158:16 169:5
134:8 268:7	budget 19:23 82:16	80:1,8,19 81:9	button 234:15	capable 7:23 13:20
boxes 134:17	157:23 197:6	82:4 84:9,12 85:10	buy 26:17 192:12	163:9
brand 37:8 40:6	budgets 43:3	85:17 86:16 87:2,4	243:6,10	capacity 59:17
breach 14:2 15:22	bug 130:17,22	87:9,21,22 91:1,7	buy-in 181:6	210:21
25:20 27:21 28:7	bugs 237:8	92:8,11,13 93:7,21	buying 43:10 103:25	car 5:11 170:11
31:18 33:25 34:11	build 29:23 76:22	93:24 94:3 95:23	137:1,1	239:16
51:6 53:24 54:3	115:22 154:14	102:12 103:18,20	buzzword 177:9	card 58:9 147:8
93:10,13,17,23	188:16 194:15	104:20,23 110:10	BYOD 237:23 238:9	148:5 228:21
97:24 143:6	205:25 219:2	110:20 112:19		267:5
154:12 159:22	266:4	114:13,17 120:6	C	cardholder 58:13
206:9 219:19	building 128:21	129:7 135:13,21	cadence 194:22	cards 61:16
235:25 236:1,2,3	150:19 188:24	136:9,21 153:23	198:20 200:4	care 40:19 49:16
236:15,24 249:2	189:10,11 191:3	161:16 169:2	cake 260:9	50:8 61:12 66:7
251:4	191:14,15 197:16	170:7,10 180:18	calculated 26:12	104:4
breaches 98:5 118:8	211:25 212:23	180:18,19,23	calculation 170:6	career 173:12
122:25 143:2	216:14 245:15	181:2,5,12,13	261:22,23	174:19 216:16
197:22 245:22	builds 219:23	182:17 186:22	California's 153:23	careful 59:10
breaching 52:9	built 130:5 150:25	187:10 189:5,8	call 66:17 79:4 90:9	119:24
break 21:12,17	151:6 175:24	198:18 200:10	139:9 183:8	carefully 100:10
69:24 120:12	189:1 215:11	203:9 204:19	198:14 214:1	Carnegie 163:23
220:25 252:8	230:7 258:13	212:14,16,17	228:19 234:15,18	carried 112:13
breathe 212:16	259:8	213:19 214:2,2,16	251:9	carrots 219:15
Brian 71:15 77:15	built-in 258:14	219:12 220:15,17	called 38:14 41:21	220:19
80:18 83:22 89:3	bulk 155:25 156:2	237:16,17 242:22	47:19 76:14 86:21	carry 239:13,14
102:3 114:5	bunch 35:20 47:8	265:1,3	133:8,10 134:6,11	carrying 165:25
115:11	136:3 144:3 266:9	businesses 2:10 21:2	138:11 146:22	166:2
Brief 22:15	bundled 233:1	21:14 38:8 39:13	147:16 150:25	carve 185:10 249:22
briefly 172:18	burden 60:15,22	43:5 70:1 71:1,6	151:6 156:6 225:3	case 10:21 25:20
215:18	85:20 96:19	73:12 74:14 75:3	228:16 267:5	32:16,18 82:9
bring 80:15 87:15	140:15 248:23	80:11,20,22 81:7	calling 58:20 132:13	94:25 100:24
184:14 191:7	249:19 250:17	81:14 82:9 83:3,24	166:8	143:19 146:1
214:23 229:1	burdensome 51:19	85:22 86:22 87:13	callout 105:5	154:14 155:2
233:25 237:21		87:18 88:2,7,10,18	calls 177:2,3 183:8	170:13,14 206:7
		88:19,20,24 89:1	190:15	228:2 236:19

258:8 270:7	52:12 54:23 67:10	55:24 67:12,23	check 13:18 125:14	51:13 57:4 75:24
cases 79:20 123:25	97:2 124:10,12	69:12 91:14 93:2	127:15 128:15	78:11,17 79:25
127:2 143:23	142:25 145:20	94:20 95:10,17	checked 73:22	81:15,21 82:6,11
152:1 188:18	150:11 151:17	104:21 107:9	checking 90:11	83:12,14 86:8
211:17 225:12	155:7 178:15,21	111:20 113:19,23	139:21 190:22	87:15 95:25 96:14
226:24 232:16	207:7 216:22	113:25 114:24	checklist 118:22	96:24 98:14 99:4
240:6 241:8	226:2 228:25	128:19 137:18	251:1	99:10 100:4,7
244:11 252:19	240:7 244:12	139:7 142:15	checklists 114:19	101:12,25 105:17
256:13 267:20	259:8 261:8	181:24 193:14	checks 102:20,22,25	110:10 178:23
catalyst 98:8	266:23	227:20 261:22	186:20	180:25 184:7
catch 131:7	certainty 247:9,14	263:19	chewy 132:22	185:25 187:15,19
catch-all 8:11	247:19	changed 128:12,22	Chicago 71:12	195:7,8,15 223:3,4
categories 102:18	certificate 225:14	155:5 201:22	chief 11:6 23:12	223:9 239:3 248:1
categorization	270:1	changes 3:24,24 8:6	76:1 81:10 106:4	248:2,4,23 249:25
164:2	certificates 225:16	8:7 16:4 48:23	121:10,13 172:12	250:2,8,14,17
category 239:8	225:18	81:17 83:5,19	children 61:13	254:1 264:14
cause 40:19	certification 57:1	91:17 94:12 96:11	chime 89:8 161:14	265:7
caused 54:6 118:8	63:11 99:8,12	99:22 105:25	206:23	CISOs 51:21 78:12
141:10 219:19	100:8,9 101:7	114:9 115:21	choice 182:4	180:17 249:19,22
causes 94:2	certifications 82:2	121:20 128:15	choices 190:20	263:16
causing 42:7	163:8	148:2 164:9	choke 64:22	clarity 202:2 204:23
caveat 203:10 234:1	certify 99:5 270:3	198:16 201:18,18	choose 12:12 117:12	class 163:23
center 36:15 41:20	cetera 128:22	202:9 207:2 252:5	204:20	classes 162:17,24
41:21 53:20 151:8	140:11 156:16,16	changing 16:6 68:12	choosing 202:15	classic 130:23
152:2	158:3 166:15	92:15 98:2 114:22	chose 202:13 205:14	classical 239:13
centered 173:21	168:20 169:4,12	channel 184:4	Chris 23:17 24:2	classification 227:8
central 174:20	CFO 36:12 236:5	characteristic	26:10 31:16 32:3	classify 168:21
220:5 237:2	chain 87:5	145:13	34:4,15 46:1,24	classifying 127:10
centralized 151:7	chain/supply 87:5	characteristics 19:7	50:12 56:15 65:15	clear 8:23 10:22
CEO 34:25 35:13	chaired 236:24	231:4 249:13	67:9 68:7	18:16 50:10
71:11 106:4	challenge 35:21	characterizing	CIO 78:5 174:15,17	109:23 195:7
248:19 264:4	38:22 39:22 42:20	198:13	174:21,23 175:11	228:5 254:3
CEO's 35:8	60:24 67:24 87:10	charge 6:22 10:20	175:14 178:21,23	clearly 178:25 180:1
cereal 268:7	112:3 123:4	10:23 14:8 17:4	178:24 179:1	click 30:23,25 132:2
CERT 270:16	154:21 197:19	18:5 19:14 74:13	195:16 237:1	159:17 170:19
certain 11:17 14:16	232:9 266:16	78:24 185:6	CIOs 180:17	263:11
38:6,6 41:3 46:1,2	challenges 29:4	223:25 224:16	circle 32:3	clicking 179:18
48:5 52:3,4 54:25	38:21 41:11 45:23	229:18 238:6	circumstances 8:11	234:14,16
63:10 85:23	51:23 58:4 67:8	chart 35:1 234:5	139:15 180:7	client 42:7 49:2
139:15 163:7	98:6 110:20	chasing 30:2	195:4 217:16	clients 31:4 40:14
180:7 186:24	135:11 137:16	chat 174:11	218:11 238:22,25	41:4 63:22 82:20
195:5 205:20	156:9	cheap 125:1,18	240:11 242:19	173:13,18
218:11 231:12	challenging 110:22	129:15 140:3,17	CIS 47:24 48:16	closely 53:21 117:23
232:16 241:13	151:25 261:20	256:4	CIS-RAM 41:22	160:18
245:11 247:8	chance 191:10 261:4	cheaper 21:5 104:20	Cisco 158:2 223:10	cloud 44:20 45:5,9
249:8,9	change 4:14 9:9	257:7 267:20	227:3	45:14 68:2 152:2
certainly 4:24 12:3	10:16 11:20 12:2	cheapest 231:22	CISO 11:6,13 36:17	152:21 227:15
12:11 27:21 38:16	16:3,9 34:9 50:25	241:1 252:20	38:25 50:25 51:2	251:10 253:6,19

253:21 258:3	244:17 248:11,19	committee 194:24	191:15 199:24	component 175:16
cloud-based 152:14	266:3,10	194:25	200:6 202:2 206:1	186:24
240:21 255:7	comes 19:12 25:17	committees 192:10	206:11 214:21	components 164:18
258:12	32:3 51:24 63:2	commodicized	220:10,12,15	175:9 185:2 192:7
clue 199:12	89:23 98:25	266:25	228:15,16 241:5	193:3
CMMC 49:25	129:12 133:21	common 13:4 19:8	256:23	comprehensive 5:25
code 18:25 203:16	147:19 150:2	19:10 33:7 133:6	company's 103:22	6:5 9:11 85:7
205:14,15 231:23	153:24 157:13	191:22 229:19	216:3	106:24 107:12
240:25	158:3 175:3,13	238:23 247:1	comparable 130:23	112:9 127:18
cognizant 69:8	177:9 180:4	259:7 260:20	compare 26:3 85:9	161:4 165:3
152:9	194:11 197:16	commonly 11:13	90:2 113:15	compromise 28:19
coin 32:24 33:23	200:10 202:6,14	24:18	compared 5:8	29:8,17 32:10
Coinbase 172:11	203:10 212:23	communicate 39:8	193:15	183:25
173:1,11	213:25 215:13,21	communication	comparing 139:21	compromised 29:25
collaborate 151:8	228:7 235:22	99:4 108:7 193:23	compensating	124:24 153:17
collaboration 61:9	241:17 245:11	communities 161:10	105:16 224:15	computational
167:15	259:7	community 30:7,9	competition 119:1	225:11
collaborative	comfort 100:4	30:19 37:5 57:15	competitors 244:19	computer 19:1,3
167:17 174:5	comfortable 100:1,2	57:25 178:20	complaint 53:5	76:8 121:17,17
colleague 77:11	247:21	179:15	complete 228:24	237:24 238:14
178:14	coming 10:23 44:13	companies 10:7	253:20	260:14,24 261:3
colleagues 207:4	50:1,3 64:14 75:6	20:2 28:8,10,15,24	completed 100:21	computers 16:6
collecting 149:17	81:12 84:2 86:21	31:14 33:8,24	completely 58:18	30:24 76:18 108:8
collection 6:16 95:4	116:7 174:21	34:16,18 36:9 38:9	108:3 127:18	computing 122:20
collectively 151:8	183:3 186:23	38:13 45:12 58:9	178:14 184:24	122:23 167:6
collectors 5:10	214:14 251:7	58:21 59:17,23	189:12 212:6	concentrating
college 163:20	255:1,18	60:16 77:25	complex 6:11 11:12	160:10
165:17	comment 72:5,9	117:10 149:14	57:5 78:22,25	concept 50:25 51:4
colleges 237:12	85:17 86:10 96:18	157:22 158:14	79:14 135:20	135:24 141:23
color-coded 147:12	96:24 134:4 201:3	161:18 163:1	141:17 167:18	194:10
Colorado 71:22,22	commentary 50:24	168:14 169:1,15	183:17 191:19	conceptually 68:14
75:18	comments 4:5,8,11	169:16,23 176:3	complexity 6:8 9:13	concern 98:21
column/delimited	20:23,24 22:7,10	178:1 184:13	11:11 130:1	116:25 118:21
149:24	44:4 72:6 102:3	186:25 232:7	compliance 53:6	168:7 256:1
combination 78:8	135:9,10 198:10	240:21 241:6,12	81:10,22 96:5	concerned 169:7
come 18:3 19:15	204:11 206:22	245:24 252:25	98:22,23 99:5	196:11 261:18
24:11,22 27:5 28:3	209:6 214:8 217:4	259:17 266:9	106:4 160:18	concerning 86:1
41:13 43:23 46:6	268:19,20,23	company 7:24 12:19	172:10 174:1	concluded 269:1,3
46:11 49:17 90:1	commercial 140:5	15:7 17:16 19:22	188:6 190:9	concludes 268:14
104:16 109:13	Commission 1:1 2:1	20:6 28:3 38:5	192:15 193:1	concluding 115:13
111:1 146:5	3:22 24:19 36:23	46:3 58:12 65:8	251:1	117:2
150:21 157:8	56:24 63:13 71:25	76:15 78:9,9 83:6	compliant 164:18	conclusions 72:18
175:15 179:10	85:16,19 86:10	106:4 108:4	complicated 225:24	concrete 20:21
183:24 196:5,18	96:18 222:7	156:18 158:8	246:23	101:3 255:16
202:24 203:6	229:10	161:23 163:4,5,6	comply 20:10 72:12	condition 128:10
205:8 208:17	Commission's 39:25	169:3,4,23 176:5,8	74:12 83:4 88:15	conditions 248:11
216:18 217:12,14	commitment 203:1	176:9,15,22 179:9	100:13,14 118:25	conduct 86:4 126:11
227:13 238:1	211:18	182:17 187:9	209:19 253:9	139:3

conducted 122:8 136:1	consistent 106:22 176:21 190:5 204:2 206:15	continuous 2:12 12:9 21:16 33:20 44:12 60:12 84:21 85:3 86:4 115:1 121:1,6,21 122:5 122:14,16,19 123:1 124:17,21 146:12 149:2 167:9 249:10 254:3	177:20 181:4 205:24,25 223:24 224:15 239:2,7 240:14	257:11,13,16,20 258:5 265:2,3
conducting 190:19	consistently 189:7	contract 7:25 148:16 241:9	controversial 53:22	cost-prohibitive 157:22
confidence 127:25	consists 126:2	contracting 241:11	conversation 97:15 117:20 118:14 194:12 196:21 250:20	cost/benefit 25:8 27:12 31:12 42:14
confidentiality 6:25 241:18 262:2,4,10	consolidate 182:1	contractor 156:18	conversations 106:18	costing 72:24
configuration 148:2	consortiums 150:20	contractually 254:19	convert 212:13	costly 123:5 145:1
conflict 186:9,20	constantly 12:4 114:22 185:19	control 7:6,15 9:23 9:24 25:10 33:20 34:3,6,10,12 41:19 47:5,5 48:13,14,18 48:25 49:19,23 50:5,9 55:11 65:19 65:24 96:8 102:2 134:18 181:7 197:4 228:7 232:2 238:2 242:21 246:8 250:22 253:20 254:14 255:11 262:23	convey 218:13	costs 2:6 20:25 21:11 23:1,20,25 24:4 33:2,3 34:10 41:12,25,25 42:2 42:14,18 72:4,18 72:21 73:17,20 75:24 77:3,16 80:22 84:2 85:9 112:24 118:23 123:24 124:2,10 124:17 149:18 150:14 154:23 182:7 183:2 201:1 201:15 206:24 207:17,25 209:18 214:9 225:19 229:11 230:4
conform 81:17	constituents 54:9 67:1	controlling 153:4,5	COO 71:13	Council 47:20
connected 32:22 55:23 59:3 145:14 228:15 234:20	construction 76:22	controls 14:20,21 18:4 25:6,11 32:6 33:14 36:2,3,19 39:11 40:17,20 47:14,23,23,24 48:16,20 50:20 63:6 64:20 65:1 66:1,4,25 67:4,20 67:22,23 68:1,4,11 69:11 90:15 105:16 106:25 114:23 115:1 139:16 143:20,25 153:2 165:14 167:8 169:6,8,8 170:10 174:4	cooperate 190:8	counsel 217:20 218:16 270:5,9
connecting 16:5 60:12	consultancies 40:9		coordinate 6:21 77:17	counsel's 192:15
connections 95:2	consultancy 40:6		coordination 227:6	counsel's 218:17
connectivity 155:22 262:19,22	consultant 24:13 46:6,7 173:12		core 104:13	counties 133:19
cons 193:23	consultants 40:5,21 46:1 74:25		Corelight 149:18	counting 138:25
consensus 206:1	consulting 23:19		corporate 39:3 45:4 60:21 95:6 103:3 189:20	country 246:6
consequence 145:8 155:17	consumer 26:13 91:20 92:10 94:19 95:3,7,13,16 103:23 106:5 120:5 176:7,15		corporation 154:6	county 133:22,25 134:3
consequences 180:21,22 261:12	consumers 14:5 19:22,25 20:4 32:15 54:1 63:4,12 63:15,18,24		correct 141:10 156:21	couple 73:8 87:12 132:16 146:13,24 181:3 183:20 192:10 194:4 219:17
consequential 66:19	consumes 154:22,23		correctly 138:25 155:13 197:20	course 49:6 54:8 82:16 153:4 235:6 257:17 262:13 268:17
conservative 73:8	contact 131:24 147:3 184:4 186:19		correlation 62:13	COURT 270:1
consider 24:9 26:25 48:12 56:4 91:18 99:21 105:1 137:3 139:5 189:13 210:3,23 216:20 257:15	contacts 189:5		cost 20:21 21:2 27:12 33:9 36:15 72:8,9,16,25 73:7 75:21 76:9,14 81:6 85:10 102:16,18 104:22 111:21 123:22 124:4 129:7,12 130:17 139:8 142:24 149:4,5 150:6,20 167:12 169:21 184:12,13,16 187:12,24 203:7,8 208:5,16,22 209:2 213:19,22 214:3,5 214:6,20 219:17 225:11,14 229:14 235:11 236:2,10 236:16 238:7	coverage 127:20
considerate 156:13 158:13 244:14	contain 85:21 101:24 126:19 159:23 230:19			
consideration 44:8 123:11 124:6 130:10 164:19 165:4 190:15 207:1	containing 94:1			
considerations 47:8 123:13 138:23 164:8	content 151:4			
considered 37:2 65:11 73:9 75:11 217:19 255:20 268:24	contention 109:6			
considering 25:10 25:11	context 24:3 36:22 81:8 161:5 177:13			
consist 8:20	context- 47:16			
	context-sensitive 36:21 56:18			
	contextualize 168:20			
	continue 124:9			
	continuing 115:9			

covered 4:25 10:5 58:24,25 67:21 137:20 161:10 227:10	202:16 205:19 Cronin 23:17 24:6 26:25 39:17 48:10 50:23 54:21 56:13 60:25 62:11 65:14 65:16 70:4	custom 142:5,5 customer 3:10,20 4:16,17,19 5:17 6:15 7:1,3,20 10:8 17:2,15,20 18:9,10 20:12 55:22 85:25 86:12 101:21,24 102:5 105:9,12,15 122:4 137:21 138:9 148:2 160:11 189:1 199:2,18 224:3,8 230:19 256:20	D	235:23,24 236:1,2 236:3,5 243:16 246:6 256:15,16 258:3 259:3 261:15 262:2,4,5 262:10,22 264:1,1
covers 5:2 8:16 228:25	cross 26:2 crunch 59:24 crunchy 132:21 Crypsis 23:19 28:6 crypto 132:12 cryptographer 222:20 cryptographic 239:21 cryptography 222:22,23 223:1	customers 5:12,13 5:18,19,23 14:6 19:23 84:10 86:1 86:11,14 90:25 102:13 104:11 176:20 188:18 220:13,14 232:3 243:5 cut 36:16 254:11 cyber 9:5 14:1 38:17 47:14 71:19 86:21 87:21 92:22 93:13 98:17 108:1 143:2 146:22 147:16 cyber- 111:16 cybercrime 43:24 cybersecurity 23:19 31:4 35:15 37:13 37:17 38:14 43:19 44:11 46:16,17 47:9 48:8 49:25 57:1 66:10 75:25 76:3,15 86:23 91:14 93:2 94:4,12 94:18 97:6 110:11 111:6 115:7 119:11 132:20 138:5 173:17 182:16 223:5	daily 74:4 167:8 198:19 damage 154:3,5 170:13 260:21,22 261:1,7 dancing 165:11 dangerous 252:8 data 14:25 26:12,21 28:7 29:16,21,24 29:25 31:8,15,19 32:8,11,12 35:17 37:24,25 38:8,17 43:12 53:24 54:2,5 54:5,13 55:9 56:17 58:14,15 59:22 64:22,25 67:17,18 67:19 89:20,22 90:1,5,21,25 91:3 91:5,22 92:1,6,10 92:10,10 94:22 95:3,6,13,16,17 101:3 103:13 105:23 106:5,10 106:10,10,11,16 106:20 107:5,7,13 107:19 108:12 116:1,3,3,4,6 123:13 138:1,1,13 138:15 141:21 151:9 152:1,2,8,9 153:3 154:10,22 154:22,24 156:1,3 157:6,11 160:11 160:15,16,21 161:7 165:15,22 166:1,6,10,12,18 166:19 167:22,24 170:6 199:2 224:22,25 225:1 225:13,21,24 226:2,17,17 227:8 227:8,10,10,23,24 228:10,19,20 229:14 234:2	data-in- 225:1 database 68:3 150:1 databases 16:7 date 100:21 237:8 David 3:5 23:5 39:17 44:16 50:23 53:17 77:11 121:23 day 21:9,20,22 22:14 28:8 51:25 79:23 124:3 145:8 158:5 185:19 190:16 191:4,20 202:5,5 208:1 214:19 221:1 223:18 251:2 day's 260:7 day's 260:8 days 52:17 54:3 64:18 147:21,21 151:13 156:1 158:19,21,21,23 245:9 260:24 DC 173:14 deadline 63:11 82:16 deal 16:17 37:24 39:7 64:20 73:12 79:16 91:19 153:22 175:17 179:1,11 225:12 229:23 238:10,11 254:17 256:3,21 266:25 dealer 104:2,12,21 170:11 Dealers 72:8 dealership 72:10 75:18,21 76:11 78:23 79:1 dealerships 5:11 72:11,22,23 74:11
COVID 44:21 145:22 152:12 COVID-19 59:17,23 60:1 CPA 233:15 crack 133:13 cracks 183:10 crafted 263:5 crazy 49:8 132:8 226:18,22 create 8:25 110:18 111:3 114:19 202:1 217:10 218:3,5 248:16 creates 33:9 88:3 creating 15:10 49:21,21 95:11 96:23 97:12 110:24 111:7 218:20 creation 9:10 creative 126:6 credentials 67:2 132:10,11 134:7 credit 9:3,3 228:21 236:11,16,18 creds 134:18 Crifasi 71:13 72:15 72:19 74:16 79:15 91:16 103:10 107:18 113:1 crime 154:9 crisis 252:15 criteria 11:18 191:22 critical 43:12 61:20 61:21 94:5 95:15 97:5 99:1 102:8 107:12 115:3 143:11 147:18 155:8 167:5 168:1 174:9 192:3 199:3	cubicles 76:22 culprits 61:9 culture 87:14 88:8 92:15 97:12 98:3 111:3,7 113:25 195:4 210:23,24 211:2 cumbersome 160:20 curious 200:23 227:11 current 3:12 4:12,15 4:15 6:7 8:14,15 8:18 9:9 10:17 11:3 12:6 13:7,16 13:23 23:23 29:22 30:3 73:13 74:10 74:10 142:1 173:3 176:21 181:16 193:16 200:19 204:25 237:19 255:14 currently 53:8 72:24 81:14 139:24 253:5 curtail 37:6 curve 214:12 cusp 144:20 custodianship 166:19	cut 36:16 254:11 cyber 9:5 14:1 38:17 47:14 71:19 86:21 87:21 92:22 93:13 98:17 108:1 143:2 146:22 147:16 cyber- 111:16 cybercrime 43:24 cybersecurity 23:19 31:4 35:15 37:13 37:17 38:14 43:19 44:11 46:16,17 47:9 48:8 49:25 57:1 66:10 75:25 76:3,15 86:23 91:14 93:2 94:4,12 94:18 97:6 110:11 111:6 115:7 119:11 132:20 138:5 173:17 182:16 223:5 CyberSecurityBase 71:11 81:9 82:5 83:12 cyberthreats 30:10 30:11,17	D D 2:2 D.C 53:21 71:14 DA's 134:18 daily 74:4 167:8 198:19 damage 154:3,5 170:13 260:21,22 261:1,7 dancing 165:11 dangerous 252:8 data 14:25 26:12,21 28:7 29:16,21,24 29:25 31:8,15,19 32:8,11,12 35:17 37:24,25 38:8,17 43:12 53:24 54:2,5 54:5,13 55:9 56:17 58:14,15 59:22 64:22,25 67:17,18 67:19 89:20,22 90:1,5,21,25 91:3 91:5,22 92:1,6,10 92:10,10 94:22 95:3,6,13,16,17 101:3 103:13 105:23 106:5,10 106:10,10,11,16 106:20 107:5,7,13 107:19 108:12 116:1,3,3,4,6 123:13 138:1,1,13 138:15 141:21 151:9 152:1,2,8,9 153:3 154:10,22 154:22,24 156:1,3 157:6,11 160:11 160:15,16,21 161:7 165:15,22 166:1,6,10,12,18 166:19 167:22,24 170:6 199:2 224:22,25 225:1 225:13,21,24 226:2,17,17 227:8 227:8,10,10,23,24 228:10,19,20 229:14 234:2	235:23,24 236:1,2 236:3,5 243:16 246:6 256:15,16 258:3 259:3 261:15 262:2,4,5 262:10,22 264:1,1 data-in- 225:1 database 68:3 150:1 databases 16:7 date 100:21 237:8 David 3:5 23:5 39:17 44:16 50:23 53:17 77:11 121:23 day 21:9,20,22 22:14 28:8 51:25 79:23 124:3 145:8 158:5 185:19 190:16 191:4,20 202:5,5 208:1 214:19 221:1 223:18 251:2 day's 260:7 day's 260:8 days 52:17 54:3 64:18 147:21,21 151:13 156:1 158:19,21,21,23 245:9 260:24 DC 173:14 deadline 63:11 82:16 deal 16:17 37:24 39:7 64:20 73:12 79:16 91:19 153:22 175:17 179:1,11 225:12 229:23 238:10,11 254:17 256:3,21 266:25 dealer 104:2,12,21 170:11 Dealers 72:8 dealership 72:10 75:18,21 76:11 78:23 79:1 dealerships 5:11 72:11,22,23 74:11

