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

FEDERAL TRADE COMMISSION

INFORMATION SECURITY AND FINANCIAL INSTITUTIONS:
FTC WORKSHOP TO EXAMINE SAFEGUARDS RULE

MONDAY, JULY 13, 2020
9:00 A.M.

VIRTUAL EVENT

2

FEDERAL TRADE COMMISSION
INDEX

3

WELCOME AND OPENING REMARKS

MR. LINCICUM: Good morning. I want to welcome everyone to the Information Security and Financial Institutions Workshop by the FTC. My name is David Linicum. I am an attorney here at the Division of Privacy and Identity Protection at the FTC. Today’s workshop is going to be looking at the Safeguards Rule, which is a rule that requires financial institutions to enact safeguards to protect customer information.

We’re going to start by looking at our current rule and what it requires of financial institutions and then move on to some of the proposed amendments that we issued. If -- and so, let’s go ahead and start the slides. Next slide, please.

Thank you. The Gramm-Leach-Bliley Act was enacted in 1999, and, among other things, it required several agencies to issue rules for financial institutions in order to have them safeguard their customer information.

In response to that, the Federal Trade Commission enacted its safeguard in 2002 and it became effective back in May of 2003. So over the next 17 years, no real changes -- well, no changes at all have been made to the rule. We think that shows how

4

flexible that rule has proven, and how robust. But we do periodically review our rules to see if there needs to be updates and we did so recently with the Safeguards Rule.

After that review, and seeking some comments from the public, we issued a notice of proposed rulemaking in March of 2019. We got quite a few comments back from proposed rulemaking, and this workshop is going to be looking at some of the issues raised both by the proposed amendments and by some of those comments. Next slide.

So let’s start with the current rule so we know where we’re starting from, what the amendments are -- would change and where they might expand upon the current rule. So the current rule applies to customer information held by financial institutions. Customer information is fairly self-explanatory. That’s information that a financial institution may hold that they received from a customer as part of providing a financial service or product.

“Financial institution” needs a little more explanation if you’re not familiar with it. I think most people when they hear “financial institution” think banks, and while banks are certainly financial institutions, they’re not covered by our rule. Our rule -- those are handled by other agencies rules. Our rule covers nonbank financial institutions and any basically financial institutions that don't have deposits. And there are a few others that are excluded.

But generally speaking they're the other kinds of financial institutions. And that's a fairly broad definition compared to what many people have in their mind. It goes anywhere from, say, payday lenders, other online lenders, debt collectors. It can -- it also applies to car dealerships, if they're involved in helping customers obtain loans for their -- or helping their customers obtain loans. It can also apply to universities, if they are involved in the financial aid process.

So the rule would apply to all -- it does apply to all customer information that a financial institution has, either their own customers or the information of customers of other financial institutions that give them that information. So it's not just the information of that financial institution or that that financial institution receives from its own customers.

The rule is based on a requirement that the financial institution have a comprehensive information

security; so a plan that lays out all aspects of security -- physical, electronic -- and is meant to protect the integrity and security of the information that they hold. Next slide, please.

So let's go over what the comprehensive information security program needs to have under the current rule. First, it has to be appropriate to the financial institution size and complexity. So a smaller financial institution, a simpler one, will have different needs than a financial institution that is very large with a complex network.

The nature and scope of activities. So that -- you know, how the information is used, how it's stored, that sort of thing. And finally the sensitivity of the customer information at issue. So a collection of emails has to be treated differently than information that includes social security members, account numbers, very sensitive information like that.

The program has to designate an employee or employees to coordinate the program. So there's someone or some people in charge and making sure that this happens. And the program has to identity the reasonably foreseeable risks, both internal and external, to the security, confidentiality and

integrity of the customer information.

So the program needs to have looked at the risks to customer information. It has to basically be based on a risk assessment and it has to then assess the security of the financial institution and the safeguards it has in place to control those risks that it's identified.

Also, the program must address employee training, information systems, and detecting, preventing and responding to attacks. So kind of a full spectrum of information security issues. Next slide, please.

The rule also requires financial institutions to -- well, design those safeguards we discussed, to control those risks, and to regularly test those safeguards to make sure they are actually working.

Also, it addresses service providers as many financial institutions use service providers to handle or process or store customer information they have. And the rule requires a financial institution to oversee those service providers by first selecting ones that are actually capable of maintaining appropriate safeguards and then requiring the company to actually maintain those safeguards by contract.

It also requires financial institutions to evaluate and adjust the information security plan based on the results of testing. So if they do a test and they find a problem, they have to actually adjust their plan to address that problem: any material changes to operations. So if the financial institution changes its business model or the setup of its network or anything basically that would impact how the financial institution operates, they need to reevaluate their information security plan. And finally a sort of catch-all of any other circumstances that they had reason to know would impact their information security program. Next slide, please.

So the current rule -- that is where the current rule lies. And like I said, it is a pretty flexible rule that covers a lot of situations. And with the proposed amendments, what we sought to do was to maintain that flexibility of the current rule while also providing more guidance about what the information security program actually has to consist of and what it needs to address.

Our plan is to have -- what we intended is for it to provide clear requirements for the financial institution so they understand what it needs to address while still allowing them to create a program that is adapted to the needs of that financial institution.

And I also want to give credit where credit is due, that our proposed amendments are based very largely on New York's cyber security regulations, which they implemented in early 2017. Next slide, please.

So the proposed rule has the same basic structure of the current rule; doesn't change it fundamentally. It's still based on the creation of a comprehensive information security program that is, in turn, based on a risk assessment that is suited to the size and complexity of that financial institution. So, again, it's going to vary depending on exactly what your financial institution looks like, what information they maintain and how they use it.

What the rule does, though, is require -- put forth more detailed requirements for the plan, what it needs to address, the areas it needs to look at, without actually telling the financial institution what they need to about those areas. It just says this is the area you need to look at and make a plan for, such as access control. Who can -- how do you control information and make sure that only those who are authorized to use it can actually use it.

Almost all the requirements are process-based and adaptable. And so, again, it doesn't say what you need to do exactly. It just gives you a process that you need to go through to make sure that all bases are covered.

And, finally, it has an exception for companies that have less -- that maintain very little customer information and exempts them from some of the requirements, primarily the written -- some of the written reporting requirements. Next, please.

All right. The proposed rule, let's go into a little more detail here. Under the proposed rule, the financial institutions have to first designate one qualified individual to be responsible for overseeing the program.

So the only change we made here substantively from the current rule is that we made it so rather than it being person or persons, it has to be one person. And that's designed to increase accountability so that, you know, someone is in charge of the program but also in case of emergency or generally process, that it's always clear who the person in charge is, where the directions are coming from and, you know, basically give direction to the program.

We also added the word "qualified" to it so that the person needs to be qualified. I think we would argue that the current rule presumes that, but we're making it explicit here.

We did use as a term of shorthand, the term CISO, or chief information security officer. We didn't intend that to imply that a specific set of qualifications was required, but I think that was the effect it had. But that was not the intention. We think "qualified," what that means will vary based on the size and complexity of the network. A very large, complex network may need something -- someone who is, you know, what is commonly known as a CISO, or as a simpler one maybe it will have someone with more modest qualifications and experience.

So the program has to be based on a written risk assessment that lays out -- that includes certain criteria for determining risks and then address how the program is going to address those risks. So, again, the main change here is we give a little more flesh on the bones to what the risk assessment has to look at and also requires that it be in writing.

Then you have to periodically perform additional risk assessments. And it's just not something that you -- you can't just do a risk assessment in the beginning and never think about it again because, as discussed earlier, things change. Certainly everyone knows in the information security field that it's constantly a moving target as new threats arise, as new vulnerabilities are discovered.

And like the current rule, there -- it needs to be tested and monitored, but a little more specificity here in that you can either monitor it through continuous monitoring or instead by at least doing annual penetration testing and biannual vulnerability assessments. Certainly people may choose to do it more often than that, but that would be the minimum requirement under the rule. Next slide, please.

So the proposed rule also addresses training. Under the proposed rule, financial institutions must provide security awareness training to personnel. So this is to all employees. I think most people who work in a company have had similar training that lays out the basics of security awareness, how to avoid phishing. You know, again, we don't go into that in detail, but, you know, it does require that there be at least basic security awareness training for everyone.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Both of those requirements, though, allow alternatives if the person in charge of the program approves them. If, for whatever reason it's not the best solution for a financial institution or it's just not a viable solution. And both of them, while they require encryption or multifactor authentication, don't go into the details of exactly how that will be implemented. That is still up to the financial institution to decide what encryption solution or multifactor authentication solution is best for them. Next one, or next slide.

All right. So let's look at the encryption requirement first. It would require that all customer information that is being held by the company or transmitted be encrypted while in transit if it's over external networks and while it's at rest.

So points to note about this is it applies only to customer information. Other information handled by the financial institution would not necessarily need to be encrypted and it would be up to the financial institution. And for the transmitted information, it only applies to external networks. It does not apply to transmissions within the financial

institution's network.

And as I said before, if encryption is not feasible for some way, then you can come up with alternative controls that have been reviewed and approved of by the person in charge of your information security program. Next slide, please.

All right. The multifactor authentication requirement would require multifactor authentication for any individual accessing customer information. So if anyone is going to look at the customer information, they need to go through a multifactor authentication process. I think most people are at least basically familiar with multifactor authentication. Most of us use it in some fashion in our online life.

But just to be clear, what we've defined multifactor authentication here is –- is that it must include two of three possible factors that it's going to need. One is a knowledge factor, or things you know. So this is our passwords or biographical information such as mother's maiden name or older addresses, that sort of thing.

Possession factor, things you have. So this might be an actual physical token that you have that gives you a code or something like that or it is

attached to your computer, or it may be a device that you have possession of, a particular phone or a particular computer that verifies that you have this factor. It can be satisfied that way.

There's also the inherence factor, which is things you are. So this would be biometric characteristics. I think fingerprints are probably the most common still, but it also might include voice prints or face recognition, or to get a little less common and more sci-fi, retina prints, that sort of thing. I mean, it's meant to include anything that anyone comes up with that is things you are.

And, again, if this doesn't work for whatever reason, the person in charge of the program can come up with a different solution. You just have to memorialize that decision in writing. Next, please.

All right. A little more detail on the proposed exception to the written requirements. We decided that the best way to measure this was the amount of information that a financial institution maintains about consumers. Because a small company that is maybe small in size, so budget or customers, may still hold information of tens/hundreds of thousands of information of consumers in today's

environment. It's something that happens. And those companies, even if they're small, if they have access and responsibility for information of that many consumers, we feel they still need to meet these requirements.

But if you're a company that really does not maintain much information, this would require -- exempt you from most of the requirements that things be in writing and the written reports and things of that nature, just to make it a little easier to comply with. Although the basic requirements would still be very much in place for anyone handling customer information. Next slide, please.

So that brings us to today's workshop. We're going to be speaking with people with direct experience providing information security to organizations, including financial institutions and other experts in the field, who, you know, have direct expertise in the information that we're talking about.

What we're looking to do today is to gather some more concrete information on the cost and benefits of the practices that we set forth in the proposed rule and to address some of the comments, just to get more information on those comments.

We are particularly interested in the costs and scalability of these requirements to smaller businesses. What will the cost be to a small business and are there solutions that are -- that scale down to your size? Are there solutions that take into account your smaller size that will be cheaper and easier to implement. Next slide, please.

All right. I believe the schedule should be on the page that you're all watching this from. But I hope you'll join us for the rest of the day. In just a few minutes after this, we'll start Panel 1. It's going to look at costs and benefits of information security programs. Then after a short break, we'll have a panel on information security programs and smaller businesses particularly.

Then after lunch, at 1:00, we'll do a panel on continuous monitoring and penetration vulnerability testing. And after a short break at 2:15, we'll do one on accountability, risk management and governance of information security programs. And finally we'll finish up the day with a panel at 3:30 on encryption and multifactor authentication. Next, please.

Throughout the day, we really hope that if you have any questions for our panelists that you'll send them to us. This being our first virtual panel, we're still -- virtual workshop, we're working out

details. Hopefully this will work well. If you send any questions to safeguardsworkshop2020@FTC.gov -- there should be a link on the page you're viewing this on –- then we will try to ask as many of those as possible of our panelists.

And then following the workshop, if you have any comments on the proposed amendments or anything that is said or presented in this workshop, go to regulations.gov and look at the Safeguards Rule entry and you can enter comments there for about a month after today.

So thank you very much and I will see you all in a few minutes on the first panel. Have a good day.

(Brief recess.)

THE COSTS AND BENEFITS OF INFORMATION SECURITY PROGRAMS

MR. LINCICUM: Good morning and welcome to the first panel of the FTC Safeguards Workshop. I'm David Lincicum, an attorney with the Division of Privacy and Identity Protection here at the FTC. And we have four panelists who were gracious enough to join us this morning. I will go through and introduce them each, and I think they'll probably raise their hand or somehow gesture just so you know who I'm talking about.

First we have Pablo Molina, who is the chief information security officer at Drexel University and a lecturer at Georgetown.

Then we have Serge Jorgensen, who is the CTO and founding partner of the Sylint group.

And then Chris Cronin, a partner at HALOCK Security Labs. And Sam Rubin, the vice president at the cybersecurity consulting firm, the Crypsis Group.

So this panel is going to address the costs and benefits of information security programs of financial institutions. You saw in my introductory remarks, I mentioned that both the current rule and the new rule are really based on risk assessment. And in order to have risk assessment, really costs and

benefits of these programs are key to that.

So let's start, and I'll ask Chris. What is a risk assessment in this context? What are people look at as far as costs and benefits and how do they start that process?

MR. CRONIN: Yeah. Well, there's what people are doing and there's what they should be doing. So I'll just very quickly say that people are not generally doing what we would consider risk assessments. What they're doing is having an auditor come in and run an audit or they'll be engaged in a maturity model assessment. Am I a one, two, three, four or five? And if they're with a consultant who isn't really grappling with real security issues or risks, then they might even hear, well, go to a three. Everyone -- all of your peers are at a three out of five, whatever that means.

That's actually commonly what's happening. What we understand the Federal Trade Commission, regulators, even litigators and information security people, are really going for is an evaluation of the likelihood and the magnitude of harm that can come from bad things that happen.

Now, we all have really good information about the bad things that happen. There are some that have yet to be invented, we know. But if we're doing an actual risk assessment, we're looking at the likelihood and impacts of things that could go wrong in environments like ours. And what you're also suggesting in the proposed updates is that there's a -- that you also evaluate the controls, which is super important. If we're going to have a good definition for reasonableness, we want a cost/benefit evaluation to say when you look at the likelihoods of impacts without the control I'm considering. Let me evaluate it with the controls I'm considering and let me see where the balance is. And as long as we've thought about the impacts to ourselves that could be harmed and the impacts to others who we're protecting, then we're actually -- we've got a good basis for reasonableness. We're just not hitting that yet.

When you do look at stuff that comes from the federal regulators and three-letter agencies, the way you see attorneys talk about things, you know, when a breach case is going on, when you're talking to information security people, they all have the essential ingredients to have a definition for risk basis of reasonableness, but it's like we're at a -- we're running a marathon; we've gotten 10 yards short of the finish line and we've stopped. And we looked

at each other and say now what do we do? Well, you cross the finish line; just do that risk assessment and compare the two and then you've got a good basis for reasonableness.

So we're excited to see even stronger direction about what that risk analysis should be. But that -- we're -- the public just hasn't gotten there yet. And we're really encouraging them to move forward there.

MR. JORGENSEN: Chris, one of the things you just mentioned there in terms of how that risk is calculated, you touched on that risk to the data that you're protecting and the risk to the consumer. And I think that's something that we see frequently missed in that risk analysis because there seems to be a preponderance of people that are saying, oh, okay, I can transfer the risk; I can buy insurance for this. And then the insurance will pay for all of that downstream impact of the risk.

But you really haven't necessarily protected the data that you've -- you are supposed to be protecting. And so it's just an interesting look at that can I transfer this or is it something I do have to protect?

MR. CRONIN: Right. Or consider the harm to

people directly. And when I'm doing litigation support, one of the first questions I ask whether among the defense or plaintiff's or regulator side is I ask when we look at the risk analysis, did we explicitly look at the kinds of harm that could come to people and did we make investments that were appropriate for protecting that harm?

When I do see a risk assessment, it's usually what is the impact to business. That's important. But that's not the only thing you should be paying attention to. When we're talking about cost/benefit analysis for reasonableness, our cost is impact to business. Right? The benefit is what we need to actually be sure we're taking a look at when we're evaluating risk to the public. Because we're seeing that missing, a lot of people are going to have a hard time demonstrating reasonableness.

MR. LINCICUM: All right. Here's a question I'll kind of ask the group, then. You talked about, you know, the bad things that can happen with a breach, and we certainly have all seen them in the news. Those are sort -- those tend to be the very bad situations.

What information do people have about the more general risks to them? You know, what kinds of

attacks are they most likely to face; how bad are they going to be? Where do they get that information and how does a company start to come to terms with what their vulnerabilities are and where the risks are?

MR. RUBIN: Yeah, this is Sam. I can speak to that. So my firm, Crypsis, does a tremendous amount of data breach incident response. So we're working with companies every day helping them respond to these types of incidents. And what I would say is that, you know, if companies kind of have their eyes and ears open, there is a tremendous amount of information whether it's threat intelligence, publications from firms like mine and other great infosec firms that are talking about the risks that are out there; the things that companies are facing.

For example, right now based on our work, what we're seeing is that the two greatest threats facing financial institutions are business email compromise -- that's threat actors getting into your email and trying to perpetrate wire fraud or otherwise monetize that access -- and ransomware. So those are the two biggest threats that we're seeing impact organizations. But for -- to answer your question, you know, what companies can do is really just -- it just takes kind of a level of effort to look to see what's out there and what your peers are facing, and just to have that awareness.

MR. JORGENSEN: I think one of the challenges there, though, is that you have to understand what the risk is, because if you purely look at it from that perspective of here's the attack vector that the threat actors might be using, and you said business email compromise or ransomware -- and, Sam, I totally agree with you in terms of the type of attacks that we're seeing. But from a risk perspective, I think a lot of people miss the incentives of the threat actors, and these attackers out there have -- can get millions of dollars from a successful attack. So from their perspective, they look at it more like what's the easiest way to get to the data that I'm going after? And where right now it may be business email compromise, tomorrow it's going to be something different.

And so if we go back to how do we do that risk analysis and that risk assessment, it's got to be around what kind of data do I have and then how do I protect that, yes, against the current threats but also how do I build out a program that appreciates that the sensitivity of that data, the risk of that data being compromised, and then how do I adjust my

protections based on the evolving threat?

And that way, I'm not always chasing the most current one, but I'm planning for the future as well.

MR. MOLINA: At Drexel University and other universities we're in the business of educating people. So we educate our community members, faculty and staff, students. I gave interviews with the regional media outlets to educate the community about some of the cyberthreats out there, some of them being business cyberthreats; others are personal.

But to be honest, I would say that the number one source of information for most people is the regular media. And some media outlets are very good at reporting what's going on and how to take precautions in organizations and as individuals against some of these cyberthreats. But others have not. So it is our experience that many of our community members are sometimes ill-informed about the different threats. They may have heard time and time again that there are phishing scams out there, and yet they fall for them. They might have heard do not click on this link or else ransomware will be unleashed upon your organization's computers, and yet they click on the link.

So it's an interesting ongoing exercise that requires -- it takes a village to educate the entire society, but particularly our employees and our clients in order to understand those cybersecurity risks.

MR. JORGENSEN: You know, one of the things that I know a few of us participated in the Sedona Working Group 11 on data security and privacy. And one of the things that that blend of legal and technological experts, one of the things that Sedona is looking at, and other organizations, is trying to find that line, that cost/benefit analysis of risk.

And, Pablo, you must be facing this from a university perspective. Companies like to maintain historic data for whatever purposes -- reasons or purposes. And I know Sam and Chris, all of us out there face this information governance problem where after a breach has occurred, the threat actors got far more data than they could have. And, Pablo, my background or experience at universities anyway has been that they'll keep registration information for not just students, but, you know, possible students or applicants or people that you send scholarship information to, going back 20 years.

And then we have to assess is that -- what's

the value of that information or should I -- could I get rid of it and reduce the risk to the organization? And I think that really comes, Chris, back full circle to what you were saying about risk analysis, risk assessment, is you can just say, okay, well, you've got antivirus, you've got these three controls, everything's protected. But where we're trying to encourage people to think about can I get rid of data, what's my information governance process, and then if I do have a business email compromise, if I do have a ransomware attack that exfiltrates data, as well, then if I can reduce the scope of that data that I'm holding, then I have a much smaller exposure, much smaller risk, and ultimately much smaller impact to consumers.

MR. MOLINA: Well, in the case of universities, we hold records for Drexel over 100 years; in the case of Georgetown where I teach, over 220 years. So you're right about -- that's the policy, yeah.

MR. LINCICUM: All right. I'm going to move on to the next topic, which is very tightly connected to what we've been talking about, and that is kind of the benefit side of the coin.

After you've assessed the risk and the

magnitude of the risk, you then have to look at a solution. In one way, the costs of those solutions are fairly obvious. You'll know how much it costs to implement. But part of the equation is also how effective are they?

Sam, you said you've been involved in a lot of, you know, common after incidents. How do companies determine which protection pays for itself, actually creates enough benefit to justify the cost?