79:6	185:24 215:8	demonstrate 34:5,9	designing 173:24	102:25 130:6
dealing 192:23	255:20,23 256:3	34:11 36:15	191:3	238:13 247:3
218:8 244:9	deemed 164:5	195:15	desire 109:6,7	devices 15:2 136:23
253:19	deeper 147:13	demonstrated	desk 258:25	145:14 146:2
dealt 76:15	default 117:8,11	150:14	desks 76:23	231:1 232:2 238:1
debate 117:16	132:9,11	demonstrating	despite 235:3	238:2 239:20,22
debt 5:10 144:1	defects 127:11	27:17	destroyed 262:6	devil 38:1
debugging 125:16	136:17,17 163:2	denominator 229:20	detail 10:12 12:22	diagram 116:4
decade-old 155:22	168:18	247:1 259:7	19:18 147:15	didn't 11:7 39:6
decent 168:6	defenders 266:12,13	department 50:2	202:18	47:5 51:7
decide 17:11 150:5	266:14	57:3 97:7 115:7	detail- 108:19	difference 78:21
200:4 207:12,13	defense 27:3 50:2	121:15 151:2	detailed 9:18 48:15	91:3 149:25
229:6 232:21	57:3 115:7 144:1	163:11 182:14	76:25 163:16	247:17
decided 19:20	153:15 177:1	219:22	170:7 217:9	differences 140:6
deciding 204:2	186:25 187:2	depend 195:4 212:3	details 17:9 22:1	different 6:10 19:15
207:1 216:6	190:9,18 204:15	230:4	38:1 147:1,14	29:18 30:20 36:25
decision 19:16 184:8	260:2	dependent 240:18	217:19	37:23,25 50:15,15
190:1 200:5	defensibility 206:18	depending 9:14	detect 15:19 16:16	52:15 54:4,22
201:22,23 202:8	define 163:21	15:14 69:12 83:8	52:15 85:4 121:25	56:16 57:6,9,11,18
204:18,23,24	defined 18:16	129:25 179:15,25	122:3 141:9	65:9,22 67:3 72:21
206:2 208:20	108:16,16	192:17,23 218:11	247:15,18	73:21 83:11,18,24
216:3 225:22	defines 138:9	depends 77:21	detecting 7:9	87:16 101:6
232:20,23 235:17	defining 137:21	125:22 188:13	detection 44:7 84:25	102:17 108:11
250:8 264:25	definitely 74:17	194:21 195:20	144:2	112:4 113:16,17
decision-maker	75:10 79:1,5 91:6	199:9 201:7	determination 53:3	116:15 117:19
189:24	129:20 130:9	207:19 213:18	53:5	127:21 138:17,18
decision-making	133:5 142:13	232:25 256:7,15	determine 16:20	152:6 161:10,22
173:25 175:9	156:15 157:2,7	257:25 258:1	33:8 46:5 51:15	163:4,15,17,23
182:22 184:21	158:14 166:17	259:4 263:5	86:13 126:24	164:7 165:20
187:6 200:16,25	168:7 169:3,24	deploy 141:18 240:7	139:4 162:3 241:5	166:2,18,20 169:2
203:11 204:12	181:8 198:9	deployed 142:2	determines 105:12	169:3,6,14 181:4
decisions 47:16 96:8	definition 5:8 25:7	266:13,15	224:13	192:10 199:14
99:24 176:6,21,23	25:22 40:7 77:21	deployment 257:16	determining 11:18	203:15,15,19
178:5 180:20	85:17 86:16 87:2,3	deposits 5:4	126:13 139:5	218:20 219:24
182:20 187:22	104:8 237:15	deprecate 231:19	devastating 93:18	224:24 225:25
189:7,21 190:7,12	degree 53:18 160:17	describe 146:11	93:23	232:24 234:8
198:2 199:15	180:6	described 41:12	develop 47:21,21	239:6 242:15
201:16,17 202:4	delay 251:13,23,25	146:16 159:20	77:24 78:17 81:24	246:18,24 249:6
202:13 203:5,14	delayed 227:13	design 7:14 66:15,16	101:1	differently 6:16
203:19,21,25	254:25	191:5 203:16	developed 41:21	65:21 191:6,9
205:12,13,19,20	delegate 119:9	designate 6:20	developer 106:7	difficult 38:23 39:16
206:6,16,17 207:8	delete 35:17	10:13 77:5 84:13	developing 181:2	54:1,17 57:20,23
215:23 220:17	deliver 147:7	181:17,20 187:20	development 15:6	66:2 159:15 183:1
235:19 265:6	delivering 60:7	187:23	39:2 80:9 146:23	185:4,9 188:6
decoder 268:7	delta 247:20	designated 90:7	161:4 188:2	196:21 227:17
decrease 191:9	demand 145:19	187:7 193:16	216:12,17	238:22 240:15
decrypt 227:4	146:1	209:13 213:1	develops 15:7	241:11 243:2
dedicated 124:11	demarcation 87:7	designed 10:19	device 19:1 102:22	252:4 257:23

262:18 264:21 265:25 diffusion 182:23 digital 151:15 229:3 diligence 173:6,8 direct 20:15,18 59:8 62:13 63:12 184:19 193:23 217:3 direction 10:24 26:6 81:12 82:24 directions 10:23 directly 27:1 132:6 150:22 director 36:17 71:18 78:5 97:25 172:10 223:12,14 directors 14:9,10 95:21 96:2,14 193:18 196:5 197:18,23 263:22 directory 134:14 disadvantage 136:12 137:8 disadvantages 209:21 disagree 204:22 disaster 257:5 disbursement 37:3 disclosure 153:19 discovered 12:5 discovery 132:3 discretion 165:7 discuss 121:19 discussed 7:15 12:2 47:25 72:10 121:23 217:2 268:21 discussing 36:22 56:23 97:20 200:14 223:17 discussion 52:13 97:15 98:7,12,12 113:21 117:16 166:23 171:2 172:16 206:13 220:23 250:25 251:2 264:13	268:13 discussions 177:9 disk 155:19 dislike 114:9 dismissive 58:18 disposal 15:23 dispose 16:1 disrupt 94:22 disruption 94:3 disruptive 207:19 distinguish 161:18 distribute 119:10 191:8 distributed 111:8 152:9 182:22 183:3 distribution 258:1 districts 233:4 dive 177:4 222:11 divergence 44:19 diverse 109:19 diversity 188:7 division 3:6 23:5 71:24 172:7 174:20 222:5 DLP 46:23 109:3 doctoral 53:17 doctors 234:23 document 41:21 99:19 207:6,16 208:24 216:7 248:17 documentation 169:13 203:8 205:20,23 207:15 208:7,8,12 215:13 215:19 217:24 218:3 documented 150:15 209:1 documenting 208:2 209:3 215:21 documents 48:14 203:17 205:1 DocX 230:8 DOD 37:24 57:3 doesn't 9:9 10:2 19:13 36:6 56:3	58:22 144:14 163:8 218:5 doing 12:10 13:10 24:7,8,9,10 25:1 27:1 35:4 38:14,15 39:3 42:20 45:5 46:6,10 48:22 57:2 58:1 61:2 63:16 74:6 87:22 88:7 92:2,6,14,21 93:25 107:24 110:13 113:22,23 117:14 119:3,4 128:16 130:3,8 132:15 136:3 138:11 141:2,16 142:12 143:7,7,8,9 148:1 153:3,11 155:11 156:15 159:4 163:9 166:7,25 182:1,17 184:12 188:14 190:23 199:6 201:11 204:7 208:7,8,8 210:17 213:13,16 226:12 238:10 250:20 257:5 259:2,3 267:7 dollar 34:8 39:24 149:16 197:11 dollars 29:13 55:16 123:23 150:16,23 154:7 197:7,8 domain 134:14,15 don't 5:3 12:22 14:9 15:4 17:9 35:18,25 35:25 36:10 37:18 43:8,16 48:12 49:13 54:2,8,11,14 55:7 58:21 63:3 81:14,14 88:2,17 108:17 113:4,5,7 117:11 118:18 153:4 155:12 159:5 206:9 217:18 227:12 247:13 251:15 door 46:11	doors 232:15 Dorkbot 150:25 dotted 169:18 double 73:19 doubt 155:17 dovetails 166:21 downstream 26:19 199:16 dozens 144:8,9 draft 50:24 draw 59:11,11 66:24 drawback 216:19 drawbacks 216:10 Drexel 23:13 30:5 32:17 37:9 drinking 61:14 drive 39:23 142:12 driven 118:24 driver 41:6 42:5 64:2,6 driver's 228:21 drivers 41:18 214:17 driving 49:8 68:10 136:15 dropping 255:2 drum 119:5 dry 131:3 DSS 112:6 due 9:4 173:5,7 Dugas 121:9 122:17 137:15 142:25 145:12 150:11 154:8 158:18 160:13 163:12 167:3 170:15 dumped 148:3 Duo 76:9 102:14 223:10 233:12,25 234:3,15 258:23 258:24,25 Duo's 102:15 duplicating 168:5 Duquesne 121:12 123:9,14 duties 190:25 dying 241:22	E E 2:2 earlier 12:2 41:12 72:11 77:11 85:13 97:6 118:7 121:23 146:16 159:20 190:10 202:17 203:2 211:25 217:24 220:8 259:15 263:15 early 9:6 16:17 67:13 237:7 ears 28:11 ease 140:9 easier 20:10 21:5 206:17 209:17 220:18 225:16 234:23 257:8 267:19 easiest 29:15 233:22 easily 60:20 104:18 138:14 191:23 easy 33:13,21 63:17 65:11 67:11 91:4 140:12 146:3 economic 37:6 41:6 41:18 42:25 50:20 57:17 economics 42:6 ecosystem 127:14 139:14 141:15 166:10 ed 194:8,14 edge 52:9 edges 58:7 educate 30:7,9 31:2 69:4 199:23 educated 92:16 educating 30:6 education 47:18,20 47:22 56:21 82:2 137:25 150:19 151:3 167:16 233:2 234:7 Educause 47:19 effect 11:9 60:1 113:19 209:3 effecting 113:25
---	---	---	---	---

effective 3:23 33:5 48:9 74:3 80:10 86:12 99:16,20 101:11 105:15 107:10 114:10 115:23 127:22 134:11 147:16 195:6 203:23 215:15 219:2 224:14 240:6 260:6	29:17 32:10 122:11 131:25 222:15,16 226:18 240:22,24 254:23 255:9,9,10 emails 6:16 131:17 160:1 embarrass 155:24 embedded 130:5 136:23 embodied 67:9 emerge 198:19 emergency 10:21 49:9 133:23 emerging 159:13 216:1 employed 77:8 270:6,9 employee 6:20 7:8 92:9 110:15 181:18 270:8 employees 6:21 12:18 13:2 16:15 31:3 45:3 60:22 90:24 91:8,9,21 123:18 181:18 188:5 232:3 employer 214:20,23 employment 216:13 enable 154:4 enabling 216:15 enact 3:9 enacted 3:17,22 enclave 162:22 enclose 76:22 encompass 104:9 encourage 32:8 117:10 158:14 168:13 encouraging 26:8 136:16 267:20 encrypt 66:20,21,22 66:23 106:5 107:20 108:7,24 225:17 229:2,8,14 247:9 261:5 encrypted 17:17,22 224:4 227:9,25	260:13 261:19 encrypting 106:16 109:2 226:19 encryption 2:18 16:24 17:8,11,14 18:2 21:20 51:12 105:4,8,12,20 106:11,18,20,20 107:3,17,23 108:2 108:13,15 109:6 117:17,21 222:1,9 223:22 224:2,2,7 224:13,19,25,25 225:1,2,21 226:6 226:23 227:17 228:8 229:21,25 230:3,6,10 244:25 247:8,9,25 248:5 249:20 250:11 255:19,21,24 256:2 257:6,11,13 257:16 259:3,6,23 265:13,22,24 266:21,24 267:19 end-user 79:17 263:10 end-users 257:17 endpoint 44:7 60:18 84:24 123:7 159:19 endpoints 44:13 45:7 84:11,13,14 84:16 89:13 91:22 ends 180:15 energy 173:18 enforce 80:1 254:2 263:1,1 enforceable 263:9 enforcement 66:17 75:8,8 102:23 267:23 enforcements 103:1 enforcing 263:3 268:4 engage 42:1 63:9 82:4,23 200:20 engaged 24:11 63:15 94:9 96:21	engagement 97:2 engaging 44:24 116:13 engineer 129:16 213:2 engineering 91:11 178:3 186:10 213:2 engineers 129:15 136:12 188:16 enhanced 222:24 enlisted 114:1 enormous 91:20 ensure 99:9 243:16 ensuring 94:2 119:8 enter 22:10 enterprise 152:7 187:2 enterprise-wide 230:5 entire 31:2 57:21 60:10 123:22 126:17 139:14 147:1 245:8 257:23 260:9 entirely 212:3 226:11 252:4 entirety 64:25 entities 109:19 210:8 211:5 218:1 entitled 72:9 entity 132:9 211:1 211:16 entrusting 243:17 entry 22:9 environment 20:1 52:9,17 58:12,13 58:14 64:14 88:4 89:14,17,18,23 90:16 95:17 103:12 104:6 106:8,25 107:14 108:21 109:5 111:17 114:16 116:24 122:20 123:8 136:8 139:20 140:9 141:4 142:1 160:9	183:14 189:23 198:16 201:19 227:14 230:7 244:15 environments 25:4 59:3,6 95:11 110:20 122:24 202:4 267:24 envision 156:17 epidemic 51:21 equal 91:18 equally 44:10 equate 55:5,10 equation 33:4 equip 184:19 equipment 241:24 242:13 equivalent 14:10 96:2,14 102:2 193:19 239:1 240:14 242:21 245:4 246:14 250:3,22,22 268:6 error 155:17,18 errors 141:10 escalate 184:9 escaping 258:15 especially 44:21 78:10 92:24 133:17 135:5 156:14 157:22 187:5 198:22,25 202:4 204:25 211:4 226:12 228:2 241:13 245:7 255:4 256:20 262:10 essence 218:18 essential 25:22 essentially 34:6,9 36:14 126:25 127:11 140:15 161:16 225:19 establish 109:23 estimate 83:16 et 128:22 140:11 156:16,16 158:3 166:15 168:19
--	---	---	---	---

169:4,12	107:21 108:2	exotic 265:24	125:23 136:11	face 19:9 28:1 31:17
EternalBlue 135:2	112:6 113:9 123:5	expand 4:14	149:19 158:6,7,7	191:17
Europe 54:14	123:9 124:2 130:5	expansive 163:16	222:8	facilities 125:15
132:14,15	133:1,22 137:23	expect 81:21 83:19	explain 36:7 38:17	facing 28:15,18 29:1
evaluate 8:2 13:22	142:6 150:23,25	95:1	47:7 108:17	31:13 69:6 252:25
25:6,10 34:2	155:20,25 163:24	expectation 100:25	explanation 4:22	fact 87:9 113:2
evaluating 27:15	164:4 182:14,18	115:16 162:15	explicit 11:4 51:15	119:22 123:7
192:12	190:17 200:14,18	252:21	138:8	137:18 139:24
evaluation 15:12	200:18 203:13	expectations 99:18	explicitly 27:5 128:4	143:3 150:13
24:21 25:8 41:24	216:1 218:8	112:5 116:2	exploit 126:20 134:1	151:22,25 152:9
51:14	219:20 225:3	expected 65:20	exploitable 132:7	152:16 155:9,11
event 1:16 14:1	229:15 233:3,10	122:15	142:2 143:24	168:9 179:21
93:17 94:1	233:12 240:2,20	expecting 81:15	exploited 127:5	208:20 213:25
events 15:19 91:14	241:9,21 242:6	107:11	exploiting 129:5	226:13 235:3
93:2 94:12 96:10	examples 100:16	expense 123:11	exploits 127:10	244:14 245:8,20
116:23 122:1	202:11 203:13,17	151:19	expose 55:3 57:15	245:25 248:10
eventually 214:13	excellent 186:6	expensive 43:10	262:11	252:6
everybody 57:25	268:16	74:1,2 123:12	exposed 54:2 236:12	factor 18:19,23 19:4
60:21 64:1 111:3	exception 10:6	124:5 129:19	exposure 32:13	19:5 49:10,13
113:11 114:1	19:19 51:1,13,14	130:7 157:15	extended 203:3	61:23,24 89:5
157:16 170:3,8,25	56:10 202:21,23	250:11 255:25	extends 189:23	90:20 94:15 95:15
213:23 228:14	203:2 250:18	256:19 265:25	extent 105:11	207:18,23,24
236:20 244:2	exchange 111:15	experience 11:15	129:22 181:24	208:6,16,23
264:18 265:15	exchanging 111:11	20:16 30:18 31:20	182:11 190:11	230:22,24,24
everybody's 98:3	excited 26:5	37:11 38:4 73:11	253:2	231:2,2,7,11,14
everything's 32:7	excluded 5:5	77:20,25 79:8 80:6	external 6:25 17:18	243:14 245:7
45:16	execute 246:23	90:23 223:5	17:24 76:16 80:3	factors 18:18 126:12
evidence 40:20	executive 36:18	242:24 250:19	82:12 90:8 104:10	139:4,5 190:14
206:9,10	79:21,22 97:4,21	experienced 33:25	105:10,13 131:16	196:19 215:6
evidencing 203:11	97:21 98:15	75:6 78:24 79:3	131:21 132:3,7,10	230:21 233:22
evolution 98:17	189:20	125:7 187:16	132:19 147:1	234:3,9,11 242:5
evolve 98:19	executives 57:5	experiences 172:19	148:21,23 150:6	faculty 30:7 37:16
evolves 261:17	263:22	experiment 198:11	151:4 189:4	121:11 237:4
evolving 30:1	exempt 20:8 85:22	experimenting	208:13 210:18	fail 93:12 242:2
111:16	exempted 86:14	196:22	213:8 215:5 224:4	failed 49:18
exact 13:15 259:9	exemption 88:13	expert 141:8 149:13	224:10	fails 87:3
exactly 9:14 10:3	exemptions 85:24	212:10	externally 129:20	failure 36:17 170:13
15:14 16:21 17:9	exempts 10:8	expertise 20:19	131:19	fairly 4:17 5:7 33:3
39:18 169:19	exercise 31:1 142:16	78:10 120:11	extra 76:21 193:9	53:1 65:6 69:17
233:8 252:10	208:21	130:7 136:25	extraordinarily	130:4 168:24
EXAMINE 1:5	exfiltrated 262:11	144:10,21,23	140:3	178:1 190:5
examining 162:3	exfiltrates 32:11	149:7 150:6	extremely 184:25	fall 30:22 58:22
example 28:16 37:7	exfiltration 261:19	156:10 157:5,14	185:5,15 225:4	183:7,10 232:5
37:12 47:15,17	existing 73:1 74:7	158:4 233:14	eye 124:9,13 185:3	239:7
52:1 55:25 56:20	74:14 75:19 76:22	247:7 258:9	185:14	falling 43:22 74:8
60:16 73:10 74:10	81:20 197:4,5	268:12	eyes 28:10	235:1
78:23 81:23 82:23	exists 38:17	experts 20:18 31:10		false 141:24
89:21 90:2,6 106:3	exonerated 88:24	68:23 71:5 120:3	F	familiar 4:22 18:13

38:7 187:18 201:9	fields 38:6	48:6 55:23 56:1,22	206:10 228:10	251:8,10,16,20
familiarity 196:6,7	fifth 174:17 222:3	57:12 65:13 72:11	229:2,6	252:14 259:25
Family 56:21	figure 41:15 42:17	74:7,12 79:15	finding 126:23	265:19
famous 245:22	54:23 72:23	80:14 85:20,24	162:12 268:3	fit 50:9 82:9 83:14
fan 105:22 115:20	136:20 137:10	86:1,11,13 88:14	fine 137:6	137:19
116:11	141:17 147:5	89:4 90:18,20	fine- 58:5	fits 127:14 138:10
far 24:4 31:18	154:19 186:16	91:15 92:10 93:3	fine-grained 58:1	five 24:13,17 40:11
103:14 111:10	219:20 248:15	94:13,15,19 95:14	fine-tune 58:2	40:11 41:5 71:4,7
232:6 248:21	figured 42:9 151:21	96:1,5,13,16,22	finest 37:10	79:7 81:16 109:16
249:13 267:2	figures 85:13 129:17	101:19 103:8	fingerprinting	156:1 257:20,21
farm 132:15	129:25	105:8,11,14	247:4	257:21
farther 205:2	figuring 136:13	111:22 137:25	fingerprints 19:7	fix 127:7 129:4
259:19	214:5	138:1,13,15,19	54:5 231:4	144:12 163:3
fashion 15:9 16:2	file 49:12 155:2	153:19 160:12	fingers 249:3	199:19 202:23
18:14 163:3	229:8,20 260:13	161:21 163:25	finish 21:20 25:25	fixed 136:17 168:23
fast 116:14 199:25	260:14,16,20	170:7,12 176:2,9	26:2 52:24 164:17	202:25
faster 182:21	268:22	181:17 182:1,13	166:22	Flee 121:13 126:14
favor 235:1	files 259:3 260:19	182:14 186:25	fintech 81:10 94:21	129:6 130:24
favorite 115:15	261:5,5	194:1 198:22	183:15	135:6 137:12,15
132:9	fill 210:1 211:11	199:1 200:5,16,19	fintechs 83:4 112:3	138:15 139:9
FBI 61:9	filled 80:16	201:8,10 209:11	116:13 182:18	142:21 143:1
feasible 18:3 94:24	filter 39:8	209:17 223:20	firewall 43:11 45:2	158:18 168:3
226:3 266:1	final 112:16 170:17	224:13,21 226:8	60:14 74:2 84:25	170:1
feature 218:25	221:1 222:3 229:9	226:19 228:3	firewalls 67:2 144:1	flesh 11:21
219:3 230:10	237:8 266:16,20	229:12 230:17	firm 23:19 28:6	flexibility 8:18
243:8,10 266:8	finalized 83:20	232:1,19 233:21	188:20 197:13	98:19 104:7
features 128:21	finally 6:14 8:11	234:7 235:16,24	213:6 233:15	203:12,19 213:9
228:17	10:6 21:19 71:20	236:20 237:14,15	258:15	223:23 237:20
fed 49:3	84:15 141:22	237:17 238:23	firms 28:13,14	255:15 267:23
federal 1:1 2:1 3:21	162:13 223:8	240:12,16 242:20	241:9,10	flexible 4:1 8:16
24:19 25:18 36:23	224:12 233:20	242:25 243:13,16	first 6:7 7:22 10:13	88:25 114:20
39:25 56:24 63:13	267:8	244:16 247:24	17:15 21:24 22:13	257:7 267:19
71:25 97:24	finance 74:24 80:8	249:23 256:16	23:4,12 27:2 61:4	flip 92:3 238:4
173:13 222:6	173:18	264:15,17 267:1	72:5 77:20 81:2,5	floor 76:23
234:8 235:7 243:4	financial 1:4 3:4,9	financially 270:10	81:19 87:1 99:17	flow 116:4
feedback 71:19	3:12,18 4:16,18,20	find 8:4 31:12 41:5	101:18 111:6	flows 166:10
85:16 199:11,21	4:21,23,24 5:2,3,7	63:8 65:23 80:7	131:21 137:24	fob 244:10
200:12	5:15,17,19,21,22	113:13,20 120:7	172:25 173:23	fobs 239:12
feel 20:4 122:11	5:25 6:8,9,10 7:5	128:2 130:14	177:1 181:24	focal 67:19
165:10 176:20	7:13,19,21 8:1,6,9	131:7 133:6 134:2	182:8,11 183:23	focus 45:9 87:11,14
217:4 222:15	8:23 9:1,13,15,20	136:16 141:24	187:1 190:19	88:8,21 92:4 94:5
247:21	10:13 12:16 13:5	143:16 144:6	194:2 198:10	119:6 163:1
feels 80:4 85:6	13:13 16:20,23	145:11,16,25	201:8,14 202:12	184:15 192:17
felt 16:25 59:25	17:1,2,6,10,21,23	154:18 158:19	202:19 204:16	222:23
FERPA 56:21 57:14	17:25 19:21 20:17	160:21 162:11	222:19 224:1,7,18	focused 83:7
fewer 86:1	23:22 28:18 36:23	163:1 164:24,25	224:23 229:6	focuses 87:19
field 12:4 20:18 42:7	36:25 37:3,10,23	167:17,17 168:17	230:21 231:9,22	focusing 86:24
44:17 48:4 265:23	39:23 41:25 43:6	187:16,20 206:9	244:8,8 245:2	93:25 117:5

folders 229:3	forums 66:15	front 185:1 208:19 232:14	gaps 33:20 77:13 82:1	218:5,8,9 220:8 253:8 255:15 264:5 265:15 267:13
folks 74:23 108:17 132:25 213:3	forward 26:9 40:2 172:15 173:9 174:11 181:6,14 207:1 258:3 265:4	fronts 173:23	garbage 133:24	given 34:2 51:19 53:7 188:7 198:25 202:14 210:2
follow 66:12 74:5 78:20 88:3 89:3,22 90:17 91:24 206:3	fosters 200:25	fruition 196:18	Garseki 158:3	gives 10:3 18:25 55:25 131:3 145:8 235:9 236:15
followed 206:15	found 75:10 78:7 79:21 113:12 185:5	frustrating 62:23	gather 20:20 151:10 154:21	giving 69:22 253:10
following 22:6 62:9 96:3 160:17 190:18 196:19 218:17	foundation 115:17	FTC 1:5 3:4,7 23:4 23:6 42:11 46:15 46:18 48:22 50:3 52:13 53:22 54:12 57:13 66:16 68:16 121:5 137:24 156:12 161:9,24 167:1 168:8 169:10 172:4,8 206:25	gathering 154:11	glad 174:14
followup 99:2 184:23 202:24 226:5 227:22 229:9 232:18 253:12 257:10	foundational 115:21 116:9	FTC's 121:4 181:16	GDPR 54:13,20	GLB 71:3 72:6,12 75:19,22 121:4,20 160:9 222:3 259:19 268:14
food 62:1	founding 23:16	fulfill 116:15 209:12	gears 181:15	GLBA 138:8 163:13 237:15
fool 248:8	four 23:7 24:13 40:11 102:17 108:11 146:10 234:5	full 7:11 32:3 146:17	general 27:25 38:5 66:11,23 125:17 129:15 147:25 179:20 192:15 217:20 218:16 235:1 239:8	global 87:5
footprint 89:16	frame 159:10 180:24	fully 102:7 103:10 181:13 188:15	generally 5:6 10:22 24:9 38:7 129:18 132:1,6,16 134:21 159:10 179:4 200:15 207:5,15 207:21,22	Gmail 228:4 254:18 255:11
forbid 183:21	framework 49:24 49:25 173:17 177:3 197:4,24,25 205:18	fun 61:7,8	generals 54:13	go 3:14 6:5 10:4,11 12:22 14:19 17:9 18:11 22:8 23:8 24:15 25:3 29:19 37:19 40:9 41:5 44:2 45:24 46:17 55:9 60:25 65:14 75:12 76:9 77:22 79:9 81:5 87:12 90:9,13 91:4 92:11 104:20 109:15 110:12 112:16 113:13 124:19,22 126:12,17 129:25 131:5 146:14 147:4,13 149:13 149:22,22 157:6 157:10 158:23 164:3,4,14 167:1 174:13 178:25 182:8 188:10 194:2 196:9 199:18 201:24 202:7,23 204:4 207:14,18 208:25 214:3 215:18 218:24 220:2
force 236:23 241:12	frameworks 47:21 50:13 174:2 196:24	function 95:4 213:23	generic 100:15,17	
forced 88:2	framing 180:23	functionality 228:24	geographical 257:25	
forcing 40:25	Franchise 72:10	functionally 250:4 250:21	geolocation 245:13 246:4	
foregoing 270:4	frank 63:23	fund 138:4 250:10 250:10	George 270:3,16	
foreign 256:9	frankly 182:25 201:19	fundamental 68:18 168:16 195:9	Georgetown 23:14 32:18	
foremost 77:20	fraud 28:20 103:13 240:5	fundamentally 9:10	gesture 23:10	
forensic 58:10	Fredrick 121:12	fundamentals 50:17 69:12	getting 28:19 36:10 40:1 48:23 52:9 61:25 62:23 92:16 98:13 109:4 119:8 129:22 148:18 155:10 164:17 166:14 181:6 208:12 213:10	
forensics 157:7	free 102:18 122:11 140:4 144:6 148:8 149:8,18 151:11 217:4 222:15 225:18 233:12,13 233:17	funding 57:3 199:15	gift 61:16	
foreseeable 6:24	freely 41:23	funds 176:11	gigabyte 124:4	
forever 144:14	frequency 126:13 139:6 140:7	funnel 99:25	give 5:20 9:3 10:24 11:20 14:22 67:23 104:1 107:25 119:19 127:6,25 135:11 147:4 148:17 152:24 164:21 166:13 212:18 217:20	
forgotten 62:8	frequently 26:14 140:19,24 142:13 227:24	funny 56:13		
form 40:5 134:22 149:9 173:22 201:10 226:19,20 228:16	friendly 240:1	future 30:3 162:19 206:17,19		
formal 208:13	friends 53:22	future-looking 174:6		
formalized 203:8,22 203:24		G		
format 160:16		gaining 196:23		
former 250:14		gaming 145:10,16		
forming 190:1		gamut 126:18 129:21		
formulate 195:24		gap 45:8		
forth 9:18 20:22 53:14 107:6,7 159:12				
fortunately 266:8				
fortune 125:10,11 149:18,22 153:21				

226:1 245:4	129:20 137:4,8	207:5,15 210:11	146:24 148:25	261:10,21,23
248:15 249:14	138:17 141:24	210:11 212:7	151:11 153:7	265:23
251:5,15,21	145:20 149:23	218:15 222:2	157:2,7 158:1	guidance 8:19 52:13
252:22 253:24	154:12,25 158:8	235:4,9 241:25	160:6 161:2	118:11 137:9
257:9 259:19	159:12,14 162:16	250:7,13,19 251:2	169:10 175:18	156:12 162:3
267:6	162:17 163:19,20	256:3 257:8 261:4	177:4 180:8	163:13 169:11
goal 35:1 126:16	163:21,22 164:11	264:7,16 267:9	181:15 184:22	guidelines 87:25
127:4	164:15,20,21	goodness 54:10	186:3 187:25	88:1
goals 110:5 180:18	165:2,19 166:1,5	Google 76:13	189:15 190:10	guiding 67:4
181:2,5,12 199:9	166:18,19 167:14	152:21 245:24	191:25 193:14	gurney 241:23
gobbledygook	167:19 169:2,6,14	gotten 25:24 26:7	195:8 200:13	Gusto 121:14
113:15	169:22 175:12	45:15 225:10	204:7,9 206:20	guys 37:18 43:22
God 183:21	178:6 180:2	243:21 267:8	209:7 211:21	61:6,23 134:12
goes 5:9 38:25 56:15	186:14 189:3	governance 2:15	214:7 218:22	146:24 244:3
121:12 129:21	190:7 199:16	21:18 31:17 32:9	219:13,25 220:21	
137:11 153:6	203:22 204:14	35:19 64:21 68:18	220:23 221:2	H
173:9 176:18	205:25 208:21	172:1,6,10,22	229:1 257:4	hacked 36:10 37:13
177:22 178:5,16	209:23 212:18	173:9,21 176:17	265:20 266:17	37:14,15,20,21
243:19 255:10	214:3,5,16,17,22	176:25 192:4	greater 91:9 93:11	92:9
266:5 267:2	217:3 219:4,6,9	governing 14:10	145:15 153:16	hackers 114:21,24
going 3:7,11 4:9	226:23 229:16	96:2,21 97:4	200:8 253:2	half 135:16 173:2
9:14 11:19 14:13	230:4 233:8 235:8	government 97:24	greatest 28:17	HALOCK 23:17
14:19 15:1,20	236:2 242:23	151:3 223:12	green 34:22,25	39:19 41:19
16:10,11 18:10,18	243:10 244:21	234:8 235:7 243:4	35:10,20 222:20	HALOCK's 62:16
20:15 21:11 23:20	245:5 248:14	government-back...	224:23 239:5	hand 23:10 109:15
24:21 25:7,20	249:11 250:10,10	245:23	246:15 247:6	209:20 251:9
27:16 28:2 29:16	250:12 254:2,8,8,9	governments 241:8	251:17,22 255:25	handed 191:2
29:17 30:15 31:24	254:9 255:3,5	GPS-based 246:8	261:8 265:19	handle 7:19 16:4,10
32:21 36:4 37:17	256:21 257:21	grabbing 156:21	grep 149:24	79:5 120:3 137:25
39:17,20 40:13	258:5,12,15	gracious 23:7	ground 118:19	189:4 237:13
42:17 45:3,18 46:9	259:24 260:21,22	grade 232:21	group 23:16,19	handled 5:1 17:21
46:24 48:8,25	261:5 262:17	graded 40:11	27:19 31:8 38:4	handles 161:8
49:14 50:9 51:10	264:8	grained 58:6	127:6 192:13	handling 17:2 20:12
52:24 53:2 55:1,5	Goldman 161:22	graining 133:10	258:22,23 260:19	65:12 224:22
57:21 58:19 63:7,8	good 3:2 22:13 23:3	134:25	grouped 164:1	handoff 215:16
63:20,20,25 64:14	24:24 25:7,15 26:3	Gramm-Leach-Bl...	groups 44:19 174:5	handshake 133:3
65:8,17,18,20 67:5	30:15 43:9 47:11	3:16	192:10	hang 234:20
67:16 71:4 74:24	47:22 54:18 55:13	grant 202:23	grow 191:14	happen 24:23,25
75:12 79:25 82:4,7	57:16 61:20 70:2	grappling 24:14	growth 111:16	27:20 36:7 51:7
82:8,13 91:4,4,7	71:2 100:22	gray 50:19,22	guarantee 197:13	62:24 97:16
92:11 93:20 94:18	103:17,20 105:3	great 28:13 36:24	guarantees 176:13	116:23 143:13
98:5,24 99:20	108:1,2 120:6,8	65:3 73:12 100:5	213:12,15	144:4 152:15
100:10 101:2,5	121:3 125:17,23	104:25 107:25	guardrails 99:13	186:16 206:4
104:22 106:7,21	125:24,25 126:6	110:7 114:12	101:8	243:13 261:21
107:6,7 112:1,2	141:8 146:13	118:15 119:4	guess 53:9 61:5	266:18
114:7 116:7 119:5	149:10 153:20,21	124:15 126:8	63:20 140:22	happened 46:19
120:12 121:19	166:7 168:14	131:9 135:10	164:1 177:16	61:4 124:20,23
126:21 129:18,19	170:20 179:1	139:1 142:22	247:17 256:6	154:19,20,20

245:17	hats 78:3	68:13 185:6	highs 147:20	Hospitality 223:14
happening 24:18	haven't 26:20 33:25	198:12 201:16	HIPAA 58:25	host 132:3 149:17
62:15 63:1,25	38:19 42:9 94:23	205:9 210:1	HIPAA-compliant	150:5 166:6
150:4,4 159:6	151:20 217:2	211:17	57:22	hosted 45:17
182:12 189:6	haystack 145:16	helping 5:12,13 28:8	hire 187:11,14,19	hosts 125:3 132:4
happens 6:23 20:1	he's 91:4	69:20 86:23 94:6	209:12 212:11,15	147:5
33:16 59:2 149:11	head 80:8,8,9	104:11 110:21	214:4	hot 175:14 178:8,22
193:12 206:12	172:13 178:2,3	180:19 199:23	hired 158:7	181:10
208:24 213:24	180:25 187:7,13	helps 41:23 46:21	hiring 75:24 77:16	hour 34:16
215:9 228:1 236:3	187:20 191:23	50:22 201:21	120:2,3 187:12	hours 147:20
happy 41:4 42:7	223:9	202:20	historic 31:15	house 136:25 188:17
157:17 174:10	heads 263:6	here's 27:18 29:6	hit 244:21 252:15	188:25 189:2
182:10 264:19	health 255:5 262:21	45:17 46:17 59:15	260:4,12 261:4	212:24 213:20
266:4	healthcare 234:6,22	197:2,5 217:1	267:5	huge 44:16 45:8
hard 27:17 36:3,7	241:21 242:6	hereto 270:9	HITRUST 115:6	144:8 170:8 203:8
36:12 39:10 41:15	262:19	hey 35:9 36:7 38:25	hitting 25:16	human 61:23,24,25
50:9,9 54:23,24	healthier 49:17	46:17 61:7 67:9	hoc 40:13	62:4 66:11 86:24
68:5 132:21	hear 4:23 24:15	128:1 133:2 136:4	hold 4:19 6:4 19:24	87:19 88:9,22
143:15 144:18	47:11 51:6 80:25	162:5 196:10	32:17 89:5 95:16	107:7,8 119:7
150:21 151:10	168:4 186:21,22	244:2 247:15	116:6 168:14	hundred 158:20
154:18 158:25	201:24 217:11	249:4	202:25	170:12
183:8,8 185:10	234:19	Hi 222:2	holding 32:13	hundreds 123:22,22
187:11 189:4	heard 30:20,22	hidden 108:13	169:16	150:16 154:6
193:3 196:17	78:12 84:2 114:14	234:12 236:10	holds 90:20 94:20	163:11
211:3 233:4	152:18 202:1	hide 107:24 143:21	202:21	hurry 253:7 254:22
255:16 264:24	259:15	hiding 45:3	holistic 85:7 128:25	hurting 49:20
hard-pressed	Hearing 269:3	high 43:5 89:21	home 60:13 61:11	hybrid 61:2,2 82:7
164:15	heart 54:11	99:23,24 118:18	165:10 227:16	82:22 84:4
hardcore 43:21	heat 178:24	118:24 132:2	238:12,14 251:11	hygiene 87:21 92:22
harder 59:25 182:24	heavily 240:18	139:11 149:8	254:7,9,11,16	108:1 146:22
hardware 235:6	heavy-handed 203:9	151:19 161:14	255:2 256:22	147:16 151:1
239:17	held 4:16 17:16 56:2	176:13 196:18	260:24	hyper-focus 161:25
harm 14:5,5 24:22	88:19 105:9 224:3	197:11 255:3	Homeland 121:15	169:17
26:25 27:5,7 53:4	help 35:16,18,23	high- 196:10 227:9	151:2	
53:10,19,24 54:1,6	41:17 42:22 44:25	high-risk 104:17	hon-tegrity 66:17	I
54:8,8,16 55:2,6,7	67:5 68:23 75:24	227:8 235:23	63:18	I/crossed 169:18
55:10	77:23 78:14,17,18	236:3	honest 30:12 63:17	I'd 38:3 51:10 53:16
harmed 25:13	79:5,9 81:24 84:6	high-tech 173:18	63:18	71:20 72:2,14
harmonizing 112:1	88:21 109:23	245:24	honesty 66:18	75:20 77:1,15 84:1
112:10	118:2 127:5 129:2	higher 47:17,19,22	hook 165:24 243:22	87:11 90:17 95:19
Hartley 162:21	140:4 145:25	129:18 137:25	hope 21:9,22 117:8	95:21 99:2 101:14
hash 205:3	151:17 157:1	150:19 151:3	235:9	102:3 103:6 105:4
hashes 133:4,7,8,12	181:5 187:21	167:16 194:8,14	hopeful 247:16	105:18 107:16
133:13	199:13 220:17,24	205:19,22 234:7	hopefully 22:1	109:13 110:2
hashing 134:25	243:15 249:22,22	highlighting 52:20	69:15 98:14	112:16,17 115:12
hasn't 26:7 219:22	258:25	highlights 117:17	Hopkins 222:21	159:24 164:15
hat 81:21 82:6,11	helped 72:20	highly 140:11	227:3	170:4 173:20
178:3 183:12	helpful 47:14 55:15	176:11 181:8,9	hospital 49:2,15	183:11 206:21
			57:21 59:6	

220:3 222:10 224:1,18 226:5 230:12 231:9 235:15 244:23 245:1 246:11 249:14,17 255:22 256:16 257:18 260:8 265:17 I'll 24:2,8 27:19 46:13 55:11,18,20 59:1 62:11 88:23 122:13 131:13 183:15 190:17 220:1 251:21 259:13 I'm 14:18 23:4,10 25:10,11 27:1 29:16 30:2,3 32:12 32:21 39:1,17 44:17 45:3,17 46:23 52:23 53:2,6 55:4 57:21 65:16 65:18 71:23 86:21 105:22 114:7,25 115:19 116:2,11 121:5 136:25 137:1 149:23 151:19 174:10,14 174:15,16 175:21 182:10 186:10,11 186:14 187:18 201:9 206:23 208:17,20 209:16 209:23 210:3 217:3,11 219:3 222:5 226:19,19 226:20 227:1,4 228:14 229:23 243:10 249:14 251:24 252:9 254:2 256:21 259:24 264:1,7 266:4 I've 16:18 44:5 45:15 49:11 51:1 54:21 64:15,20 76:15 82:19 102:14 119:5	144:21 145:14 153:14 173:1 174:4,16 175:22 176:2,7,8 194:13 196:22 257:24 263:25 265:22 ICSI 125:24 idea 102:15 106:19 108:14 110:14 111:14 210:20 219:6 Ideally 128:16 ideas 39:15 identifiable 228:20 identified 7:7 99:23 identify 99:24 110:9 110:25 129:3 161:11 191:7 200:7 202:25 240:5 identifying 35:22,23 139:14 177:18 identities 179:7 identity 3:6 6:23 23:6 33:19 67:16 69:3 71:24 172:8 222:6 258:21,22 259:2 IDs 249:9 Iglesias 121:3,5 124:15 125:19 126:8 129:6 130:24 131:9 135:6 137:12 139:1 142:20 146:6,14 148:11 148:20,25 150:9 153:7 160:7 161:2 166:21 168:2 170:1,16,24 ill 143:9 ill-informed 30:19 illegal 61:8 imagination 48:16 imaginations 54:24 imagine 61:13 135:16 145:15 immediately 244:20	252:1 immense 62:18 immensely 69:21 immune 256:11 impact 8:8,12 26:19 27:9,13 28:22 32:14 34:8,22 47:8 52:14,15 59:16 64:19 93:7,16,17 94:1 135:13 137:4 141:6 166:19,23 205:5 215:6 220:12 259:21 impacted 165:16,22 impactful 67:6 impacts 25:3,9,13 25:14 51:16 143:18 144:16 181:12 204:19 imperative 212:21 212:24 213:4 implement 21:6 33:4,15,22 35:18 36:2 39:10 50:21 64:6,18 65:11 75:21 76:6,8,12 78:18 81:25 84:7 101:20 102:16 103:2 122:16 169:5 181:4 182:16 191:1 216:3,4 230:17 237:2 252:17 implementation 34:10 82:24 115:1 124:17 173:16 181:7 188:2 223:24 251:13 implemented 9:6 16:21 17:10 40:17 40:20 46:25 75:18 102:11 143:20 169:9 implementing 34:2 39:15 64:3 73:21 75:14 77:6 90:14 106:2 169:22 181:21 235:20	implicate 188:4 implications 67:18 138:3 implied 231:14 implies 113:11 imply 11:7 importance 115:25 important 25:7 27:10 37:5,7 44:10 48:11,22 74:17 75:2 84:5 87:17 92:17 93:20 104:8 106:17 112:12 115:4 124:12 133:17 135:23 137:17 138:24 145:12 153:13 154:4 156:24 161:24 162:25 169:12 177:13 184:2,18,25 185:15,18 187:5 192:8 194:5,9 203:18 204:23 210:5,19 215:17 216:5,20 218:15 241:18 259:22 importantly 155:1 167:25 impractical 242:17 impression 38:5 improve 86:23 improvement 98:16 improving 40:18 in- 84:3 136:24 188:16,24 189:1 212:23 in-house 80:15,15 81:15 85:11,12 95:9 118:10 127:1 129:13,19 136:19 158:7 188:16,23 189:3,10,11 212:1 212:5,12,20,22,25 213:7 214:14 inappropriate 241:16 incentive 214:20	incentives 29:12 117:13 incentivize 168:13 incentivized 214:22 214:24 incentivizing 136:15 incident 13:24 14:2 28:7 33:25 36:8 38:15 53:13 62:17 62:17,17 86:6 103:13 125:16 126:1 154:12 158:20 173:23 178:6,7 180:4 183:21 184:2 192:13 206:7,8 213:24 218:13 219:18 incidents 28:9 33:7 58:10 61:6,22 62:18 122:24 197:21 207:9 include 18:18 19:8 19:11 121:24 191:3 230:21 includes 6:17 11:17 173:3 174:2 175:1 222:24 including 16:5 20:17 166:12 173:24 174:5 231:21 245:22,24 265:6 inconvenience 53:4 53:11 incorporated 263:21 increase 10:19 77:12 200:16 229:13 increased 65:1 increasing 60:1 146:1 increasingly 13:4 151:25 239:19 incredibly 47:10 incur 238:6 independent 186:18
---	---	--	--	--

independently 153:1	241:5 253:7	173:12,15 174:6	226:25 239:18	institutional 165:6 215:10
indicated 34:15 174:15	influential 184:19	174:24 175:2,6,10	242:14 245:14	institutions 1:4 3:4 3:9,13,19 4:16,25
indicators 35:22 94:17	info 160:11	177:10,12,14	246:1	5:2,3,7,20 7:14,19
indistinguishable 160:2	information 1:4 2:6 2:9,16 3:3,10,20	178:17 179:2,6,10	insider 191:10	8:1 10:13 12:17
individual 10:14 18:9 74:15,19,23	4:16,17,18 5:17,19	181:18 182:23,25	insight 135:11 214:16 215:5	13:14 17:2 20:17
75:4 77:2,5,17,22	5:20,21,25 6:3,6	185:1 188:3	256:5	23:22 28:18 37:1
77:22 78:1,22	6:13,15,17,18 7:1	192:16,25 193:25	insourcing 125:10	57:2 72:11 74:8,12
79:13 80:23 81:21	7:3,9,11,20 8:2,10	194:6,14 210:14	install 225:15,18	79:16 85:21,25
95:25 97:7,9,18	8:13,20 9:11,16,24	210:22 215:22	installed 139:20	86:2,13 88:14
101:21,23,25	10:8 11:6 12:3,25	218:4 219:1	instance 208:17 227:1 236:5 254:4	96:13 101:20
102:4 105:17	14:12,15,21,23,24	222:21,25 224:3,8	255:11 258:23	103:8 105:8
109:22 110:4,12	15:18,24 16:14,15	224:9 230:19,23	264:4	122:15 125:21
113:10 119:9,13	16:19 17:2,16,20	238:21 247:19	instances 202:3 223:19 238:19	149:2 151:6
119:16 163:7	17:20,24 18:6,9,11	255:8,12 259:20	instant 94:7	156:14 163:23,24
201:23 230:18	18:21 19:21,24,25	261:19 266:1	Institute 47:13 86:22 121:17	175:1 176:12
individually 233:7	20:3,7,13,16,19,21	informative 171:2 230:12 235:14	158:19 222:22	181:17 182:1
individuals 30:16 42:3 77:14 81:19	20:24 21:11,13,19	268:13	223:6	194:1 198:22
111:1 193:24	23:1,13,21 24:20	informed 96:21 173:25 181:13	institution 4:18,21 4:23 5:18,21,22,25	200:17,20 201:1,9
industries 48:1 50:15	24:24 25:21 27:24	184:8	6:8,9,10 7:5,21 8:7	201:11 209:17,19
industry 38:22 48:6 48:13 50:17 51:3	28:2,12 30:13	infosec 28:14 36:18	8:9,24 9:2,13,15	217:7 223:20
94:23 117:13	31:17,21,24 32:1,9	infrastructure 131:5,6 160:5	9:20 13:6 16:20,24	224:21 226:9
130:19 161:12	35:19 36:14 39:22	227:15 238:23	17:6,11,21,23	230:17 232:1,20
164:6 196:23	40:25 43:4,17	251:11 253:4	19:21 37:8 80:14	233:21 235:17
199:1 233:25	45:19,20 47:20	260:9	86:11 89:4 90:19	238:23 240:16
234:6 244:2	48:12 53:20 55:22	ingest 149:20	90:20 91:15 93:3	243:13 249:23
industry- 36:21	55:22 56:1,4,8,20	ingestion 123:24 124:3	94:13,15,20 95:12	264:15
industry-adjusted 48:11	57:12,15 62:14	ingredients 25:22	95:14 105:11,14	instructions 48:20
industry-sensitive 47:16	64:21 65:7,9,13,13	inherence 19:5 231:2	111:22 123:17,19	instructor 223:6
industry-specific 112:5	66:13 68:19 69:2	initial 88:5 134:10 147:8	125:23 138:2,10	insurance 26:17,18 108:4
ineffective 47:1	69:25 71:1,5 72:4	initiated 254:12	150:7 161:21	intact 241:23
inexpensive 224:20 226:7	76:2,25 77:6,17	initiatives 174:6	163:25 164:5	integral 17:1 53:7
infeasible 105:14 224:14	80:19 85:25 86:12	inject 51:20	175:7 182:5	integrate 202:15
infected 62:23	89:5,6 90:19 91:5	innovating 40:12,18	185:22 192:9,22	integrated 116:8 119:8 181:9
influence 91:6 184:20 219:8	96:3,4,6,12,16,22	innovative 167:17	193:6 209:12,14	219:11
	99:25 101:9,17,21	inordinate 57:24	217:15 224:13	integrating 183:14
	101:25 102:5	input 198:3 220:24	229:13 236:10	integration 94:25
	103:5,21,22,23	insecure 33:18 128:4	237:15 238:13	integrations 183:17
	105:9,12,15,24	inside 59:4 60:8 91:10 132:22	240:12 242:20	integrity 6:3 7:1 66:18
	108:20 111:15	insider 191:10	244:17 247:24	Intel 162:23
	115:17,23 121:11	insight 135:11 214:16 215:5	248:13 254:14	intellectual 143:12
	121:13,24 122:4	instance 208:17 227:1 236:5 254:4	264:19	intelligence 28:12 183:22 256:9
	124:22 125:12	institution 's 18:1 96:1,5,16,22		intelligent 135:19
	126:10 137:19,22			
	138:9,24 143:5			
	154:19 160:10,23			
	161:5 162:15			
	172:2,12,20			

<p>136:11 intend 11:7 intended 8:22 161:4 163:18 intense 146:5 147:23 intent 143:10 intention 11:9 77:10 intentionally 165:12 192:18 interact 113:8 133:19 234:10 interacting 233:5 interaction 108:22 148:15 interactive 113:21 interest 40:1 186:9 186:20 195:22 interested 20:25 51:17 206:23 217:11 229:11 270:10 interesting 26:22 31:1 35:7,7 38:12 44:1 48:2,19 57:4 118:14 129:10 132:18 210:3 217:5 237:12 interests 189:8 internal 6:24 49:4,4 76:17 81:23 82:11 84:6 90:13 101:24 102:5 103:3,21,22 131:17 132:19,24 133:1,6,11 135:5 136:10 148:4,21 150:6 190:22 192:16 211:12,15 230:18 246:1 internal-eyes-only 217:21 internally 78:16 82:10 131:20 157:10 208:22 212:2 218:21 International 121:16 internet 41:20,21</p>	<p>148:4 246:17,25 261:16 interpret 254:10 interpretation 201:23 interviews 30:8 intimated 232:25 intricacies 35:15 introduce 23:8 71:7 71:9,20 89:18 91:8 142:8 172:18 222:11,19 introduced 16:8 introducing 71:10 introductory 23:22 intrusion 92:19 139:7 142:16,17 144:2,2 invalidating 108:10 invented 25:1 inventors 266:9 inventory 14:24 101:4 116:3,3,4 125:6 145:9 146:3 invest 159:4 216:16 232:21 investigate 15:21 155:13,16 investigated 142:18 investigation 154:12 155:2 investigations 58:10 155:23 investing 44:6 investment 42:25 43:9 44:6 investments 27:6 invite 206:22 invoices 41:13 involve 80:6,8 involved 5:12,14 33:6 75:11 98:13 165:1 188:7 190:1 190:3 234:9 236:5 236:6,8,21 259:1 involves 234:13 IOT-type 130:6 IP 131:15 147:4,14</p>	<p>245:3,6,11,12,14 245:20 246:13,16 246:18,22 IPs 148:17 irony 41:9 ISAC 223:14 isn't 24:14 51:22 113:6 164:11 197:18 261:15 ISO 48:14 ISP 123:15 254:9,10 issue 3:18 6:15 53:19,24 54:7,16 90:10,18 103:25 110:8 170:12 183:24 184:18 195:10 196:5 206:22 208:3 217:5,12,22 219:8 219:19 232:8 262:10,12 issued 3:14 4:6 issues 4:9 7:11 24:14 36:22 58:8 84:23 127:7,8,24 128:1,2 141:3,5,12 161:13 162:23 183:9 185:20 217:7 219:11 222:9 268:21 it's 5:20 6:13 7:7 9:10,14 10:22 11:24 12:4 14:24 15:22 16:21 17:5,6 17:17,18 18:18 19:11 20:1 21:10 25:23 26:22 27:8 28:12 29:17,20 31:1 33:17 34:17 35:2,7,10 36:7,17 38:12,23 40:1,6 41:22 44:1 46:24 46:25 47:1,4 49:12 51:25 52:2,14 53:1 53:7,9,18,25 54:23 54:24 56:14 57:11 57:16,18 58:19,22 58:24,25 59:1,9,16</p>	<p>59:18,25 60:21 64:11 85:3 87:18 89:23 90:11 91:16 94:21 97:3 98:12 100:10,11 101:10 103:17,19 104:18 104:19 108:2,13 110:7,24 111:4 112:1,1 113:2,3,14 113:17,18 118:19 130:18 135:19 138:18,19 140:17 140:23 143:3 149:6 152:10,20 152:21,22 155:8 157:18,22 158:12 159:24 164:15 165:12 167:13 169:10,12,23 178:23 179:11 181:11 182:23 183:1,3 184:1,18 184:25 185:4,4,5 185:10,15 187:4 188:17 189:3 190:5 191:1 192:3 192:8,25 193:1,8,8 194:5,8,9,11,14,15 195:16,18 196:16 197:21 198:4,14 201:12,16 203:9 203:17,20 204:9 204:19,23 207:15 207:17 208:10,13 209:11 210:3,5,19 211:13,17 212:4 214:5,17,18 216:19 218:14 219:11 220:22 230:4 239:24 247:11 248:8 item 116:11 149:16 183:4 195:2 items 99:11,22 196:11 231:6 iterative 199:21</p>	<p>jacking 232:7 jam 244:11 James 71:13 72:14 72:15 74:5 79:11 87:12 91:13 103:6 107:16 112:20,20 115:24 Jersey 172:13 job 45:1 57:23 112:12 163:9 166:7 179:16 185:5 213:5 264:2 264:3 jobs 220:20 Johns 222:21 227:2 join 21:9 23:8 71:8 joined 222:8 joining 37:17 71:11 71:16,22 72:1 121:9 172:4 173:11 220:22 223:2,8 joint 203:1 joke 132:20 Jorgensen 23:15 26:10 29:3 31:6 35:6 38:12 44:1 45:11,22 46:13 51:23 58:4 64:2 67:7 70:3 judges 90:3 July 1:12 237:4 jump 60:3 146:10 198:7 259:24 justification 248:4 248:24 250:1 justifications 249:20 249:24 justify 33:9 170:9 187:12</p>
<hr/>				
J				
<hr/>				
K				
<hr/>				
<p>Karthik 172:13 175:19,21 177:15 178:15 186:4 188:3,10 190:10 190:17 196:2 198:6 204:11</p>				