MR. RUBIN: Sure. Yeah, I mean, the unfortunate reality of what I see often is that it is that knee-jerk reaction in a post-breach scenario that makes it easy for leadership teams to see and understand what additional controls they need to implement because they're basically saying how can I make sure this never happens again?

And so, you know, whether it's, you know, insecure remote access, multifactor authentication, poor identity and access management, whatever the control gaps were, maybe no continuous monitoring, that makes it easy to see what they need to add or implement.

So that's one side of the coin. But where we want to get to is kind of for companies that haven't experienced a breach or incident in the recent

past, like, how -- to your question, how can they evaluate the benefit of implementing any given control. And, you know, I think an answer is some of the analysis that Chris was talking about where in a risk assessment, it allows you to demonstrate essentially the return on a control because a proper risk assessment, what it will do is it will take a probability of loss and a dollar impact and that allows you to essentially demonstrate how a change or implementation of control can kind of reduce the costs of a breach and relatedly kind of demonstrate the value or return on control.

So that's kind of the rigorous risk assessment method way to assess the benefit. Not always as Chris indicated at, you know, the top of the hour what we're seeing companies do at this point, but I think it's a place that they can get to.

Where we are right now, again, as companies have been kind of having this knee-jerk reaction, maybe the next layer of maturity is when they're using these risk matrices where you have, you know, a likelihood and an impact and the red and green and yellow.

I had a matter recently where I was talking to a CEO and he said how can I get more green on my

chart? And that was his goal for, you know, reducing risk, which, you know, it's better than nothing, I would argue, but if we can get to that point where we're doing something a little bit more rigorous, we would all be better suited.

MR. JORGENSEN: You know, that's a really interesting -- it's an interesting metric. And I think from a CEO's perspective, that may be "the" metric, is hey, what do I need to do to make this thing green? And if you tell me that it's get these business units in line with our security program, our risk analysis or whatever it is, then that may be what the CEO can do because ultimately they can't do it.

Should they have to understand the intricacies of cybersecurity or do they know that all they really have to do is help Pablo get to the registrar's office and actually delete data that they don't actually need anymore and help implement this information governance program, and that will turn a whole bunch of other things green?

So I think part of the challenge from identifying what those key performance indicators are, identifying what those metrics are, that can help leadership manage the risk for something that they really don't understand and maybe don't need to

understand, but rather just need to support the effort to implement those controls, but then appreciating the benefits of those controls becomes really hard.

And I know, Sam, you're probably going to talk about this, too, of trying to understand something where the only benefit is something doesn't happen. And it's really hard to explain that of, hey, we won; there's been no incident.

MR. RUBIN: Yes, right. Or companies really -- you don't get a bonus for not getting hacked, right? So, yeah, if that's your metric of success, it can be very hard. And, you know, when a CFO looks at that and they're looking at their profitability, you know, information security essentially just becomes a cost center. And so without a way to demonstrate the benefit, you know, we see things get cut or just a failure of, you know, whether it's a CISO or director of infosec to persuade his executive team to add those necessary controls.

MR. MOLINA: And risk analysis is very industry- and context-sensitive. Even though we're here discussing these issues in the context of financial services and the Federal Trade Commission, the truth of the matter is that there are a great variety among different financial services institutions.

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

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

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

analysis. So sometimes the devil is in the details.

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

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

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

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

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

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

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

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

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

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

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

So there is an aspect of the business that's pushed by a certain level of we've got to make the clients happy. If we tell them they have to get to five, they'll go find someone else who will tell them to get to three. And this is a real economic driver that pushes organizations away from thinking about what is reasonable.

The irony here is that if you actually are thinking about what's reasonable and you're taking this risk-based approach, you've got the challenges that we just described earlier. We've got the costs, we know what those are; the invoices come in. Right? The salespeople tell us what the number will be. The benefits, that's hard to figure out. This is a big problem.

So in order to help people get through these economic drivers, away from thinking about what a reasonable security control would be, HALOCK worked with the Center for Internet Security and just developed this document called Center for Internet Security's Risk Assessment Method, CIS-RAM. It's freely available for anybody. But it helps you do this evaluation where you can say what are my financial costs, what are the costs and benefits to my

mission, the reason why we engage in risk to begin with? What are the costs and benefits to the individuals who are at risk in my organization and to get people to systematically think about this.

So what we're seeing as a real driver away from the right behavior is just the economics of trying to have a happy client in the field causing people to do things other than think about reasonable, because they haven't quite figured out what that process is.

And I think the FTC has a real opportunity here with this round of the Safeguards Rule to tell people, by the way, what we mean by reasonable, this is a cost/benefit analysis. So think about the costs to your mission, your objectives, why you're in business and your obligation to protect others with and without the safeguard and we're going to figure out whether the costs and benefits balance.

So that's part of what we're seeing as a challenge that gets people away from doing the right thing and something that I think the Safeguards Rule could help people get back on the right track.

MR. MOLINA: One of the ways in which we measure the progress we made in many aspects of economic activity is we'll look at the investment

levels. Ardent (phonetic) reported late last year, on average U.S. organizations are spending between 5 percent and 8 percent of their technology budgets in information security; as low as 2 to 4 percent in manufacturing businesses, and as high as 10 to 15 percent financial services, which is quite a wide range between 10 and 15 percent.

What we don't get from those numbers is whether we're making a good investment with that money. Just because you're buying the most expensive advanced firewall does not mean you're protecting, as Serge mentioned before, the data that is critical to your organization, or as Sam mentioned before, that you're addressing the threats that are lingering out there.

So we still don't have enough research and enough actuarial information to understand the risks very well but also to understand whether or not what we're spending in cybersecurity is really taking us to the level that we should be at. And the suspicion that most of us have without hardcore research is that we're really falling behind the bad guys. And proof of this are the mounting losses that come from cybercrime.

MR. RUBIN: Yeah, I agree with that.

MR. JORGENSEN: You know, it's interesting -- go ahead, Sam.

MR. RUBIN: Okay, sure. Yeah, I agree with those comments. And just, you know, based on what I've seen out there often is sometimes you see strong investment in tools, right? Like, you know, investing in an endpoint detection and response or putting in a SIM, but without consideration of the people that you need to support those tools.

So, I mean, just equally important is the cybersecurity team to support ongoing security operations, to provide that continuous monitoring to look at the telemetry coming from your endpoints, to look at the logs.

And so just, you know, back to the question, David, of what we're seeing out there, that's a huge shortcoming that I'm seeing in the field. Another one you know, along the lines of what you were saying, Serge, is that divergence in business groups, I see that also with organizations moving to the cloud and to SaaS, you know, especially in this COVID time where we're all working remotely, you know, from our laptops. You know, some of us, you know, may be engaging in a little bit of shadow IT when we shouldn't be, looking for applications to help us get our job done and organizations having this kind of legacy protection model of, you know, the firewall and I'm going to protect my employees kind of hiding behind the corporate local area network. And what they're not doing is kind of protecting the cloud applications, protecting the SaaS applications, like Office 365, and protecting the endpoints.

So I think that that's a huge gap right now and area of focus. So, again, you know, cloud, SaaS, and then obviously having the right people.

MR. JORGENSEN: And I think, Sam, you just touched on it, too, where companies are thinking they can leverage the risk assessment that's been done for their SaaS provider or their cloud solution. And I can't tell you how many times I've gotten the obligatory, well, everything's secure because I have it hosted in AWS and here's Amazon's SOC 2. And I'm looking at it going, I appreciate that their information is secure, but what about your information? How is that working for you?

MR. RUBIN: That's right.

MR. JORGENSEN: So it is one of those very big challenges, yeah.

MR. LINCICUM: Let me go ahead and move on to the next question, something that came up I think

Chris was talking about how certain consultants will have a certain approach. And that's a question I have with a company that is starting this process of setting up a program or updating it based on a new rule or new standard. How do they determine what they should be doing? I mean, a consultant will come in. Are there standards that a consultant will be working towards? Are there qualifications that tell you, oh, this person is going to get you in the right place? Or are you just kind of doing it one at a time on people who come through your door? What standards are there out there?

MR. JORGENSEN: I'll tell you one of the most powerful pieces that we've been able to use to address that question is your own FTC publication on cybersecurity basics and just putting that out there and saying, hey, here's a cybersecurity basic book; go through these scenarios in here of FTC actions and things that have happened already and make sure that your programs are addressing those areas, because I think something that that does is it really helps people understand that even if I have anti-virus and even if I have -- I'm being told that I have DLP -- and going back to Chris' point of, it's a three, therefore it's implemented and I have a policy for it,

but it got turned way down and it's now ineffective because it started blocking all of my outbound mail because I use a nine-digit number that looks like a social security number, but it's not really. So I turned down that control or I didn't put that control in place.

So in terms of being able to explain the impact and some of the considerations with a bunch of war stories, I think that cybersecurity basics manual is -- has been incredibly useful.

MR. LINCICUM: Good to hear.

MR. MOLINA: There are others. We all use the National Institute of Standards and Technology cyber controls. They have been very helpful. But also, for example, as I mentioned, many of these decisions are context- and industry-sensitive.

So, for example, those of us in higher education, we get together through an organization called Educause. And many of us belong to the Higher Education Information Security Council. So there we develop the risk analysis and we develop frameworks that are very good for higher education. They map to the other controls, they map to the NIS controls and they map to the CIS controls and many of the other ones we discussed, but they have been tailored for our

own industries.

So the interesting part would be to work with partners. I would suggest particularly for organizations that are not mature in this field to work with partners and vendors who have a certain specialization in the financial services industry because they can provide that nuanced approach to cybersecurity and risk analysis that are going to make them very, very effective in those efforts.

MR. CRONIN: Yeah, Pablo's right that the industry-adjusted approach is an important thing to consider. Now, we don't have one information security control standard per industry, right? But there are a variety of security control documents like ISO 27002, NIST 800-53, which is more detailed, but also leaves a lot to the imagination of the reader. CIS controls can be very specific and practical. There are a lot of these control sets that people use.

What's interesting is when you look at the instructions for each of these controls, they all tell you to do risk analysis. This is one of the really important things that FTC is doing with the proposed changes to the Safeguards Rule, by getting more specific about what this means, because no matter what control set you look at, you're going to see things that just can't be applied.

We had a client, a hospital, that was -- they were fed up with their security team, their internal security team, because the internal security team was saying use multifactor authentication; you must do it. Now, that sounds like of course you would; you've got it in the proposed rules. It was driving the physicians crazy because they would be in emergency situations and they wouldn't have their second factor with them, you know, where's my phone; I've got to get in to get this patient's record; she's having an allergic reaction; where's her file? It's on the system, but I don't have the second factor; what am I going to do?

The hospital has a mission, right, and the mission is patient care outcomes. The patients have to come out healthier than they were before or they failed their mission. And physicians were pushing back saying your security control of multifactor authentication is hurting our mission. You're creating -- in other words, you're creating a risk to our mission.

So these control standards, when you look at the NIS risk management framework and the cybersecurity framework, and you look at CMMC, this

new pending standard that's coming out for suppliers of the Department of Defense. You look at what's coming out from the FTC since you've uttered a word about this. You have to analyze the risk.

I say that you use whatever control standard looks like what you can do with your business, what's practical with your people and your technologies, you have to have that standard of care. But then those control standards are going to be hard to fit and hard to negotiate unless you have a real clear understanding of what that risk is.

MR. RUBIN: Yeah, I agree with that, Chris. I would sum it up by saying these frameworks, you know, there's a lot of them out there, obviously different ones that apply to different industries. You know, you pick the ones that are right for your organization, your industry. Get the fundamentals as you're saying but then leverage the risk assessment to get -- to assess where you are in that gray area of controls that you may not have, you know, economic resources or time to implement all of them. And the risk analysis helps with that gray area.

MR. CRONIN: And, David, just one quick point on a draft commentary, on the recommended -- on the proposed rule change is this concept of the CISO

signing off on an exception. So if I've got multifactor authentication, unless the CISO signs off, one real big problem we've got in the industry as well is this concept of risk acceptance without someone knowing what risk they're accepting.

We hear it a lot. Why did this breach happen? Well, we didn't do X, Y or Z. Why? Well, they accepted the risk. Was it your risk to accept or was it someone else's?

One thing I'd recommend going into these proposed rules is that, as you mentioned something like encryption or multifactor authentication where the CISO can sign off on an exception, that that exception should be based on the risk evaluation and to make that explicit. You can do it if you determine that the likelihood and the impacts of the problem are either acceptably low for all interested parties or there's no safeguard that would be appropriately burdensome given the risk.

So there's a way to inject that risk reasonableness because there is an epidemic of CISOs signing off on risks that isn't their risk to accept.

MR. JORGENSEN: One of the challenges also is -- comes in under risk mitigation at the end of the day, I think, but it's post-incident risk mitigation.

So when you use that example of multifactor authentication, it's one thing if that access provides that physician with access to a certain part of the medical record or for a certain number of medical records or something like that. And we still look at this as very black and white. So when you look at risk analysis, risk mitigation, I think the knee-jerk way to do that is to prevent a threat actor from breaching the edge, from getting into an environment at all.

And one of the pieces that's in a lot of standards that we're talking about, and certainly in some of the FTC guidance, is that discussion about post-incident impact. And so it's much, much different if the impact is limited and I detect things quicker versus if I have a threat actor running around in my environment for days, months, years, and able to access anything they want.

So that would be another piece that I think could use some highlighting in any sort of publications or new regulations.

MR. LINCICUM: I want to make sure that we get to ask some questions from the audience. I'm going to move on to that now and maybe we can finish up with one last question after we do that.

We have one question. It's fairly lengthy, so I'm going to try to parse it out as best I can for us. It asks what role should a determination of substantial harm and inconvenience play in the determination of -- it says complaint requirements -- I'm wondering if they mean compliance requirements -- in the space, given that it's an integral part of the rule both currently and as proposed?

So I guess it's asking, you know, how much should you be looking at the substantial harm and inconvenience and how much does that play a part? And how does that standard affect the nature of appropriate risk assessments, incident response and so forth. So anyone who think they got that, please answer.

MR. MOLINA: I'd love to, but I think that, David, you are the lawyer here. Me, I have a doctoral degree, but it's not in law. But I think that we understand the issue of harm. I also serve on the board of the Electronic Privacy Information Center in Washington, D.C., and we work very closely at times as friends of the FTC, sometimes in a more controversial relationship trying to push on the boundaries on this.

The issue of harm for any data breach is something that we have not solved. It's very, very

difficult to prove harm to consumers because you really don't know whether your data was exposed because of the breach today or the one two days ago from a different organization, or another one. There are no fingerprints to data that tells you what data caused the harm.

Hence, when you cannot address the issue of harm. Of course, organizations, we don't want to harm our constituents. We want to protect them, we want to do business with them out of the goodness of our heart. We also don't want to get into trouble with the regulators, particularly not with the FTC or the state attorney generals of any -- or the GDPR data protection authorities in Europe. We just don't want to do any of these things.

But the issue of harm is an almost -- a very difficult one to tackle. And to my knowledge, there have been no good solutions, not even on the other side of the Atlantic with a much more advanced privacy regulation and the GDPR.

MR. CRONIN: Yeah, I've got a slightly different take on that. Pablo, I agree with you as we look back. It's certainly hard to figure that out. It's hard to sometimes use our imaginations, too.

But what we can say is there are certain

risks that we're not going to take, whether I know what the subsequent harm will be or not. And I know that -- if I have a risk that could expose some number of a kind of sensitive record, that's something I'm not going to accept. And I might even equate that with some level of harm my organization might suffer. So even if we don't have a way to quantify that harm, there are ways for us to say qualitatively I would not want X amount of data of X type to go out, and I would equate it with this much harm that I could suffer, therefore, I'll put a control and that safeguards us both to some level.

I think this is actually a good opportunity for us to think about qualitative ways to talk about risk, where quantitative methods are helpful for other questions like dollars.

MR. LINCICUM: Okay. We have another question, and it is also a very lengthy one. I'll try my best to get to the meat of it so we can do multiple. Okay, I'll see if I can paraphrase.

Basically, the question asks since the rule would only affect customer information, information that's actually connected to a financial transaction, does that change how a risk assessment would be done. And it gives an example of -- let's see, registration

of student information that's not related to financial aid may be held for a variety of purposes by a university. And doesn't that affect -- you know, if you only have to consider some of the information, does that affect how you do the risk assessment, I think is the meat of that question.

MR. MOLINA: I think I can take it since student information, that seems to be under my purview. Those are the things that I see. So I would sign an exception for and accept the risk -- just kidding. I would never accept the risk for anything, thank you very much.

MR. CRONIN: That's very funny.

MR. MOLINA: But in academics, it's sensitive. It goes back to what Chris and Serge and some were saying that we have different business units and business processes and data elements, and we have to take a context-sensitive approach to those. So you're absolutely right.

For example, student information is mostly regulated by FERPA, the Family Education Rights Privacy Act, whereas the financial aid transactions that we're discussing under the Safeguards Rule are mostly regulated by the Federal Trade Commission.

And by the same token, you mentioned the

57

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

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

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

58

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

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

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

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

59

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

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

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

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

60

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

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

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

MR. CRONIN: Go ahead, Pablo.

MR. MOLINA: So I noticed sadly we were doing a little bit of a hybrid online learning, hybrid remote work, until we moved to 100 percent remote. A number of things happened. You know, first we went to all Zoom sessions. And guess what? Then we got into Zoom bombing incidents because the bad guys realized, hey, this could be fun. And some of them were not fun. Some of them were even illegal and required collaboration with the FBI to report the culprits and everything else.

Then we realized that people working at home without peers on their side, multitasking, taking care of their children. Some of them I imagine they started drinking at 10:00 a.m. in the morning based on some of their reactions and the things they did of sending gift cards or small things like that. People were tired. They were afraid reading the news and everything else.

So I would say that people who are known for good critical thinking, sometimes they were suspending their critical thinking. So they brought us more security incidents than we've seen before based on the human factor. And the bad guys will take advantage of the human factor because that has been done since the beginning of human beings getting together in a social

way, scamming each other out of food or tools or anything like that.

So that is one part that we have seen right here. That human element that has resulted into added risk because well-trained people, people who once a year are taking our security awareness training, all of a sudden in the middle of the pandemic seem to have forgotten many of the things they had learned, many of the business practices that they have been following before.

MR. CRONIN: Yeah, you're right. And I'll just cap it off quickly because there's a -- there's such a direct correlation between the way we behaved in the pandemic and the way information security has been happening.

HALOCK's business has been just thrust upon with incident after incident after incident, taking on just an immense number of incidents, because of the stuff that we're talking about, people moving remotely. And they're spending less on preventive stuff. So we're not actually preventing the thing; we're paying at the end of it when we're actually getting infected. It's a very frustrating thing to have this problem happen both in your public life and in your professional life. But it's what we see

happening.

Now, where it comes to organizations that just don't have the resources or organizations that must move for the sake of their consumers to do things that are more risky now, the one thing we tell people is if you cannot afford the security controls that you were affording before, you're going to have to tell people. And you may find that they're still going to engage in that risk with you.

So if you're not able to meet a certain deadline and you miss a security certification because you've got -- be direct with your consumers and tell them this. And I think the Federal Trade Commission would be 100 percent behind this. You have to let the consumers know the nature of the risks they're engaged in when they're doing business with you. And it's not always an easy thing to be honest, but it's the right thing to be honest. And consumers are often very understanding when they see that something is not going right because, guess what, it's not going right everywhere.

So our urge to our clients when they can't afford the preventive measure is to say just be frank with your consumers and business partners, let them know what's happening or you're going to just make

things worse for everybody.

MR. JORGENSEN: We have seen a driver towards implementing solutions, though, that have been on the table for a long time, too. And I think everyone here has touched on some of those solutions. And recently, though, I think the driver to implement those solutions has gone up, and it's really raised the level of awareness up to leadership, because where you used to have to argue about multifactor authentication and somebody would say, well, you know, it's only 10 percent of our users are accessing remotely, therefore, the risk is small.

Now with 100 percent of users accessing an environment remotely, they're coming back and going, oh, okay, well, I've accepted that risk for years because I thought the risk was small. Now, I understand that it really is large and I need you to implement it in the next 15 days. And suddenly they're willing to have that workforce impact and willing to deal with some of those controls that I've talked about, information governance and limiting access to data and testing those choke points and making sure that if people are accessing things remotely, what do they have access to, and making sure that they can't get to the entirety of the data set.

65

And adding those controls in has, I think, increased because of the pandemic response.

MR. LINCICUM: Great. We are just about out of time, but I wanted to ask one last question. And if you all could take about a minute answering a fairly big question, but, you know, as best you can.

We've talked about how information security is very particular for each company. It's going to have different needs. But are there some information security practices that are just so universal and so easy to implement that they should be just considered absolutely required if you were handling sensitive information like financial information?

MR. CRONIN: Go ahead, Pablo.

MR. MOLINA: Chris, after you, please.

MR. CRONIN: Okay. Because I'm probably going to say what you were saying because you've been saying these things, too. I'm going to take a step back and say let's not talk about each control that should be expected because our risk analysis is going to show us how to apply those things differently, in different ways.

What I will say is you find the security control standard that looks like it addresses the risk that you've got in your organization and apply those

66

controls the best you can. And where they're difficult to apply, you do a risk analysis to see whether you can accept the risk or whether there are alternative controls that provide you the security safeguards you need.