207:6 211:22	138:23 140:14	69:2 73:22,25	194:13,22,23	knowing 51:5 199:2
214:7 220:1	141:13 142:10	74:20 75:1,5 78:3	195:14,21,22,23	knowledge 13:7
Katherine 71:23	144:19 146:9,11	79:7,25 89:8,15,20	196:3 198:15,18	18:19 54:17 78:16
77:19 86:17 222:4	147:8 150:21	90:3,5 92:5 97:1	198:20,25 199:10	136:19 215:3,10
keep 13:10 31:21	151:16 156:18	102:6 104:11,12	199:20 200:2,10	215:11,15 230:22
90:25 98:23	157:2 158:10	104:23 108:17	200:21,24 201:2,8	knowledgeable
108:23 124:9,13	159:21 162:23	114:2,8 118:4,15	203:3,7 206:21	166:9
127:17 133:15	176:24 177:8	123:5,7,18 124:4	207:5,7,10,13,17	known 11:13 15:15
143:21,23 144:5	185:20 188:7	124:20 125:6,13	207:20,21,22,23	61:19 139:22
154:25 158:22,22	190:4 193:23	126:20,21 127:6,9	208:6,19,20	231:13
165:3 167:20	194:23 198:12,17	128:14 129:16	209:20,25 210:10	knows 12:3 187:17
185:3,14 220:9	199:9 200:2,10,15	130:6 133:24	211:1,5,6,6,7,7,19	211:1 216:14
262:2	200:24 208:21	135:19,20 136:2	214:15,22 215:12	
keeping 143:25	209:2,14,21	136:23,25 137:23	216:6,10,13	L
173:25	212:22 215:16	138:3,4,14,15,16	217:15,18,23	Labs 23:18 155:20
keeps 156:3	217:13 218:20,25	139:10,24 140:10	218:3,6,8,12,14,17	156:2
Kerberoasting	220:1 234:12	140:14,14,20,21	218:18,19,24	lag 38:10
133:9 134:24	239:7,13 241:1,25	141:4 142:17	219:9 225:21	landfill's 134:1
Kerberos 133:10,12	244:5 256:11	143:3,4,5,9,14,21	226:11,14,23	landing 250:16
key 24:1 35:22	258:2,3 261:17	143:24 144:2,6,8	228:2,3,11,19,23	landline 234:18
84:20 85:1,8 98:17	kinds 5:7 27:5,25	144:14 145:13,20	229:4,10,22,22	landscape 68:12
107:19 108:22	137:3 193:12	146:3 147:25	230:20,22 232:14	89:19 198:15,16
109:5 111:2 117:5	206:25 218:7,19	148:8,14 150:11	233:16 234:9,19	199:13 202:13
142:9 199:5 212:1	224:24 256:14	150:22,23 151:2	235:18,18,25	language 77:7,10
212:4 239:12,16	kingdom 68:1	151:14,18 152:4,6	236:3,9,9,12,14,21	107:10 224:7
keys 67:25 160:5	knee-jerk 33:12	154:13 155:5,15	237:3,9,14,22,24	laptops 44:23 89:16
170:21,22 239:22	34:19 52:7	156:11,15 157:1,4	238:8,11,12,13	large 6:11 11:11
247:10	knew 60:17 148:7	158:1,2,2,8 159:5	239:5 240:1,5	57:5 64:17 73:4
kicks 228:8	know 4:13 6:13 8:12	159:7,12 160:24	241:1 242:3 243:1	84:14,15 95:13
kidding 56:11	10:20,24 11:13	161:15,21 162:19	243:3,15,22,24	131:12 161:21
Kiersten 71:18 86:9	12:21,22 14:25	162:21,22 163:11	244:1,7,11,13,20	163:4,10 169:20
92:15 93:1 96:18	15:4 18:20 20:18	164:1,14 166:1,9	244:21 245:6,8,18	169:23 189:23
110:2 115:24	23:10 25:1,19	166:13 168:5,17	246:16,20,22	245:22 258:6
117:2	27:20,25 28:10,24	168:18,21,21	247:6 248:16	largely 9:5
kind 7:10 27:19	31:6,7,16,22 33:3	169:11,18 174:23	249:5,6,8 250:3	larger 79:14 165:21
28:10,25 29:21	33:7,17,17 34:3,15	175:4,8,14 177:5,8	251:1,17,22,24	165:22
32:23 33:24 34:10	34:21 35:1,2,6,15	177:11 178:15,23	252:2,2,5,9,15	lasting 252:21
34:11,13,19 38:10	36:4,12,14,16,17	178:24 179:7,8,9	253:1,7,23 254:4	Lastly 122:5
45:1,3,5 46:10	38:12 40:12 41:13	179:18,20,21	254:15,17,18,24	late 43:1
55:4 60:8 68:10,15	44:1,4,6,15,18,21	180:3,5,6,11	255:1,5,7,8 256:4	law 53:18 112:5
69:11 75:1,3	44:22,23,23 45:2,9	181:16 182:11	256:4,8,21,23	236:1
103:12 104:9	49:10 50:14,16,20	183:16,21 184:12	257:8,21 258:24	Lawrence 155:20
113:10 123:9	53:9 54:2 55:1,2	185:10,10,11,13	259:3,4,7 260:9,10	156:2
127:20 128:19	56:3 59:21 60:9,11	185:14,21,25	261:13,23 262:6,9	laws 216:1,13 246:6
129:11,12,21,22	60:13,13,16,19,20	188:7 190:2,5,11	262:13,22,25	lawyer 53:17
129:23 130:6	61:4 63:15,25	190:16,19,23	263:4,8,10,11	lax 132:18
131:13 132:20	64:10 65:6 66:13	192:6,9,11,18,21	264:23 265:23,24	lay 14:12,17
134:20 135:12	66:22,25 68:11,25	193:1,11,22	266:6,17,25 268:7	layer 34:20 204:16

217:21	legitimate 15:25	lies 8:15 187:6	11:20 12:7 16:22	145:10 149:20,20
layers 204:15,17	legs 160:12	life 18:15 62:24,25	19:9,18 20:10 35:4	149:23 153:9,12
lays 6:1 11:17 12:20	lender 95:1	176:1	44:24 61:2 66:11	154:13,17,22,22
13:25 231:5	lenders 5:10,10	light 170:9 201:18	68:14 73:6 79:4	154:25 155:1,22
lead 77:23 78:6	lending 81:11 107:1	lightning 218:23	114:3 123:6	156:21 157:3,9
106:24 109:25	lengthy 53:1 55:18	265:12	126:21 130:18	158:17,22 253:20
175:24 179:1	lens 95:22 130:13	likelihood 24:22	132:18 159:7,10	253:23 254:17,23
185:24	lessen 14:5	25:3 34:22 51:16	163:12 168:10	258:25
leader 111:13	lesser 253:2	likelihoods 25:9	170:4 175:12,23	long 25:12 64:4
leadership 33:13	lesson 77:12	likewise 198:10	178:14 191:5,6	154:25 188:19,20
35:24 64:8 97:3	let's 99:17 186:10	limit 14:21 260:20	195:11 203:10	200:9 201:21
98:13 111:12	188:14 206:8,15	260:22 261:6	207:6 219:23	204:1,8 209:13
175:5 179:4,12	225:17	limitations 116:21	226:22 239:12,25	216:20 219:9
180:1,15 184:9	let's 3:14 4:12 6:5	131:11 153:11	243:9 252:8	220:16 224:15
185:21,22 194:7	10:11 17:14 24:2	253:18	253:10	247:25 251:12
195:5,17,19,23	55:25 57:20 59:19	limited 52:15	live 110:14 123:15	255:4 264:13
leads 207:24	59:20 65:19 80:7	110:22 145:19	164:14 205:1	long- 252:23
learn 137:11	100:17 104:20	limiting 64:21	212:16	long-term 253:1,3
learned 62:8 256:10	letters 37:9	Lincicum 3:2 23:3,5	lives 80:5 194:24	longer 15:24 113:11
learning 61:2	level 28:25 41:3	27:18 32:21 38:2	LMS 95:2	190:12 191:5,12
216:16 249:11	43:20 55:6,12	45:24 47:11 52:22	loan 95:2 104:3	191:19 193:7
leased 255:20,23	60:11 64:8 73:2,13	55:17 59:14 65:3	loans 5:12,13	look 9:19,22 11:22
256:3,22 257:4,6,9	75:5 79:18 83:9	69:14 77:11	local 45:4 76:14	16:13 17:14 18:10
leave 116:19 117:11	90:4 92:18 97:23	line 25:25 26:2	149:7 230:3	21:11 22:9 24:4
215:8 237:20	100:4 118:19	31:12 35:11	located 15:2	25:9,17 26:22 27:4
260:15 261:5	133:22 139:11	149:16 177:1	location 152:2	27:5,14 28:25 29:6
263:6	144:23 161:15	183:4 187:2	246:18	29:15 33:1 42:25
leaves 48:15	179:12,22 180:5	190:19,21,22	LOCK 71:16 78:7	44:13,14 48:19,25
leaving 174:20	194:7,17 195:10	233:19 240:17	84:2,9,18 85:6	49:23,25 50:2 52:5
239:10	203:21 205:16	244:22 256:22	89:11 90:10 102:7	52:6 54:23 67:10
lecturer 23:14	209:4 211:8	lines 44:18 59:11,11	102:11	67:16 82:19 84:19
121:17	219:24 241:4	109:24 158:18	LOCK's 77:25	89:19 92:13,13
led 223:10	250:8,9,16 262:19	162:7 190:9,18	LOCK's 77:20	93:14 94:3 108:19
Lee 71:20 75:16,17	263:22 264:13,17	255:20,23 256:3	locked 242:12	113:17 116:20
75:20 76:24 78:20	264:17	257:4,6,9	log 122:21 149:21	117:22 122:22
90:17 119:19	levels 43:1 108:11	lingering 43:14	233:9 234:16	124:6 138:21,24
121:12 126:15	178:20 180:2	Lincicum 3:5	240:23 244:12	139:19 140:8
129:9 135:8	leverage 45:13	link 22:3 30:23,25	log- 249:8	163:22 166:2,18
139:10 156:5	50:18 95:6 166:13	links 179:18	log-in 85:1 125:5	166:20 169:2,6,14
161:14 165:8	liability 116:20	Linux 125:4 142:6	logged 132:11 134:8	169:19 173:9
168:4	218:20	list 75:4 131:17,25	134:15,17 155:16	176:12 186:15
leeway 166:12	liberal 163:19	listen 186:14	logging 122:21	187:14 199:8
left 72:3 109:12	license 228:21	listening 222:14	124:21 125:15	200:3 202:7 204:4
216:24 218:23	229:18	268:16	131:5 149:11	206:14 207:14
legacy 45:2 60:6	licenses 230:6	literally 128:6	153:14,17 154:2,4	229:17 240:3
legal 31:9 111:23	233:12 257:18	litigation 27:1	154:10 155:21	248:24 260:11
148:16 206:18	licensing 229:17	litigators 24:20	156:7 158:14	266:11 267:3
216:5 218:16	233:1	little 4:21 10:7,12	logs 44:14 122:22	looked 7:2 25:25

72:20 132:11 205:24 234:2 246:1 looking 3:7,11 4:9 20:20 25:2 31:11 36:13 38:4 44:25 45:18 53:10 57:23 58:15 60:6 75:23 75:25 76:4,7,16,19 76:21 78:4 83:1 85:12 110:1 118:5 140:21 165:19 169:11 172:15 174:11 180:15 197:4 230:5 233:15 234:3 242:10 247:13 249:8 264:20 looks 9:15 36:12 47:3 50:6 65:24 69:14 89:14 114:16 120:9 127:16 142:8 157:14 163:4,5 165:7 181:1 213:23 258:24 264:7 lose 92:9 197:13 260:7,8 losing 215:10 loss 34:8 103:13 197:2 losses 37:6,10 43:23 lost 39:7 69:14 261:16 lot 8:16 27:16 29:11 33:6 48:16,17 50:14 51:6 52:11 58:20 68:20 74:1 79:8 80:10 84:7 87:16,19 91:5 92:5 92:20 97:23 104:11,19 112:5 113:20 117:25 118:20 119:3,25 123:13,24 124:25 127:24 128:17 136:2 140:3,5	145:15 149:5 150:12,12 151:1 151:12,17 152:1 152:10,11,13 153:6,13 154:21 154:23 155:8 157:19 159:4,6 160:14 168:5 173:8,17 176:3 180:15 183:16 198:21 199:1,16 201:11 202:14 203:4,20 207:3 210:8,10 212:7 215:25 227:5 228:2 231:21 232:24 238:10 239:5,7,19 242:15 242:25 243:19 245:23 249:11 251:6 252:3,16,23 253:21,25 254:13 256:24 257:5,6,7,7 258:25 260:11 264:14 267:16,17 lots 238:14 love 53:16 82:21 116:7 129:11 168:9 206:21 low 43:4 51:17 low-risk 196:11 235:23 lowest 247:1 259:7 lows 147:21 lunch 21:15 luxury 185:12	maintain 7:25 8:18 9:16 10:7 13:7 20:7 31:14 60:10 85:25 101:2 151:16 225:15 267:22 maintained 13:19 16:12 maintaining 7:23 181:21 maintains 19:22 209:14 major 138:3 199:17 204:20 205:11,13 205:22 207:7,8 216:6 228:25 252:5 majority 140:2 143:2 making 6:22 11:4 43:9 58:6 64:23,24 92:15 101:1 116:24 129:17 139:16 175:4 176:6,19 177:2,3 177:20 179:19,23 180:20 181:13 190:7,15,20 193:11 197:15 203:14 218:19 219:7 225:22 226:24 252:5 261:24 265:7 267:18 malicious 206:10 maliciously 143:7 malware 92:19 man's 240:22 manage 35:24 37:6 58:14 124:11 143:15 144:12 146:3 175:21 185:3 187:22 210:13 212:4 258:10 managed 78:8 95:9 152:4 158:9 189:9 management 2:15	14:11 16:3 21:18 33:19 49:24 67:17 69:4 79:18 84:24 85:1 96:8 98:17,25 99:24 104:2,3,12 104:13,21 109:20 109:21 172:1,6 185:7 186:1 190:21 195:17 196:16 197:25 202:21 203:16 204:17 205:18 211:14 212:10 219:8,10 220:6 225:15 258:22 264:14 management's 96:10 manager 71:21 75:17 managers 170:22 manages 210:5 managing 71:18 145:24 152:8 167:23 177:18 185:19 186:10,11 196:12 210:6,12 210:18 212:2 213:2,3,7,21 mandate 262:7 265:21 mandated 243:4 mandates 117:9 mandating 117:18 mandatory 160:1 manipulate 260:18 manner 114:3 129:3 manpower 112:2 manual 47:9 manually 123:3 139:25 manufacturer 136:22 manufacturing 43:5 map 47:22,23,24 147:4 map-based 223:1 mapping 197:20	maps 134:13 marathon 25:24 March 4:7 175:24 Marchany 223:2 226:10 228:1,13 229:16 235:22 242:22 244:18 248:7 249:1 253:13,16 256:19 258:19 259:24 260:2 263:7,24 266:23 marching 201:25 margins 120:6 market 83:3 marketing 243:8,14 marketplace 83:18 massive 92:1 148:5 Mastercard 93:9 matched 82:21 material 8:5 96:6 113:18 mathematical 247:14 matrices 34:21 Matt 222:20 226:11 226:21 227:2 229:24 239:4 254:1 256:23 261:2 262:9 266:24 267:7,16 matter 34:24 36:24 48:24 86:9 88:17 92:9 167:13 187:17 195:22 214:3 251:3 matters 96:6 220:12 Matthew 222:19 223:15 224:19 246:11 251:15,21 265:17 268:11 mature 48:4 115:9 maturity 24:12 34:20 40:10,14 57:1 115:4,7 174:3 214:12 McCarron 71:2,23 74:5 75:15 76:24
	M			
machine 225:19 249:11 machines 59:2 260:5 magnitude 24:22 33:1 maiden 18:21 mail 39:8 47:2 mailbox 147:3 main 11:20				

78:20 79:10 80:12 81:1 83:21 85:15 88:12 89:2 90:17 91:13 92:25 94:10 95:18 99:2 101:13 103:4 105:3 107:15 109:11 111:18 112:7,15 114:4 115:11 117:1 119:18 120:8 222:2,5 226:4 227:22 228:9 229:9 230:11 232:18 235:13 238:16 240:9 242:18 244:16,23 246:10 247:3,22 248:22 249:16 251:6,20 252:12 253:12,15 255:17 256:18 257:1,10 258:18 259:11,13 260:1 263:14 264:11 265:9 266:19 267:12 268:10 McCloskey 71:21 McManamon 71:15 77:19 80:18 83:25 89:7 102:6 114:7 mean 15:13 19:11 33:10 38:18 42:13 43:11 44:10 46:6 53:6 73:21 79:13 108:18 127:24 128:3,8 137:22 144:11 145:13,23 154:9 157:19 158:19 159:4 161:15 177:12 195:12 207:10,22 208:1 226:10,13 228:1 239:10 246:16 249:2,13 251:22,23 253:25 256:1,1,2 258:19 260:20 261:8,9 263:9 265:19,22	266:23 meaning 66:18 93:11 128:9 141:24 162:4 165:23 meaningful 101:9 199:11 200:12,12 204:19 212:14 means 11:10 24:17 40:16 48:24 69:2 78:22 139:23 145:21 149:18 155:12 162:2 163:6 194:10 260:7 meant 6:2 19:11 127:3,14 129:1 measure 15:3 19:20 42:24 63:23 197:15 220:11 measurement 250:6 measures 67:6 measuring 92:22 meat 55:19 56:6 mechanism 196:22 220:16 mechanisms 99:17 130:16 196:17,25 243:22 media 30:9,14,14 medical 52:4,4 133:23 mediocre 40:25 medium 74:20 medium- 196:11 medium-sized 84:12 109:19 mediums 147:20 203:15 meet 20:4 63:10 145:25 152:12 184:9 meeting 112:9 205:3 meetings 205:5 meets 176:18 229:21 member 81:20 93:8 121:12 members 6:18 30:7	30:19 37:16 57:15 179:15 233:16 memorialize 19:16 206:11 memorializing 202:13 memory 134:7,18 mention 173:2 mentioned 23:23 26:11 40:10 43:12 43:13 47:15 51:11 56:25 77:3,11 92:15 97:6 118:7 157:15 178:22 183:6 190:10,17 201:6 211:24 224:24 237:22 259:6 263:16 mentioning 136:7 message 205:4 messages 179:18 238:6 messaging 195:6,19 met 191:24 method 34:14 41:22 104:16 204:2 231:23 241:2 248:5 264:6 methods 55:15 114:23,24 226:23 249:20 metric 35:7,9 36:11 metrics 35:23 220:16 MFA 102:4,12 117:12,16 233:11 233:17 238:24 239:8,8,12,24,25 240:13 241:16 242:1,4,7,15 243:1 244:3,5 245:2,4 246:14 250:10 266:5 267:2,19 Michele 172:11 174:13 175:18 178:11 184:23 186:5 192:1 194:2 198:21 206:21	209:23 211:21 217:3 219:14 Michigan 71:17 microphone 71:19 microsegmentation 144:1 Microsoft 133:9 134:6,14 152:20 229:20 230:6,9 mid-sized 144:19 241:12 middle 62:7 million 90:6 165:25 197:7,8,13,14 millions 29:13 Mimikatz 134:4,6 mind 5:9 15:9 108:23 127:17 144:5 161:9 167:20 241:17 244:17 mindset 119:12 mine 28:13 minimize 259:21 minimizes 201:23 minimizing 94:1 minimum 12:13 89:9 114:10 194:20 198:21 211:13 mining 132:12 minorities 144:23 minute 65:5 218:23 265:16 minutes 21:10 22:13 109:12 216:24 misbehavior 247:13 misinterpretation 106:1 missed 26:14 missing 27:16 115:20,21 mission 42:1,15 49:15,16,18,20,22 123:20 214:19 mistake 148:7 mistakes 180:14 misunderstood	108:6 misused 108:3 misusing 16:15 mitigate 14:5 264:22 268:8 mitigated 147:9 242:5 263:18 mitigating 143:19 143:25 177:19 265:2 mitigation 51:24,25 52:7 mix 74:23 mixed 82:21 Mm-hmm 112:7 model 8:7 24:12 45:2 57:1 81:19 82:3 115:4,8 182:19 183:9 186:25 189:14 190:4,9 191:14,15 191:21 192:4 200:3 204:15,21 237:18,21 249:10 models 40:10,14 81:6,8,18 173:24 187:4 254:25 moderating 121:6 modern 239:17 modest 11:15 Molina 23:12 30:5 32:16 36:20 42:23 47:12 53:16 56:7 56:14 61:1 65:15 66:10 moment 67:15 120:13 192:23 207:11 222:10 228:7 249:2 Monday 1:12 131:22 147:1,7,22 147:24 148:6,18 monetize 28:21 money 43:10 57:25 92:20 150:22 158:5 159:5 208:21 214:23 236:19 256:24
---	--	--	---	---

265:2	244:5 259:13	named 188:21	124:13 125:7	243:24 254:24
monitor 12:8 118:3	moved 61:3 152:13	naming 109:22	137:8 138:4,6,7,8	255:8
122:2 123:21	236:22	Nather 223:8	138:13 144:10	negotiate 50:10
125:3 155:23	movement 245:9	231:12 232:24	148:12,15 149:15	253:5
monitored 12:7	moving 12:4 44:20	240:15 245:5	151:21 152:8,22	negotiations 116:18
monitoring 2:12	62:19 115:4 126:8	249:24 252:14	152:23,24 154:19	neither 250:24
12:9 21:16 33:20	139:2 153:8	257:3,20 262:8	154:24 155:3	270:5
44:12 60:12 69:8	159:22 160:7	264:12 267:15	156:25 157:5	nervous 256:17
84:21 85:2,3 86:4	181:6,14 246:24	National 47:13 72:7	163:6,15,21 164:4	Nessus 125:5
115:2 121:1,7,21	265:4	256:8	164:17,18,19,23	net 93:16
122:5,14,16,19	MSSP 79:24 83:10	natural 201:12	164:24,25,25	NetEnterprise
123:1 124:18,21	multifactor 2:18	nature 6:12 20:10	165:3,4,5,6 167:6	176:8
125:2,3 131:6	16:24 17:8,12 18:7	53:12 63:15 89:4	167:11,23 169:15	network 6:11 8:8
146:12 149:3,8,9	18:8,11,13,17	90:19 141:14,22	169:24 183:18,21	11:11,12 16:6 18:1
156:16,20 159:1	21:21 33:18 39:6	161:7 166:17,18	184:6 185:14	45:4 60:21 78:25
167:4,10 236:11	49:5,19 51:2,12	183:17	186:12 187:14	79:14 84:25 89:16
236:16,18 249:10	52:1 64:9 67:2,11	navigate 134:16,23	188:21 189:11	102:5 123:22
254:4	76:7 101:18,20,22	necessarily 17:22	191:7 192:7,22	125:2,3,6,13 126:1
month 22:10 83:16	102:9 103:8,11,15	26:20 125:11	194:17 197:1,5,6,6	128:11,22 131:17
83:16 84:12,14,17	104:1,4,14,25	127:24 149:15	202:17 204:3	132:3,7,10,19,19
102:19,21,24	113:1 117:6,7,9	164:2 165:24	207:12 210:12,15	132:24 133:1,7,9
123:8	222:1,10 223:22	180:22 216:21	212:12 218:13	133:11,16,21,25
months 52:17 93:6	230:12,17,20	231:25 232:13	219:16 220:19	134:2,2,6,19 135:5
103:14 128:8	231:8,11 235:20	233:14 262:16	227:12 229:7,17	136:4,11 141:2,3
156:3 164:14,20	236:25 238:19	267:25 268:5	230:2 239:20	141:16,19 142:15
202:24 252:22	240:22 241:7	necessary 13:21	240:12 241:24	145:10 147:2
moreso 136:6 166:4	242:9 244:25	36:19 114:10	242:15,20 246:4	148:3,4,21,22,24
morning 3:2 23:3,8	247:25 248:6	136:24 155:12	251:13 253:2,4,5,9	149:8,9 150:3,4
61:14 71:2,4,8,12	249:21 259:22	165:2 235:4 242:4	254:22,24 255:12	153:16 155:21,23
71:16 120:10	265:13 266:21	need 8:9 9:21,22	262:7 263:2	156:1,3,7 159:20
123:6 148:6	multiple 55:20 78:3	10:3,4 11:12 13:1	267:22	170:19 225:23
259:16	85:13 111:14,23	13:9,9,16 14:16,25	needed 60:18 75:6	246:2 254:8,9,10
morning's 150:13	126:2 152:5 192:5	15:3,8,17,18,21,24	82:12 262:19	network-based
morning's 152:19	204:22 205:5	17:22 18:11,19	needing 135:22	246:21
mother's 18:21	multiply 236:15	20:4 27:14 33:14	needle 145:16	networks 17:18,24
motion 66:20,22	multitasking 61:12	33:21 35:9,18,25	needs 4:2,21 6:6,10	60:13 101:24
107:23 108:2,15	mute 80:24 93:4	36:1 38:9 44:9	7:2 8:21,24 9:1,19	105:10,13 224:5
224:25 225:2,21	235:21	58:21 64:17 66:5	9:19 11:2 12:6	224:10 230:19
226:2,11	muted 142:19	68:23 69:1,2,3,4,6	13:25 14:1,13,17	neutral 198:12
motivated 126:6	170:15	69:8 73:10 74:22	14:18 15:8,25 16:9	never 12:1 33:16
motivation 168:12	myriad 197:1	75:9 83:9 84:5	16:16 65:9 74:18	56:11 57:14
Motors 71:21 243:7		88:19,20,25 89:9	75:13 93:21 104:9	152:10 233:7
mounting 43:23	N	90:7 91:24 92:4	108:16,19 143:13	243:5 250:19
move 3:13 26:8	N 2:2	104:3,25 113:16	146:2 152:12	263:25
32:21 40:2 45:24	NADA 72:20,20	114:18,24 115:21	156:13 180:14	new 9:5 12:4,5 13:7
52:24 58:13 63:4	name 3:4 18:21 37:8	117:20 119:23	186:16 191:24	16:5,5 23:24 46:4
82:17 95:19	71:23 121:4 172:6	120:7 122:23	195:1 199:18	46:5 50:1 52:21
116:14 214:13	203:17 222:4	123:23 124:9,10	227:18,20 242:2	57:1 72:25 85:22

95:19 128:20	102:13 131:19	objective 168:12,13	okay 26:16 32:5	200:7 268:19
130:11 145:25	149:4 242:8	objectives 42:15	39:1 44:3 55:17,20	onsite 79:17
147:10 159:21	note 17:19 122:10	180:23	59:1 64:15 65:16	open 28:11 68:2
162:3,16 172:13	169:12 203:18	obligation 42:16	67:16 89:2 91:24	113:21 132:4
182:14,18,19	224:6	obligatory 45:16	95:18 109:11,18	140:13 157:25
189:22 190:14	noted 177:5	obtain 5:12,13	111:18 112:15	162:2,21 217:8
191:2,7 200:15	notice 4:6 153:13	obvious 33:3	114:4 118:9	230:1 237:17
227:14 252:5	206:9	obviously 45:10	186:21 206:15	242:2 257:18
254:25	noticed 61:1 243:9	50:14 60:9 113:1	211:6 216:23	260:16,16
news 27:22 38:20	noticing 73:4 190:21	127:3 129:13,17	218:22 224:23	Opening 2:4 3:1
61:17 153:21	notification 153:23	138:3 160:20	226:4 232:18	OpenVAS 140:14
nice 261:10 263:24	236:1	162:20 184:13	246:10 247:22	operate 107:22
269:2	notifications 184:10	213:19	248:22 249:16	112:3 131:16
nicely 166:21	noting 214:18	occasion 214:25	251:15,20,22	178:19 207:21
Nicholas 121:15	notion 127:20	occasionally 13:18	252:12 253:12	209:9 211:2 218:2
Nick 124:16 125:19	NotPetya 262:13	occur 140:22 144:4	256:18 257:1,10	operates 8:9 199:24
126:8 129:11	novel 130:11	occurred 31:18	258:18 264:11	214:2 261:1
130:25 134:4	nowadays 239:10,14	odds 215:1	265:9 267:6	operating 140:19
145:12 149:1	239:17	OECD 66:14	old 66:14	173:24 174:3
150:9 151:11	NSA 155:24,25	of-the-moment	older 18:21	218:16 242:7,11
153:11 154:8	nuanced 48:7 130:4	59:15	OmniSOC 151:7	242:14
156:6 157:4 170:2	nuances 141:9 211:6	offer 83:12 117:10	onboarding 202:19	operation 73:13
170:23	number 30:13 41:14	offered 236:18	once 62:5 83:19	144:25 151:16
nine-digit 47:3	47:3,4 52:4 55:3	offering 80:19	97:17 128:24	210:9 217:25
ninety- 158:20	61:4 62:18 72:21	offerings 83:8	131:24 134:9	operational 60:24
NIS 47:23 49:24	76:18 83:8 86:11	offers 152:3 233:12	141:13 147:13	140:15
NIST 48:15 160:18	86:15 88:6 89:12	office 35:17 45:7	157:25 159:23	operations 8:6
173:16 231:18	89:12,13 90:24,24	60:8 192:15,16	162:12 183:23	44:12 60:5,11 69:1
nitty-gritty 207:7	91:8,21,21 94:24	218:17 229:20,25	194:20 241:21	74:24 80:9 151:7
no-brainer 226:13	96:20 98:5 102:6	230:7,9 236:4,4	one-and-done	190:20 261:25
noisier 159:10	102:12 107:2,2	245:15 254:18	194:11	opinion 77:15 79:11
nonbank 5:2	143:4 150:14	255:10 258:24	one-pager 99:21	88:12 216:2 265:8
noncompliance	151:5 170:5,11	259:6	205:4,13	OPM 97:24
118:23	182:3,6 197:3	officer 11:6 23:13	one-two-three 67:14	opportunities 200:8
nongovernmental	228:17 230:8	76:2 106:4 121:11	one-way 98:12	opportunity 42:11
256:12	231:16,17,22	121:13 172:12	one's 97:25	55:13 86:18 265:3
nonprofit 86:21	232:6,16 261:7	195:17	ones 7:23 14:23	opposed 37:20
Norin 172:11	numbers 6:18 43:8	officers 81:10	37:24 47:25 50:15	60:13 169:18
174:14 178:13	73:3 93:14 197:10	193:25	50:16 94:17 95:15	251:1
184:24 192:2	197:12 228:20,21	offices 76:23	159:7 180:2,4	option 129:20
194:4 207:3	228:21,22 229:5	official 96:15	198:22 228:17	234:17
209:25 217:14	246:17	oftentimes 111:13	258:7 264:16	options 82:19 83:18
219:15	numerous 167:7	139:18	ongoing 31:1 44:11	83:24 116:16
norm 225:23	nurses 59:6 234:23	oh 26:16 40:12 46:8	69:7,7 97:16 98:7	181:3,4 240:8
normal 159:11	NYDFS 169:11	58:21 64:15 69:16	264:13	267:17
225:13 252:22		158:4 243:10	online 5:10 18:15	Oracle 152:21
normalize 151:9	O	254:22 267:6	61:2 81:11 95:1	oral 218:10
normally 60:19	objections 231:21	oh-so- 156:1	107:1 198:18,23	oranges 117:19

209:12 215:6 216:21 passage 201:20 passcodes 234:25 passport 228:22 password 67:12,14 170:22 179:19 229:22 230:1 240:23 passwords 18:20 133:5 230:23 266:6 patched 135:3 patches 128:11 135:1 patching 133:14 path 106:21 107:4 216:16 patient 37:24 49:16 241:22 patient's 49:11 patients 49:16 patterns 240:4 247:13 pay 26:18 85:11 129:22 219:23 payday 5:9 81:11 95:1 107:1 paying 27:11 62:22 94:16 129:12 158:5,10 208:14 208:17 215:14 230:6 payload 131:23 payment 58:9 95:4 222:25 pays 33:8 236:10 PC 79:17 PCI 58:8 89:21 90:3 90:4 103:19 112:6 115:6 228:19 PDF 146:25 peers 24:16 29:1 40:16,23,23 61:12 pen 126:23 127:9,17 127:23 128:5,7,14 131:4,14,18 135:4 135:12 136:3,14	138:11,12,13 146:17,22 153:25 penalties 235:25 pending 50:1 penetrating 167:9 penetration 2:12 12:10 21:16 76:13 86:4 115:2 121:1,7 121:14,22 122:6,7 126:9,15 127:19 128:17,19,23,25 129:10,14,24 130:8,12,23 131:2 131:12 135:23 136:5,5,22 152:17 159:3 162:6,7,9 168:19 212:9 Pennsylvania 144:22 people 4:23 5:8 6:22 12:11,19 14:22 18:12 20:15 24:3,7 24:8,21 25:21 26:16 27:1,6,16,24 29:11 30:7,13 31:23 32:8 41:17 42:4,8,13,20,22 44:8 45:10 46:11 46:22 48:18 50:7 57:19,22 61:11,16 61:19 62:5,5,19 63:5,8 64:23 68:23 69:4 74:13 76:4 79:3,7 92:16 107:25 108:18 113:7,22 114:15 128:18 132:18 133:15 135:3,16 135:18 137:5,10 143:6 148:1 151:12 152:11 155:10 156:10,19 158:22 159:15,16 163:11 164:16 167:16 168:11,23 169:3 176:5 180:16 189:25 192:23 201:24	204:21 205:23 212:11 225:15 226:14 231:24 232:13 233:3,14 233:17 234:2 236:12,18 239:11 240:1,2,4,7 242:3 243:2 246:20 251:11 252:3 259:1 261:18,24 262:5 267:2,3 people's 179:7 per-fee 144:7 percent 43:3,3,4,6,7 61:3 63:14 64:11 64:13 93:9,12 118:7 156:8,22 225:6,11 234:21 236:17 255:2 264:23 percentage 255:3 perfect 110:8 137:22 199:25 228:23 267:10 268:3,4 perfectly 203:20,23 perform 11:23 37:4 68:24,25 99:8 performance 35:22 141:3 performed 139:6 performing 173:5 period 143:25 237:6 periodic 122:6 periodically 4:2 11:23 13:17 permanent 253:2,3 permissible 209:11 permission 155:6 260:18 permissions 260:16 permit 80:14 247:23 perpetrate 28:20 perpetrator 154:14 person 10:18,19,23 11:2 14:8 17:4 18:5 19:14 46:9 59:3 77:8 78:6,24	79:23 80:7,16 97:8 113:12 134:8 179:1 181:10,11 181:20,25 184:12 184:18 185:1,6,11 185:13,18 186:8 187:7,12,23 188:8 188:21,23 189:2 189:12 190:4,6 193:17 195:21 209:13 213:1,4,5 214:4 219:6 220:5 220:7,9,13 223:25 224:16 248:9 251:18 personal 30:11 237:24 personally 228:20 250:14 251:24 262:6 personnel 12:18 13:1,5,8 74:14 125:8,17 126:5 156:25 167:12 188:4,8 189:4 258:9 persons 10:18 perspective 29:6,11 29:14 31:14 35:8 39:2,4 60:4,24 81:12 112:19,21 127:16 145:2,2 160:13 185:7,8 195:5 196:4 211:4 212:18,19,20,21 213:17 217:22 226:6 247:17 249:18 252:3 perspectives 120:11 193:10 persuade 36:18 PHI 59:8,9 phished 159:15 160:6 phishing 12:21 30:21 107:22 131:18,22 132:17 134:10,22 146:18	146:19 159:25 160:2 179:18 phone 19:2 49:10 231:15,16,17 232:6 234:18,19 238:5 239:15,22 246:17 256:22 phones 237:22 238:5 239:14,17 phonetic 43:1 158:3 phrase 156:7 physical 6:2 18:24 76:20 245:16 physically 242:12 physician 52:3 physicians 49:8,18 pick 50:16 130:2 147:18 218:25 219:5 234:18 258:7 picked 234:5,6 picking 72:2 picture 67:10 83:17 147:25 235:9 254:16 piece 52:19 100:9 117:25 183:6 189:22 218:10 243:15 pieces 46:14 52:11 193:12 207:23 piggyback 135:9 146:10 165:8 PII 143:12 228:19 pile 257:3 piling 120:1 pity 248:8 pivot 75:16 place 7:6 14:3 16:1 16:4,8 20:12 34:17 39:7,8 46:9 47:6 67:21 68:5 73:23 74:9 86:7 90:22 93:22 101:17 102:9,22 108:23 114:11,12 115:22 119:14 126:5 137:24 156:20
--	--	--	---	--

164:10,24 165:1 167:7 191:1 193:12 202:19 204:4 214:11 242:21 262:1 placed 176:19 places 140:18 152:11 216:2 plaintiff's 27:3 plan 6:1 8:2,5,10,22 9:18,22 13:12,25 13:25 14:3 15:17 16:3,9,19 86:7 249:15 planning 30:3 152:7 173:24 184:3 252:23 plans 94:8 238:3,5 platform 140:10 152:22 platforms 228:25 play 53:4,11 87:1 90:1 176:24 179:16,17 186:20 187:1 215:14 players 107:2 playing 178:3 179:23 plays 178:21 179:4 179:21 187:12 please 3:15 6:4 7:12 8:13 9:7 10:10 12:14 13:11 14:14 15:16 16:17 18:6 19:17 20:13 21:6 21:21 53:14 65:15 71:9 80:21 97:1 105:19,19 109:14 110:2 119:20 122:11 217:6 222:11,15 239:4 245:6 251:9 253:15 260:1 265:18 267:13,15 268:22 plenty 232:4 plethora 67:3 plug 68:15	point 34:16 35:3 38:14 39:18 46:24 50:24 67:19 73:5 81:19 91:16,17,23 92:7,19 103:10,17 103:18 105:3 108:16,22 109:2,3 109:5 113:4,25 124:20 128:6 131:24 140:1 148:9 181:20,25 183:15,23 184:3 186:18 187:12,23 188:8 189:2,12 190:6 193:16 209:13 220:5 225:5,10,20,25 229:1 233:23 247:2 249:3 250:2 265:21 266:2,6 point-in-time 199:7 pointed 267:16 points 17:19 64:22 83:11 87:12 94:25 116:10 117:5 224:6 254:6 policies 122:2 169:19,20 policy 32:20 46:25 102:20,22 103:1 169:13 202:2 polished 140:11 political 113:18 polls 123:2 Ponemon 158:19 poor 33:19 240:22 poorly 113:23 popped 147:11 popular 132:24 134:5 146:21 234:6,17,21 235:7 population 165:18 165:23 portfolio 175:1,11 175:17 211:4 243:15 portion 167:22 portions 72:20	ports 132:5 147:5 pose 109:13 position 86:20 116:12 positive 83:17 117:5 117:15 positives 141:24 possess 231:14,16 possession 18:23 19:2 230:24 231:1 231:14 possibility 77:13 247:18 possible 18:18 22:5 31:22 104:18 140:20 142:13 156:23 160:22 241:10 244:24 248:21 249:19 267:21 possibly 74:25 81:16 133:4,13 195:17 263:4 post-breach 33:12 post-incident 51:25 52:14 157:8 PostgreSQL 150:1 posture 161:20 potential 84:22 126:18 127:10,11 166:19 196:9 197:22 potentially 74:21 78:11 109:3 141:5 165:15 186:9 189:22 197:3 199:21 pouring 154:13 poverty 233:19 240:17 power 180:16 powerful 46:14 PowerPoint 230:8 practical 48:17 50:7 232:15 239:24 242:1 245:6 268:5 practice 103:18,20 139:19 145:1	170:9 207:5,16 223:13 practices 15:6 20:22 62:9 65:10 precautions 30:16 precedent 206:3,14 predecessor 264:2 preferences 82:14 premium 102:24 preparation 240:20 prepare 69:21 131:22 prepared 91:11 159:8 preponderance 26:16 prescriptive 68:11 69:10 162:5 168:10 presence 198:23 200:7 present 194:19 197:2 212:5 presentation 263:16 presented 22:8 99:19 217:7 presenting 198:1 president 23:18 71:15 121:10 172:11 248:19 press 207:1 234:19 234:20 236:9 pressure 244:4 presumably 250:1 presumes 11:3 pretend 246:22 pretty 8:15 13:15 39:4 91:12,18 146:5 147:16 148:19 179:11 252:15 255:3 prevent 52:8 155:10 260:21 263:13 preventing 7:10 62:21 154:1 prevention 93:19 94:6 144:2 preventive 62:20	63:23 previous 99:24 176:4 206:14 price 83:11 157:21 236:13 256:2 257:23 prices 120:5 pricing 82:18 83:2 83:14 84:8 102:15 258:8 primarily 10:9 160:10 173:15,22 primary 184:1 237:16,16 263:9 principal 201:15 principle-based 66:13 principles 66:12 67:5 printer 133:2,3 prints 19:9,10 prior 129:4 174:18 198:10 202:7,8 215:19 priorities 127:7 prioritize 162:13 priority 98:18 privacy 3:6 23:6 31:8 53:20 54:19 56:22 66:15 67:18 67:19 71:24 100:14 105:23 172:8 175:22,25 215:25 222:5,24 241:23 246:6 private 173:14,17 privilege 215:21 216:8 260:25 proactive 38:15 84:22 92:21 109:7 115:3 129:3 153:15 261:6 proactively 130:16 136:16 162:11 168:17 probability 34:8 247:16,21 249:5 250:6 264:15
--	---	---	--	---

probably 15:14 19:7 23:9 36:4 65:16 73:19 92:10 106:5 124:4 128:23 135:16 140:22 143:3 145:21 146:21 159:8 163:10 166:1 168:4 186:14 198:21 242:11 252:23 258:11	200:11 208:15 218:7 product 4:20 102:13 146:21 149:6 186:12,14 206:5 220:14 229:17 234:3 products 149:1 189:1,10 199:14 212:1 230:9 259:9 professional 62:25 83:13 106:1 professor 222:21 profit 120:6 profitability 36:13 program 6:6,20,21 6:23 7:2,8 8:13,20 8:25 9:11 10:15,21 10:25 11:16,19 13:10,23 14:8,12 14:16,25 15:8 16:1 17:4 18:6 19:14 29:23 35:11,19 46:4 68:19,21 74:15 77:7,18,24 78:24 81:25 84:7 85:8 89:6 90:21 96:4,7,12,17,23 99:23 100:2 114:11,20 115:18 115:23 126:11 128:25 138:5 148:12 161:5 165:19 173:3 175:2,4,6,7,9 176:5 177:14 178:19 181:22 182:16,25 184:20 185:1,6,20,25 186:2 188:3 190:22,25 191:3 191:11 192:3,20 195:3 197:5,16 199:4,8 210:5,15 210:17 211:10 212:3,4 215:22 219:1,3 223:25 224:17	programs 2:7,9,16 21:12,13,19 23:2 23:21 24:1 37:13 37:17 46:20 71:1,5 72:4 74:13 161:20 168:15 172:2,20 172:21 174:25 181:19 191:16 progress 42:24 197:15 198:24 266:12 progression 186:1 194:14 project 75:12 203:16 projects 82:15 174:7 proof 43:22 proper 34:6 77:23 79:24 99:12 167:8 168:22 properly 13:20 133:25 136:13,20 155:23 162:13 168:21 property 143:12 proposal 164:13 proposed 3:13 4:6,8 4:10 8:17 9:4,8 10:11,12 12:15,16 13:12 19:19 20:23 22:7 25:5 48:22 49:7 50:25 51:11 53:8 72:6,7 74:8 75:21 77:2,4,7,10 80:13 81:17 83:5 83:19 85:18,21 88:15 95:20,24 99:22 101:15,19 101:22 103:7 105:5,6,7 107:9 112:18,23 114:9 115:13,20 119:20 121:19,23 122:1,5 166:24 181:19 193:15 200:21 209:9,10 223:18 223:23 224:2,6,11 227:11 229:11	230:14,16 231:5 238:18 247:22 253:17 254:4,15 255:14 259:19 265:14 proposing 66:14 pros 182:19 193:22 prospect 252:25 prospective 84:4,4 89:20 protect 3:9 6:3 15:4 15:5 26:24 29:22 37:8 42:16 45:3 54:9 57:12 58:22 59:12,24 67:2 69:1 69:6 103:20,21,23 105:8 122:23 143:11 153:3 160:17,19,23 167:24 179:11 194:16 228:11 261:11,25 262:5 protected 26:20 32:7 59:5 89:24 155:2,3 247:10,19 protecting 25:14 26:13,22 27:7 43:11 45:5,6,7 58:7 151:14 167:23 179:2,6,7,8 179:17,24 199:5 211:19 262:3 protection 3:6 23:6 33:8 45:2 54:14 59:25 60:18 71:25 159:19 172:8 222:6 protections 30:1 166:14 protects 199:1 protocols 93:22 94:4 101:17 proud 156:2 prove 54:1 proven 4:1 provide 8:23 12:17 14:8 44:12 48:7 66:4 78:9 82:23	84:23 87:25 88:21 94:23 118:11 138:20 165:6 187:21 198:3 200:8 203:2 214:24 226:6 239:6 243:21 249:18 253:22 264:3 265:16 provided 72:8 233:11 provider 13:3 45:14 72:15,25 73:1 77:9 80:17 82:5 96:9 105:24 108:5 158:9 241:21 242:6 providers 7:18,19 7:22 13:14,17 83:2 101:1 104:5,10,19 105:2 106:15 116:13 166:11 188:15 213:12,16 232:10 253:6,21 262:20 provides 52:2 84:3,9 84:19 85:6 102:25 122:22 providing 4:20 8:19 13:20 20:16 76:24 78:11,14 85:2 87:25 101:9 199:20 204:8 proving 159:18 provision 209:16 proxies 245:13 psyche 267:9 public 4:6 26:7 27:15 62:24 72:5 217:7,15 236:7 241:19 244:7,12 256:20 267:8 public-facing 68:3 public/private 174:7 publication 46:15 publications 28:13 52:21 published 139:22
---	---	--	--	---

pull 134:7 182:24
pulled 82:13 102:14
 103:11
pulling 82:11
purchasing 189:21
pure 185:7
purely 29:5 205:7
purpose 15:25 87:3
 153:9
purposes 31:15,16
 56:2 160:9 250:15
purview 56:9
 108:24 180:14
 217:20
push 53:23 137:9
 168:10 234:15
 267:3
pushback 39:9
 106:12,14
pushed 41:3
pushes 41:7
pushing 40:7 49:18
put 9:18 47:5 55:11
 66:8 73:23 87:10
 90:21 101:17
 156:20 183:11
 189:8 190:25
 200:17 210:10
 228:4 238:21
 242:16,20 252:19
puts 140:14
putting 44:7 46:16
 156:12 164:10
 188:17 200:24
 247:11
Python 149:25

Q

QRadar 157:20
Quade 270:3,15,16
qualifications 11:8
 11:15 46:8
qualified 10:14 11:1
 11:2,10 13:1 74:14
 74:23 75:3 77:1,5
 77:17,21 78:1,22
 79:12,22 80:16,23
 95:25 101:25

105:17 119:9
qualifier 205:12
 212:23
qualitative 55:14
 196:16,25
qualitatively 55:8
quality 40:25 149:9
 214:24
Qualys 140:11
quantifiable 264:18
quantification
 196:24 197:24
 198:10 199:22
 220:7
quantify 55:7
quantifying 264:16
quantitative 55:15
quarter 180:24
 197:17,17
quarterly 143:14
question 27:18
 28:23 34:1 44:15
 45:25 46:2,15
 52:25 53:1 55:18
 55:21 56:6 59:16
 65:4,6 67:8 88:5
 89:3,8 93:21
 100:11,12,15,17
 100:18 106:6
 107:3 109:12,18
 110:7 111:19
 112:16 160:8
 161:3 166:22
 182:3,6,11 184:11
 195:12 196:13
 209:24 215:2,19
 217:6 227:22
 232:19 235:16
 240:10 242:2
 246:12 249:18
 251:10,19,23
 255:18,19 257:11
 257:11 259:14,14
 261:9 262:8
 263:15
questioned 178:8
questioner 183:24
 259:18

questions 21:23
 22:2 27:2 52:23
 55:16 85:16 86:25
 100:19 101:3
 122:10 150:3
 178:9 181:23
 208:4 217:1
 222:14,15 238:17
 251:7 265:10
 268:17,18
quick 50:23 124:1
 189:19 265:12
quicker 52:16
quickest 252:20
quickly 14:19 24:8
 62:12 85:5 99:13
 129:25 148:8
 164:12 168:17,20
 184:8 198:17
 202:5 216:25
 218:24
quite 4:7 42:9 43:6
 73:4,7 91:23 124:5
 160:20 167:3
 219:22
quotes 72:23

R

raise 23:9 109:15
 185:20 195:10
 251:9
raised 4:10 64:7
 238:17
raising 100:6 101:11
Randy 223:2,15
 226:5 229:10
 232:25 235:15
 242:18 248:2
 250:5 257:12
 261:12 266:20
 267:16 268:11
Rangarajan 172:13
 175:20,21 177:16
 186:5 188:12
 196:3 204:13
 211:24 220:3
range 43:7 78:13
 83:15 84:10 89:1

129:7
ransomware 28:21
 29:8 30:23 32:11
 92:20 259:15,21
 260:3,4,10,12,13
 260:24 261:4,10
 261:11,17 262:9
 262:14 263:3,10
 263:13
rarely 149:23
rate 94:20 95:16
 132:2
rates 225:8
rationale 203:2,6
rats 229:3
Raw 156:3
reach 108:25 183:21
 184:4
reached 265:20
 266:2,6
react 94:7 122:20,23
reaction 33:12
 34:19 49:12 245:9
reactions 61:15
read 37:9 38:19
 113:14 149:23
reader 48:16
readers 239:19
Readiness 71:19
 86:22
reading 61:17
ready 146:11
real 3:24 24:14 40:6
 41:6 42:5,11 50:10
 51:3 60:5 72:22
 131:2 134:21
 154:18 242:10
realistic 158:15
 161:19 203:20
realistically 263:1
reality 33:11 110:13
 138:14 159:18
 169:21
realization 245:10
realize 232:8
realized 61:6,11
 143:15
reallocate 199:15

really 13:9 14:25
 20:6 21:22 23:24
 23:25 24:14,21,24
 26:8,20 28:24 32:3
 35:6,16,25 36:3,7
 36:9 37:12 43:19
 43:22 46:21 47:4
 48:21 54:2 59:10
 64:7,17 67:6,15
 68:4 69:19 72:21
 73:4,17,19,20
 74:22 75:2,8,13
 79:18,22,25 80:4,6
 84:21 85:7 86:25
 87:19 88:8,18
 90:13 91:3 92:4,17
 92:23 94:4 97:8
 104:1,7,9 105:1
 107:3,19 108:15
 108:22 109:9,10
 110:8,13 114:11
 114:13,15,19
 115:8 117:21,22
 118:2,11 119:4,6
 125:1,25 127:4,14
 128:15,24 129:2
 129:10 130:13,19
 134:11,11 135:20
 136:11,11 137:16
 137:19 138:1
 139:13,13,25
 140:12,12 141:16
 141:16 142:3,3
 143:17 149:10
 151:10 153:13,14
 155:7,12 156:13
 157:14,23 158:1,1
 158:6,6 161:24
 162:4,4,7,25
 164:16 165:13
 168:11 169:16,20
 170:9 173:23
 174:9,10 177:1
 180:17 181:1
 183:18 184:18
 187:9 189:4 193:3
 193:9,9 196:20,21
 199:5 202:17