So those are the two things I say are universal, a standard of care and a risk analysis where you think of yourself and others and put the risks in balance.

MR. MOLINA: So I believe that cybersecurity is a little bit like human behavior in general. It works better when you follow principles. So if you do a principle-based information security, you know the old standards we've been proposing from the OECD and many other forums for many years: privacy by design, security by design, something the FTC is very strong about in enforcement, which I call hon-tegrity, honesty and integrity, meaning do as you say, say as you do so that you'll be transparent and consequential in your actions. Things like encrypt in motion, Encrypt at rest.

You know, things like encrypt in motion, encrypt at rest, always there are general things. And then from there you can draw into the specific controls that tells you, you know, security awareness

67

for your workers and your constituents and, sure, firewalls and protect the credentials with multifactor authentication. There's a plethora of different controls. But if you act with a few guiding principles, it's going to help you align all of your efforts into some really impactful measures.

MR. JORGENSEN: I think one of the challenges as we try to answer that question is -- it was embodied by Chris and Pablo's response of, hey, you have to look at the big picture. And certainly it would be easy to say, yes, multifactor authentication; yes, change your password.

Something I saw as early as two weeks ago, one-two-three is not an acceptable password in 2020. But if you really scale it up for a moment and said, okay, how am I going to look at identity and access management, and so then access to what, and the data privacy and the implications of the data security and data privacy around that access becomes a focal point.

So are there controls that are so basic that you should have in place? Yes, I think we've covered them here. But the problem is that those controls may change over time and it's the controls that give access to what then becomes part of that challenge. So if I have remote access into the keys to the

68

kingdom, then those controls that are so basic and you have to appreciate that I can't have an open cloud storage bucket or a database that's public-facing. So those are those really basic controls and security that should be in place. But it's hard to say specific for what without that risk analysis that Pablo and Chris were just talking about.

MR. RUBIN: Yeah. And I agree with everything that's been said here, and that is the driving kind of basis for risk assessment. So I think instead of, like, prescriptive controls, you know, because of the changing threat landscape and all the variation in organizations, it's helpful to think of things a little bit more conceptually, which in a way -- not to kind of plug this too much, but in a way it's what the -- it seems like the FTC Safeguards Rule is trying to do when it's saying things like you have to have governance. Like, that's just a fundamental part of an information security program which, believe it or not, a lot of organizations don't do.

You have to have a program, which is, again -- it sounds like basics but that's what we're talking about. You need some people that are experts to help you out, whether it's to perform the risk assessment or to perform the technical, you know, security operations. You need to protect your sensitive information, which means you need to know where it is, what it is; you need to have identity and access management around it; you need to educate your people about what the risks are and what the threats are that your organization is facing. You need to protect your organization in an ongoing basis with ongoing monitoring, and you need to be cognizant of your third-party risk.

I think those things aren't prescriptive controls and are more kind of just baseline fundamentals that will change depending on time and threats.

MR. LINCICUM: It looks like maybe we lost Sam, or maybe everyone. Hopefully not. I want to -- oh, everyone else seems to be there. Well, that was unfortunate for Sam but fairly well timed in that we are out of time.

I really want to thank everyone for your time in both being on this panel and helping us prepare for it. It was immensely valuable. And I want to thank everyone for giving us some time watching it.

We'll be taking a short break now and the next panel will be at 10:45, about information

security and smaller businesses. Thanks, very much. Have a good one.

MR. JORGENSEN: Thank you.

MR. CRONIN: Thank you.

(Whereupon, a recess was taken from 10:32 a.m. to 10:47 a.m.)

INFORMATION SECURITY PROGRAMS AND SMALLER BUSINESSES

MS. MCCARRON: Good morning. Welcome to the second panel of the GLB Safeguards Rule Workshop. This morning, we're going to be talking with five experts about information security programs and smaller businesses.

I would like to introduce the five panelists who will join me this morning. If you could all please just wave or acknowledge when I introduce you. I would like to begin by introducing Rocio Baeza. She is the CEO of CyberSecurityBase. She's joining us this morning from Chicago.

Next, James Crifasi. He's the COO and CTO of Redzone Technologies here in the D.C. area.

Brian McManamon is the president of TECH LOCK, and he's joining us this morning from Troy, Michigan.

Kiersten Todt is the managing director of the Cyber Readiness [microphone feedback].

And, finally, I'd like to introduce Lee Waters, who's the IT manager of McCloskey Motors, joining us from Colorado Springs, Colorado.

My name is Katherine McCarron. I'm an attorney in the Division of Privacy and Identity Protection at the Federal Trade Commission, and thank

you very much for joining us.

I'd like to begin by picking up from where we left off on Panel 1, where we talked about the costs and benefits of information security programs. As part of its public comment, in the first round of the GLB Safeguards Rule's proposed -- comments about the proposed amendments, the National Automobile Dealers Association provided a technical cost study as part of its comment. It was entitled the Average Cost per U.S. Franchise Dealership, because as we discussed earlier, auto dealerships are financial institutions under the GLB Safeguards Rule and must comply with the Safeguards Rule itself.

I'd like to begin with speaking with James Crifasi. James, you're an IT service provider and you did some work on this cost study. What can you tell us about the requirements the study assumed and its conclusions about the costs of those requirements?

MR. CRIFASI: Sure. So Redzone Technologies helped NADA with portions of the study. NADA looked for really costs across a number of different shapes and sizes of dealerships. They also got real vendor quotes from those specific dealerships to figure out what is it currently costing them to do these safeguards; what would it cost for a new provider to do them, or for their existing provider to add the level of service required.

We can see from the numbers that they're really quite large. And what we're noticing here is that from a small/mid-sized business point of view, they start becoming a little bit unaffordable here. The cost structure that was used is actually quite conservative. There's a couple of things that aren't even considered within the study.

So, for example, the need for additional staff is not part of this study. In our experience, in working with small businesses, there's a great deal of bringing systems to a current level of operation required before you could even make use of these safeguards or the technologies required to adhere to them.

So those auxiliary costs are really not within the study at all. Our belief is that based on this study, really it will be probably double or triple those costs to really get the value out of implementing the different safeguards. I mean, it's one thing to be able to say, you know, we've checked the box, we put the system in place. It's another thing to actually get the value out of it.

I know in Panel 1 that was something that

was talked about a lot is not just have an expensive firewall or not just have an expensive audit system, but actually use it and make sure it's effective and useful on a daily basis.

MS. MCCARRON: As a follow up, James, where did you see -- when you were doing this study, where did you see existing security in financial institutions falling short of the proposed amendments? And where were there already resources in place?

For example, the current rule, the current Safeguards Rule, which the automobile dealerships comply with, requires financial institutions to have people in charge of their programs. And so can businesses use existing personnel as the qualified individual responsible for the program?

MR. CRIFASI: I think from what we've seen, they definitely can. What is important, though, is it needs to be a team effort. So not so much a specific, single individual, but when we're talking about a small and medium business and, you know, there might be a very small IT staff or potentially almost no IT staff for the business, we really need to see that “qualified individual” be a mix of folks. Sometimes, it's going to be someone on the operations or finance side; possibly outsourced consultants such as us or

one of the other panelists. You know, that kind of team effort is what's really important to have the smaller businesses able to do that kind of qualified individual task list.

There's one level where, you know, there's advice needed that is coming from someone experienced in security, but there’s another requirement for enforcement. And that enforcement is really where we need a team effort.

What we've definitely found is that if the business is not involved and this is considered an IT project, the effectiveness is going to go way down. And so really all of the business needs to be on board with implementing these safeguards.

MS. MCCARRON: Thank you very much.

I would like to pivot now to asking Lee Waters. Lee is an IT manager at an automobile dealership in Colorado Springs and he has implemented the existing GLB Safeguards Rule in his business.

Lee, I’d like to ask you how much would it cost your dealership to implement the proposed amendments to the GLB Safeguards Rule?

MR. WATERS: Well, we started by looking at the costs for hiring outside help, the CISO and the cybersecurity analyst. And we’d be looking at on

average in our area about $180,000 for a chief information security officer; another $76,000 for a cybersecurity analyst. If we outsourced the work that these two people would do, we would still be looking between $120,000 and $240,000 a year.

On top of that, we’d have to implement multifactor authentication; looking at about $50 per computer to implement something like that, or we could go with an outside resource like Duo, which would cost us about -- between $3 and $9 per user per year. And with our dealership, that's about 55 users.

So we also have to implement annual penetration testing. If you do a search on Google, it says average cost is about $4,800. I called a local cybersecurity company that I’ve dealt with in the past. For their external test, we’d be looking at $2,160. For an internal test, which is based on the number of computers we actually have, we would be looking at $7,360 per test.

We would also have to update our physical security. We’d be looking at about $215,000 for extra construction to enclose existing cubicles and build offices for desks that are out on the showroom floor.

MS. MCCARRON: Thank you, Lee, for providing this detailed information.

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

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

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

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

In TECH LOCK's experience, most companies do

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

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

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

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

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

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

MS. MCCARRON: Thank you.

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

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

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

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

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

MS. MCCARRON: Thank you.

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

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

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

81

MS. MCCARRON: Thank you, yeah.

MS. BAEZA: Awesome. Well, first of all, I just want to say thank you so much for having me on the panel. So there are two slides that I want to share. If we can go to the first slide.

So when I think of cost models being available to small businesses, so these are the three models that I see. And for context, so CyberSecurityBase is in the business of serving chief compliance officers in the fintech space, and we are specialists in the online payday lending space, so my perspective is coming from that direction. So as we're thinking about, all right, how are small businesses that don't have -- don't currently have a CISO in-house and they're not expecting to appoint one in the next two to five years, how can they possibly conform with the proposed changes?

So there are three models that I would want to point these individuals to. The first model is one where an existing member of the team is wearing the CISO hat. Now, I would expect that this individual sits in the compliance space of the organization and they're bringing in internal teams. So, for example, technology teams to supplement and to help develop and implement the program. And for any areas where there

82

may be skill gaps, that can be supplemented with either certifications or some type of education.

For the outsource model, so think of the situation where a small business is going to engage as a risk provider like CyberSecurityBase to wear the CISO hat.

And the third one is going to be a hybrid approach. And I think this is going to be the best fit for small businesses. So think of the case where someone internally is accountable and is wearing the CISO hat and they are pulling in internal resources and external resources as needed. And these researchers are going to be be pulled based on the preferences of the organization. Access to talent, timelines, any specific projects that have a specific deadline, and, of course, budget.

So if we move on to the next slide, so we have some sample pricing for what some of these options might look like. And I've got to say, so when we're working with our clients, so they tell us that they love being able to to have a mixed and matched approach, having a hybrid approach where they may engage with us to provide say, for example, strategic direction, implementation support or outside assurance.

83

So what we're looking at here is this is a table that has sample pricing for service providers that are in the market today that small businesses, that fintechs can tap into and comply with the proposed changes.

So we have company A, they are app sec focused. They have a security-in-the-box solution, and they have a number of offerings depending on the level of support that the organization may need. We have an MSSP that, based on the size of the organization, they have different price points.

And CyberSecurityBase, so we offer the CISO service as a professional service, and we also have pricing available to fit part-time virtual CISO support. So as you can see here, we have a range of $200 a month estimate to $15,000 a month. And, to me, this paints a positive picture that there are different options in the marketplace today. And I expect there to be more once the proposed changes are finalized.

MS. MCCARRON: Thank you very much, Rocio.

Brian, I would like to ask you as well. Can you talk us through your understanding of what the different options are for smaller businesses?

MR. MCMANAMON: Sure. And I think there was

84

a slide that I'd like to show that represents those costs. Coming from what we've just heard, TECH LOCK provides these services from both an in- and outsource prospective as well as a hybrid prospective. We do need that -- or we think it's important to have that internal skilled security resource that can help implement a lot of the elements of a security program.

So what you see here is sample pricing that TECH LOCK provides to our small/medium-sized business customers, all the way from -- if you see, the range there is starting with small at 25 to 250 endpoints for $2K to $5K per month. A medium-sized business we would designate as 250 to 750 endpoints for a $5K to $15K a month; a large, 750 to 1,000 endpoints at $15K to $30K; and then finally a very large organization can be anywhere up to 2,500 endpoints and up to $50K per month.

The type of services that TECH LOCK provides, and if you look at the revisions to the Safeguards Rule, some of the key elements of that rule is really around continuous monitoring, being more proactive with potential threats. So some of the services that we provide that address those issues are related to vulnerability management, endpoint detection and response, network and firewall management, log-in SIM. And what's key there is all on the back end we're providing 24/7/365 monitoring. So it's that continuous monitoring to make sure that you can not only detect those threats but also respond to them very quickly.

And what TECH LOCK feels is this provides really a holistic and comprehensive view of satisfying the key elements of a strategic security program. And if you compare those costs that I just showed to the cost that a small/medium-sized business would have to pay, they brought that technology in-house, those resources and staffing in-house, you'd be looking at multiple six figures, I think, as you saw earlier in this panel.

MS. MCCARRON: Thank you. Now, one of the questions that the Commission has sought feedback and comment about is the definition of a small business.

And in the proposed amendments to the Safeguards Rule, the Commission has suggested that in order to reduce the burden on smaller financial institutions, the proposed amendment would contain a new section that would exempt smaller businesses from certain requirements.

The exemptions would apply to financial institutions that maintain customer information

concerning fewer than 5,000 customers. Such financial institutions would not be required to have a written risk assessment. They would not be required to conduct continuous monitoring or annual penetration testing and biannual vulnerability assessment. They would not have to have a written incident response plan in place, or have a written annual report by the CISO.

So, Kiersten, as a threshold matter, the Commission seeks comment on whether the use of the number of customers about whom a financial institution retains customer information is the most effective way to determine whether financial institutions should be exempted, and, if so, whether 5,000 customers is the appropriate number. So would you share with us your thoughts about the definition of a small business?

MS. TODT: Sure, Katherine. Thanks very much. And thanks also for the opportunity to participate.

Just to understand the position from which I'm coming, I run a nonprofit called the Cyber Readiness Institute, which works with small businesses in helping them improve their cybersecurity by focusing on human behavior.

So I think there are really two questions at

play here. The first is what you asked around what the definition of a small business is for this purpose, and what that definition fails to acknowledge is that regardless of size, every small business is part of a global value chain/supply chain under the safeguard rules that we're talking about.

So to make that demarcation, I think, is not actually appropriate because it doesn't allow or account for the fact that every business has a role. The challenge there, however, is that you cannot put -- if you focus so much on the technology, I'd like to go back to a couple of the points that James made, which is particularly for small businesses you have to focus on the culture. And when you don't have the resources to allocate and bring in a CISO, and I think Rocio had walked through a lot of the different versions that we can use and I think that's important, it's recognizing that small businesses have to do the basics, and a lot of that really focuses on human behavior. That ability to do the basics and to do cyber hygiene should -- no business should be -- not be accountable for doing that. Every small business should have to do that.

But we also have to make sure that in providing guidelines, while we may be able to provide

very rigid guidelines for security, if small businesses are then forced to do workarounds and don't actually have the ability to follow them, that creates an -- even more of an unsafe environment.

So to answer your initial question, I don't think there should be a number on this. All small businesses should be responsible for doing the basics, but we have to really focus on the culture of security and the human behavior element, particularly for small businesses that don't have the resources to allocate to some of these more technological requirements.

MS. MCCARRON: So, in your opinion, is such an exemption appropriate at all, or should all financial institutions regardless of size be required to comply with all of the proposed amendments?

MS. TODT: I don't think size should be a matter, but I don't think that the required amendments really are appropriate for all small businesses. So I think that all small businesses need to be held accountable, but we need to work with small businesses to help them and to provide resources that focus on human behavior.

So I'll answer it in two ways that we should not -- no small businesses should be exonerated. But the rules need to be more flexible to address the

89

cover and the range of small businesses.

MS. MCCARRON: Okay, thank you.

Brian, a follow up question: How does the size of a financial institution and amount and nature of the information that they hold factor into an appropriate information security program?

MR. MCMANAMON: Yeah, I would agree that, you know, just to chime in on the last question, I think there are a minimum set of standards that need to be adhered to by small businesses. The way TECH LOCK views businesses and the way we scope the work that we do is based on number of users, number of endpoints, and then also number of sites and what their processing environment looks like.

So if you think about, you know, servers, workstations, laptops, the network footprint, any of those elements in an organization’s environment may introduce a threat into that environment. So you have to look at that total threat landscape.

From a data prospective, you know, when we do audits on, for example, PCI or high trust, we follow that data, right, all the way from the -- where it comes into the environment and to how it’s protected at each step, whether it's storage or processing all the way through to the back end. So

90

data does come into play in terms of size.

And if you were to compare, for example, to how PCI judges the size of an organization, you know, they do it based on level of transactions that a PCI data processor would process annually. So, you know, for example, over 6 million transactions, it would be designated that they would need to have an audit by an external auditor. Very small businesses would just have to go through what they call a self-assessment. But the issue that TECH LOCK has seen with those self-assessments, it’s more of checking the box. Right? And that’s what we’re trying to avoid here. We want businesses to really go through that internal risk assessment and make sure that they are implementing the appropriate security controls for their environment.

MS. MCCARRON: Lee, I’d like to follow up with you about the issue of the size of a financial institution and the nature of the information that that financial institution holds, as a factor, into the appropriate data security program that they put into place.

Can you tell us from your experience whether it's the number of employees or the number of customers that you keep data about that’s relevant to

91

to your business?

MR. WATERS: Well, I don't think the type of data really makes much difference as an attacker is just going to go for something easy that he’s going to get a lot of information from. So the amount of data would definitely have an influence on whether a business is even going to be attacked or not.

The number of employees can also introduce other risks. The more employees you have, the greater you are at risk for either inside attacks or just social engineering. So you have to be prepared for pretty much everything from all sides.

MS. MCCARRON: James, how do you view the risks of how cybersecurity events change based on the size of a financial institution?

MR. CRIFASI: From our point of view, it’s the point of view of the risk that changes, but we consider it pretty much equal risk. We have some small businesses we deal with that just have an enormous amount of consumer records, and so they might have a few number of employees or a few number of endpoints, but the amount of data available there is just quite vast. And so from that point of view, we would say, okay, they need to follow all of the safeguards, right? Because they just have such a

92

massive amount of data, they can’t get away with just doing the basics.

On the flip side of that, we see small businesses where really they just need to focus on the basics. I know in Panel 1 they talked a lot about doing risk assessments and assessing what data is there, where it is and how it is. And there’s a point of view for a small business that says if they get hacked at all, it doesn't matter if they lose employee data, financial data, consumer data, they’re probably going to go out of business.

So there’s a shift to me that says that when we look at a small business and we look at something like the safeguards, that doing the basics, or as Kiersten mentioned, changing the culture and making sure people are getting educated and understand security becomes more important, because really they can assume the level of risk, they can assume that at some point they will get an intrusion or malware or ransomware. And there’s a lot of money that can be spent better doing proactive security against these types of attacks or cyber hygiene versus measuring a risk when really we can just assume it in most businesses, especially on the small/medium size.

MS. MCCARRON: Thank you.

Kiersten, what is your view about how risks of cybersecurity events change based on the size of the financial institution?

You're on mute.

MS. TODT: You still do this after three months of Zoom. I still think that the smaller the business, the more impact it can have. So one of the things that one of our member organizations, Mastercard, has researched is that 56 percent of organizations can suffer a breach by a third party, meaning that there is a greater attack surface. Sixty-seven percent of small businesses fail to survive a cyber breach.

And so when we look at these numbers, we understand that there is a much smaller, if any, safety net for small businesses. So the impact of a breach, the impact of an event, can be much more devastating. And that's why when we talk about prevention, we're also talking about resilience. Because what is so important -- and this is going back to your other question, why every business needs to have basic protocols in place, because you don't want a breach to be devastating and to actually take down the business.

By focusing on resilience, what we're doing

then is minimizing the impact of an event, containing it, and ensuring that it causes the least amount of disruption to that small business. And so as we look at overall cybersecurity protocols, it's really critical that we both focus for small businesses on prevention and what they can do, but also helping them to respond and react, which is why instant response plans and those others elements are the basics for all small businesses to be engaged in.

MS. MCCARRON: Thank you.

Rocio, do you have thoughts on the risks of cybersecurity events, how that changes based on the size of the financial institution?

MS. BAEZA: Sure. So I think size of a financial institution is a factor, but I don't think it's the one that we should be paying attention to. I think the ones that are better indicators for cybersecurity risk are going to be two things: the volume of consumer records that a financial institution holds and also the rate of change.

So in the fintech space, it's awesome. They're using technology and data to disrupt the industry and provide services that haven't been feasible in the past. And so there's a number of integration points, right? So take the case of an

online payday lender, we should expect them to have an LMS to process loan applications, connections with data vendors, and maybe an outsourced consumer function, payment collection processing activities. And then there's also services and IT systems that the corporate teams are using to leverage the data and the technology to better serve the consumer.

So, to me, because we have this web of applications and systems both managed in-house and outsourced, every time there is a change to any of these environments, that is creating additional risk. And that's elevated as we're seeing if the institution is processing large volumes of consumer data.

So I think size of the financial institution is a factor. I think the more critical ones are the volume of consumer data that they hold and the rate of change within their data processing environment.

MS. MCCARRON: Okay, thank you.