205:15 208:5,10 208:23 210:11,11 215:20 216:11 217:2 218:15 220:23 225:14 228:5 231:15 234:6,16 239:7 241:17 242:16 244:14 245:22 246:25 248:9 250:7,23,24 253:8 256:7,19 262:3 266:1,4,16 rearchitect 253:4 reason 8:12 17:5 19:14 42:1 78:1 114:21 128:13 141:8 143:4 145:4 234:22 241:25 247:7 254:24 257:9 reasonable 40:1 41:8,10,19 42:8,13 245:3 246:13 reasonableness 25:8 25:16,23 26:4 27:12,17 40:8 51:21 reasonably 6:24 102:1 122:15 239:1 240:13 242:20 reasons 31:15 57:17 183:20 231:22 235:11,11 253:7 262:21,21 rebelled 243:5 rebuild 267:25 received 4:19 160:1 217:1 227:23 receives 5:22 recess 22:15 70:5 120:14 171:3 221:3 recognition 19:9 recognize 110:19 161:24 recognizing 39:1	87:18 169:21 recommend 51:10 128:18 145:1 198:4 246:3 recommendation 236:23 recommendations 96:11 167:1 237:1 recommended 50:24 102:21 recommending 181:3 record 15:18,21 49:11 52:4 55:4 95:25 131:6 203:19 217:24 236:14,14 240:24 recorded 270:5 recording 155:25 records 32:17 52:5 91:20 94:19 166:1 170:8,12 217:8 236:12 recovery 154:2,3,5 257:5 red 34:22 reduce 32:2,12 34:10 85:20 122:24 139:15 197:6,7 reduced 270:4 reducing 35:1 197:18,21 Redzone 71:14 72:19 reevaluate 8:10 refer 233:18 reference 188:12 referenced 188:4 referring 106:8 116:2 regard 237:11,13 regarding 14:11 96:3 regardless 87:4 88:14 103:18 106:18 regards 127:13	142:9 168:24 regimes 111:23 regional 30:9 registrar's 35:17 registration 31:21 55:25 regs 255:14 regular 30:14 194:20 195:13 199:11 regularly 7:15 regulated 56:21,24 120:4 176:11,15 regulation 54:20 58:23 166:6 regulations 9:5 52:21 57:13 110:19 130:21,21 137:4 160:19 182:13 187:18 227:10 237:13 253:17 254:5 255:15 263:5,13 regulations.gov 22:9 268:20 regulator 27:3 regulators 24:20 25:18 54:12 178:8 regulatory 37:10 57:9,17 111:23 184:9 215:24 reinforce 192:2 202:8 reject 202:14 205:14 related 56:1 84:24 96:6 121:20 122:24 142:21 146:12 181:23 268:20 270:6 relatedly 34:11 relates 116:12 209:8 relation 161:13 relations 236:7 relationship 53:23 98:14 111:22 152:7 210:7 218:15 relationships 210:13	relative 270:8 relatively 170:20 251:12 released 158:2 releases 236:9 relegate 119:10 relegated 184:17 relevant 90:25 136:24 157:12 161:12 211:7 reliable 241:2 relies 107:13 rely 163:6 176:6 202:17 258:12 relying 166:11 183:7 215:3 245:20 remained 147:10 remarks 2:4 3:1 23:23 remediate 162:13 219:23 265:5 remember 152:16 158:21 243:6 remind 178:19 179:15 207:12 reminders 179:21 remote 33:18 60:10 61:3,3 67:25 104:5 125:5 146:20 204:25 252:17 remotely 44:22 62:20 64:12,14,24 251:11 remove 186:9 repeat 117:20 repeatable 162:14 163:3 168:14 replaced 241:14 report 61:9 86:7 96:15 98:10 99:6,7 99:11,17 101:7 113:14 141:25 144:8 147:7,8,13 148:5 180:3 191:23 193:17,20 198:23 199:3 200:9,11,17	208:14,15 217:9 234:1 reported 14:1 37:14 43:1 REPORTER 270:1 reporting 10:10 30:15 95:21 96:19 97:13,14 98:8 109:23 110:4 156:2 174:2 184:10 196:4 198:20 200:3 201:15 233:9 reports 14:9 20:9 130:22 148:18 207:8 218:7,9,9 220:8 represent 180:13 representatives 161:17 192:14 represented 193:6 193:10 220:6 representing 175:6 represents 84:1 165:21 reprioritize 199:15 reputation 57:17 reputational 265:6 request 133:12 requested 217:25 requesting 132:25 requests 96:18 173:6 217:8 218:19 require 9:17 12:23 13:13,18 14:7 15:8 16:22 17:8,15 18:8 20:7 37:25 95:24 101:19 105:7 121:24 122:1 181:19 187:19,19 223:20 224:3,11 230:16 259:20 260:25 261:9,25 262:1 required 3:17 11:8 61:8 65:12 73:2,14 73:15 86:2,3 88:14
--	--	--	--	--

88:17 109:9,25 118:5 193:17 224:21 226:8 237:23 requirement 5:24 12:13 13:15,24 17:15 18:8 75:7 77:2,4 95:20 96:19 96:25 97:13 98:8 101:8 102:7 103:7 103:19 105:2,20 107:17 115:15 182:13 191:2 200:1,14,24 201:2 215:24 218:18 224:2,8 230:13 244:6 263:12 requirements 8:23 9:18 10:1,9,10 13:13 17:3 19:19 20:5,8,11 21:1 53:5,6 57:7,10 72:17,18 85:23 88:11 97:1 98:4,23 101:15 106:23 111:10 112:9,11 113:5,6 116:9 118:4,16,25 148:14 169:13,14 176:19 181:24 201:9 206:25 209:19 267:10 requires 3:8,12 7:13 7:21 8:1 11:22 31:2 74:12 118:1 136:18 181:17 200:19 requiring 7:24 102:4 255:19,21 rescans 147:19 research 39:2 43:16 43:21 57:2,3 79:4 151:6 160:24 163:24 167:24 222:23 223:12,13 223:14 249:11 257:24 researched 93:9	researcher 121:16 researchers 82:13 126:2 167:25 resell 102:14 reserve 236:19 reside 60:23 resilience 93:19,25 resilient 191:16 resolve 178:6 resource 76:9 84:6 145:2 184:14 211:15 resourced 184:14 resources 50:21 59:17,24 63:3 74:9 82:11,12 85:12 87:15 88:10,21 103:3 110:23 112:2,12 118:21 119:25 145:18,19 145:24 167:6 168:22 184:20 211:12 resourcing 129:13 183:2 201:18 202:10 respect 110:19 respective 229:24 respond 14:4 28:8 85:4 94:7 121:25 130:25 178:6 responded 98:6 responder 132:23 133:7 134:24 244:8 responding 7:10 192:12 response 3:21 13:24 28:7 38:15 44:7 53:13 65:2 67:9 84:25 86:6 94:7 125:16 126:1 131:3 165:9 173:23 178:12 184:2 189:17 215:23 219:18 259:12 responses 96:11	responsibilities 111:1,8,14 174:8 188:19 191:6,8 responsibility 20:3 77:13 97:8 98:1,4 109:24 110:5,11 110:15 116:22,23 119:11,17 174:24 175:3,16 179:6,12 182:2,5 194:17 209:14 responsible 10:14 74:15 77:5 88:7 96:15 109:22 110:3 113:10,11 119:13,15 166:9 167:22 177:18,19 177:20 179:22 181:21 186:1,8 192:11,19 210:17 rest 17:18 21:9 58:12 66:21,23 105:10,13,21 106:10,16 108:15 224:5 225:1,24 227:9 238:11 265:10 restore 260:5 restricted 97:7 160:16 restriction 246:5 restrictions 152:12 245:3 246:13 247:4 rests 110:11 result 108:9 236:23 resulted 62:4 245:21 results 8:3 96:9 152:25 251:4 retail 124:1 173:19 223:14 retain 154:25 216:7 retaining 80:22 retains 86:12 retina 19:10 return 34:6,12 200:12 revenue 39:5	reverse 209:2 review 4:2,5 101:5 205:14,15 reviewed 18:4 101:4 105:16 224:16 reviewing 183:13 reviews 203:16 revisions 84:19 revisit 201:17 revisited 201:7 revolving 145:22 rewrite 262:24 rhythm 219:12 rid 32:2,8 229:7 rig 145:10 right 10:11 14:15 17:14 18:7 19:18 21:7 26:25 27:13 27:18 28:16 29:16 32:19,21 34:18 36:9,11 39:19 41:13 42:6,20,22 44:6 45:8,10,21 46:9 48:10,13 49:15 50:16 56:19 57:22 59:14,15,18 60:11 62:3,11 63:17,20,20 80:25 81:13 89:22 90:11 91:25 94:25 107:2 108:5,8 114:22 116:21 117:7 119:4 125:15 129:13 137:1 139:16 144:20 146:15 154:9 155:18 157:6 158:20 160:7 165:12,16,21 170:24 175:5 176:6,7 177:2,3,4 192:22 193:7,10 195:12,14,24,24 197:24,25 200:4 209:3 213:16 214:1 216:21 219:25 226:1 227:15 236:13	237:9 243:7 244:16 246:17 251:18,20 252:7 258:20 259:17 261:16,23 263:14 right-sizing 165:13 Rights 56:21 rigid 88:1 rigorous 34:13 35:4 ring 268:7 rings 202:6 ripped 237:3 rise 203:21 205:15 risk 2:15 7:4 9:12 11:17,21,24,25 15:3 21:18 23:24 23:25 24:3,9 25:2 25:22 26:2,6,11,12 26:13,15,17,19 27:4,8,15 29:5,10 29:20,20,24 31:12 32:2,4,4,14,25 33:1 34:5,7,13,21 35:2,12,24 36:20 37:6,25 39:11,12 41:22 42:1,3 45:13 47:21 48:8,21 49:21,24 50:4,11 50:18,22 51:4,5,8 51:8,14,19,20,22 51:24,25 52:7,7 53:13 55:3,15,24 56:5,10,11 57:8 59:21 62:5 63:9 64:12,15,16 65:20 65:24 66:2,3,7 68:6,10,24 69:9 82:5 86:3 90:13 91:10,17,18 92:6 92:18,23 94:18 95:11 96:7,8,19 98:17,24 100:4,18 100:20,22 114:12 115:15 116:8,10 119:3 146:16 170:6,8 172:1,5,10 173:4,13 174:1,3 176:6 177:19
---	---	---	--	---

180:20 181:5	174:15 175:20	39:21 40:3 42:12	132:13 134:23	22:2 122:12
183:13 187:2,22	215:18	42:21 46:5 48:23	142:5 149:12	222:16
190:8,21,21	Robinhood 172:14	50:25 53:8 55:21	182:25	safer 244:20 245:15
192:15 193:1	175:22,23 176:4	56:23 57:13 58:24	Rutgers 172:12	safety 93:16 241:20
195:17 196:16,18	robs 113:7	59:1,19 68:16 71:3	174:16,16,18,22	243:8,10,14 244:7
197:7,8,24,25	robust 4:1 102:21	72:12,13 74:10,11	194:8	244:12 262:20
198:16 199:13	102:22,25	75:19,22 77:3		sake 63:4 184:2
200:20 201:10	Rocio 71:10 80:18	80:14 84:20,20	S	salary 78:12
202:9 203:22,24	80:21,23 83:21	85:19 96:6 99:5	s/George 270:15	sales 39:4 243:9
204:16 205:17,18	87:16 94:11 99:3	100:13,14 101:15	SaaS 44:21 45:6,9	salespeople 41:14
205:19,22,23,24	105:18 111:24	105:6,6 109:9	45:14 166:11	Sam 23:18 28:5 29:9
211:2,9 212:10,11	115:12	112:18 117:9	183:16	31:16 33:6 36:4
215:4,9,23 220:7	Rocio's 108:22	121:4,20,24 122:1	Sachs 161:22	43:13 44:2 45:11
227:10 232:16	rock 38:19	122:5 137:18,24	sadly 61:1	69:15,17
235:24 236:20	role 53:3 78:11	138:8,9 161:3,11	safe 176:20 177:21	sample 82:18 83:2
242:5,10 248:14	80:16 87:9 97:11	163:14 167:21	245:19	84:8
250:6,12,23,25	111:4 126:10	172:4 181:16,19	safeguard 3:19,22	sanitize 242:8
263:17,18,23	174:23 175:17	193:15,16 200:15	42:17 51:18 87:6	sanity 127:15
264:1,4,7,9,9,13	176:24 179:4,16	200:19,21 209:9	103:19 111:5	SANS 223:6
264:16,18,23	179:17,25 181:1,9	209:10 222:4	117:8 160:9	satisfied 19:4
265:1,2,6 268:8	209:13,22 210:1	223:18,23 224:11	227:18,19 230:14	satisfying 85:7
risk- 200:4	211:11,13 233:6	229:12 230:15	safeguards 1:5 3:8,9	save 153:21 154:6
risk-based 41:11	roles 174:8 175:2	237:11 238:18,24	4:4 7:6,14,16,24	241:24
176:23 201:16	178:15 191:5	247:23 251:13	7:25 13:21 22:9	saw 23:22 67:13
203:14	rolling 174:1 190:4	253:9 259:19	23:4 40:3 42:12,21	85:13 97:23 148:5
risk-to-cost 232:20	252:4	263:21 265:15	48:23 55:11 56:23	262:13
235:17	room 105:25 205:3	268:14	57:13 58:24 66:5	saying 14:18 16:18
risks 6:24 7:3,6,15	216:2	rule's 209:19	68:16 71:3 72:6,12	26:16 32:4 33:15
11:18,19 24:15	rooms 189:6	Rule's 72:6	72:13,25 73:15,21	44:18 46:17 49:5
27:25 28:4,14 31:5	root 40:19	rulemaking 4:7,8	74:11 75:14,19,22	49:19 50:13,18
43:17 51:22 55:1	round 42:12 72:5	268:24	77:2 80:14 84:20	56:16 65:17,18
63:15 66:9 69:5	112:17 114:6	rules 3:18 4:2 5:1	85:19 91:25 92:14	68:17 128:1 162:5
91:9,14 93:1 94:11	218:23 265:12	49:7 51:11 80:2	96:5 100:13 101:2	205:18 234:2,15
96:7 99:23,25	rounding 174:17	87:6 88:25 103:19	101:15 105:5,6	264:6
114:14 122:24	route 158:9	110:18 111:5	112:18 114:2	says 9:21 12:25 53:5
175:8 186:13,16	Rubin 23:18 28:5	135:12 137:4,9,19	121:20 137:18,24	76:14 92:8,12
186:23 189:8	33:10 36:9 43:25	140:20 164:9	138:9 161:3	217:6 237:14
191:16 194:16	44:3 45:21 50:12	165:24 168:6	163:14 165:15	244:2 247:15
196:12,14 197:1	60:3 68:8	227:18 262:1	167:21 172:4	257:12
197:20 198:13,18	rule 1:5 3:8,8,12,25	266:17	181:16 222:4	scalability 21:1
199:12,17 231:12	4:1,4,12,15,15,25	rules/ 140:7	223:18,21,23	scale 21:3 67:15
259:16	5:1,2,16,24 6:7	run 24:11 58:8	227:12 229:12	252:18
risky 63:5 196:9	7:13,21 8:14,15,16	86:21 119:3	237:11 238:18	scales 229:13
256:15	8:18 9:8,9,17	123:17 131:3,23	247:23 251:13	scamming 62:1
road 191:10	10:11,12,17 11:3	144:13,24 147:6	253:9 254:15	scams 30:21 115:6
roadmap 217:10	12:6,13,15,16	152:17,23 155:23	259:19 265:15	scan 141:5,17
rob 108:24	13:12,16,23 20:23	182:23 216:20	267:11 268:14	142:14,16 147:6
Robin 172:6 173:1	22:9 23:23,24	running 25:24 52:16	safeguardsworks...	148:20,21 254:6,7

254:10,12	second 49:10,13	67:18 68:4,19,25	190:6,19,25 191:2	202:12 203:3
scanned 147:23	71:3 122:1 170:3	70:1 71:1,5 72:4	191:16 192:16,25	208:14 215:25
scanner 147:19	174:1 183:12	74:7 75:7 76:2,21	193:25 194:6	234:5,8,14,25
scanners 143:6	186:24 190:20	77:6,18,23,24 78:6	196:8,23 197:5,8	235:7 241:22
scanning 126:22	195:2,2 202:20	78:10,18 80:19	198:15 199:4,16	250:15,16
139:13,19,25	204:17 220:11	84:6,7 85:8 88:1,8	202:21 204:15,18	seeing 27:16 28:17
140:19 141:11,13	230:24	89:6 90:15,21	206:7,8 210:15,22	28:22 29:10 34:16
143:13 147:17	second-class 219:10	92:17,21 96:4,7,10	212:5 213:1,5,14	38:10,22 39:13
153:25 168:19	secondly 184:6	96:12,16,23 97:5,6	213:17,21,21	42:5,19 44:16,17
scans 132:4 140:21	section 85:22	97:11,22 101:17	215:22 216:5	60:4 95:12 115:5
141:1,23 142:13	sections 116:21	102:20 103:12	219:1,8,9 220:6,11	116:17 141:15
167:9	sector 173:13,14,18	104:15 105:24	222:21 223:10,11	197:21,22 199:13
scapegoat 113:12	213:22	106:24 107:25	223:13,21 228:20	243:18
249:2	sectors 234:6	108:11,25 109:7	229:5 232:14,22	seeking 4:5
scenario 33:12	secure 13:10 15:6,9	109:21,25 112:6,9	233:19 236:4	seeks 86:10
156:17,19 157:3	15:13 16:1 45:16	113:25 114:10,20	239:20 240:17	seen 27:21 44:5
196:9 242:10	45:19 102:2	114:23 115:8,18	242:23 243:15,16	60:15 61:22 62:3
scenarios 46:18	104:16 105:15	115:23 116:23	245:9,16 256:8	64:2 74:16 90:10
scene 154:9	108:21 111:17	119:13,23 120:3	257:22 259:16	97:22 132:8
schedule 21:7	115:10 127:25	121:11,13,15,25	264:18 266:2	213:22 240:20
scheduled 100:22,22	128:4 155:3 239:2	124:11 126:1,10	security-in-the-box	243:12 260:25
scholarship 31:23	239:17 240:14	128:25 129:3,15	83:7	segment 170:19
schools 151:5	242:21 247:10	129:16 130:15	Security's 41:22	segmentation
sci-fi 19:10	259:20	136:10,16 139:16	Sedona 31:7,10	133:17,21 159:20
science 121:17,18	secured 242:12	139:22 142:3	see 4:2 15:20,22	segmented 133:25
scope 6:12 32:12	securing 167:5	151:2,7 153:9	22:12 25:11,19	segregated 141:16
89:11 105:2	266:1	156:23 157:24	26:5,14 27:8 28:25	segregation 190:25
137:18 141:14	security 1:4 2:7,9,16	158:9 160:1,5	33:11,13,21 36:16	segue 209:7
scoping 135:24	3:3 6:1,2,3,6,17,25	161:5,19,20	44:5,19 48:25	selecting 7:22
score 205:17	7:5,11 8:2,10,13	162:11,12 163:2,8	55:20,25 56:9	selection 258:6
Scott 121:14 131:10	8:20 9:5,11 11:6	163:11 165:19	58:11 62:25 63:19	self- 90:10
135:15 136:2	12:3,17,20,23 13:1	166:13 168:15,18	66:2 73:3 74:6,7	self-assessment 90:9
137:5,6,7 138:11	13:4,8 14:2,12,15	169:5 170:21,22	74:22 79:12 81:8	self-explanatory
138:12,17 146:7	15:9,16,19 16:12	172:2,10,14,20	83:15 84:8,10 92:3	4:17
146:14 148:11,25	16:19 17:1 18:6	173:3,12,15 174:6	99:13 102:17	selling 176:10,11
157:4 159:1,4	20:16 21:12,13,19	174:24 175:2,7,10	103:24 106:14,21	send 21:24 22:1
170:16	23:1,13,18,21	175:22,24,25	108:12 111:13	31:23 131:25
Scott's 135:9	24:14,20 25:21	176:13,17,20	116:7 117:12	148:16 228:5
Scott's 135:10	31:8 35:11 36:14	177:1,10,13,14	118:23,23 122:19	230:1 233:3
scramble 252:16	38:5,8,16 39:11,14	178:2,3,5,17	127:4 131:5 134:4	sending 61:16
scrape 134:17	39:22 40:1 41:1,19	179:10 180:21,25	134:15 135:4	226:19,20 227:1,4
scratch 267:25	41:20 43:4 44:11	181:12,19 182:25	138:21 139:21	229:23 231:23
se 125:3 127:24	47:4,20 48:12,14	183:9,12,18	141:15,19 147:9	sends 240:24
search 76:13 228:18	49:3,4,4,19 58:1	184:15,17 185:1	157:11 158:25	senior 96:15 97:3,4
searching 133:2	59:1,22 60:5,11	186:11,13,16	159:3,5 162:1,10	97:20,21,23 98:15
seat 175:14 178:8,22	61:22 62:6,14 63:6	187:1,5,6,8,13,20	165:14 173:7	172:11 180:2
181:10 243:3,3	63:11 65:7,10,23	187:22 188:3,19	181:8 186:13	184:19 193:25
sec 83:6	66:4,13,16,25	189:2,12,14 190:3	194:16 198:18	194:7 223:6

sense 97:13 111:16 200:1 261:14 267:10	189:11 199:1,14 200:6 212:1,8 216:15 225:7 234:7 240:21 242:25 255:7	shied 242:25 shift 60:9 92:12 243:18	simple 147:2 148:19 224:20 226:7	sleeping 114:22
sensitive 6:18 55:4 56:15 65:12 69:1 160:16 161:1 166:1 195:11 199:2 209:18 224:22 226:16,17 228:10 238:21	set 11:7 20:22 48:25 60:6 64:25 78:10 89:9 101:8 118:16 145:3 149:19 156:16 158:6 161:4 177:11 192:3,18 193:3 203:25 206:3 226:15 233:15 236:8 254:20 255:16 256:21 258:17 264:2	ship 186:15 shipped 186:13 short 21:12,17 25:24 69:24 74:8 184:5 191:18	simpler 6:9 11:14 simplified 187:6 simply 103:25 233:4 234:14 261:19 262:15 266:7	slide 3:15 4:11 6:4 7:12 8:13 9:6 12:14 13:10 14:14 15:16 16:17 17:13 18:6 20:13 21:6 81:5 82:17 84:1 233:24
servicing 78:5 81:9 185:24 189:1	sessions 61:5 123:6 150:13 152:19	shortage 125:17 shortcoming 44:17 shorter 199:20 shorthand 11:5 shouldn't 44:25 263:17	simulation 126:16 single 74:19 77:16 79:12 80:7 103:2 103:14 107:4 109:22 110:3 181:20,25 182:24 183:4,5 184:3,4 186:7 187:7 188:8 189:24 190:4,6 191:23 193:16 204:4 219:6 245:7	slides 3:15 81:4 slightly 54:21 159:25 slower 159:12 slowest 241:1
serve 53:19 95:7 123:16 188:17 210:21	sets 48:18 205:5	show 65:21 84:1 141:25 159:16 178:6	sit 151:13 180:1	small 19:22,23 20:2 21:2 61:16 64:12 64:16 73:12 74:20 74:21 77:18 78:2 78:23 79:13,15 80:22 81:7,13 82:4 82:9 83:3 84:11 85:17 86:16,22 87:2,4,13,18,22 88:1,6,9,18,19,20 88:24 89:1,10 90:8 91:19 92:3,8,13 93:12,16 94:3,5,9 104:20 108:4 110:10,20,21 111:13 112:19,22 113:13 116:12 117:23 118:2,18 118:20,24 119:2 120:5 122:15 125:23,24 135:22 136:9,9 138:1 151:20,22 157:22 157:23 158:6 163:5,6,19 165:17 165:18 167:21 169:2,22 170:7,10 178:1,1 187:9 203:21 241:9,10
served 217:15 223:12	setting 46:4 99:18 175:4 176:5 177:2 225:2	showed 85:9 shown 256:13 showroom 76:23 shows 3:25 side 27:3 32:24 33:23 54:19 61:12 74:25 92:3 100:18 134:3 135:21 145:8 184:18 203:7 215:25 259:1	sites 89:13 107:22 sits 81:22 sitting 108:8 situation 82:4 180:4 229:23 252:7	situations 8:16 27:23 49:9 176:9 185:21 187:13 219:18 244:17 267:23
server 132:12,13,14 149:20 226:15	settings 217:16 setup 8:7 160:5	sides 91:12 173:7 sign 51:13 56:10 147:3 148:10,12 148:16 235:4 248:8,16 253:6	sit 151:13 180:1 sites 89:13 107:22 sits 81:22 sitting 108:8 situation 82:4 180:4 229:23 252:7	six 37:8 85:13 128:8 129:17,25 147:21 164:14,20
servers 16:5 89:15 108:8	seven 158:21 174:21 176:1 189:25	sign-on 103:2 sign-up 147:2 signature 142:7 signatures 140:8 significant 128:15 128:19 142:14	situations 8:16 27:23 49:9 176:9 185:21 187:13 219:18 244:17 267:23	six-month 237:6 Sixty-seven 93:12
serve 53:19 95:7 123:16 188:17 210:21	severe 127:5,12 severity 147:12,17 shadow 44:24 shape 125:24 170:20 207:23 228:15	signing 51:1,22 148:9 signs 51:2 SIM 44:8 85:1 232:6 similar 12:19 142:8 182:12,15 201:6 206:2 225:7 243:12	sit 151:13 180:1 sites 89:13 107:22 sits 81:22 sitting 108:8 situation 82:4 180:4 229:23 252:7	size 6:8 9:13 11:11 19:23 21:4,5 83:10 87:4 88:14,16 89:4 90:1,3,18 91:15 92:24 93:2 94:13 94:14 95:14 99:1 161:6,18 164:3,4 207:20 210:2
served 217:15 223:12	share 81:5 86:15 105:19 116:22 175:15 183:22 195:6,19 246:12 260:14,16,20 262:21	signing 51:1,22 148:9 signs 51:2 SIM 44:8 85:1 232:6 similar 12:19 142:8 182:12,15 201:6 206:2 225:7 243:12	sit 151:13 180:1 sites 89:13 107:22 sits 81:22 sitting 108:8 situation 82:4 180:4 229:23 252:7	small- 109:19 small/medium 92:24 small/medium-siz... 84:9 85:10 102:12 114:13 135:13
services 36:23,25 39:23 43:6 48:6 60:7 78:9 80:19,23 84:3,18,23 94:23 95:5 105:24 123:2 123:3 132:25 133:23 137:1 146:11,13 149:2 150:13 152:14,18 164:25 174:25 179:8 182:13,15	shared 179:14 180:5 180:11 244:1,6 sharing 120:11 179:19 219:18 she's 49:11 sheriff 133:23 sheriff's 134:2	signing 51:1,22 148:9 signs 51:2 SIM 44:8 85:1 232:6 similar 12:19 142:8 182:12,15 201:6 206:2 225:7 243:12	sit 151:13 180:1 sites 89:13 107:22 sits 81:22 sitting 108:8 situation 82:4 180:4 229:23 252:7	small- 109:19 small/medium 92:24 small/medium-siz... 84:9 85:10 102:12 114:13 135:13