I'd like to move to a new topic, which is the requirement in the proposed amendment that there be reporting to the board of directors. And I'd like to talk about this from the lens of a smaller business.

The proposed amendment would require the CISO or the qualified individual to record in writing

at least annually to the financial institution's board of directors or the equivalent governing body regarding the following information: the overall status of the information security program and the financial institution's compliance with the Safeguards Rule and material matters related to the information security program addressing such risks such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations, and management's responses thereto, and recommendations for changes to the information security program.

So for for financial institutions that do not have a board of directors or equivalent, the CISO must make the report to a senior official responsible for the financial institution's information security program.

Kiersten, the Commission requests comment on whether the burden of this risk reporting requirement outweighs the benefits of, number one, having the governing body engaged in and informed about the state of the financial institution's information security program, and, two, creating accountability for the CISO. So can you comment on that? And, also, if you think the written requirement should have other requirements, please let us know.

MS. TODT: So I certainly think engagement with any sort of senior leadership, whether it's a governing body like a board or a senior executive on security, is critical because this is not, as was mentioned earlier, security, cybersecurity, should not be restricted to one individual, to an IT department, to an IT person. It really is now the responsibility and accountability of every individual within an organization to have an understanding of his or her role in security.

So creating that culture, again, and having that reporting requirement makes sense. But I would like to adjust that word around reporting. It should be a conversation. It should be a discussion and ongoing -- I would argue that it should happen more than once a year because this -- while there is an accountability within an individual, again, the organization has accountability.

So we're discussing this with a senior executive. That senior executive has accountability for the security of the organization. We've seen a lot at the senior level where -- we saw it in the Federal Government with the OPM breach where the director at the time said it was no one's

responsibility.

What we have to get to in changing that culture is that it's actually everybody's responsibility. And so having requirements to update on what's going on on the number of breaches, on how things are being responded to, where the challenges are, that should be an ongoing discussion. And if the catalyst for that is a reporting requirement, I think there could be value in that, but it is not just a static written report.

I would assert that it has to be a discussion. And it's not a one-way discussion; that it is about getting leadership involved and that hopefully there is a relationship between the CISO and the board or -- and the senior executive that allows for improvement, that allows for adjustment and evolution, because with cyber risk management, the key here and the priority should always be agility and flexibility to evolve with the threat.

So the concern sometimes is when you have compliance -- most of the time when you have compliance requirements, they often can't keep up with where the threat is going. And that's why risk management, when it comes to an organization of any

size, is critical.

MS. MCCARRON: I'd like to ask a followup to Rocio on this one, which is speaking of the communication between the CISO and the board, should the board have to certify compliance with the rule?

MS. BAEZA: So I think that an annual report to the board and then having the board report or perform some type of certification, that can be used as a way to ensure organizational accountability and also accountability for the CISO. But I think that if either of these two items, the annual report or the certification, if they don't have the proper guardrails I can see it quickly turning into a burdensome administrative test that outweighs the benefit of what we're trying to accomplish here.

So I think that in order to have effective mechanisms, let's talk about the annual report first. So if we're setting expectations for a 40-page document to be presented to the board on an annual basis, that's not going to be effective. Instead, if we consider using a one-pager that summarizes the items that are in the proposed changes, things like the status of the program, identified high risks, previous management decisions to identify the high risks, and using that to funnel information up to the

board so that they can say, yes, we're comfortable with the program or, no, we're not comfortable and being able to articulate between the board and the CISO what that comfort level is, what that risk tolerance is, I think that can be a great way of raising organizational accountability and also accountability for the CISO.

Now, if you think about the certification, I think that if the certification piece isn't worded carefully, it's going to be an administrative burdensome task. So if the question -- if it's one question that someone from the organization has to submit so you can comply with the Safeguards Rule, do you comply with the privacy rule, that's a very generic question. So we have to be very specific.

Some examples are instead of asking a very broad, generic question, let's get into specifics. So on the risk assessment side, the question -- so these would be yes-or-no questions. Do you have a written risk assessment, yes or no; when was it last completed; what's that date; when is the next scheduled risk assessment scheduled for; very good specifics.

The thing about the case of a third-party vendor, there's an expectation to oversee service providers, making sure that they can develop and maintain safeguards. Well, there's going to be very concrete questions. Do you have third-party data inventory? When was it last reviewed? When are you going to review it next?

And by having a different structure around the certification and also the annual report requirement, they can set up guardrails so that the organization is providing meaningful information. It's very specific. And I think that that will be a more effective approach of raising organizational and CISO accountability.

MS. MCCARRON: Thank you very much.

I'd now like to turn to two of the requirements of the proposed Safeguards Rule that are specific to the technologies or the types of information security protocols that are put in place.

The first one is multifactor authentication. The proposed amendment would require financial institutions to implement multifactor authentication for any individual accessing customer information. Multifactor authentication, according to the proposed amendment, shall be utilized for any individual access in your internal networks that contain customer information unless your qualified individual or CISO

has approved in writing the use of a reasonably equivalent or more secure access control.

Brian, I'd like to ask you for your comments on this approach to requiring MFA for any individual accessing customer information in an internal network.

MR. MCMANAMON: Sure. Number one, you know, TECH LOCK fully supports this requirement. It is absolutely critical that organizations have multifactor authentication in place for accessing their systems or any of their applications.

To support that, TECH LOCK has implemented MFA for a number of our small/medium-sized business customers. The product that we normally use and we resell is Duo. So what I've done is pulled some pricing from Duo's website just to get an idea of what it would cost a SMB to implement.

As you can see there, there's four different categories of cost all the way from free for up to 10 users to $3 per month. And what that adds is some additional security policy checks. $6 per user per month is the most recommended that has more robust device trust checks in place; more robust policy enforcement, and then all the way to $9 per use per month. That's their premium subscription that has the most robust device trust checks. It also provides

application policy enforcements. And then you can implement single sign-on for some, their access to internal corporate resources.

MS. MCCARRON: Thank you very much for that information.

James, I'd like to ask you as well for your thoughts on the proposed amendments requirement that financial institutions shall use multifactor authentication.

MR. CRIFASI: Our point of view is we fully support multifactor as well. When we're pulled into an environment that has had some kind of security incident or data loss or ACH wire transfer fraud, so far in the last, say, 12 to 18 months every single one would have been stopped by having basic multifactor authentication.

So from our point of view, it's a good basic business practice at this point regardless of the Safeguard Rules or PCI or any other requirement. It's just a good business practice to have, just to protect the internal information as much as it is to protect the company's own internal information as much as it is to protect their consumer information.

I think the one thing that we see that becomes an issue is, you now, simply buying a

multifactor doesn't really give you a solution there because you have outsourced dealer management systems or loan management systems and you need to make sure the multifactor will actually take care of all of the service providers as well as remote access into your environment.

So I think flexibility there is really important. But at the same time, the definition really needs to encompass all of those kind of auxiliary and external providers, some of which we know from helping a lot of customers, they won't support it. You know, the dealer management system or associate management system, or core banking system, they won't support the multifactor.

And so we, as security technologists, we have to come up with an alternative method to secure that high-risk area. And it is available, it is possible, it's things that can easily be done. Those service providers don't always like it, but it's a lot cheaper than, let's say, telling a small business go change out the dealer management system that you've used for the last 20 years. The cost on that is going to be much more than that business can, you know, adapt to.

So I think multifactor is great, but we need to really consider those third parties and service providers in scope of that requirement.

MS. MCCARRON: A good point, thank you.

Now I'd like to turn to encryption, which is the other specific callout in the proposed Safeguards Rule -- amendment to the proposed Safeguards Rule.

The proposed amendment would require financial institutions to protect by encryption all customer information held or transmitted by you both in transit, over external networks and at rest.

To the extent that a financial institution determines that encryption of customer information either in transit, over external networks or at rest is infeasible, the financial institution may instead secure such customer information using effective alternative compensating controls reviewed and approved by the qualified individual or CISO.

So, Rocio, I'd like to begin with you, please. Could you please share with us your thoughts about this requirement of encryption both in transit or at rest.

MS. BAEZA: So, I'm a big fan of this specification. So as a data privacy advocate, as a provider of information security services, I welcome the changes. I think that there is room for

misinterpretation by an untrained professional that might be tasked with implementing this.

So, take, for example, if I were to ask a CEO or a chief compliance officer, does your company encrypt consumer data, they'll probably say yes. If you ask that question to a system administrator or a software developer, they're going to be asking -- they should ask -- what environment are you referring to, what systems are we talking about, and then are we talking about data in transit or data at rest. Data in transit, the encryption of data in transit has been standard. There's no -- there's no pushback with that.

The pushback that I tend to see from service providers and partners is when we're talking about encrypting data at rest. And I think that the specificity is important so that whenever we're having conversations about encryption, regardless of what our technical background is and what our idea is around encryption -- the encryption of data that we can't see, I think we're going to get to a path where there's more consistent application and understanding of the requirements, and that's what will ultimately lead to comprehensive application of IT security controls in the environment.

In the online payday lending space, so we have a number of players, right, a number of systems. And the question around encryption, it really applies to every single path that you can think of where a system is talking to another system, where data is going back and forth from one vendor to another or where data is going back and forth from a human to a human.

So the only way that this proposed change can be effective is if there's particular language to make sure that we're expecting this to be comprehensive; not just the critical application that the organization relies on but the whole data processing environment.

MS. MCCARRON: Thank you.

James, I'd also like to ask for your view on the encryption requirement.

MR. CRIFASI: So I think specificity is really the key there of what data are we talking about, where, and how you want to encrypt it. So as an example, there was a study that said three-quarters of all phishing sites operate under SSL. So that's encryption in motion.

And in doing that, they all hide from all the great security stuff that we like to give people

and that everyone thinks is good, basic cyber hygiene. So it's a good example of how encryption in motion can be completely misused.

We have a small insurance company we're working with right now who their service provider misunderstood that and they're now trying to over-encrypt, I would say, the communication between their servers and their computers that are all sitting right next to each other. As a result of what they're trying to do, though, it is now invalidating three or four different levels of security that used to be able to see and do something about the data, and now it can't because it's hidden in this encryption tunnel.

And so for us, while we like the idea of encryption at rest and in motion, it really has to be well defined and it needs to be defined to the point where, you know, folks like us don't have to explain to people what does it mean, how does it work and what does it look like. It needs to be very, very detail-oriented in terms of we're talking about information that's perhaps not in a secure environment, or to Rocio's point, the system interaction is really a key place. But we have to keep in mind, the more we encrypt, the more we rob visibility and purview from our security systems that might actually reach out and take action.

So at one point we're encrypting it, but at the other point we're potentially stopping our DLP from blocking that from getting out of the environment. And I think that's a key point of contention there between a desire for encryption and a desire to actually have proactive security that's able to do something useful. So specificity, to me, is really required in that rule before it should be really applicable.

MS. MCCARRON: Okay, thank you. So we have about 10 minutes left. We have a question that has come in from the audience which I'd like to pose, and then whoever would like to answer this just please raise your hand and go for it. And then after that, I would like to have some wrap-up thoughts from all five of you.

Okay. So the question from the audience is small- to medium-sized entities have diverse management structures and often take a team approach to security management. Are there alternatives to naming a single responsible individual and/or annual reporting to the Board that would help establish clear lines of responsibility and accountability among the team required to lead security?

So they're looking for your thoughts. And, Kiersten, I'd like to have your thoughts, please. What are the alternatives to a single responsible individual and/or reporting to the board that would achieve the goals of responsibility and accountability.

MS. TODT: I think it's a great question because it really gets at this issue of, in a perfect world it would be wonderful to be able to identify a CISO for every small business to say all of the responsibility for cybersecurity rests within this individual and everyone can go about and do what they've been doing. But that's not really the reality that we live in anymore. The idea, again, that every employee has this responsibility. And I think a team approach particularly for smaller businesses is what is more viable.

Again, we don't want to create rules and regulations that do not respect or recognize the challenges of these small business environments. So we're not actually helping the small businesses but we're challenging them to do more with limited resources.

And so by creating a team, it's where you have to then identify and articulate specific

responsibilities to individuals that come together. And I think one of the key advantages to this type of approach is it does create that culture of everybody has a role within the organization, whether it's toward the Safeguard Rules, but I would argue it should just be for the basics in cybersecurity first. Then you are creating that culture because you have the responsibilities distributed across the organization.

And as far as the accounting requirements, you always want to make sure that you are exchanging with your leadership, whomever that is. And oftentimes in small businesses we see that a leader can have multiple responsibilities. But the idea here is to have that exchange of information so that there is an evolving sense and growth toward a more cyber-secure environment.

MS. MCCARRON: Okay, thank you.

And then one last question from the audience. How does it, or should it, change the analysis of the cost and benefits of a vendor relationship if the financial institution must address multiple legal and regulatory regimes?

Rocio?

MS. BAEZA: The way we do that is by

harmonizing. And it's going to take work and it's going to take resources and manpower. So many fintechs have this challenge. They operate in different states. They are subject to state-specific law that are a lot industry-specific expectations around security. For example, PCI DSS.

MS. MCCARRON: Mm-hmm.

MS. BAEZA: The only way that you can be comprehensive in meeting your security requirements across the board is through a process of harmonizing what all the requirements are. And that takes work and effort and resources. And it's an important job that has to be carried out. That's the only way that you can do that.

MS. MCCARRON: Okay, thank you.

So now I'd like to go to the final question. I'd like to do a speed round of your thoughts on the proposed amendments to the Safeguards Rule from the perspective of a small business.

So let me start with James. James, could you tell us what -- from the perspective of someone who works with small businesses, what do you like about the proposed amendments and what do you think you don't like or that have too many costs? Thank you.

MR. CRIFASI: So, obviously multifactor authentication. We like the fact that it's in there and it's universal. We strongly believe in that. I think from the point of view of things we don't like about it, the written requirements, what we don't like about that isn't that there are written requirements. What we don't like about it is that it robs people of the ability to interact.

And so as an example when we talk about having one individual that's responsible, it kind of implies that everybody else is no longer responsible because you found one person who is now the scapegoat. And so what we find in the small businesses if we go in and we read someone's board report and it's 40 pages of gobbledygook about how they compare against all of these different things that they need to do for different states and we look it, it's very bloodless. It's very political. There's no material in there to actually effect change.

What we find works a lot better is to have that be an interactive discussion and actually open it to be able to talk about what are people doing well, what are they doing poorly, and how can we change that. And I think that brings them more into a culture of effecting change from a security point of

view. It gets everybody enlisted with it. And so from the safeguards statement, you know, I wish it was a little bit more oriented in that manner.

MS. MCCARRON: Okay, thank you.

Brian, may I turn to you next for your -- speed round of your thoughts?

MR. MCMANAMON: Sure. Yeah, and I'm going to talk more about, you know, what I like versus what I dislike. I think the proposed changes are the minimum necessary to have an effective security program in place. And really starting with the annual risk assessment, I think that's a great place to start for small/medium-sized business, really understand the risks. And we've heard about that in these panels around people, process and technology and really understanding what that threat environment looks like for that particular business.

We need to get beyond the traditional checklists that are out there and really create a flexible and adaptive security program. And the reason for that is because the hackers aren't sleeping. Right? They're constantly changing their methods and businesses, and their security controls need to change with those hackers' methods.

More specifically, I'm in agreement with the

implementation of controls around continuous monitoring and penetration testing. I think being proactive to those threats is critical. And then moving towards more of a maturity model is important for SMBs. That's what we're seeing from some of the scams that are out there from PCI to HITRUST, the upcoming Department of Defense cybersecurity maturity model. So really starting with that basic security strategy and then continuing to mature that over time is what will make SMBs more secure.

MS. MCCARRON: Thank you, Brian.

Rocio, I'd like to turn to you next for your concluding thoughts on the proposed amendment.

MS. BAEZA: Absolutely. So there's -- my favorite part is the requirement for a risk assessment. So the expectation that it's written and that it serves as a foundation for the information security program.

Two things that I don't like, I'm not a big fan of, one, I think it's missing -- the proposed changes are missing foundational elements that need to be in place in order to be able to build an effective information security program.

And I think James and Kiersten alluded to this with the importance of having basics and being

specific of what data we're talking about and where. So the basics that I'm referring to are expectations around having data asset inventory, a data inventory, a third-party vendor inventory, a data flow diagram. Like, we have to be very specific with what we're talking about. What data do we hold, where is it coming, where is it going? And I would love to see that be integrated either as part of the risk assessment requirements or as a foundational step that is -- that the risk assessment points to.

The other item that I'm not a fan of is the weak position that small businesses have as it relates to engaging service providers. So fintechs are able to move very fast because they're able to partner up with different third-party vendors to fulfill very specific options. But these third-party vendors have very canned terms of use. We're seeing less and less negotiations of agreements and more of this is our canned agreement, take it or leave it.

And, like, if you look at the liability limitations sections, it's right there. They're wanting not to accept responsibility, share responsibility for any security events that happen in the environment that they're making available. And, to me, that's a concern.

MS. MCCARRON: Thank you very much.

Kiersten, may I have your concluding thoughts?

MS. TODT: Thank you. So I think some of the key points that are positive are focusing on things like multifactor authentication. I believe that right now multifactor authentication should be a default. And my hope for something like the Safeguard Rule that mandates multifactor is that it now starts to encourage those companies that can offer it and make it a default but don't and leave it up to the user to choose to do MFA that you start to see incentives in the actual workspace and across industry for doing so. And I think that could be a very positive output from something like this.

The debate and the discussion we had on MFA versus encryption, I think, highlights why those two are not the same. And so mandating both of those is a very different -- it's apples and oranges. And so I don't need to repeat the conversation around encryption, but I think it is not -- they can't really be bucketed together and so we really have to look more closely at what we're asking small businesses to do.

The other piece is that a lot of what we've

talked about requires an outsourcing. And when we do that, then we have to really be able to help small businesses monitor and work with third-party vendors and outsourcing requirements to know what they should be looking for and what's required of those third-party -- those third-party vendors.

I mentioned earlier that 56 percent of our organizations suffer breaches caused by third-party vendors. So it's just enough to say, okay, if you can't do it in-house, then you should outsource it. We have to really provide that guidance and that specificity.

Now, to what I don't like, I think this is -- it's an interesting conversation that we've had because I know there's been support for this is great because it starts with a baseline set of requirements. I would assert, however, that I think that baseline is still very high for small businesses. I don't think it's actually at the ground level. I think that we're assuming that small businesses have a lot more resources than they have. And my concern there is that we then get into a checklist, and then you start to see noncompliance and you start to see costs for small businesses being driven very high in order to comply to all these requirements. And that affects

their competition.

And if we ask small businesses to do too many things, we run the risk of doing a lot of things not great and not really doing the basics right. And so I think going, again, to the drum that I've been beating in all of this is we really have to focus on the human behavior of the whole organization, getting those basics integrated and ensuring that by having a qualified individual that does not delegate and distribute and then relegate all authority and responsibility for cybersecurity.

We have to get out of the mindset that there is an individual responsible for security within an organization and get to that place while there might be somebody who's responsible for overseeing it, every individual within an organization has that responsibility.

MS. MCCARRON: Thank you very much.

Lee, I would like to give you the last word. Can we have your thoughts, please, on the proposed amendment?

MR. WATERS: I like the fact that we are addressing the security. But we need to also be careful not to overregulate it. Now, the smaller businesses, they can do a lot with the resources they

have, but when you start piling on too much and they have to start hiring outside businesses, third-party vendors or hiring overpaid security experts to handle something that's been regulated, it starts affecting consumer prices; it starts affecting the small business profit margins, and it's just not good for anybody. So we just need to find a balance here.

MS. MCCARRON: Very good. Well, thank you. It looks like we are out of time. I want to thank all of you for our time this morning. And thank you for sharing your perspectives and your expertise. We're going to take a break now and we'll be back with Panel 3 in a moment.

(Whereupon, a recess was taken from 11:49 a.m. to 1:01 p.m.)

CONTINUOUS MONITORING, PENETRATION, AND VULNERABILITY TESTING

MR. IGLESIAS: Good afternoon and welcome back to the FTC's workshop on the GLB rule. My name is Alex Iglesias and I'm an IT specialist at the FTC, and I will be moderating this panel on continuous monitoring, penetration testing and vulnerability testing.

Joining me on this panel are Thomas Dugas, who is the assistant vice president and chief information security officer and an adjunct faculty member at Duquesne University; Fredrick Lee, who goes by Flee, who is the chief information security officer at Gusto; Scott Wallace, who is a penetration tester at the Department of Homeland Security; and Nicholas Weaver, who is a researcher at the International Computer Science Institute and a lecturer in computer science at UC Berkeley.

This panel is going to discuss the proposed changes to the GLB Safeguards Rule related to continuous monitoring, vulnerability testing, penetration testing.

As David discussed earlier, the proposed rule would require information systems to include audit trails, to detect and respond to security

events. Second, the proposed rule would require policies and procedures to monitor the activities of authorized users and to detect unauthorized access, use of or tampering with customer information. Lastly, the proposed rule are continuous monitoring or periodic penetration testing and vulnerability assessment, whereas penetration testing would be conducted annually and vulnerability testing would be biannual.

I would note if you have any questions during this panel, please feel free to email them to safeguardsworkshop2020@FTC.gov.

To get us started, I'll ask Tom, what is continuous monitoring and can businesses and other institutions big and small reasonably be expected to implement continuous monitoring.

MR. DUGAS: Thanks, Alex. And thanks for having me as part of the workshop and on the panel. So continuous monitoring is the ability to see and react to activity within your computing environment based on logging and log aggregation. The analysis of those logs provides us the ability to take a look at what we need to do to react or protect our computing environments to reduce risks related to incidents and breaches.

That continuous monitoring could be done with systems and services or polls, or it can be done manually. While these services are also very valuable, part of the challenge is that it can also be very costly. For example, you know, one of the sessions this morning talked a little bit about the fact that for, you know, a 3,000-plus endpoint environment, it would be about $50,000 a month for a university like Duquesne, for example, which is kind of a small/mid-sized university. It would be about $600,000 a year in expense in that consideration.

Universities are so expensive in these considerations because we have a lot of data. Duquesne itself has about 9,000 students. And we act as both an ISP to those students who live and work here on campus and also basically serve our institution in the businesses that we actually run. We almost have, you know, 1,800 employees as well that are working to support our institution and our mission.

So being able to continuously monitor that entire network can cost hundreds and hundreds of thousands of dollars. And we need to make sure because those are based on ingestion costs in a lot of cases.

Just as a quick analysis based on retail costs for a tool like Splunk, for example, we have about 200-gig-plus in ingestion a day. And that would probably cost us about, you know, $600 per gigabyte annually. So that can be quite expensive when you get to that consideration when you look at something like that. It would be about $120,000-plus for a university like ours.

So we need to continue to keep an eye on those costs and certainly need to make sure that we have the dedicated security staff to manage them. So it's certainly important. I think it's very valuable, but it's also something we need to keep an eye on to make affordable as well.

MR. IGLESIAS: Great. Thanks, Tom.

Nick, do you have anything to add on the costs, benefits or implementation of continuous monitoring?

MR. WEAVER: Yes. So when things go wrong, you want to know what happened. And the whole point of continuous monitoring of systems and logging all that information is so that when something does go wrong, you can ask what happened; what got compromised; what did not. And there are -- there's an unfortunate tradeoff here. There's a lot of tools that are actually really cheap for this.

So for network monitoring, there's the Zeek network monitor. For monitoring end hosts, per se, you’ve got Syslog, Linux and Sysmon on Windows, and these both support remote log-in. You’ve got Nessus to inventory your network and know what's on it.

But to use those tools, you need experienced personnel. So you’ve got basically a tradeoff here. If you're outsourcing the work, you're spending a fortune. If you're insourcing the work, you aren't necessarily spending a fortune because if you're the system administrator, you want this information anyway. You want to know what’s on your network. You want to be able to check that everything is working right. And the logging facilities are just as useful for debugging incident response. But there's a general shortage of good personnel in this space and they aren't cheap.

MR. IGLESIAS: Nick, do you think those are accessible to smaller businesses and smaller institutions?

MR. WEAVER: It depends. So if you're a small institution but have one or two good experts, you're in good shape. So like at ICSI, we're a small outfit but we have a really good system administration

team of two and a network security incident response team that consists of multiple researchers who specialize in this.

But that's -- we're able to do that because we have the personnel already in place. And so it's how good and creative and motivated is your system administration staff.

MR. IGLESIAS: Great. Thanks, Nick. Moving on to another topic, what is penetration testing and what role does that have in an information security program? How often should an organization conduct these tests and what factors should go into determining the frequency of these tests? And I would ask that to Flee.

MR. LEE: Yeah. So penetration testing is effectively just attack simulation, with the goal being to try to actually just go across the entire gamut of potential vulnerabilities that a system/infrastructure may contain, and then actively try to, you know, truly exploit those systems.

So, you know, we're going to talk a little bit more later about vulnerability scanning, but think about, like, pen testing as being not only finding vulnerabilities but trying to determine which vulnerabilities are true by essentially having your

staff, either outsource or in-house, or even in some cases automated tools act like an actual attacker. Obviously these are meant to be somewhat benign attacks. But the goal is to actually really see how severe a vulnerability could be if exploited, to help give a group an understanding about, you know, what are the issues to fix and also what are the priorities of the issues.

So, you know, when you do a pen test, you also are not only classifying the potential exploits or potential defects there but essentially also how severe those things are.

With regards to, like, how and where that actually fits into the ecosystem, it really is meant to be almost like a sanity check of what the system looks like from an attacker's perspective. Something to actually keep in mind, though, is that a pen test is not, like, completely comprehensive. And that’s actually one of the weaknesses of a penetration test, is kind of like this notion of coverage. How many different parts of the system were you able to test; how effective were your tests?

So just because a pen test doesn't have a lot of issues, per se, does not necessarily mean that a system is secure but it does give some confidence of

saying, like, hey, at least these types of issues were tested for; we did not find these issues in these particular areas, but it doesn't mean that something is explicitly secure or insecure. The other thing to actually take into account is that a pen test is literally just an assessment at a specific point in time. So just because a pen test was actually done six months ago does not mean, and most likely is not meaning, that the system that was tested is in the same condition. More than likely, software has been updated; patches were applied; the network itself may have changed.

So that's actually part of the reason to think about, you know, how you do pen testing to really be a check against significant changes that actually were made to a system. Ideally you're doing a penetration test at least annually. However, a lot of people would recommend that you also do a penetration test with any kind of significant change to the system. So if you’ve actually added new features to the software that you’re building, if you’ve changed the network topology, et cetera, you probably want to do a penetration test again.

But, once again, that really is part of a broader holistic security program. Penetration tests in and of themselves are not sufficient. It's meant to actually just really be yet another tool to help identify security weaknesses in a proactive manner so that you’re able to actually fix things prior to an attacker exploiting them.

MR. IGLESIAS: Thanks, Flee. And what would those typically cost a business and what is the range for that?

MR. LEE: And so this is where it gets really interesting. For the penetration test -- and I love that Nick kind of already got onto this. You’re always paying some kind of cost when it comes to resourcing, right? Obviously you can have in-house talent that can actually do that penetration test. Security engineers in general are not cheap. So, you know, there's no such thing as a security engineer that’s making less than six figures. And obviously this is going to generally be at the higher end of that. So in-house is going to be expensive for you.

Going externally definitely is an option. That kind of goes across the gamut. But to some extent you are kind of getting what you pay for. So it's not uncommon for kind of like an 80-hour penetration test to start at at least $40K, but that can actually quickly go up to six figures depending on

the complexity of the system, the specific vendor that you pick, and also how much you want to have tested.

So if you want to have somebody doing testing on something that is actually fairly nuanced, so, for example, you built an embedded system of some sorts or, you know, kind of like an IOT-type device, that expertise is way more expensive than somebody just doing a penetration test for a “basic website.” So that definitely is one of those things to take into consideration.

There are some new novel type alternatives. Because when you think of a penetration test, if you think of it from the lens of what you really want the outcome to be, the outcome should be trying to find vulnerabilities or security weaknesses in the system proactively. And so there are other mechanisms like things such as bug bounties, which can make that cost a little bit less. But it’s also one of those areas where as an industry we haven't really solidified on that being adopted. And particularly around things like regulations, to get regulations to start accepting bug bounty reports as being at least comparable to a “classic penetration test.”

MR. IGLESIAS: Thanks, Flee.

Nick, did you want to respond to that?

MR. WEAVER: I just want to add one other real valuable thing from the penetration test, is it basically gives you a dry run on all your response. So whether or not the pen testers succeed, you should go back and see in your logging infrastructure, your monitoring infrastructure, did you record this. Did you catch this either before or even after you find out.

MR. IGLESIAS: Great.

Scott, did you have anything to add, and specifically are there any limitations with penetration testing at large?

MR. WALLACE: Yeah, so sure, I’ll just kind of talk about what it's like on a typical pen test for us. So we get all of the IP addresses that we're allowed to operate in on both the external and the internal network. We also get a list of emails for a phishing campaign. And so the pen tests that we normally do are one week externally and then one week internally.

So on the external week, the first thing we do on Monday is we prepare for the phishing campaign. We have a template and a payload that we run by the point of contact. And then once that's all been approved, we send that out to the email list. And we

generally get beacons off of that. We have a surprisingly high click rate. Other things that we do on the external network are do host discovery and vulnerability scans on the hosts that are open and have ports available.

There's generally not much that is directly exploitable on the external network, although there are some crazy things that we’ve seen. So, like, my favorite one was there was an entity that had default credentials on the external network. And so we just looked up the default credentials, logged on to the server and there was all of this crypto mining software that was running on the server and calling back to Europe. So he was using them as a server farm, whoever was doing that over in Europe.

But generally we’ll get a couple beacons off of the phishing campaign, and from there it gets more interesting because people are a little more lax on their internal network than their external network. So the kind of joke is that in cybersecurity, that it's hard and crunchy on the outside and soft and chewy on the inside.

And so we'll do things like -- Responder is a popular technique to use on the internal network whereby there's all sorts of folks requesting services on the internal network. So, for example, if somebody is searching for a printer, we'll just say, hey, yeah, on that printer, here's a handshake, talk to me. And then so we can possibly get some hashes from that. And weak passwords is definitely one of the most common vulnerabilities that we find on the internal network. So we could get hashes from Responder, we could get hashes from a technique called Kerberoasting. On a traditional Microsoft network, you have a ticket graining system called Kerberos, which is authentication on the internal network, and you can request hashes from Kerberos. And so that is another way that you can possibly crack some hashes.

And then patching is another big vulnerability that people don't keep up with as well as they should. And another one is network segmentation. And this has especially been important as we've been working throughout the 2020 elections because states and counties interact with each other for the voting process.

And so when it comes to network segmentation at a county level, for example, you could have the sheriff and the emergency medical services and the board of elections and the, you know, garbage all on the same county network but not properly segmented.

So, in other words, you could exploit the landfill’s network or the sheriff's network and be able to find your way to the elections side of the county. And so, yeah, Nick, I see his comment here. But Mimikatz is very popular. So when we're spreading around a Microsoft network, there's a tool called Mimikatz that actually allows you to pull credentials out of memory if that person is logged on to the box.

So traditionally what we'll do once we get that initial beacon from the phishing, there's a really, really effective tool called BloodHound. And the guys that wrote it are very smart. We used to work with them. And basically what it does is it maps out active directory in the Microsoft domain. And so you can see where the domain admins are logged in to.

And what you want to do is navigate to those boxes that they're logged in to so that you can scrape the DA’s creds out of memory and then you control the network.

So that's sort of a summary of kind of what it's like in the real world on a test. We generally use some form of phishing to get beacons and then running BloodHound to navigate to where the admins are. Responder is another one. Kerberoasting, like I said, to get more hashing from the ticket graining

system, and then patches. Some of these like EternalBlue and some of these things that came out even years ago people have still not patched. So that's traditionally what you'll see on a pen test, especially on the internal network.

MR. IGLESIAS: Flee, did you have something to add?

MR. LEE: Yeah. I actually wanted to piggyback on several of Scott's comments because actually they were great. And, also, Scott’s comments give some insight into some of the challenges of these kind of rules, and pen testing in particular, how it will impact a small/medium-sized business or organization.

Everything Scott said was true. But I can imagine that probably half the people actually watching this audience didn't understand a word that he said. And not because the people in the audience aren't, you know, intelligent, but because it’s actually really technically, you know, complex.

And on the side of a business or somebody else, a small organization needing to have a penetration test done, one of the important things is actually understanding the scoping, this concept of what should we test but also how the test should be

conducted.

So, like, Scott spoke a lot about, you know, what it's like actually doing a bunch of pen tests, in particular like, hey, should it be a network penetration test; should it be a penetration test of just, say, like a web application. But even moreso, he was mentioning tests that were for things that are actually, like, in a Windows environment.

So if you are a small business or a small organization that doesn't have internal security experts or really, really intelligent maybe network engineers, you may be at a disadvantage for actually figuring out how to actually properly test. So you can actually have a pen test done, but the true value that we're driving for here is incentivizing and encouraging businesses to proactively find security defects and get those defects fixed.

It also requires that they have either some in-house knowledge or some assistance in actually trying to figure out how to properly test their business. So a traditional like OWASP top ten or like a web-type penetration test, if I'm a manufacturer of, you know, like, embedded devices, that test isn't relevant to me. But if I don't have the necessary in-house expertise, I wouldn't know which test I’m buying, if I'm buying the right services or not.

And that actually is one of the things that we have to worry about when we consider these kinds of rules and regulations and how they're going to impact people that may not have a Scott on their team. So if you have a Scott in your organization, you're fine. If you don't have a Scott in your organization, you're going to be at a disadvantage. And we need to make sure that whatever rules and guidance we push down still allow for people to actually figure out and actually learn that process as it goes along.

MR. IGLESIAS: Thanks, Flee.

Tom, did you want to add anything on this topic?

MR. DUGAS: And, Flee, I think that's spot on. One of the challenges that I think is really important to make sure we cover in part of the Safeguards Rule change is the fact that the scope of the rules must really fit the information that's covered.

What are we defining as customer information; how does it apply? I mean, the perfect example is what we have the -- you know, why we are part of the FTC Safeguards Rule in the first place for higher education is because we handle financial aid

data. Financial aid data is really just a very small subset of what we do here at the institution. But it obviously, you know, could have major implications for us in terms of what we need to do to, you know, fund and staff a cybersecurity program.

So we need to make sure that as we're thinking about what we need to cover in terms of the rule, we need to be very explicit about what that GLBA Safeguards Rule defines as customer information and how it fits in institution because arguably, when we're doing a pen test, if I had called Scott and said, Scott, I want you to do a pen test but I only need you to pen test that financial aid data, but the reality of it is is that, you know, he could easily maybe get the financial aid data as, you know, Flee was talking about from somewhere else, you know, or I think Scott was talking about by going in a different way, from a different subsystem. Maybe it's not my financial aid system; maybe it's my admission system. Maybe it's something else that actually would provide that beacon that allows them to look in and see what's there.

And so those kind of considerations are very important as we look at this information to make sure we're counting for it correctly.

MR. IGLESIAS: Great. Thanks, Tom.

Moving along to vulnerability testing, how often should an organization conduct vulnerability testing and what factors should they determine -- what factors should they consider in determining the frequency? Should testing be done, performed when there's been a change in the system or an intrusion attempt? Can it be automated and what does it cost?

And I would call to Flee to answer.

MR. LEE: Yes. So, you know, the TLDR here is that at a super, super high level, you can just think about vulnerability testing and vulnerability scanning as trying to just do a really, really broad sweep of the entire ecosystem and identifying things that could, under certain circumstances, reduce the security controls. Right? So making something weaker.

Oftentimes when we think about this in practice, what does it look like? It's scanning your environment for the software that's installed and comparing and checking to see if that software has any known published security vulnerabilities.

This is often done via automated means. In fact, I don't know of anybody that currently does vulnerability scanning manually anymore. It really is

now at a point where we can actually automate the majority of it. And that automation can be extraordinarily cheap because there's actually a lot of free tools that actually can help with that. But there's also a lot of commercial tools out there.

Some of those differences could be the frequency with which they update some of the "rules/ signatures," the things that they actually look for in the environment, all the way to the ease of actually using the platform. So, you know, like a tool like Qualys, et cetera, is actually highly polished, made to make it really, really easy for somebody that can utilize it. There's also open source tools such as OpenVAS that kind of, you know, puts the -- you know, essentially the operational burden onto the organizations that's utilizing it.

But because it's so cheap and because it is automated, most places should try to have vulnerability scanning operating as frequently as possible. So I know that the rules are actually looking for, you know, these vulnerability scans to occur probably like, I guess, twice a year. But I would argue to say that it's actually one of those things that is achievable more frequently.

Some of the things to actually watch out for is how vulnerability scans actually work. So because they are doing some active things on the network, there could be network performance issues even inside of a, you know, test environment. There could be issues where a vulnerability scan could potentially impact those systems and the uptime itself. So that actually is something to watch out for, and part of the reason why it's good to actually have an expert on staff that can actually detect those nuances and also correct any errors that actually may be caused by the vuln scanning.

One of the other issues also to worry about with vulnerability scanning is, once again, kind of like this nature of scope, like how much of your ecosystem are you seeing and can you see. So in a really, really well segregated network, doing a vulnerability scan can be complex. You have to figure out where do you actually deploy the tools so you can actually see all of the network.

The other thing to actually also think about is how do you actually aggregate all that data. And, also, finally because of the nature of vulnerability scans, you also have to worry about this concept of false positives, meaning that you're going to find things that will show up on a report that in your

current environment or how things are actually deployed are not actually truly exploitable or not really, really security weaknesses.

So sometimes that will appear when maybe you're running custom software, like a custom version of a Linux package, for example, and that package itself is not vulnerable but it has a signature that looks similar to something else, which can introduce some overhead with regards to that key work effort.

But to actually kind of, like, summarize, it can be automated. And because it can be automated, teams should actually drive towards doing those vuln scans as frequently as possible, and definitely there should be a vulnerability scan after any significant network or application change, and always there should be a vulnerability scan after a intrusion exercise, whether it's a true, you know, intrusion attempt or just an alert that was actually being investigated.

You’re muted, Alex.

MR. IGLESIAS: Sorry about that. Thanks, Flee. Tom, related to this topic, do you have anything to add? That would be great. And then specifically how much do these type of things typically cost an organization?

MR. DUGAS: Well, certainly. I

couldn't agree more with Flee. Vulnerabilities account for the vast majority of cyber breaches in the world today. In fact, you know, it’s probably up there, you know, with the number one reason why, you know, information is being targeted, is because of a breach. People have the automated scanners, they're out there doing it maliciously. If you're not doing it yourself, somebody else is doing it for you and you just don't know if they're just doing it with ill intent.

So we're trying to protect our critical assets, our PII intellectual property, and I think that the scanning of this needs to happen at -- you know, we try to do it quarterly and at least annually. But we realized that there’s -- it's hard to manage this because every time you find a vulnerability, you have to assess whether that vulnerability really impacts your university or not, or your organization. Because in that case, it could have mitigating controls that you’ve already implemented just to, you know, keep that vulnerability at bay; to hide it from the attacker.

And in some cases, you can actually keep that, you know, system from being exploitable for a period of time and keeping other mitigating controls,

defense and debt, microsegmentation, firewalls, you know, intrusion detection, intrusion prevention system. There’s a whole bunch of things that can happen to allow that to occur.

But you’ve got to keep a mind that when you find all these things, you know, whether it's a free toll or an automated toll, or a per-fee toll, you get this, you know, big, huge report with dozens and dozens of pages of things that someone has to take action off. You need to have expertise on staff to understand what those vulnerabilities mean, how to manage them, how to actually fix them, because that’s not something you can just do. I can run a toll tool, you know, forever, but if the tool doesn’t have somebody behind it to analyze and understand whether or not it impacts your organization and you have to do something with it, and what you have to do, that’s the hard part.

And for -- we’re kind of a mid-sized organization. We’re right on the cusp of where we have that expertise. But I’ve got to tell you, of the 25 universities we partner with in Pennsylvania, we're one of the minorities who have that level of expertise that could run this continuously. Most of them can't. They can't sustain that operation, even though it is a best practice, something I recommend. It's costly to them from a staffing perspective, resource perspective and the tool set, too.

MR. WEAVER: Agreed. One other reason, though, why you want to do this and when you have automation, you want to basically -- if you have your system automated, you basically want it, like, every day, is that a side consequence is this also gives you an inventory. It tells you what is actually on your network. So when the CTO's son logs in a gaming rig, you actually find it.

MR. DUGAS: And, Nick, that's an important characteristic. I mean, I don't know about Berkeley, but I have 30,000 connected devices. I've got to imagine you're a lot greater than that. So trying to find that gaming system is a needle in a haystack sometimes when you're thinking about unlimited amount of resources in most IT organizations. We have unlimited demand for limited resources.

And certainly we're going to talk, you know, probably more about what this means for how organizations are revolving around COVID. But, I mean, we're even more struggling now with the way we're managing our IT resources than we ever did because we're trying to find a new way to help meet

demand that's increasing, and at least in our case in terms of IT needs. So, 30,000 devices, yeah, it's easy to inventory it, but trying to, you know, manage 30,000 systems and all of the vulnerabilities that come around with that is pretty intense.

MR. IGLESIAS: Thanks. Tom.

Scott, did you have anything you'd like to add to this topic?

MR. WALLACE: Well, I can just kind of piggyback off of it and jump into topic four if we're ready and kind of describe some of the other services that we have related to continuous monitoring and a couple other services. Does that sounds good, Alex?

MR. IGLESIAS: Go for it, Scott.

MR. WALLACE: All right. So what I described earlier was a risk and vulnerability assessment that we do, which is sort of the full pen test. If you want just a phishing campaign, we have that as well, if you just want to do the phishing test. We also have just the remote campaign.

Probably our most popular product, though, is called cyber hygiene. And before I was on the pen testing team, I was on the software development team with a couple of smart and great guys that wrote this. And basically what it is is it's a PDF that you get

every Monday that details your entire external network. And so it's a very simple sign-up process and anyone can sign up. You just contact our mailbox and give us your IP space. We go ahead and end map that, figure out where the hosts and ports are, and then run the vulnerability scan on that.

And the report we deliver every Monday will kind of have an initial report card at the top. And so you'll see mitigated vulnerabilities, vulnerabilities that have remained and new vulnerabilities that have popped up. They'll all be color-coded based on their severity.