small/mid-sized 73:5 123:10	232:12 257:23 268:3,4	246:6 247:11 249:9,10 263:8	165:4	47:13 49:23 50:9 52:12 66:14 80:2 89:9 161:12 229:21 237:19
smaller 2:9 6:9 21:1 21:5,14 32:13,14 32:14 70:1 71:1,6 75:3 78:22 79:6 80:10,20 83:24 85:20,22 93:6,15 95:22 110:16 119:24 125:20,20 159:7 164:22 184:13 185:9 209:18 240:16 241:3 258:11	solutions 21:3,4 33:2 54:18 64:3,5 64:7 152:7 258:10 258:13 263:2 267:18	sorts 130:6 132:25 265:5,7	spectrum 7:11 speed 13:9 112:17 114:6 164:23 265:12	standpoint 161:20 161:20 183:12 205:7 264:7 267:1
smallest 188:25	solve 167:18 262:17 262:18 268:7	sought 8:17 85:16	spend 149:7,21 208:21	start 3:11,15 4:12 21:10 24:2,5 28:3 58:11,17 73:6 112:20 114:12 117:12 118:22,23 120:1,2 129:24 130:21 148:18 151:21 161:24 167:2 172:17,23 177:7,15,16 182:10 188:10 209:24 214:13 219:4 224:1,18 227:7 239:4 245:1 265:17 266:18
smart 134:12 146:24 187:22	solved 53:25	sounds 49:6 68:22 146:13 250:13	spending 43:2,19 57:24 62:20 125:9 125:11 208:1	started 47:2 61:14 75:23 122:13 175:23 243:7
smartphones 231:25 238:4	SomaLogic 157:20	source 30:13 39:5 140:13 157:25	spent 92:21 173:11 257:5	starting 4:13 39:13 39:14 46:3 84:11 114:11 115:8 198:11 245:2
SMB 102:16	somebody 38:24 64:10 79:5 119:15 130:3,7 133:1 135:21 140:12 143:8 144:15 147:25 151:12 155:5 157:10 158:8,10 165:25 166:2 178:2 186:19 187:9,11 187:15,16,20,21 195:18 208:17 212:2,5,12,20,22 212:25 213:1,20 247:18 255:9 258:15	SOX 158:3	spike 148:5	starts 117:9 118:16 120:4,5 177:1
SMBs 115:5,10	someone's 113:14	space 53:7 81:10,11 81:22 94:21 107:1 125:17 147:4 150:12 178:17	Spirion 228:16	startups 176:2,4
SMBv1 262:24	somewhat 127:3	speak 28:5 160:14 183:15 228:7 237:4	split 211:13 214:19	state 54:13 96:21 153:22 172:12 182:18 209:11 223:11 241:8
SMS 231:7,10,13,14 231:19,25 232:5 232:12,17 234:25 235:3 238:7	son 145:10	speaking 5:6 20:15 72:14 99:3 180:16 205:16 251:12 264:22	splitting 149:25	state-mandated 233:9
smartphones 231:25 238:4	soon 148:17 235:8	specialist 121:5	Splunk 124:2 149:22 157:15,16 157:18	state-specific 112:4
SMB 102:16	sooner 244:21	specialists 81:11	spoke 136:2 220:8	statement 114:2
SMBs 115:5,10	sophisticated 246:21 256:12	specialization 48:6	spoofed 245:8	states 112:4 113:17 133:19
SMBv1 262:24	Sorry 142:20 170:16 251:16	specialize 126:3	spot 137:16 237:12	statewide 174:5
SMS 231:7,10,13,14 231:19,25 232:5 232:12,17 234:25 235:3 238:7	sort 6:14 8:11 14:13 15:12 16:7,11 18:22 19:10 27:22 38:2 40:12 52:20 97:3 134:20 146:17 170:9 175:8 177:2,22 199:7 207:20 217:19 220:16 225:22 226:1 231:13 239:16 242:25 243:12,21	specific 11:7 16:22 48:17,24 66:24 68:6 72:23 74:18 82:15,15 100:15 101:10,16 105:5 110:25 116:1,5,16 128:6 130:1 147:14 185:11 203:6 208:16 215:22 223:21 246:22 257:14 260:10	spread 261:15	static 98:10
SOC 45:17	sort 6:14 8:11 14:13 15:12 16:7,11 18:22 19:10 27:22 38:2 40:12 52:20 97:3 134:20 146:17 170:9 175:8 177:2,22 199:7 207:20 217:19 220:16 225:22 226:1 231:13 239:16 242:25 243:12,21	specifically 114:25 131:11 142:23 151:3 163:14 183:19 193:5 209:10	spreading 134:5	status 14:11 96:4 99:23 163:25
SOC 45:17	sort 6:14 8:11 14:13 15:12 16:7,11 18:22 19:10 27:22 38:2 40:12 52:20 97:3 134:20 146:17 170:9 175:8 177:2,22 199:7 207:20 217:19 220:16 225:22 226:1 231:13 239:16 242:25 243:12,21	specialization 48:6	Springs 71:22 75:18	stay 206:15 247:19 248:21 255:3
SOC 45:17	sort 6:14 8:11 14:13 15:12 16:7,11 18:22 19:10 27:22 38:2 40:12 52:20 97:3 134:20 146:17 170:9 175:8 177:2,22 199:7 207:20 217:19 220:16 225:22 226:1 231:13 239:16 242:25 243:12,21	specific 11:7 16:22 48:17,24 66:24 68:6 72:23 74:18 82:15,15 100:15 101:10,16 105:5 110:25 116:1,5,16 128:6 130:1 147:14 185:11 203:6 208:16 215:22 223:21 246:22 257:14 260:10	SSL 107:22 162:21 225:3	
SOC 45:17	sort 6:14 8:11 14:13 15:12 16:7,11 18:22 19:10 27:22 38:2 40:12 52:20 97:3 134:20 146:17 170:9 175:8 177:2,22 199:7 207:20 217:19 220:16 225:22 226:1 231:13 239:16 242:25 243:12,21	specific 11:7 16:22 48:17,24 66:24 68:6 72:23 74:18 82:15,15 100:15 101:10,16 105:5 110:25 116:1,5,16 128:6 130:1 147:14 185:11 203:6 208:16 215:22 223:21 246:22 257:14 260:10	staff 30:8 73:11 74:21,22 78:3 79:2 79:17 124:11 126:7 127:1 138:5 141:9 144:10 149:13,15,19 156:19 233:3 237:2,4	
SOC 45:17	sort 6:14 8:11 14:13 15:12 16:7,11 18:22 19:10 27:22 38:2 40:12 52:20 97:3 134:20 146:17 170:9 175:8 177:2,22 199:7 207:20 217:19 220:16 225:22 226:1 231:13 239:16 242:25 243:12,21	specific 11:7 16:22 48:17,24 66:24 68:6 72:23 74:18 82:15,15 100:15 101:10,16 105:5 110:25 116:1,5,16 128:6 130:1 147:14 185:11 203:6 208:16 215:22 223:21 246:22 257:14 260:10	staffing 85:12 145:2 183:2 257:16	
SOC 45:17	sort 6:14 8:11 14:13 15:12 16:7,11 18:22 19:10 27:22 38:2 40:12 52:20 97:3 134:20 146:17 170:9 175:8 177:2,22 199:7 207:20 217:19 220:16 225:22 226:1 231:13 239:16 242:25 243:12,21	specific 11:7 16:22 48:17,24 66:24 68:6 72:23 74:18 82:15,15 100:15 101:10,16 105:5 110:25 116:1,5,16 128:6 130:1 147:14 185:11 203:6 208:16 215:22 223:21 246:22 257:14 260:10	stakeholders 161:10 204:22	
SOC 45:17	sort 6:14 8:11 14:13 15:12 16:7,11 18:22 19:10 27:22 38:2 40:12 52:20 97:3 134:20 146:17 170:9 175:8 177:2,22 199:7 207:20 217:19 220:16 225:22 226:1 231:13 239:16 242:25 243:12,21	specific 11:7 16:22 48:17,24 66:24 68:6 72:23 74:18 82:15,15 100:15 101:10,16 105:5 110:25 116:1,5,16 128:6 130:1 147:14 185:11 203:6 208:16 215:22 223:21 246:22 257:14 260:10	stand 211:12	
SOC 45:17	sort 6:14 8:11 14:13 15:12 16:7,11 18:22 19:10 27:22 38:2 40:12 52:20 97:3 134:20 146:17 170:9 175:8 177:2,22 199:7 207:20 217:19 220:16 225:22 226:1 231:13 239:16 242:25 243:12,21	specific 11:7 16:22 48:17,24 66:24 68:6 72:23 74:18 82:15,15 100:15 101:10,16 105:5 110:25 116:1,5,16 128:6 130:1 147:14 185:11 203:6 208:16 215:22 223:21 246:22 257:14 260:10	standard 46:5 48:13 50:1,5,8 53:12 65:24 66:7 106:12 226:18 227:19,20 228:8 264:3	
SOC 45:17	sort 6:14 8:11 14:13 15:12 16:7,11 18:22 19:10 27:22 38:2 40:12 52:20 97:3 134:20 146:17 170:9 175:8 177:2,22 199:7 207:20 217:19 220:16 225:22 226:1 231:13 239:16 242:25 243:12,21	specific 11:7 16:22 48:17,24 66:24 68:6 72:23 74:18 82:15,15 100:15 101:10,16 105:5 110:25 116:1,5,16 128:6 130:1 147:14 185:11 203:6 208:16 215:22 223:21 246:22 257:14 260:10	standards 46:7,11	

stays 247:10	student 56:1,8,20	226:7	151:14,19 154:24	243:23 247:16
stealing 231:17	150:23 160:10,23	suggest 48:3	155:3,4 160:22	260:3
stem 150:20	165:18 237:23	suggested 85:19	163:15 165:6	system/infrastruc...
step 65:18 89:24	students 30:8 31:22	suggesting 25:5	167:3,6,23 168:11	126:19
116:9 201:12	31:22 37:16	250:3	169:15 172:25	systematically 42:4
204:7	123:14,15 165:20	suited 9:12 35:5	174:14 175:4,20	systems 7:9 73:13
steps 13:6 40:3	165:21 167:25	sum 50:13 203:20	176:12,16,19	95:5,9 102:10
207:8	237:4,24 238:2	summarize 142:10	177:20 178:13	104:2,3 106:9
sterile 242:7,11	studies 189:19	265:16	179:19,23 181:13	107:2 108:25
stick 202:11 219:17	study 72:8,16,17,20	summarizes 99:21	182:10 184:24	121:24 123:2
sticks 219:16 220:19	73:9,11,18,19 74:6	summary 134:20	193:9,12 194:4	124:21 126:20
stolen 261:20	107:21 157:9	super 25:6 139:11	198:8 201:5	141:6 146:4
stop 262:24	160:24	139:11 199:25	218:19 219:7	152:18 160:11
stopped 25:25	stuff 25:17 62:19,21	supplement 81:24	226:24 227:3	202:16 212:24
103:15	107:25 153:20,20	supplemented 82:1	233:8 249:14	213:7,11 222:25
stopping 109:3	153:25 155:19	211:16	252:9 255:25	228:12 230:3
storage 68:3 89:24	158:2 238:9	suppliers 50:1	268:5	233:6 240:3,5,7
154:22,23 166:12	254:19,23 258:24	support 27:2 36:1	surface 93:11	252:5,6 256:15
222:25	259:10 261:6	44:9,11 79:17,17	Suricata 149:10	266:2,13,15
store 7:20 230:2	264:10 267:7	79:24 82:24 83:9	surprisingly 132:2	
stored 6:14	subject 112:4	83:15 102:11	survive 93:13	T
stories 47:9	187:17 195:22	103:11 104:12,14	susceptible 167:10	T 169:19 248:7
storing 239:21	217:8,16,25	118:15 123:19	suspect 252:19	table 64:4 83:2
story 38:20	subjected 166:5	125:5 174:25	suspending 61:20	tables 194:20
straightforward	subjects 194:18	211:5 230:9 244:3	suspicion 43:20	tackle 54:17 148:8
148:19	submit 100:13 179:3	257:17 258:20	sustain 144:25	tackling 151:19
strain 60:5	submitted 268:19	259:1	sweep 139:14	tag 163:12
strange 15:20	subscription 102:24	supporting 214:21	Swiss 223:11	tailored 47:25
strategic 78:15	subsequent 55:2	supports 102:7	switch 181:15	take 21:4 30:15 34:7
82:23 85:8 175:9	subset 138:2	258:24	Sylint 23:16	54:22 55:1 56:7,18
strategy 78:18 115:9	substance 222:12	supposed 14:22	synchronize 57:6	57:8 61:23 65:5,18
182:7 218:25	substantial 53:4,10	26:21 59:5,7	Syslog 125:4	79:2 93:23 94:25
streams 259:3	substantively 10:17	181:11	Sysmon 125:4	104:4 106:3 109:1
stressed 252:6	subsystem 138:18	sure 6:22 7:16 9:24	149:17,18	109:20 112:1,2
strong 44:5 66:16	succeed 131:4	10:4 13:19 14:22	system 16:5,9 49:13	116:19 120:12
stronger 26:5 193:8	success 36:11 174:9	15:13 16:11 27:14	73:23 74:2 78:4	122:22 128:5
strongly 113:3	191:22	33:10,16 44:3	104:12,13,13,21	130:9 144:9 150:8
198:3	successes 180:13	46:19 52:22 57:7	106:6 107:5,5	164:9,19 166:17
structure 9:9 16:6	successful 29:14	58:6 64:23,24 67:1	108:22 125:12,25	169:24 179:14
73:7 101:6 176:17	199:23	72:19 74:3 77:19	126:6 127:15,21	186:15 190:12
176:18 194:21	sudden 62:7 243:9	79:15 80:1 83:25	127:25 128:9,16	191:1,11,19 200:2
229:18 258:21	suddenly 64:18	85:3 86:17 87:24	128:20 130:1,5,15	206:6,25 208:25
260:14	252:15	90:14 92:16 94:14	133:10 135:1	214:17 216:18
structures 109:20	suffer 55:6,10 93:10	101:1 102:6 104:3	138:19,19 139:7	218:4 220:25
struggle 60:16,22	118:8	107:11 111:11	143:24 144:3	222:10 236:18
struggling 145:23	sufficiency 250:18	114:7 123:23	145:7,16 150:25	238:15 251:7
stuck 219:22 232:4	sufficient 129:1	124:10 131:13	156:8 160:24	253:17 254:16
241:4	sufficiently 224:20	137:9,17 138:6,24	189:23 228:4	258:9

taken 59:18 70:5 120:14 171:3 191:5 207:9 221:3	tasked 106:2 193:24	212:11 225:10	248:11 250:9	85:15 89:2 92:25
takes 28:25 31:2 112:11 158:19,25 167:18 185:23 193:7 195:5 208:11	tax 240:20	247:12 267:17	terrible 246:19	94:10 95:18
talent 80:15 82:14 129:14 151:9	teach 32:18	technologists 104:15	test 7:16 8:3 76:16	101:13 103:4
talk 25:19 36:5 40:21 55:14 65:19 77:1 83:23 93:18 95:22 99:17 113:9 113:22 114:8 126:21 131:14 133:3 145:20 158:13 159:2 175:13 190:2 195:21 196:25 201:14 230:13 238:25 258:16	teaches 222:22	technology 43:3 47:13 81:24 85:11 87:11 94:22 95:7 114:15 162:15 167:13 176:3 188:15 216:15 224:12 246:7 250:2 258:2,17	76:17,19 99:14 127:9,17,19,21,23 128:5,7,17,19,23 129:10,14,24 130:8,12,23 131:2 131:14 134:21 135:4,23,25,25 136:5,5,13,14,20 136:22,23,25 138:11,12,13 141:4 146:18,20 152:24 159:3	105:3 107:15 109:11 111:18 112:15,24 114:4 115:11 117:1,4 119:18 120:8,9,10 171:1 187:25 191:25 196:1 200:13 209:5 216:23 220:21 222:17 223:15 226:4 230:11 233:25 235:13 238:16 240:9 246:10 251:6 255:17 258:18 265:9 266:19 267:12,15 268:10 268:11,12,15,25
talked 27:19 64:21 65:7 72:3 74:1 92:5 118:1 123:6 151:11 167:3 220:5 232:7	team 36:18 44:11 49:3,4,5 74:18 75:2,9 79:21,22,25 80:10 81:20 109:20,25 110:15 110:24 126:1,2 137:5 146:23,23 178:2 186:8 187:6 190:24 191:2,8 197:15 202:23 204:15,18 210:18 210:19 211:14 223:9 237:2	technology- 257:13	tested 12:7 128:2,9 130:2	thanks 70:1 86:17 86:18 122:17,17 124:15 126:8 129:6 130:24 137:12 139:1 142:20 146:6 148:25 150:9 153:7 168:2 170:1 170:24 172:3,14 172:25 174:12 175:18,20 178:10 184:22 198:6 204:10 211:21 214:7 219:13 220:24 221:2 225:17
talking 20:19 23:11 25:20 27:11 28:14 32:23 34:4,24 46:1 52:12 62:19 68:7 68:22 71:4 74:19 87:6 93:19 106:9 106:10,15 107:5 107:19 108:20 116:1,6 138:16,17 153:14 154:8 177:7 183:16 196:7 217:23 227:23 249:7 250:21,23 258:20	teams 33:13 60:5 81:23,24 95:6 142:12 175:25 177:2 187:1,3 190:3,8 191:13,13 191:20 199:17 202:22 204:17	telco 232:7,10	testers 121:14	that's 4:18 5:7 10:19 16:7,24 24:18 26:14 27:9,10 28:19 32:19 33:23 34:13 35:6 36:11 39:5,12 40:3,6,23 41:2,15 42:19 44:16 45:8,13,21 46:2 50:1 52:11 55:4,23 56:1,13 58:8 59:4,4 60:9
tampering 122:4	Tech 71:15 77:19,25 78:7 84:2,9,18 85:6 89:10 90:10 102:7,11 223:3,3 226:25 227:1,2,7 229:14 235:19 237:10,23 248:3	telemetry 44:13 156:23,24	testifies 177:22	
tap 83:4	technical 68:25 72:8 106:19 183:17 196:20 201:18 233:17 263:19 264:3,5,7,10	tell 35:10 40:24 41:4 41:5,14 42:12 45:15 46:8,13 48:20 63:5,7,12 72:16 80:21 82:20 90:23 112:21 144:21 172:18 232:13 248:12 258:5 267:2	testing 2:13 8:3 12:10 21:17 40:17 64:22 76:13 86:5 96:9 115:2 121:2,7 121:8,21,22 122:6 122:7,8 126:9,15 126:23 128:14 130:4 131:12 135:12 139:2,4,6 139:12 146:23 149:3 153:25 162:6,8,10 167:5 168:19 212:9	
target 12:4 184:1 259:5	technically 135:20	tells 54:5 66:25 145:9 150:8	tests 126:12,13 127:22 128:25 131:18 136:3,7 152:17,17 159:6 167:9	
targeted 143:5	technique 132:24 133:8 224:12	template 131:23	Texas 150:24 223:9 223:11 233:2	
task 75:4 100:11 236:23	techniques 222:24 240:2	ten 136:21 151:5	text 149:24 231:5 238:5,6	
	technological 31:10 88:11 180:21	tend 27:22 106:14 235:3	text-only 238:3	
	technologically 250:21 264:22	tended 234:4	thank 3:16 22:12 56:12 59:14 69:19 69:22 70:3,4 71:25 75:15 76:24 79:10 80:12 81:1,3 83:21	
	technologies 50:7 71:14 72:19 73:15 101:16 187:11	tends 39:9		
		tens 150:15		
		tens/hundreds 19:24		
		term 11:5,5 220:16 239:9 252:24		
		terms 26:11 28:3 29:9 47:7 78:11 79:12 90:1 108:20 116:17 138:4,7 146:2 149:16 195:13 207:17 208:11 210:23 213:10 218:6 226:22 235:16		

60:15 90:12,25	165:10 168:7	207:7 216:9 220:4	207:9 210:22	119:5 124:12
93:18 95:12 99:20	173:8 189:25	220:11 227:11	211:7 213:14,16	125:19 126:22
102:24 107:22	192:5 197:12	229:19 241:17,25	214:25 216:6,8	128:14 130:12,13
108:21 109:5,7	210:22 214:3,5	246:7 248:18	219:17 220:4	137:15,16 138:17
110:13 112:13	215:2 225:1	252:20 253:13	225:17 229:25	139:12,18 141:20
114:12 115:5	238:14 247:14	255:6 259:8	230:22,25 231:3	143:12 151:24
120:4 127:18	258:23	260:11 261:7,17	233:1 236:9	156:9 157:4,16
129:17 137:15,19	thereto 96:11	263:25 265:24	238:15 239:11	158:12 161:17
139:20 140:16	they'd 249:3	266:5	242:8 245:17	164:13,15,20
144:12,17 146:1	they'll 23:9 24:11	things 3:17 12:2	247:21 251:25	165:9 166:21,23
149:14 152:3,19	31:21 41:5 106:5	13:19 14:13 18:19	252:8 253:20,23	167:3,4 169:10
159:13,21 160:25	they're 4:25 5:6,11	18:23 19:6,12 20:8	253:25 254:13	175:12 177:23,23
161:3 163:21	13:6,20 15:2,10,13	20:9 24:23,25 25:3	258:13 261:10	179:5 180:11
165:15,25 166:2	20:2 24:10,13	25:19 26:10 27:20	262:3 265:7 267:9	182:11,19,22
169:20 176:24	33:15 34:20 36:13	28:15 31:6,9,10	think 3:25 4:22,24	184:6,11,16,25
190:12,21,22,24	39:21 45:5 51:5	35:20 36:16 39:12	11:2,8,10 12:1,18	185:2,3,15 187:4
192:20 195:6,15	60:7 62:20 63:8,15	39:23 42:8 46:19	13:3 18:12 19:7	187:13 188:12,13
203:23 208:6,15	63:16 64:14 78:2	48:22,25 52:15	23:9 26:14 29:3,11	188:18 189:18,19
212:6,22 213:2,3	81:15,23 92:10	54:15 56:9 59:24	32:3,8 34:3,17	190:2,11,13
213:18 216:19	94:22 106:7 108:6	60:23 61:4,15,16	35:8,21 37:18	191:18 192:3,5
218:14 225:22	108:9 110:1	62:8 63:4 64:1,23	38:13 42:4,8,11,14	194:5,9,16,19,22
227:10 228:6	114:22 116:14,21	65:18,21 66:6,20	42:21 45:8,11,25	194:25,25 195:3,5
229:1 230:11	116:24 137:4	66:22,23 68:14,17	46:21 47:9 51:25	195:8,8,9,13,20
234:21 239:25	153:2,5 166:14	69:10 73:8 93:8	52:7,19 53:14,16	198:14,25 199:6
242:23 244:21	179:19 180:2	94:18 98:6 99:22	53:18 55:13,14	199:22 200:1,2,23
245:18 246:25	185:25 190:7,14	104:18 113:4,16	56:6,7 58:5,19	201:5,8,12,15,21
250:19 254:2	191:9 198:2	115:19 117:6	59:19 63:13 64:4,6	202:3,11,21 203:7
258:4 264:8 266:3	210:11 214:21,22	119:3,3 124:19	65:1 66:8 67:7,21	203:10,17,20
266:16	214:23 224:15	127:12 129:4	68:10,13 69:10	204:1 207:5,10,15
theater 242:7,11,14	225:5 250:9,10	130:9,17,20 132:2	74:16 77:20 78:15	207:17,18 208:25
theirs 176:13	265:4	132:8,23 135:2,23	81:6 82:3,8,9	209:25 210:3,5,14
themes 177:6	they've 110:13	136:7 137:2	83:25 84:5 85:13	210:19,20,22
theorem 247:14	152:13 202:1,25	139:14 140:8,24	86:25 87:7,15,17	211:11,17,24
theoretically 153:15	211:5 215:11	140:25 141:2,25	88:6,16,17,19 89:9	212:22 213:5,25
there's 6:21 14:2	thing 6:14 14:14	142:1,23 144:3,6,9	89:15 91:2 93:6	214:11,18 215:2
16:21 19:5 24:6,7	16:7,11 18:22	148:1 151:1	94:14,15,17 95:14	215:12,18 216:4
25:5 36:8 39:24	19:11 27:10 35:10	152:13 153:2	95:15 96:25 97:2	216:10,14,19
40:5 50:14 51:18	39:3 42:21 48:11	155:9 156:5,12	98:8 99:6,10,16	217:2,2,4 218:14
51:20 60:4 62:12	51:10 52:2 57:16	158:12 162:18,20	100:5,8,9 101:10	219:5,9 220:4
62:12 75:7 92:7,12	62:21,23 63:5,17	164:8,10,23 165:1	103:24 104:7,25	225:6,20 232:9
92:20 94:24 95:5	63:18 73:22,24	166:12,16,24	105:25 106:16,21	233:24 236:13
100:25 101:2	100:24 103:24	168:1,8,25 169:11	107:4,18 109:5	239:11,12,24
102:17 106:12,12	128:4 129:16	169:12 175:15	110:7,15 111:2	240:11 242:19,24
106:22 107:10	131:2,21 141:20	177:21,21 186:6	112:23 113:4,24	243:18 244:1,4,18
113:18 115:14	149:17 151:10,24	187:24 188:17	114:9,12 115:2,20	247:1 249:25
118:15 143:15	152:23 160:4	196:19 197:22	115:24 117:4,14	251:18,19 253:3
144:3 151:19,22	170:4 185:12	198:9 201:22	117:17,21 118:13	253:10 255:2,13
157:17,19,20	186:7 188:25	204:6 205:8,9,11	118:17,18,19	257:8 262:4 263:7