And then once you go deeper into the report, you'll get details on the IP and what specific vulnerability it is and additional detail. And so that is called cyber hygiene. It's pretty effective because the scanning is based on the severity of the vulnerabilities. So when we pick up critical vulnerabilities, the scanner comes back and rescans that every 12 hours. And highs are every 24, mediums are three days and lows are six days.

And so when you get it on Monday, your more intense vulnerabilities have been scanned very recently. And so when you get it on Monday, you have a general picture. And like somebody said, you know,

people doing things over the weekend -- we had a customer who did some configuration changes on their network one weekend and accidently dumped the whole internal network on the internet. And so there was a massive spike in the report card that they saw when they got it at 6:00 a.m. on Monday morning. So they knew that they had made a mistake so they were able to tackle it quickly. And that's totally, you know, free at the point of signing up for anybody that would like to sign up.

MR. IGLESIAS: And, Scott, what would an organization need to sign up for that program?

MR. WALLACE: Well, there's not many requirements. We just -- you know, we might have an interaction with you and then all you need to do is send -- you'll sign the legal contract and then you'll give us your IPs. And then as soon as the next Monday, you'll start getting your reports. It's pretty straightforward and simple.

MR. IGLESIAS: And it would just scan the external network or would it also scan the internal network? How does that work?

MR. WALLACE: Yeah. It's just the external network.

MR. IGLESIAS: Great. Thanks, Scott.

Nick, are there any other products and services available to institutions for continuous monitoring and/or testing and what would these normally cost?

MR. WEAVER: There's a lot. And the cost is often a -- basically it's a product of how much you're willing to spend and how much local expertise you have. So for network monitoring, you have free high quality network monitoring in the form of Zeek and Snort and Suricata and all those that are really good at logging everything that happens.

But if you're running them yourself, you've got to have an expert on staff, or you can go with one of the companies that's outsourcing the skill. And so you don't need necessarily as much skill on staff, but now you have a big dollar line item. In terms of collecting on end host, it's the same thing. Sysmon is free; Corelight costs a fortune. But Sysmon means you have to have experts on staff who are able to set up a server to ingest the logs, to analyze the logs.

Similarly for log analysis, you can spend a fortune and go with Splunk, or you can go, these are logs I'm rarely going to read and so it's column/delimited text and you're using grep and Python, or you might be splitting the difference and

tossing it in the PostgreSQL database.

And so basically what it comes down to is you have your questions. What's on the network? What's happening on the network? What's happening on the end host? And you basically then have to decide where in the internal expertise versus external cost tradeoff you are as an institution. And that basically tells you what approach you have to take.

MR. IGLESIAS: Thanks, Nick.

Tom, did you have something to add?

MR. DUGAS: I did. And, you know, certainly there are a lot of tools in this space and a lot of services. In fact, this morning's sessions demonstrated a number of them and what those costs are. They're well documented. They can be tens of thousands or hundreds of thousands of dollars annually.

In order to get around that, at least in higher education, we've done so by building consortiums to try to stem the tide of the cost because it's very hard to come up with that kind of money when we know it directly ties back with, you know, student tuition dollars, for example.

So the University of Texas at Austin, for example, built a system called Dorkbot, which does a

lot of the same things that the hygiene service at, you know, the Department of Homeland Security does but specifically for government and higher education to actually analyze that external web content.

And then a number of Big Ten schools and other research institutions built something called the OmniSOC, which is a centralized security operations center for universities to collaborate collectively together and then normalize data and talent, because it is a really hard thing to do even if you gather all the great tools that Nick talked about, which are free and available for a lot of people, somebody still has to sit there and watch them 24/7, 365 days a year and make sure that we're protecting, you know, our assets, our digital assets from attackers. And trying to maintain that kind of operation without a partner who can help you do that certainly can be a lot.

So, you know, for big organizations, they're tackling it well. I'm sure there's a high expense to it for small organizations. Some of them haven't even figured how to even start. So we need to just balance out the fact that there's both big and small between them.

The other thing that I think is becoming increasingly challenging, Alex, is the fact that at

least in a lot of cases the data is not even at my location in a data center anymore. It's in a cloud service or offers a service somewhere else that's being managed, you know, by another organization or multiple organizations.

So I may have, you know, several different enterprise relationship planning software solutions that are actually managing data. So we need to be cognizant of the fact that data is being distributed in ways that it's never been before. In a lot of places, people have done a lot of paper abatement to meet COVID restrictions and needs because of the way we're working and they've moved a lot of things to cloud-based services because of that in order to make that accommodation happen.

So we've got to remember the fact that even if we run penetration tests and vulnerability tests, that's for our systems and services. And we heard from this morning's sessions, what if that's at Amazon, and what if it's with Microsoft or whether it's with Google or Oracle or some other cloud platform where it's not here? Because then I need to ask them to do the same thing and they need to run the same test and they need to give me the validations and results, not just myself.

And now we're independently validating all of their controls and all of their things that they're doing to protect my data that they own or they're controlling. They don't own it, of course, but they're actually controlling on our behalf. So there's a lot that goes into that.

MR. IGLESIAS: Great. Thanks, Tom.

Moving on to the next topic, what is the purpose of security logs and audit trails? How are these beneficial to organizations and are there any limitations doing this? And I would ask that to Nick.

MR. WEAVER: So logs and audit trails are really important. You notice actually a lot of the tools that I've been talking about are really logging. So you can theoretically do proactive defense on the network and the like. But the greater value is actually the logging itself. You got compromised. What did the attackers get? What did they not get? Because if they did not get your financial disclosure stuff or stuff like that, not only is that good for you, or good news, but that might save you a fortune because now you don't have to deal with the State of California's notification business.

And basically what it comes down to is the pen testing and the vulnerability scanning, and stuff

like that is all about preventing attacks. The logging is all about recovery: being able to do a true damage assessment and a true recovery. And that's why logging is so important, is because it does enable this damage assessment and recovery that in the end might save your corporation hundreds of thousands of dollars.

MR. DUGAS: And to add what Nick was talking about, I mean, it's like a crime scene. Right? So that -- you're logging all this data and you're gathering it all, and if you ever have to do an incident or a breach investigation, you're going and pouring through those logs in order to, you know, build a case against that perpetrator or to ascertain what they did, how they did it and what they got access to.

If you didn't have those logs, you would have a real hard time being able to find that information you need to figure out what happened and why it happened or how it happened. And so the challenge is that you can -- you gather a lot of these logs and logs consumes data and storage, and that data and storage consumes a lot of costs. And so you have to make sure you understand how much data you need to retain for logs and how long you're going to keep

them, and more importantly those logs have to be protected as if it's a case file and an investigation. They need to be protected and secure to make sure that it can't be altered; to make sure they're not being, you know, changed by somebody who doesn't have permission to do so.

So certainly it's something that is really critical for what we do. But it's also a lot of things we do after the fact. We're not -- we're not -- we've got to still prevent people from getting in and doing it, but after the fact if you don't have them, you don't really have the necessary means to actually do anything to investigate correctly.

MR. WEAVER: And there's one other problem of you don't know until after you're trying to investigate what you wish you logged. And so as a consequence, when in doubt, error on more aggressive and error on basically right only.

So a big blob of disk that just gets stuff because, like, for example, Lawrence Berkeley Labs does very aggressive logging of the network. And they have used decade-old logs of connectivity in investigations. And a properly run network monitor would embarrass the NSA with how aggressive you do it.

So, for example, the NSA did bulk recording

of network data for five days, and they were oh-so-proud. Lawrence Berkeley Labs does bulk reporting of network data and keeps it for months. Raw packets, just because it might be useful in an analysis.

MR. LEE: I like one of the things that you called out there, Nick. And particularly you said this phrase, a well architected network logging system. And I 100 percent actually agree with you, and I think one of the challenges, though, is like how many people have the expertise to actually do that.

And that's where, you know, some of this guidance and things like that that the FTC is putting together really needs to be considerate, also, especially of the capabilities of the institutions doing this. You know, because, yes, we can definitely actually set up monitoring, et cetera, et cetera. But envision a scenario where it's like a 200-person company or like a 400-person contractor or that kind of scenario. Do they have the people on staff that can actually put monitoring in place so you're actually effectively grabbing the correct logs?

I 100 percent agree with you. Like, you want as much security telemetry as possible. Some telemetry is actually more useful and more important than others. And you do need trained personnel that can actually help make that useful. You know, it's definitely great to just have kind of, like, all of the logs, but then you also get into the scenario that I think you, Nick and Scott, have already, you know, touched on. Well, now you also need the expertise to actually go through that data. Right? So, like, having the forensics is great and there are definitely third parties that can come in post-incident that can study the logs that you have. But it's also useful internally that you have somebody that can actually go through that data and see if it actually is useful or relevant.

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

And, once again, there are open source tools

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

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

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

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

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

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

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

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

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

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

MR. WALLACE: Yeah.

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

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

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

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

MR. IGLESIAS: Great. We have another question that’s asking, the Safeguards Rule is intended to set development of the comprehensive information security program in the context of what’s appropriate to an organization size and type as well as nature and sensitivity of the data the organization handles.

With that in mind, how should the FTC work with different stakeholders, communities, covered by the rule to identify for organizations what the relevant standards for their industry may be in relation to these issues?

MR. LEE: I can chime in on that at a high level. I mean, there are tons of, you know, like essentially business organizations and representatives. I do think it's useful to distinguish between the size of these companies. What’s appropriate and realistic from a security posture standpoint and security programs standpoint for a large financial institution, you know, such as Goldman Sachs or Bank of America, is very different than what it is for a 200-person company. And it's important that the FTC recognize that and really start to hyper-focus on particular behaviors that they want

to see and the outcomes of those behaviors.

And what that means is being open to examining the new guidance to determine if it's really, really truly outcome-based, meaning that not being overly prescriptive and saying that, hey, you have to have penetration testing, thinking more along the lines what you really want out of penetration testing.

The assumption is that you want penetration testing because you want to see businesses have ways that they can proactively find security weaknesses, and then once finding those security weaknesses, properly prioritize those and then finally remediate those weaknesses in a repeatable way, with the expectation that software and information technology is always going to have new vulnerabilities.

There are always going to be classes of things that we're not taking into account today that may, you know, in the future end up being vulnerable. Like, obviously we're all aware of things like, you know, the Hartley vulnerability that was in open SSL a while back, or the, you know, SSE/secure enclave issues that Intel has had, or all of these other kind of classes of vulnerabilities.

So it's important that we really actually

focus on do companies have the ability to find security defects, and do they have the ability to actually fix those in repeatable fashion. And what that looks like at a large company should be different than what that looks like at a small company. And what that means is a small company may need to rely on just one individual who doesn't have certain certifications or doesn’t have security in their title but is still capable of actually doing the job versus a large organization that, yeah, probably has, you know, hundreds of people in their security department.

MR. DUGAS: So I want to tag a little bit onto that. Because as we have guidance in the GLBA Safeguards Rule specifically towards organizations of different sizes, we need to make sure they're expansive enough that we -- and detailed enough that they're applying to the different organizations the way that they're intended to.

So going back to a small liberal arts college versus Berkeley, are they going to be applied the same? If not, we need to define what that’s going to look like and how we’re going to apply it to those different institutions based on their Carnegie class, for example, in research institutions. Applying on some financial institution status and basically how

they're being, you know, grouped, I guess, in their categorization is not necessarily the same. We're not -- we can't go based on the size of a bank, for example. We need to go based on the size of an institution, how we're actually deemed in our industry.

But when we have all of these different considerations and things that are being applied for the changes in the rules, we’ve got to take into account that putting these things into place for some organizations isn’t just going to be something we can do quickly.

I think the proposal said something like, you know, it should apply six months after go live. I’d be hard-pressed to think it’s going to be a year. It would likely be two years where people are really getting to it where they need to finish all the components that they need to to get compliant.

So we need to take that into consideration, too. I just don't think six months is going to be enough. We’re going to have to give enough time and effort into this to allow those smaller organizations to get up to speed with the things they need to, to find the partner they need to, get the tools in place they need, to find the services they need to get involved with and actually get the things in place that are going to be necessary.

So comprehensive, yes, we need to keep that all in consideration. But the specifics here, we need to be very particular about what we need to do and make sure we need to provide some institutional discretion about what that looks like as well.

MR. LEE: Yeah. And I want to piggyback also on your response again, Tom, because I think there’s one other aspect to home in on. I feel like we may just be dancing around -- and not intentionally, but it’s like we’re right on the tip of our tongues, which is really right-sizing these controls and what we actually want to see out of these safeguards to the amount of data that’s potentially impacted. Right?

So if you're a small college, yeah, you have a small student population. What you should be looking for from that security program is going to be different from a university that has 200,000 students. Right? And that 200,000 students represents a larger amount of data. And that's a larger impacted population. It's not meaning to say that anybody should necessarily be off the hook, but the rules that apply for somebody that’s carrying a million, you

know, records of sensitive data is probably going to look different than somebody that’s only carrying 2,000.

And even moreso that some of these businesses that are going to be subjected to this regulation may not actually even host the data themselves. And are we doing a good job where we're actually maybe calling that out? We want them to be, you know, responsible and knowledgeable about where data flows in their ecosystem. But if they are relying upon third-party SaaS providers for various things, including, like, data storage, how much leeway do we give them to leverage, you know, these security protections that they’re getting from these third parties, et cetera.

So those are all things to actually definitely take into account because the nature of the data is going to look different, the nature of that impact or potential data custodianship is going to look different.

MR. IGLESIAS: I think this dovetails nicely into our last question to finish up this panel. Based on the discussion we’ve had, what impact do you think the proposed amendment would have? Are these things organizations should be doing or are there any other

recommendations you have for the FTC? And we'll go ahead and start with Tom.

MR. DUGAS: Sure. I think I talked quite a bit about this. But I think all of the monitoring of testing is absolutely critical for securing our computing resources. We need to make sure we have those in place. There are numerous threats and attacks daily, and without proper controls such as penetrating tests, vulnerability scans, continuous monitoring, we're susceptible to them.

But we also need to understand that there's a cost associated with it, whether it's personnel or whether it’s technology. And no matter how we do that, in some ways we're only going to be able to do that through collaboration and partnership with other people like us. In higher education, we are very collaborative and we do find ways to find innovative ways to solve these complex problems. But it takes time to get that going as well.

So just keep in mind that, again, the Safeguards Rule only applies to that very small portion of the data that we are actually responsible for managing and protecting. But we need to make sure we also protect our academic and research data as well just as importantly. Our students and our researchers

and things they produce are just as critical to us.

MR. IGLESIAS: Thanks, Tom.

Flee?

MR. LEE: Yeah. You’ll probably hear me duplicating a lot of Tom’s answers. But, you know, like I said, I believe these rules are decent, but there’s definitely some additional areas of concern and things for the FTC to actually be aware of.

I love the fact that this is actually trying to push to be a little bit more prescriptive, but we have to make sure that people really understand the actual motivation here and the overall objective. The objective should be to incentivize, to encourage and hold companies accountable for having good, repeatable and understandable security programs.

And fundamental towards that is having the ability to, you know, quickly, proactively find security weaknesses and defects via, you know, vulnerability scanning, penetration testing, et cetera, to actually quickly contextualize those so we can actually, know, properly, you know, classify them, apply the proper resources, and actually get them fixed. But that should allow for people to actually have a fairly broad agreement with regards to, like, how they accomplish those things.

In particular, because these companies are going to look different, a small business of 200 people is definitely different than a company of 2,000, a company of 20,000, et cetera. And their security capabilities, their ability to implement these controls, are going to look different. But we should be more concerned with the outcome that we want from those controls rather than how those controls are actually implemented.

I do think it's great that the FTC is, you know, looking at guidance for things like the NYDFS, et cetera, but it's also important to note that things like some of the policy requirements or documentation requirements are going to look different at these companies, and we need to make sure that when we're holding companies accountable for it that we really hyper-focus more on the outcome that we want as opposed to if they, you know, dotted every I/crossed every T, and if their policies look exactly like a large bank's policies because that's really not the reality. And then recognizing that the cost of implementing this is going to be burdensome for small companies in a way that it's not for a large company. So that's definitely something we need to take into account.

MR. IGLESIAS: Thanks, Flee.

Nick?

MR. WEAVER: Second or third, everybody. But I'd like to add one little thing that Tom touched on, that we should in some ways have number and type of data at risk as part of the calculation, because a small business that nonetheless has detailed financial records on everybody in the U.S. would be a huge risk in practice and really doesn't justify sort of light small business controls.

While a used car dealer, the number of financial records at issue might be a few hundred or a few thousand, and so the damage in case of a failure is so much less in that case.

MR. DUGAS: You're muted, Alex.

MR. IGLESIAS: Sorry about that. Scott, for the final word?

MR. WALLACE: Yeah, not much to add. Just segment your network and don't click on anything weird and you'll be in relatively good shape.

MR. WEAVER: And get security keys. Security keys and password managers.

MR. WALLACE: Amen, Nick.

MR. IGLESIAS: All right. Thanks, everybody. We're out of time for this panel, but I want to thank each of you for your time today and for a very informative discussion.

(Whereupon, a recess was taken from 2:02 p.m. to 2:16 p.m.)

ACCOUNTABILITY, RISK MANAGEMENT, AND GOVERNANCE OF INFORMATION SECURITY PROGRAMS

MS. WETHERILL: Welcome back. Thanks for joining us at today's FTC Safeguards Rule workshop. Our next panel will address accountability, risk management and governance. My name is Robin Wetherill. I am an attorney with the Division of Privacy and Identity Protection here at the FTC.

And with me today are Adrienne Allen, director of security, governance, risk and compliance at Coinbase; Michele Norin, senior vice president and chief information officer at Rutgers, the State University of New Jersey; and Karthik Rangarajan, head of security at Robinhood. So thanks to all of you for being with me today; looking forward to this discussion.

So I wanted to just start by asking each of you to briefly introduce yourself and tell us a bit about your experiences working in and around information security programs and in particular the aspects of those programs that touch on accountability and governance.

So, Adrienne, would you like to start us off?

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

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

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

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

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

MS. WETHERILL: Thanks, Adrienne.

Michele, would you like to go next?

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

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

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

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

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

MS. WETHERILL: Great. Thanks, Michele.

Karthik?

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

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

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

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

177

really starts with the first line of defense, security teams sort of making the right calls and setting the framework for making the right calls.

MS. WETHERILL: Great. So to dive right in, you know, as a few of you have noted, one of the themes of this panel is accountability. So I thought it would be useful to just start by talking about this word, accountability, which has become, you know, kind of a buzzword or often comes up in discussions around information security.

And so just to set a baseline, you know, what do we mean by accountability in the information security context and how important is it as an element of an information security program?

So, Karthik, would you like to start us off?

MR. RANGARAJAN: Yes. I guess we'll start with what accountability is. For me, accountability is who's responsible for identifying and managing risk as well as mitigating who is responsible for the many controls, who is responsible for making sure things are safe and things are accounted for, who testifies when something goes wrong? These are sort of the parameters I think about when I think about accountability.

And in most organizations, at least in

178

companies that are fairly small, you may have a small security team, you may have somebody that is the head of engineering or head of IT playing the security hat. And, to me, accountability is about who makes the security decisions and, when something goes wrong, who is going to show up to resolve the incident or respond to the incident, and, afterwards, when you're being questioned by the regulators, who is in the hot seat answering those questions.

MS. WETHERILL: Thanks.

Michele, did you want to add something to that response?

MS. NORIN: Sure. And I touched on this a little bit. I completely agree with my colleague Karthik. You know, there are certainly roles that are automatically accountable for what goes on in the information security space.

I will add to that, as well -- and we operate this way with our program -- we like to remind our community that there are varying levels of accountability. Certainly the CIO plays a big part in accountability. You mentioned the hot seat. You know, it's usually the CIO who, along with the CISO, the CIO is also there, you know, taking the heat for what went wrong; why'd this go wrong. So clearly the

179

CIO, your lead IT person, also bears a good deal of accountability for protecting information assets.

I would submit that your organization generally, the leadership, also plays a role in accountability. I think any organization has a responsibility for protecting your information assets and protecting, you know, people's identities and protecting, you know, your services and what you do as a company. And in today's world, you know, information security and the threats that come with that and how we protect, it's a pretty big deal. And so leadership bears some level of responsibility and accountability for that as well.

We also take a shared approach. We like to remind members of our community, depending upon the role they play or the job that they do, that they have a role to play as well in protecting our assets. Not clicking on links and phishing messages, you know, making sure they're not sharing their password. You know, some of those general awareness tips and reminders also plays to the fact that, you know, everyone is responsible and has some level of accountability for playing their part in making sure we're protecting our assets.

And so depending upon your role and where

180

you sit in the organization, clearly the leadership, the senior levels, they're going to be the ones -- me, you know, who I report to, will be the more visible ones when it comes to an incident or a situation. But, you know, at a very broad level it is shared to some degree as everyone, you know, could be a vulnerability in certain circumstances.

MS. WETHERILL: Great.

Adrienne?

MS. ALLEN: Yeah, I agree with what both other panelists have shared. I think, you know, I agree that accountability ultimately is about ownership and being able to represent the successes, mistakes, needs of whatever is in your purview to leadership. And in a lot of ways that ends up looking like speaking truth to power. These people, the CISOs, the CIOs, you are really partnering with the business to understand what those business goals are and helping the business to then understand what are the risk outcomes of making those decisions. There may be security consequences or other technological consequences that just aren't necessarily thought of when the business is framing its objectives for the year, for the quarter or whatever the time frame is.

So the CISO, the head of security, whatever

181

that role looks like, is really partnering with the business to understand those goals, developing, recommending some options, maybe even a couple different options for how to implement controls to help the business achieve those goals within the risk appetite, getting that buy-in and then moving forward on that control implementation.

So I definitely see it as a highly integrated, highly partnering type of role, but ultimately, yes, it is the person in the hot seat and it's also the person that is supposed to understand the business goals, how that impacts security and making sure the business is fully informed before moving forward on something.

MS. WETHERILL: Great. So to switch gears, you know, while the FTC's current Safeguards Rule requires financial institutions to designate "an employee or employees" to oversee their information security programs, the proposed rule would require that they designate a single point person who's responsible for implementing and maintaining the program.

So I have three related questions about this change in the requirements. First, to what extent is a single point person already typical of what

182

financial institutions are doing to consolidate responsibility?

And, question number two, what are the benefits, if any, of that as a choice for how to organize responsibility in your institution?

And, question number three, what are the costs of that as a strategy?

And, Adrienne, would you like to go first on this one?

MS. ALLEN: Sure. I'm happy to start with the first question. You know, I think to the extent to which this is already happening, there is a similar requirement in other financial services regulations. So, for example, the New York Department of Financial Services already has a similar ask for someone to oversee and implement the cybersecurity program.

So for any company doing business in the State of New York, fintechs, for example, this isn't that new. And I think the pros of having this model is that it does or can make decisions better and faster.

I think when decision-making is distributed you can run into a diffusion of information. It's harder to pull together a single view of how an information security program is running. Frankly,

183

it's also -- it can be very difficult to understand what the staffing and resourcing costs are when you have a distributed view. It's not coming out of a single line item. And you can sometimes have analysis paralysis. Without that single ownership, the accountability piece that we just mentioned, you can fall into traps of each relying on someone else to make a hard call. And there are hard calls in security. So with that model issues can sometimes fall through the cracks.

And I'd also like to put on my third-party security hat for a second. From the standpoint of reviewing another vendor's third-party risk, before integrating them into your environment -- and, again, I'll speak from the fintech point of view where we're talking about a lot of SaaS vendors, you know, very technical integrations that can be complex in nature. You really do need to understand who oversees security specifically within that vendor organization for a couple of reasons. One, it might be during an incident. God forbid you need to know who to reach out to or even share threat intelligence with.

On the first point, every once in a while a questioner or an issue will come up with a vendor. Attackers may even try to compromise a vendor on their

184

way to trying to get at a primary target. So it's important for the sake of the incident response planning process to be able to have a single point of contact, or at least a single channel to reach someone to work with within a short amount of time.

I think secondly, it doesn't need to be a CISO but it should be someone who can make that type of informed decision or quickly and appropriately escalate to leadership so you meet regulatory reporting notifications if you have any.

I think sometimes, to the last question, the cost of doing this with one person, you know, for smaller companies is obviously the cost of that resource. You might not be resourced to bring in someone to focus solely on security.

I think another cost is that sometimes even if you have someone, security can get relegated to a side issue. So it's really important that that person is senior or influential enough to direct and equip program resources and to be able to influence decision-making.

MS. WETHERILL: Great. Thanks, Adrienne.

Michele, did you want to followup on that?

MS. NORIN: Sure. I completely agree with Adrienne. I think it's extremely important to have a person in front of the information security program. I think that there are so many components to understand, to manage, to keep an eye on. I think it's difficult to do that if it's part of someone else's job. And so I found that it's extremely helpful to have a person in charge of that program just from a pure basic management perspective and understanding perspective.

That gets difficult when you're smaller. I get it. You know, it's hard to, you know, carve out one person to do everything, you know, or one specific thing. We don't always have the luxury of having that. But if you've got one person who you know, this is, you know -- this is it, you need to keep your eye on this, I think it's extremely important to have that.

When you're bigger, it makes it even more important that you have that, that person who is just every day constantly thinking about and managing this kind of a program, and to raise those issues and situations, you know, to their leadership, to the institution or organization's leadership appropriately. And so it takes having someone who is dedicated in that way to serving as the lead of a program, a CISO or otherwise, that, you know, they're

responsible for the management and the progression of the program.

MS. WETHERILL: Great.

Karthik, did you have anything to add?

MR. RANGARAJAN: Yeah. Adrienne and Michele said some excellent things, and I won't say the same thing. I will add that one benefit of having a single person or team that is responsible for this is you remove the conflict of interest, potentially.

Let's say I'm managing the engineering organization and I'm also managing security. And the product organization is telling me that they need this shipped tomorrow, and I see there are security risks, I'm probably going to listen to the product organization and ship it and then take a look at the security risks and figure out what needs to happen there.

But if there was an independent point of contact, if there was somebody who does not have that conflict of interest, they can play those checks and balances. They can say, okay, I hear what the business wants, I hear what you're trying to do, but these are the risks that are coming up.

The second component to this is certain financial companies have the three-layer defense model

where there is the security teams who play the first line of defense, and then there is the enterprise risk and the audit teams.

Even in those models, I think it's especially important that the why's of security, the simplified decision-making, lies on the security team or on the single person that is the designated head of security.

For a really small company, for somebody that may have outsourced all of their business -- all technologies, it might be hard to hire somebody or justify the cost of hiring a point person that plays head of security. And I think in those situations, the way I look at it is you don't need to hire somebody that is 20 years a CISO or something like that. You can find somebody that is experienced, that knows about the subject matter.

Most of the regulations that I'm familiar with don't require you to hire a CISO but require you to designate somebody as head of security. So find somebody that can provide value for you, that can help you manage risk and make security decisions in a smart way, and designate them as your point person. And then you get two things for the cost of one.

MS. WETHERILL: Great. Thank you for your

answers on that.

So the development and implementation of an information security program, as Karthik just referenced, can implicate not only IT personnel but also employees who work in other areas like compliance. So does it make it more difficult, you know, given that kind of diversity of involved personnel, to have a single point person and why or why not?

And, Karthik, I can go back to you to start us off on this one.

MR. RANGARAJAN: Yeah. I think in reference to my last answer, I think it depends on what the organization is doing. Let's say all of your technology providers are fully outsourced, you don't build in-house software, you don't have engineers in-house, and it's just putting things together to serve your customers. In those cases, I think you could outsource your security responsibilities, too, as long as you're outsourcing to a firm, as long as -- I would say you need a named person that you are working with, but you can outsource it. You don't have to have this person in-house.

However, if you are building anything in-house, even if it is the smallest thing, if you're serving products to a customer that you built in-house, then I would say having a point security person in-house is unavoidable. Because it's going to be really hard for an external personnel to handle all of the contacts of the business, understand everything that is happening, and be in the the rooms where the decisions are being made, and do it consistently so that the business' interests are put ahead and risks are managed appropriately.

So if you are building in-house products, if you're building in-house services, you absolutely need a point security person. But if you're completely outsourcing it, then I would say you could consider an outsource model for security.

MS. WETHERILL: Great.

Adrienne, did you have anything to add to that response?

MS. ALLEN: Yeah. I think just maybe a quick analogy. One of the studies I think the Corporate Executive Board recently did was actually how software decisions are made when you're purchasing a new piece of software, potentially something that is a large system; it extends across the environment. They said that while there is a single decision-maker, there's actually an average of seven people that are

involved in forming that decision.

And I think, you know, when we talk about other teams being involved in security and ultimately kind of rolling up to a single person, that model is actually fairly consistent here, too. You know, it's very unlikely that a single point person for security would be making decisions in a vacuum. They're going to have to cooperate with teams, like with risk and compliance, the three lines of the defense model that Karthik mentioned earlier. And that's great.

You know, I think to the extent that it does make decisions take longer sometimes, that's absolutely true. I think you can do it efficiently, but they're still taking new factors into consideration before making calls.

But at the end of the day, you know, again, I'll unpack an example that Karthik mentioned. If you're following the three lines of defense where you have, you know, the first line security, conducting operations, making these choices; you have a second line risk management that's noticing the risk about the program; third line internal audit that's checking on what the others are doing, you know, it very well may be that you have another team that's asking the security program to put segregation of duties in

place. That will take time to implement. It's the new requirement being handed to the security team, to include in a building and a designing of that program.

But at the end of the day, you -- while it may have taken you a little bit longer to design roles and responsibilities a little bit differently, to identify maybe you need to bring someone else new into the team to distribute those responsibilities differently, they're still taking the time to decrease your chance of insider threat down the road.

So while the overall program might take longer in some ways because you are working with other teams, by virtue of working with those other teams you're building a model that can grow with the company; you're building a model that is more resilient to the types of risks that security programs face.

So I think the short answer is, yes, it can take longer and it does make it more complex to work with these other teams, but at the end of the day, their bottom-tier model, you're altogether working on a common success criteria, and then you have the single head that can more easily report out on how all of those needs are being met.

MS. WETHERILL: Great. Thank you.

Michele?

MS. NORIN: Yes. I will reinforce that. I think it's critical to have a program, a set of processes and a governance model that accounts for multiple units. In my view, I don't think there's any one unit that can do all -- you know, that can address all of the components of what would need to be done. So it's important to have the partnerships.

I know for us as an institution, we have a couple of different working groups and committees that are responsible for, you know, the process around evaluating the software that we buy, or for responding to an incident. And those -- that group is made up of representatives from all of these other areas: IT, our risk and compliance office, our general counsel's office, our information security, IT, audit, internal audit sometimes is on there depending upon the focus.

So, you know, we set that up intentionally in that way so that they are all responsible for the process and a program that's well-rounded and, you know, will address all of the aspects of the institution as best we can. Right? If we need to add people in the moment depending on what we're dealing with, we can do that.

But it's not just information security.

193

It's not just, you know, the risk and compliance. They have to work together. And so we've worked really hard to set up those components, those partnerships, working arrangements, in that way specifically so that each area of that -- of the institution is represented.

And you're right. It takes longer, but in the end, it's better, it's stronger, because we took the extra time to really -- to really make sure we had all the right perspectives represented in the process. So I just throw my advocation for, you know, making sure that happens with those kinds of pieces in place as well.

MS. WETHERILL: Great. So, another change that the proposed rule would make, compared to the current rule, is that this single designated point person would be required to report to the organization's board of directors or whatever the equivalent of that is, in an organization that doesn't have a board at least annually, and that the report would have to be in writing.

So, you know, we're wondering about the pros and cons of that kind of direct communication between the individuals who are tasked with overseeing information security and the board or senior officers

194

of financial institutions.

So, Michele, did you want to go first on this one?

MS. NORIN: Sure. A couple of thoughts here. So one is, I think it's important for information security as a topic be at the board -- at the senior leadership level of whatever organization you are a part of. For me, it's Rutgers or higher ed, as well as the board. I think it's important that they understand what that concept is, what it means, what comes with it. It's not a one-and-done conversation.

I know for the boards that I've worked with with in higher ed, it's a progression of information. It's a way to build awareness about what we do, how we protect, where we see risks. And I think for their level of responsibility, they need to be aware of those subjects, those topics.

So I think that topic should be present at those tables on some regular basis, at a minimum once a year. It depends on your structure, your board cadence. You know, I think your board has to be brought into that kind of topic. I know for us that topic lives at the audit committee, which is a committee of our board. So I think -- so I think the

195

topic needs to be there.

The second thought, the second item here for me is I think who is the voice of that program can depend upon your culture, your circumstances as leadership. I think it takes a certain perspective to share that messaging in a way that's effective and clear for the audience. If your CISO can do that, I think it's great. I think the CISO should have a voice there. I think they should -- at a fundamental level, if they have to raise an issue that might be a little sensitive, they have got to have avenues to do that, right? I mean, no question.

But in terms of regular awareness, I think that, you know, you've got to have the right voice to demonstrate that. Sometimes that's a CISO, sometimes it's the CIO, sometimes it might be some other leadership, your risk management officer, possibly. Somebody -- and maybe it's all of those voices that share in that messaging with leadership.

And so I think that just depends on, you know, who the person is, how well they can talk about the subject matter, you know, what's the interest of the leadership and the board, and then, you know, how do you formulate that right -- the right voice around that, around the topic.

196

MS. WETHERILL: Thank you.

Karthik?

MR. RANGARAJAN: Yeah. You know, from my perspective, when you're reporting to the board of directors, one issue that can come up is the familiarity of the board with the topics that you're talking about, so the familiarity of the Board with security.

One -- a potential risky scenario is you go to the board and say, hey, these are our high-, medium-, low-risk items, and they get concerned that there are so many risks that you are managing. And the question that gets asked might be why are there so many risks? Why haven't they gone away or something like that?

And it's -- with qualitative risk management mechanisms, it might be hard to say, well, this is a high risk but it may not actually come to fruition because of these following factors or things like that. It gets -- it becomes a really technical, really difficult conversation.

One mechanism that I've been experimenting with that is gaining traction in the security industry as a whole is this quantification frameworks, which is instead of qualitative mechanisms that talk about here are the myriad of risks you need to worry about, you present to the board here's how much of a loss over the next X number of years that you're potentially looking at based on our existing control framework and the existing security program, and here's why we need we need the budget that we need in order to reduce the risk, and having, say, X million dollars to reduce the security risk by Y million dollars or something like that.

And the numbers don't have to be absolute. The dollar amounts are more of a high watermark for me than actual numbers. There's no way that I can guarantee that the firm will only lose X million or Y million a year. But it is a watermark that we can use to measure the progress that the team is making when it comes to building out the program.

If quarter over quarter, year over year, this watermark isn't reducing, then board of directors should be able to challenge us and say maybe you're not mapping your risks correctly, or vice versa if it's reducing but we're seeing more incidents, we're seeing potential breaches, things like that, then the board of directors should be able to say maybe you don't have the right risk quantification framework or the right risk management framework.

So presenting to them in such a way that they're actually able to use that to make decisions and provide input is something I would strongly recommend. It's something that we have been trying out.

MS. WETHERILL: Thanks, Karthik.

Adrienne, did you want to jump in?

MS. ALLEN: Sure. I just have one or two things to add. I definitely agree with both of the prior comments. First, quantification is likewise something that we're starting to experiment with as well, and it can be a very helpful kind of neutral way of characterizing some of the risks.

I do think it's worthwhile to call out that, you know, security landscape, the threat and vulnerability environment, the risk landscape, changes so quickly. For most businesses that do any kind of business online, you know, they may see risks on a daily basis that emerge. So having an annual reporting cadence is -- you know, I agree with Michele, probably the bare minimum for a lot of the financial institutions, and especially the ones that do have an online presence to be able to report out on progress over time.

I think that, you know, especially given

that a lot of the financial services industry protects very sensitive customer data, knowing where those critical assets are, being able to report out on the overall effectiveness of the security program and protecting those is really key.

I think what you end up with if you're doing this on an annual basis is sort of a point-in-time look at where the program has been over the last year. And so it kind of depends, again, on the goals of bringing the board in. You know, is it that we actually want meaningful feedback on a regular basis? Do we want to clue them in to the types of risks that we're seeing, help them understand the risk landscape so that they can make different products or services decisions, maybe reallocate or reprioritize funding? A lot of security is going to have downstream effects on other teams. If there are major risks in one area, maybe IT or even customer service, that needs to go fix something.

So providing, you know, even shorter, more iterative types of feedback potentially with that quantification, I think will ultimately be more successful in helping to educate the board on the type of pace that the company operates within. If that pace is not super fast, then annual may be perfect.

And I think as a requirement, annual makes sense.

I think, you know, in order to kind of take a look at your model for reporting to the board, decide on the right cadence, that may be a more risk-adjusted decision based on the type of financial services company that you are. And if you do have that online presence, then you might want to identify opportunities to provide greater visibility throughout the year than just one long report at the end, which, you know, again, kind of comes back to the business visibility to produce that type of report, make it meaningful, get the meaningful feedback in return.

MS. WETHERILL: Great. Thank you. So that requirement that we were just discussing is an example of a kind of trend in the new rule to generally increase the amount of decision-making that financial institutions have to put into writing. So that report to the board is one example. Another example is that while the current rule requires that financial institutions engage in a risk assessment, under the proposed rule, you know, that assessment would have to be also in writing.

So we are curious what you think about, you know, that kind of requirement, whether putting decision-making into writing fosters accountability within institutions or what are the benefits or costs of that as, you know, a procedural requirement.

So, Adrienne, do you want to comment on that?

MS. ALLEN: Sure, yeah. So I think my answer is similar to what I just mentioned, is it depends mostly on how it is used and revisited over time. So I think, yes, you know, first as financial institutions, most requirements that I'm familiar with ask for some form of a risk assessment. So financial institutions, a lot of which are most likely doing this anyway, I think it's a natural step for asking that they should be written.

So let me talk first about the benefits and then the costs. I think on principal reporting decisions it's helpful when you're taking a risk-based approach. You want to be able to revisit decisions in light of technical changes, resourcing changes, additions to the environment, or, frankly, just the passage of time.

I think it helps you understand how long ago a decision was made, whether things have changed. It minimizes individual interpretation of that decision. So people might hear something and then go off with their separate marching orders, each thinking that

they've heard a version of that. And it does create clarity over company policy.

I think there have been many instances, especially in environments where decisions are being made quickly all day throughout the day where something comes up, it rings a bell, you then have your prior analysis to go look back on. You can then either reinforce that prior decision that was made or adjust it based on the changes in the risk appetite or resourcing.

I think two examples here stick out to me. First, we see this all the time in the third party landscape, memorializing decisions about why you chose to accept or reject a given vendor comes up a lot. You might be a year later choosing to integrate that vendor with three of your critical systems. So you really do need to be able to rely on the earlier detail and some of the tradeoffs that you made when onboarding them in the first place.

And then, second, it also helps with exception management. I think security often holds other teams accountable for their own work. You may grant a team an exception to go fix something and in three months time you can come back, followup with them, identify whether or not they've fixed it, hold

them to that joint commitment that you both made earlier, and provide the rationale for the exception and why, you know, they may or may not see it extended if they haven't been able to do that. So, yes a lot of value to being able to track these decisions over time, come back to the specific rationale.

I think on the cost side, you know, formalized documentation can be a huge time cost to the business when it's too heavy-handed. So I do want to caveat that a little bit. I think when it comes to evidencing decision-making there should be more flexibility.

For example, in some of the examples I just gave, we might be making risk-based decisions in different mediums and different ways: IT service management tickets, code reviews, project design documents, to name a few examples. So I think it's important to note that businesses should have the flexibility to record decisions in different ways. I think it's perfectly realistic that the sum of a lot of those small decisions might rise up to the level of going into more formalized risk assessment, and that's perfectly effective as well.

So, again, there may be a formalized risk assessment. There may be a set of other decisions

that are made outside of that. I think as long as you have a consistent method of deciding when and what is appropriate for what, then it shouldn't all need to be in a single place where you can go back and look at all of that.

So, overall, yes, writing things down is a great step, but there are many ways of doing it. As long as everyone is aligned on how you are providing visibility then it's great. That's what I would say.

MS. WETHERILL: Thanks, Adrienne.

Karthik, do you have any comments on written decision-making?

MR. RANGARAJAN: Yeah. I agree with everything Adrienne just said. Going back to the three layers of defense model where the security team is the first layer and then you have the risk management and audit teams as second and third layers, whenever the security team makes a decision that impacts the business in meaningful ways, maybe it's to choose a major vendor or other vendor, whether it is an outsourcing model or anything that people may disagree with, there may be multiple stakeholders. It's important to have clarity on how that decision is made and why that decision is made.

And especially now in the current remote world that we live in, written documents have gone much farther than they used to before. You can't just get into a meeting room and hash it out. And so writing a one-pager or writing a message on Slack has had more impact than multiple sets of meetings would have.

So purely from an efficiency standpoint, I have actually come to believe that writing things down is more helpful than not writing things down. Even though it might seem as overhead, even though it might seem as undue process, writing things out for major decisions -- and that's the qualifier I want to add, major decisions. You don't want to write a one-pager for why you chose to reject this code review over that code review. That doesn't -- that doesn't really rise to the level everyone is speaking. Well, maybe tying it to a risk score, tying it to the -- tying to the overall risk management framework and saying for all higher or critical risk decisions, we want to have a written documentation for why certain decisions were made.

If risk is accepted for our higher -- major risk is accepted, people have written documentation as to how we accepted this risk, what controls we looked at, what controls we are going to build and how we

attained that consensus across the company, so that the next time you have to make a similar decision you can follow the precedent that was set.

And this doesn't just happen for third-party vendors. This doesn't have to be just for product decisions. This could even be for actions you take in the case of a security incident or something like that. Let's say you have a security incident but you don't notice or you don’t find evidence of breach or don't find evidence of any malicious activity, you could write that down, memorialize it in the company so that the next time something like this happens you don't have to have this discussion all over again. You can look back at your previous precedent and say, okay, this is what we followed, let's stay consistent with our decisions so that not only do you now have an easier way to make decisions in the future, you also have defensibility for your legal and audit partners in the future.

MS. WETHERILL: Great.

Michele, I’d love to know if you have any comments on this issue, in particular, and I invite other panelists to chime back in. But I’m interested if anyone thinks there are costs associated with these kinds of requirements that the FTC should take into

consideration in deciding whether to press forward with some of these changes.