265:20 266:16 267:8 thinking 37:16 41:7 41:10,18 45:12 61:20,21 81:13 138:7 145:17 162:6 185:19 201:25 207:14 254:22 256:6 thinks 108:1 206:24 251:3 third 15:11 82:7 93:10 105:1 157:8 166:14 170:3 173:7 190:22 202:12 204:17 209:6,8,12,21,25 212:3,7,8 213:10 215:4,6,17 216:9 216:11,21 231:2 241:6,12 third- 118:5 third-party 69:9 80:17 100:24 101:3 116:4,15,16 118:3,6,8 120:2 166:11 173:3 183:11,13 206:4 209:15 210:4,8,21 211:3,16 212:15 214:9,13 216:18 240:18 Thomas 121:9 thought 25:12 64:16 177:6 180:22 195:2 238:4 243:1 252:14 thoughts 86:16 94:11 103:7 105:19 109:16 110:1,2 112:17 114:6 115:13 117:3 119:20 194:4 252:13 255:23 265:13,17 266:20 thousand 170:13 thousands 19:25	123:23 150:16,16 154:6 threat 28:12,19 29:7 29:12 30:1 31:18 38:18 52:8,16 58:15 68:12 89:18 89:19 98:20,24 114:16 183:22 191:10 198:15 232:11 threatening 255:9 262:11 threats 12:5 13:8 28:17,22 29:22 30:20 43:14 69:5 69:13 84:22 85:4 115:3 167:7 179:10 three 18:18 24:12,15 24:16 32:6 40:11 40:15,15,15,16,22 40:24 41:6 46:24 81:7,18 93:5 108:10 147:21 175:23 181:23 182:6 190:9,18 202:16,24 204:15 222:8 230:21 233:16 261:3 three-layer 186:25 three-letter 25:18 three-quarters 107:21 threshold 86:9 throw 39:18 193:11 thrust 62:16 ticket 133:10 134:25 tickets 203:16 tide 150:20 tier 215:20 ties 150:22 tightly 32:22 time 13:8 27:17 30:20,20 44:21 46:10 50:21 64:4 65:4 67:23 69:12 69:18,20,22 78:19 95:10 97:25 98:22	104:8 115:9 120:9 120:10 128:7 143:16,25 154:18 158:4,25 159:5 164:21 167:19 170:25 171:1 174:4 180:24 184:5 191:1,9 193:9 198:24 201:8,20 202:12 202:24 203:6,8 206:2,12 207:12 207:18,24 208:5 208:10,23,25 212:17 214:11 216:22 244:10,12 244:13 251:12 252:4 253:11 255:4 257:5 258:10 265:2,20 267:7 268:2,12,25 timed 69:17 timelines 82:15 times 45:15 53:21 228:2 232:5 241:15 249:9 257:24 tip 165:12 tips 179:20 tired 61:17 title 163:8 TLDR 139:10 TLS 225:3,18,20 today 20:20 22:11 54:3 83:3,18 143:3 162:18 171:1 172:9,15 220:24 222:18 223:16 235:10 257:7 261:10 263:16 266:22 267:17 268:9,17,22 269:1 today's 172:4 179:9 today's 3:7 19:25 20:14 Todt 71:18 86:17 88:16 93:5 97:2 110:7 117:4	token 18:24 56:25 tokens 230:25 233:4 235:6 told 46:23 80:3 tolerance 100:5 211:2,8 toll 144:7,7,7,13 Tom 122:13 124:15 137:13 139:1 142:21 146:6 150:10 153:7 160:8 165:9 167:2 168:2 170:4 Tom's 168:5 tomorrow 29:17 186:13 tongues 165:13 tons 161:15 tool 124:2 129:2 134:6,11 140:10 144:13,14 145:3 228:23 tools 44:6,9 62:1 124:25 125:7 127:2 140:4,5,13 141:18 150:12 151:11 153:14 157:14,18,20,25 164:24 174:25 228:9,18 top 34:15 76:6 136:21 147:8 259:16 topic 32:22 95:19 126:9 137:14 142:21 146:8,10 153:8 159:25 194:6,19,23,24 195:1,25 209:7 211:23 219:10 topical 59:15 topics 194:18 196:6 268:21 topology 128:22 tossing 150:1 total 89:19 257:15 totally 29:9 148:8 touch 60:22 172:21	234:10 touched 26:12 38:2 45:12 64:5 157:5 170:4 178:13 touching 173:10 track 16:16 42:22 203:5 traction 196:23 Trade 1:1 2:1 3:21 24:19 36:23 39:25 56:24 63:13 71:25 222:6 tradeoff 124:25 125:8 150:7 208:6 208:23 tradeoffs 202:18 trading 158:4 traditional 114:18 133:9 136:21 traditionally 134:9 135:4 traffic 226:13,16 trails 15:18 121:25 153:9,12 trained 13:5 156:25 training 7:9 12:16 12:17,20,24 62:6 77:23 159:17 160:1 216:12 257:17 transaction 55:23 transactions 15:19 37:4 56:22 90:4,6 transcribed 270:7 transcription 270:4 transfer 26:17,23 103:13 215:3,16 transferring 78:16 transit 17:17 105:10 105:13,20 106:10 106:11,11 224:4 227:9 transition 237:6 translate 212:13 transmission 225:13 transmissions 17:25 transmitted 17:17 17:23 105:9 224:4
---	---	--	---	---

<p>224:9,10 226:17 226:18 transparent 66:19 traps 183:7 treat 160:15 treated 6:16 tremendous 28:6,11 trend 200:15 tried 57:19 257:24 triggers 263:9 triple 73:20 trouble 54:11 233:18 261:13,14 Troy 71:16 true 57:18 126:25 135:15 136:14 142:17 154:2,3 190:13 210:14 211:18 truly 126:20 142:2 162:4 trump 242:23 trust 89:21 102:22 102:25 176:5 210:10 245:9,10 245:21 trusted 58:7,7,11,13 59:3 245:25 truth 36:24 180:16 try 22:4 39:23 53:2 55:18 59:10 60:22 67:8 126:17,20 140:18 143:14 150:20 160:15,17 160:20,21 183:25 216:25 217:17 228:10 240:5 246:19 254:17 258:7,13 trying 28:20 31:11 32:7 36:5 38:18 42:7 53:23 58:2,17 68:17 90:12 99:15 108:6,10 126:24 130:14 136:20 139:13 143:11 145:15,25 146:3 151:15 155:15</p>	<p>159:22 168:9 184:1 186:22 198:4 218:3 219:21 232:8,21 tuition 150:23 tuning 220:25 268:15 tunnel 108:13 turn 9:12 35:19 101:14 105:4 114:5 115:12 209:23 230:12 231:9 235:15 252:10 turned 47:1,5 turning 99:13 turnover 215:4 turns 231:15 Twenty 234:21 twice 140:22 two 16:21 18:18 24:12 26:3 28:17 28:22 40:11 54:3 66:6 67:13 76:4 81:4,16 86:25 88:23 94:18 96:23 99:11 101:14 115:19 117:17 125:23 126:1 164:16 173:2,22 182:3 187:24 198:8 202:11 207:11 214:25 215:20 220:4 223:19 226:24 230:21 247:20 249:24 259:16 262:3 two-factor 236:22 236:25 237:5 243:23 267:4 two-week 159:9 tying 205:16,17,17 type 29:9 38:20 55:9 82:2 84:18 91:2 99:8 111:2 130:11 142:23 161:6 170:5 181:9 184:7</p>	<p>199:23 200:5,11 217:16,21 226:12 226:22 238:9 240:25 247:12 249:12 259:9 267:7 types 28:9 39:20 92:22 101:16 128:1 191:16 199:12,21 225:2,7 249:7 259:16 typewriting 270:4 typical 131:14 181:25 typically 79:20 129:7 142:24 260:15</p> <hr/> <p style="text-align: center;">U</p> <p>U 174:20 175:3 U.S 43:2 72:10 170:8 uber-cheap 230:5 UC 121:18 ultimate 209:14 ultimately 32:14 35:13 106:23 176:25 180:12 181:10 190:3 199:22 210:16 216:14 265:1 umbrella 57:8 226:25 unaffordable 73:6 unauthorized 122:3 unavoidable 189:3 uncommon 129:23 understand 8:24 24:19 29:5 31:4 33:14 35:14,25 36:1,5 39:14,14 43:17,18 46:22 53:19 58:18 59:12 64:17 86:20 92:16 93:15 114:13 135:17 144:11,15 154:24 167:11 168:11 180:18,19</p>	<p>181:2,11 183:1,18 185:3 189:5 194:10 199:13 201:21 213:11 understandable 168:15 understanding 50:11 63:19 83:23 97:10 106:22 114:16 127:6 135:24 175:5,8 185:8 undue 205:11 unfortunate 33:11 69:17 124:25 158:25 unit 39:9 192:6 219:18 units 35:11 37:23,23 38:24 39:16 56:16 192:5 universal 38:10 65:10 66:7 113:3 universally 225:5 universities 5:14 30:6 31:20 32:17 37:15,22 123:12 144:22 151:8 160:15 237:12 university 23:13 30:5 31:14 37:2,20 38:25 39:2 56:3 57:22 121:12 123:9,10 124:8 143:18 150:24 160:9 165:20 172:13 174:16,18 228:12 236:8 unleashed 30:24 unlimited 145:17,19 unpack 190:17 unsafe 88:4 untrained 106:1 unusual 225:22 upcoming 115:7 update 76:20 98:4 140:7 updated 128:11</p>	<p>263:21 updates 4:3 25:5 updating 46:4 upgrade 60:18 upper 79:18 uptick 243:9 uptime 141:6 upwards 78:14 urge 63:22 usability 235:11 usable 232:15 usage 225:6 use 7:19 9:16,25,25 11:5 18:14 46:14 47:3,12 48:18 49:5 50:5 52:1,20 54:24 73:14 74:3,14 86:10 87:17 102:1 102:13,23 103:8 116:17 122:4 125:7 132:24 134:22 197:14 198:2 224:14 226:23 228:10 229:16,20,25 231:7,19,25 232:14 233:22,22 234:4,10,17 235:3 238:4,24 239:16 240:1,2,12,21 241:6,16 242:6 243:2 246:4,18 247:24 251:4 258:14,23 260:23 265:25 267:19 useful 47:10 74:4 109:8 125:15 156:4,24 157:1,9 157:11 161:17 177:7 user 76:10 102:20 117:12 227:20 229:19 234:9,10 234:12 249:9 262:2,4 users 16:14 60:12 64:11,13 76:11 89:12 102:19</p>
---	---	--	--	--

122:3 226:15 234:13 235:2,12 237:9 238:20 245:25 261:13 uses 234:22 usually 27:9 178:23 utilize 140:13 utilized 101:23 utilizing 140:16 uttered 50:3	118:3,6,9 120:3 183:16 206:5 243:20,20 244:2,5 258:12 verifies 19:3 verify 13:6 versa 197:20 227:5 version 142:5 202:1 239:14,25 244:20 versions 87:17 258:14 versus 52:16 77:16 79:13 92:22 114:8 117:17 150:6 163:9,20 235:23 266:12 viable 17:7 110:17 vice 23:18 121:10 172:11 197:20 227:5 victim 244:9 videos 159:17 view 73:5 85:7 91:13 91:16,17,23 92:8 93:1 103:10,17 107:16 113:4 114:1 182:24 183:3,15 192:5 231:10 245:2 246:12 250:3 251:24 viewing 22:3 views 89:11 village 31:2 violations 96:10 Virginia 223:3,3 226:25 227:1,2,7 229:14 235:19 236:1 237:9,23 248:3 virtual 1:16 21:24 21:25 78:11,17 79:24 83:14 virtue 191:13 visibility 108:24 176:22 200:8,11 204:9 visible 180:3	voice 19:8 195:3,9 195:14,24 210:16 231:4 voices 195:18 volume 94:19 95:16 volumes 95:13 voluntarily 262:5 voting 133:20 VPN 246:18 vuln 141:11 142:12 vulnerabilities 12:5 16:8 28:4 126:18 126:24,25 130:15 133:6 139:22 143:1 144:11 146:4 147:9,10,11 147:18,19,23 162:16,24 217:9 vulnerability 2:13 12:11 21:16 84:24 86:5 121:1,7,21 122:6,8 126:22 127:5 132:4 133:15 139:2,3,12 139:12,25 140:19 140:21 141:1,5,13 141:17,22 142:14 142:16 143:16,17 143:21 146:16 147:6,15 152:17 153:25 162:21 167:9 168:19 180:7 198:16 212:9 218:6 254:6 254:7 vulnerable 15:11 142:7 162:19	54:14 55:9 57:14 69:15,19,22 81:3,4 81:18 90:12 93:22 107:20 110:18 111:11 120:9 124:20 125:12,13 125:14 128:23 130:2,3,13,25 131:1 134:16 137:13 138:12 145:5,6,7 146:18 146:19 156:23 158:14 159:16 161:25 162:7,9,10 163:12 165:8,14 166:8 169:7,17 171:1 178:11 184:23 194:2 198:7 199:11,12 200:7 201:3,17 203:9 205:12,13 205:19 208:13 210:25 211:12 212:8,20 216:7,7 216:24 233:20,21 234:16 238:25 244:19 248:9 249:25 253:23 262:1 264:6 268:10 wanted 65:4 135:8 172:17 229:10 231:18 232:19 240:10 248:2 268:15 wanting 116:22 wants 186:22 264:5 war 47:9 Washington 53:21 watch 140:25 141:7 151:13 watching 21:8 69:23 135:17 watermark 197:11 197:14,18 Waters 71:21 75:17 75:23 79:1 91:2 119:22	wave 71:9 way 18:3 19:4,20 25:19 29:15 30:2 33:2 34:14 36:15 38:3 40:18 42:13 47:1 51:20 52:8 55:7 62:1,13,14 68:14,15 75:12 84:10 86:12 89:10 89:11,22,25 99:9 100:5 102:18,23 107:9 111:25 112:8,13 130:7 133:13 134:3 138:18 140:9 145:23,25 152:12 160:16 162:14 163:18 169:23 176:21 178:19 184:1 185:24 187:14,23 192:19 193:4 194:15 195:6 197:12 198:1,12 206:17 209:8 214:3 219:2 220:9,18 226:16 226:17 227:6,17 228:15 232:16 238:15,21 240:4 244:4 246:19 248:15 249:4 256:11 261:12 ways 38:4 42:23 55:8,14 65:22 88:23 152:10 162:10 167:14,17 167:18 170:5 180:15 191:12 203:15,19 204:7 204:19 217:18 225:25 231:17 232:24 239:6 242:16 266:10 we'll 69:24 132:23 133:2 134:9 167:1 we're 68:22 71:4 73:4 74:19 120:11 125:24 126:4,21	
V					
vacuum 190:7 validating 153:1 validations 152:24 valuable 69:21 123:4 124:12 131:2 value 32:1 34:12 73:20,24 87:5 98:9 136:14 153:16 158:16 187:21 203:5 208:9 256:16 variation 68:13 variety 36:25 48:14 56:2 174:25 various 38:4,24 166:11 176:16 vary 9:14 11:10 15:14 varying 178:20 vast 91:23 143:2 vault 247:11 vector 29:7 263:9 vendor 72:22 100:25 107:6 111:21 116:4 130:1 173:4 183:19,24,25 202:14,16 204:20 204:20 209:15 213:13 229:17 253:19,21 258:16 259:8,9 vendor's 183:13 vendors 48:5 80:22 95:3 116:15,16	W				
walk 248:3 walked 87:16 Wallace 121:14 131:13 146:9,15 148:13,23 159:9 160:3 170:18,23 want 3:2 9:3 25:8 33:24 39:5 52:18 52:22 54:8,9,11					

131:15 134:5	106:21 107:11	web-type 136:22	150:3,4 161:5,19	134:13 141:1
136:15 138:25	108:4,20 109:2,3	website 102:15	195:22 208:9	142:9 148:22
143:11 144:22	110:21,22 115:5	130:8 225:6	210:24 214:10	161:9 173:5,20
145:23,24,25	116:1,5,17 117:23	week 131:19,19,21	232:4 236:1,10	176:23 184:5
146:10 151:14	118:19 138:6,11	weekend 148:1,3	266:17	188:5 191:19
152:13 153:1	144:19,20 145:20	weeks 67:13	whatsoever 252:1	193:2 202:22
159:10 162:18,20	155:9,9 163:22	weigh 217:4	where's 49:10,12	210:8,12 212:17
164:2,5 166:7	164:21 165:12	weird 170:19	white 52:6	213:11 214:17,24
167:10,14 227:14	169:15 170:25	welcome 2:4 3:1,3	who's 15:1 119:15	216:22 217:12
227:15 229:3	173:4 175:12	23:3 71:2 105:24	177:18 181:20	218:12 219:15,21
230:5 237:14	179:24 183:15	121:3 172:3 222:3	219:7 220:25	220:15 238:12
248:14 250:12	192:23 193:22	223:15	247:15	244:14 247:7
252:7 255:4	197:21,21 198:11	well-rounded	why'd 178:25	248:16 249:4
265:20 266:10	199:13 218:20	192:20	why's 187:5	250:4 252:3 254:6
we've 65:7 66:14	we've 18:16 25:12	well-trained 62:5	wide 43:6	254:16 255:2
67:21 73:22 74:16	25:15,24,25 32:23	Wendy 223:8,10,15	widely 15:15,15	256:5,22 258:8
75:10 133:18	41:3,12 46:14 51:3	227:3 229:24	231:23 262:22	260:7,8 266:7
150:19 223:17	60:15 61:22 84:2	231:9 232:19	willing 64:19,20	268:1
238:10 243:12	97:22 114:14	237:22 240:10	149:7 214:6	workarounds 88:2
251:10 266:2	117:25 118:14	243:19 244:7	248:13,13	worked 41:19 60:17
267:7	132:8 152:16	245:1 246:16	win 39:10 266:14	174:4 176:2,7,8
we'd 75:25 76:6,16	155:10 164:9	249:17 251:15,18	Windows 125:4	193:2 194:13
76:21	166:23 175:5	251:21 252:11,12	136:8 228:25	217:13 237:7
we'll 21:10,12,15,17	193:2 219:17,19	254:21 257:2	wing 236:7	257:4
21:19 42:25	219:21 220:5	261:2,3 264:4	winning 266:11	workers 67:1
120:12 132:16	237:22 260:25	267:13 268:11	wire 28:20 103:13	workforce 60:10
177:16	265:20 266:5	went 61:4 178:25	wiser 263:6	64:19 216:14
we're 3:11 4:13 11:4	weak 116:12 133:5	weren't 254:22	wish 114:2 155:16	working 7:17 21:25
20:15,19,20 21:25	weaker 139:17	Wetherill 172:3,7	won 36:8	28:8 31:8 39:24
21:25 25:1,2,7,14	weakness 254:15	174:12 175:18	wonderful 110:9	44:22 45:20 46:7
25:15,16,23,24	255:14	177:4 178:10	wondering 53:6	61:11 73:12 79:7
26:5,7,8 27:11,14	weaknesses 127:19	180:8 181:15	193:22 209:16	79:20 82:20 108:5
27:15,15 28:7,17	129:3 130:15	184:22 186:3	word 11:1 50:3	123:19 125:14
28:22 29:10 30:6	142:3 162:11,12	187:25 189:15	97:14 119:19	133:18 152:13
32:7 34:16 35:4	162:14 168:18	191:25 193:14	135:17 170:17	172:19 176:2,4,15
36:21 37:2,14	wear 82:5	196:1 198:6	177:8 220:2	188:21 191:12,13
38:14,15,16,21	wearing 78:3 81:20	200:13 204:10	263:12 267:14	191:21 192:10
39:13,19 42:5,17	82:10	206:20 209:5	worded 100:9	193:4 215:7,7
42:19 43:9,19,22	Weaver 121:16	211:21 214:7	227:18	216:11 227:16
44:16,22 52:12	124:19 125:22	216:23 218:22	words 49:21 134:1	233:2 251:11
55:1 56:23 58:2,8	131:1 145:4 149:5	219:13,25 220:21	240:23	260:19
60:4 62:19,21,22	153:12 155:14	what-if's 212:5	work 12:19 19:13	works 66:12 78:7,16
62:22 81:13 82:20	159:24 160:4	what's 24:18 29:1	22:1 28:16 38:15	86:22 112:22
83:1 85:2 87:6	170:3,21	29:15 30:15 31:25	48:2,5 53:21 61:3	113:20 213:19
90:12 93:19,25	web 95:8 136:6	32:9 38:5 41:10	72:16 76:3 88:20	246:8 247:16
95:12 97:20 99:15	151:4 226:15	48:19 50:2,6 60:6	89:11 108:18	workshop 1:5 3:4,7
99:18 100:1,2	web-based 226:12	85:1 100:21 118:5	112:1,11 118:3	4:9 20:14 21:25
103:11 106:15,17	226:16	125:13 138:21	123:15 125:9,10	22:6,8 23:4 71:3

<p>121:4 122:18 172:4 222:4,17 268:15,17,22 269:1 workspace 117:13 workstation 59:8 workstations 59:7 89:16 world 38:17 57:16 59:21 60:7 110:9 134:21 143:3 179:9 205:1 231:24 232:10 238:11 253:22 worried 256:8 worry 137:3 141:12 141:23 197:1 worse 64:1 220:14 worth 37:9 58:20 214:18 236:11 260:7,8 worthwhile 198:14 wouldn't 136:25 243:2 256:24 wouldn't 49:9 wrap 265:11 wrap-up 109:16 write 205:13 206:11 220:7 248:4,24 249:19 250:13 writing 11:22 19:16 20:9 95:25 102:1 193:21 200:17,22 200:25 204:6 205:4,4,8,9,11 248:1 250:1 written 10:9,10 11:16 13:24 14:8 19:19 20:9 86:2,6 86:7 96:25 98:10 100:19 113:5,6 115:16 201:13 204:11 205:1,20 205:23 217:9 268:19,20,23 wrong 25:3 124:19 124:23 177:22 178:5,25,25</p>	<p>wrote 134:12 146:24</p> <hr/> <p style="text-align: center;">X</p> <hr/> <p>X 2:2 51:7 55:9,9 197:3,7,13 xls 230:8</p> <hr/> <p style="text-align: center;">Y</p> <hr/> <p>Y 51:7 197:8,13 yards 25:24 yeah 24:6 28:5 32:20 33:10 36:11 39:17 43:25 44:3 45:23 48:10 50:12 54:21 62:11 68:8 81:1 89:7 114:7 126:15 131:13 133:2 134:4 135:8 146:2 148:23 159:9 160:3 163:10 165:8,17 168:4 170:18 180:10 186:5 188:12 189:18 196:3 201:5 204:13 208:13 209:5 211:24 220:3 226:10 228:13 245:5 246:15 256:1 257:3,4 258:19 261:8 262:8 264:12 266:23 year 43:1 62:6 76:5 76:10 97:17 123:11 140:22 151:13 158:20 164:15 174:17 180:24 194:21 197:14,17,17 199:8 200:9 202:15 207:11 209:1 237:2 238:1 year's 236:11 years 3:24 31:24 32:18,19 52:17 64:15 66:15 81:16 104:22 135:3</p>	<p>164:16 173:2,22 174:19,21 175:23 176:1 187:15 197:3 207:11 223:5 225:4 229:4 256:10 265:22,23 267:4 yellow 34:23 yes-or-no 100:19 York 182:14,18 York's 9:5 you'd 38:19 85:12 you'll 21:9,23 33:3 66:19 148:16 168:4 170:20 you're 4:22 15:5,11 15:15 16:10 20:6 21:8 22:3 25:4,20 26:13 32:19 36:4 38:7 40:12,12,17 40:18,19,25 41:10 42:15 43:10,11,14 48:25 49:20,21 50:18 56:19 62:11 63:7,10 93:4 128:21 129:4,11 142:19 145:17 154:10 156:20 170:15 176:10 178:7 185:9,17 186:22 188:20,25 189:11,12,21 190:18 191:14,15 191:21 193:7 196:4,6 197:3,19 199:6 201:16 208:1,8,12,14 210:17,18 211:25 212:23 213:7,13 213:13 214:6 215:6,14 235:20 244:8,9 259:2 you've 26:3,21 32:5 32:6,25 33:6 40:16 40:19 41:11 49:7 50:3 59:10 63:12 65:17 104:21 125:4,5,8 128:20</p>	<p>128:22 143:20 144:5 149:12 157:15 158:21 185:13 195:14 215:7 258:25</p> <hr/> <p style="text-align: center;">Z</p> <hr/> <p>Z 51:7 Zeek 125:2 149:9 zero 245:9 Zoom 61:5,6 93:6</p> <hr/> <p style="text-align: center;">0</p> <hr/> <p style="text-align: center;">1</p> <hr/> <p>1 21:10 72:3 73:25 92:5 234:19,20 1,000 84:14 1,800 123:18 1:00 21:15 1:01 120:15 10 25:24 43:5,7 64:11 102:18 109:12 233:12 236:17 10:00 61:14 10:32 70:5 10:45 69:25 10:47 70:6 100 32:17 61:3 63:14 64:13 156:8 156:22 255:2 11 31:8 11:49 120:14 12 58:9 103:14 147:20 120,000 76:5 120,000-plus 124:7 121 2:13 12th 268:23 13 1:12 15 43:5,7 64:18 229:4 236:13,15 265:23 267:4 15-minute 220:25 15,000 83:16 156,000 237:9 15K 84:14,14</p>	<p>16 237:4 17 3:23 172 2:16 18 103:14 180,000 76:1 180K 78:13 197 158:19,23 1984 238:10 1992 223:7 1999 3:17</p> <hr/> <p style="text-align: center;">2</p> <hr/> <p>2 43:4 45:17 2,000 166:3 169:4 2,160 76:17 2,500 84:16 2:02 171:3 2:15 21:17 2:16 171:4 20 31:24 104:22 187:15 229:4 265:23 20,000 169:4 200 83:16 169:2 200-gig-plus 124:3 200-person 156:17 161:23 200,000 165:20,21 2000s 245:22 2002 3:22 2003 3:23 2010 223:5 2013 236:24 2016 236:23 2017 9:6 175:24 2019 4:7 2020 1:12 67:14 133:18 215,000 76:21 220 32:19 222 2:18 23 2:7 24 147:20 24/7 151:13 24/7/365 85:2 240,000 76:5 25 84:11 144:22 250 84:11,13</p>
---	---	---	--	---

27002 48:14
2FA 239:12,14
 244:3
2K 84:12

3

3 2:4 76:10 102:19
 120:13
3,000-plus 123:7
3:18 221:3
3:30 21:20
3:31 221:4
30 174:19 223:5
30,000 145:14 146:2
 146:4
30K 84:15
33,000 237:24
365 45:7 151:13
 254:18 255:10

4

4 43:4
4,800 76:14
4:31 269:3
40 113:14
40-page 99:18
400-person 156:18
400K 78:14
40K 129:24
451 223:13
48.5 264:22

5

5 43:2 236:17
5,000 86:1,14
 237:25
50 76:7
50,000 123:8
50K 84:16
55 76:11
56 93:9 118:7
5K 84:12,13

6

6 90:6 102:20
6,000 236:14 237:25
 238:1
6:00 148:6
600 124:4

600,000 123:11
60s 243:3

7

7,360 76:19
71 2:10
750 84:13,14
76,000 76:2

8

8 43:3
80 225:6
80-hour 129:23
800-171 160:18
800-53 48:15

9

9 76:10 102:23
9,000 123:14
9:00 1:13
90s 257:5