MS. NORIN: So I don't have a whole lot to add to my -- to what my colleagues have said. I think, you know, it is generally good practice to document. And as Karthik said, not every little nitty-gritty thing, but, you know, certainly major reports, major decisions, processes, steps that have been taken, incidents, all of those things.

I mean, I think that if anything, you know, in a year or two years after that particular moment in time, you need to remind yourself, why did we decide that? You know, why did we decide that? What were we thinking? And you can go back and look at the documentation. So I just think it’s generally good practice to document.

In terms of costs, you know, I think it’s just the time factor. I think if you go overboard, yes, it can be overly disruptive and it depends on sort of, you know, your organization, your size, how generally you operate, you know, how much process and procedure you have generally. I mean, you know, that factor -- those pieces can shape, you know, how much you do and then thus the time factor which then leads to the costs.

I mean, if you’re spending all day documenting and you can't get anything else done, that might be an issue and you might -- there might be questions about that.

So, to me, the cost is really the time factor and the tradeoff of, you know, who is it that’s doing the documentation, and then what are they not doing because you’re doing documentation? And is there value add there and what’s that balance?

So to me it’s really time and effort in terms of what it takes to actually do the documentation. If you’re getting an assessment by an external party and it’s a formal process, yeah, I want to see the report. You’re paying them to assess you and produce a report that’s actionable. And so there is a cost factor, and that -- in that specific instance where I’m paying somebody to come in and do this for us.

But I know that up front and I have a decision to make about, you know, the fact that I’m going to spend money on that kind of an exercise. So it seems to me the biggest cost internally is just really the time factor, and maybe the tradeoff if you don't document and something happens and then you have to go back and take the time to think about what you

209

did a year ago because you should have documented and you didn't. So there is kind of the reverse cost effect as well if you aren't documenting at the right level.

MS. WETHERILL: Yeah, thank you for your comments on that. So you brought up third parties, which makes a great segue because the next topic I would like to ask about relates to the way that third parties operate under the proposed rule.

So the proposed rule would specifically state that it's permissible for a financial institution to hire a third party to basically fulfill that designated point person role as long as the institution maintains kind of ultimate responsibility for overseeing that third-party vendor.

So I'm wondering if that provision makes it easier or financial institutions, particularly those who may be sensitive to costs, like smaller institutions, to comply with the rule's requirements and, you know, whether on the other hand there are disadvantages to allowing third parties in that kind of a role.

So, Michele, I'm going to turn it back over to you to start us off on this question.

MS. NORIN: So I think, you know, third

210

parties can be -- can be helpful to fill that role, particularly given the size of your organization. I think it's an interesting balance to consider. I'm an advocate for even if you have a third-party who manages your program, I think it's important to have someone inside the organization who is managing that relationship.

We work with a lot of third-party entities in all aspects of our operation. And as much as, you know, we put a lot of trust in what they do and they're really good partners and they do really good work for us, we need to be managing that. Sometimes you just have to manage those relationships. And I think the same would be true for an information security program. You still need someone who is ultimately the voice inside your organization responsible for that program, whether you're doing it with your own team or you're managing an external team. I think it's important.

I also think that the idea of having a third-party serve in that capacity, particularly around information security, I think there's things to consider there in terms of what is your culture, what's the culture of your organization. Is that -- you want -- I advocate for having an organization who

211

knows you as an entity. They know your organization, your culture, how you operate, your risk tolerance. That might be hard to do from a third-party perspective, especially if they have a portfolio of entities that they support. You know, they've got -- they have to know your nuances to know, okay, well, you know, what things are relevant here and, you know, what are the aspects of their level of tolerance around risk that we have to account for in the program.

So I think it can fill a role if you don't want to stand up your own internal resources. But maybe it's a split role, at a minimum, with management, but maybe even your team itself where you still have some internal resource as well as being supplemented or bolstered by a third-party entity.

I just think in these cases, it's helpful to have ownership within and that true commitment to protecting, you know, the assets from within the organization.

MS. WETHERILL: Great. Thanks, Michele.

Karthik, did you have anything to add on that topic?

MR. RANGARAJAN: Yeah. I think I mentioned this earlier, but if you -- if you're building

212

products and services in-house, then it becomes key that you have somebody internally managing the program, even if you depend entirely on third parties to manage the program. But it's key that you have somebody present the what-if's of security in-house that's not completely outsourced.

Third parties, there are a lot of good services you can get from third parties if you want penetration testing, vulnerability assessment, even risk management. You don't have to become an expert in risk assessment technologies. You can hire people to do that for you. But you need somebody in-house that can translate that and that can convert that into something that is meaningful for your business.

So if you hire a third-party to do all of it, they don't live and breathe with your business. They don't work with your business all the time. So they are only going to give you the perspective, the outside perspective. But to get an inside perspective, you might want to have somebody in-house.

From my perspective, is it imperative to have somebody in-house? I think that's kind of where the qualifier comes in, where if you're building in-house systems, then, yes, it becomes imperative that you have somebody in-house, even if that is not a designated security person, even if it is somebody on engineering that's managing these -- or some engineer in IT that's managing these folks. But it is imperative that there is some person, there is a person whose job it is to think about security for the firm.

If you're not managing in-house systems, if everything is external, as I said, everything is outsourced, then there is more flexibility, I believe, for these in terms of getting these third parties to understand how these outsourced systems work. You can get guarantees from our outsourcing providers, too, where if you're -- at least if you're doing vendor security assessments and things like that at the outset, you can get guarantees from these outsource providers that they are doing the right things from a security perspective.

So that's where this is. It depends on how your business works. There is obviously a cost associated with having somebody in house that is managing security for you. Security is almost always seen as a cost sector, even though that is the function everybody looks for when there is the biggest incident that happens.

But I think it comes down to the fact that

you have to make the call that is right for your business and how your business operates. And no matter which way you go, there's going to be a cost. Whether you hire a person or whether you outsource, there's going to be a cost and it's figuring out which cost you're more willing to accept.

MS. WETHERILL: Great. Thanks, Karthik.

Adrienne, did you have any comments about the costs or benefits of using a third-party?

MS. ALLEN: I agree with what's been said before. I think there is, again, a time and a place, and it very well may be along the maturity curve that you start with a third-party and eventually move towards someone coming in-house.

I agree that, you know, they actually are going to have less insight into some of the business drivers. It's going to take more work to get there. And I do think it's worth noting, too, that at the end of the day they still do have that split mission and even cost incentive between their employer and the company that they're supporting. And that is not nothing. You know, they're going to be incentivized to bring in money for their employer and they're also incentivized to provide the best quality work for you. But sometimes -- and on occasion those two things may

be at odds.

I think there's also the question of knowledge transfer, too. If you are relying solely on third parties then turnover may be more of a risk. You just have less insight into some of the external factors that might impact the third party that you're working with. So if you've been working with a dedicated partner for a while and they leave or something else happens, then you might be at risk of losing some of that knowledge, that institutional knowledge, that they've built up.

So, again, I think, you know, maybe this is where some of the documentation and just process comes into play. Not that you're paying for them to do that, but in order to have effective knowledge transfer when you have some kind of a handoff. That becomes even more important with third parties.

And then I think briefly, Robin, just to go back to the prior question on documentation, and actually really tier two is that there may be an element of privilege that comes up when documenting part of an information security program or specific risk decisions that may have been made in response to a particular regulatory requirement.

We see this a lot on the privacy side, for

example, where the laws are still emerging in some places and there may be room for a particular opinion about the company's decision to implement something or not implement something. So I think that partnership between legal and security also becomes more important when deciding, you know, what are the major things that we want to document; when do we want to retain attorney/client privilege in some of those things.

And then same thing here with third parties as well. You know, I think one of the drawbacks of working with third parties is that you can't really allow for their own training and development. There are employment laws around that. And so, you know, I think ultimately building into a workforce that knows your services, your technology, enabling them to invest in their own career path and learning development is something that you can't do with a third-party. You basically take them as they come. So I think that's another drawback as well. But it's more important to consider the long run, not necessarily right away when using a third party but certainly as you work with one over time.

MS. WETHERILL: Okay. Thank you, Adrienne.

We just have a few minutes left, so I want to very quickly try to address some of the audience

217

questions that we received. And here's one that I think we haven't discussed, and I think this really -- I'm going to direct this to Michele, but if others have comments, feel free to weigh in. But I think this is an interesting issue.

So the question says, please address the issues that may be presented at public institutions subject to open records requests. And if the annual written report is detailed as to vulnerabilities, could that create a roadmap for bad actors?

And so I'm interested to hear if this is an issue that has come up in any of your work and how you have kind of worked around that.

MS. NORIN: It has absolutely come up. Having served, you know, in public institution settings, we are subject to overt type circumstances. And so we try to balance that as best we can. We don't -- you know, there are ways that we can get to the details that would be considered sort of under the purview of our general counsel that would give us some layer of at least internal-eyes-only type of perspective. But it is an issue.

And, you know, we were talking about documentation earlier. Everything that is as a record of our operation is subject to being requested by

218

outside entities. And so it is what it is. We operate around that and we do the best we can in, you know, just trying to create documentation and enough information that we can take action on. But it doesn't give away or create an even bigger vulnerability for us in terms of, you know, how we produce those kinds of reports.

I know, for example, in dealing when I give reports to our board sometimes, I will give reports that are oral, not always on a piece of paper. Depending upon the certain circumstances, that may be an approach that, you know, would work in a particular incident or something that I need to convey.

But, you know, I think that's where it's important to have a really good relationship and operating procedure with the legal counsel or general counsel's office so that, you know, we are following, you know, the essence of the requirement of those kinds of requests, but yet also, you know, making sure that we're not creating a different kind of liability internally.

MS. WETHERILL: Okay, great. So we have one minute left. So as a lightning round, if everyone could just very quickly go around and say, you know, if you had to pick kind of one strategy or feature of

219

an information security program that for you is the best or most effective way to build accountability into the program, what would that feature be? And I'm going to start with Adrienne.

MS. ALLEN: I think if I had to pick one, it would be going back to that idea of a single person who's accountable and making sure that they have enough influence to make security management an issue. I think, you know, as long as security is going to be a second-class topic to some of these other management issues, then it's much less likely to get integrated with the rhythm of the business.

MS. WETHERILL: Great, thanks.

Michele?

MS. NORIN: So we like to work with carrots and not always sticks, but sometimes if we need a stick a couple things we've done in the past is cost sharing in incident response situations with the unit that has caused an issue. So if we've had a breach, for example, and we figure out that it was something that we've been trying to work with a particular department around and it just hasn't quite stuck, then sometimes having to pay to remediate builds a little bit of a different level of awareness.

MS. WETHERILL: Great. All right.

220

And, Karthik, I'll let you kind of have the last word, so go ahead.

MR. RANGARAJAN: Yeah. I'd say the biggest thing -- I think I would say two things. One is having the central point person that we've talked about, having security be represented at management and having this person write these risk quantification reports I spoke about earlier, having that will give a way to keep accountability for this person and for the company as a whole.

The second thing is measure why security matters for this company. Like, how does it impact your customers; how does having this person make your product better or worse for customers, and how can this work well for the business and the company in the long term, having some sort of mechanism to metrics along that can help the business make these decisions in a much better way. And it will make it easier for us to have the carrots and sticks we need to do our jobs well.

MS. WETHERILL: Great. Well, thank you so much again to all the panelists for joining us. It's been a great discussion. We really appreciate your help and your input today. And thanks to everyone who's tuning in. We will now take a 15-minute break and then be back with our final panel of the day. So thanks again and have a great afternoon, everyone.

(Whereupon, a recess was taken from 3:18 p.m. to 3:31 p.m.)

ENCRYPTION AND MULTIFACTOR AUTHENTICATION

MS. MCCARRON: Hi. Good afternoon and welcome to the fifth and final panel of the GLB Safeguards Rule workshop. My name is Katherine McCarron. I'm an attorney at the Division of Privacy and Identity Protection of the Federal Trade Commission.

This afternoon, I am joined by three experts who will address the issues of encryption and multifactor authentication. I'd like to take a moment to introduce them, please, before we dive into the substance of our panel.

I would also like to say that if anybody listening in the audience has questions for our panelists, please feel free to email those questions to the email address safeguardsworkshop2020@FTC.gov. Thank you very much for participating in the workshop today.

First I would like to introduce Matthew Green. Matt is a cryptographer and associate professor at the Johns Hopkins Information Security Institute, where he teaches cryptography. His research focus is in the area of applied cryptography and includes techniques for privacy enhanced information storage, anonymous payment systems and

bilinear map-based cryptography.

Randy Marchany, who is joining us from Virginia Tech, he is the CISO of Virginia Tech and has been there since -- has been acting as CISO since 2010. He has 30 years of experience in cybersecurity and has been a senior SANS Institute instructor since 1992.

Finally, Wendy Nather is joining us from Austin, Texas. She is the head of advisory CISO team at Duo Security, now part of Cisco. Wendy has led security at a Swiss bank and in Texas state government. She has served as research director for the security practice at 451 Research, and was research director for Retail Hospitality ISAC.

So, welcome Matthew, Randy and Wendy. Thank you very much for participating in the panel today.

Now, as we've been discussing throughout the day, these proposed amendments to the Safeguards Rule are process-based. However, there are two instances where they would require financial institutions to adopt specific security safeguards. And that would be in encryption and multifactor authentication. However, the proposed Safeguards Rule allows flexibility and implementation and alternative controls if approved by a person in charge of the program.

So, first of all, I'd like to start with encryption. The proposed encryption requirement would require that all customer information held or transmitted be encrypted both in transit over external networks and at rest.

Some points to note about the proposed amendment's language. First, the encryption requirement would apply only to customer information, and it would apply only to transmitted information when it's transmitted over external networks.

The proposed rule does not require any particular technology or technique. Finally, if a financial institution determines that encryption is infeasible, it may use effective alternative compensating controls that -- as long as they're reviewed and approved by the person in charge of the program.

So I'd like to, first of all, start by asking Matthew whether encryption has become sufficiently inexpensive and simple to adopt that it should be required for all financial institutions when handling sensitive data?

MR. GREEN: Okay. Well, first off, there are, as you just mentioned, different kinds of encryption. There's encryption for data in motion and there's encryption for data at rest. In the data-in-motion setting, we have some types of encryption, for example, SSL and now called TLS, which have become extremely efficient over the last few years and efficient to the point that they're almost universally adopted. I think website usage is above 80 percent and other types of services are using them at similar rates.

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

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

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

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

MS. MCCARRON: Okay. Thank you very much.

Randy, I'd like to followup with you. Can you provide your perspective on encryption and whether it has become sufficiently simple or inexpensive to adopt that it should be required by all financial institutions?

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

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

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

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

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

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

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

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

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

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

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

And that’s -- you bring up a great point because before you can encrypt it, you have to find it. And we're all digital pack rats. We have folders from, you know, 15, 20 years ago that may have Social Security numbers in them.

So, yes, we have to find it first; decide do we still need it. If the answer is no, get rid of the file. If the answer is yes, then encrypt it.

MS. MCCARRON: And then a final followup for you, Randy. I wanted to ask, you know, the Commission is interested in the costs of these proposed amendments to the Safeguards Rule. So as a financial institution scales up, how much does it increase the cost to encrypt data, and just using Virginia Tech as an example?

MR. MARCHANY: Well, if you're going to use a vendor product, you need to look at their licensing structure. They may have a charge per license, per user. It may be a blanket thing. A common denominator might be to use Microsoft Office file encryption. It meets the AES standards. It's password, you know, based. But you can, you know, deal with that situation. But if I’m sending something to Matt or to Wendy at their respective things, I could use Office encryption and then out of

band send them the password and they can open it up and do whatever they need to and store it using their own local encryption systems.

So it’s going to depend on the costs. But if I were looking at uber-cheap enterprise-wide, we're already paying for Microsoft licenses and encryption is already built into the Office environment. So spreadsheets, .xls, DocX, PowerPoint and a number of other Microsoft Office products all support that encryption feature.

MS. MCCARRON: Thank you. That’s very informative. I’d like to turn to multifactor authentication and talk about the requirement that would be in the proposed amendments to the Safeguard Rule.

The proposed amendment would require financial institutions to implement multifactor authentication for any individual accessing internal networks that contain customer information. And as all of you know very well, multifactor authentication must include two of three factors. The first is the knowledge factor, which is things that you know such as passwords or biographical information.

The second factor is the possession factor, things that you have. That could be tokens or

possession of devices.

The third factor is the inherence factor, things that you are, such as biometric characteristics, fingerprints or voice.

The text of the proposed amendment lays out these items, but what it doesn't say is whether or not you can use SMS as an appropriate factor for multifactor authentication.

So, Wendy, I’d like to turn to you first and ask, what is your view on whether SMS is an appropriate factor for multifactor authentication?

MS. NATHER: Well, there are certain risks with SMS that are very well known by now. Sort of the implied possession factor for SMS is that you possess the phone. But what it really turns out to be is that you possess the phone number and attackers do have ways of stealing that phone number out from under you, which is NIST had announced that they wanted to deprecate the use of SMS.

But when they made that announcement, there were a lot of objections, including from me, for a number of reasons. First of all, it's the cheapest and most widely available method for sending a code out. And in most of the world, people do not necessarily have smartphones. They have to use SMS.

So for financial institutions who cannot control the devices that their partners or their customers or even their employees are using, they're stuck with what’s available. So there are plenty of times when you have to fall back to SMS.

Now, as far as the phone number or the SIM jacking problem, I have talked to telco companies that are trying to address that issue. They realize that it's a problem. And I think a big challenge will be to get telco providers around the world to get together to address that threat.

So is SMS the best solution? No, it isn't. But we don't necessarily tell people that they have to use, you know, bank-level security on their front doors, either. It may be practical and usable for a certain number of risk cases. And so there's no way to bar them from using SMS.

MS. MCCARRON: Okay. As a followup question, Wendy, I wanted to ask you, how do financial institutions make that risk-to-cost decision? So when they're trying to decide do we invest in bank grade security or something else, how do they make that decision?

MS. NATHER: In a lot of different ways. And as Randy intimated, some of it depends on licensing, how things are bundled together. When I was working for the Texas Education Agency, for example, we could not afford to send people, staff, in the districts hard tokens. We simply couldn't afford it. And the other problem was that interacting with our systems was more of a role than it was an individually assigned account. So we were never able to be sure exactly who was going to be using an account to log in and do the state-mandated reporting. So that's an example.

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

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

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

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

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

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

You can see here that SMS passcodes are

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

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

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

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

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

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

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

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

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

We moved to two-factor authentication in 2016 as a result of a recommendation from a task force that I chaired back after we had a breach in 2013. And multifactor was -- two-factor authentication was one of the recommendations. Our CIO basically gave our team, the central IT staff, a year to implement it. And, you know, we ripped the band-aid off, so to speak. July of 16, all faculty, staff and students were two-factor.

Now, we had a six-month transition period where we could get the early adopters and we worked out most of the bugs before the final date. But, you know, right now we have over 156,000 users at Virginia Tech.

Again, with regard to the Safeguards Rule, universities and colleges are in an interesting spot with regard to the regulations because we handle, you know, financial aid. So that says, yes, we're a financial institution under the GLBA definition. But that's not our primary business. So our primary business is not financial. It's a much more open model.

And so under the current standards, we have that flexibility to -- where they leave it up to us to adjust to our model. I bring this up because, as Wendy mentioned about with the phones, you know, we've -- BYOD, every student at Virginia Tech is required to own a personal computer. 33,000 students. You know, we have 6,000 of them, or somewhere between 5,000 and

6,000 come every year. They own their own devices. We don't control those devices. Some of the students have text-only plans. Some of them don't have -- more than I thought don't have smartphones. They use flip phones. They may have their phone or text plans charge them for text messages, and so they incur a cost if they're using SMS.

And so, you know, how do you -- you have to address that type of stuff. BYOD for us is not a big deal. We've been doing it since 1984. But a lot of the rest of the world is now, you know, how do we deal with this with work from home? You know, are you using an institution, you know, owned device or are you using your home computer? So there's lots of things you have to take into account that way.

MS. MCCARRON: Thank you very much.

Now, one of the questions that is raised by the proposed amendments to the Safeguards Rule are whether there are instances where multifactor authentication is not appropriate for users accessing sensitive information, or put another way are there circumstances where it may be more difficult within a common infrastructure for financial institutions affected by the rule to use MFA?

In those circumstances, I want to talk about

what would be -- what are reasonably equivalent or more secure access controls that could be approved by a CISO?

So, Matt, can I start with you, please?

MR. GREEN: So, you know, there are a lot of different ways to do this, to provide alternative access controls. A lot of them really do kind of fall under the general category of MFA because MFA is just such a broad term.

But leaving that aside, I mean, nowadays one of the things that most people think about when they think about MFA and 2FA is these little key fobs that you carry around. This is kind of the classical version of what 2FA is. But nowadays we carry phones with us basically everywhere. Your phone can be your car key. It can be sort of everything that you use. And phones nowadays have modern secure hardware processors inside them. They have biometric sensors and readers. So we can increasingly get a lot of the security we need just through these devices that we already have by storing cryptographic authentication keys on the devices and then using the phone to actually activate those.

It is MFA but I think it's a more practical version of MFA that's maybe a little bit more, you

know, friendly for people to use. And then there are other techniques that people can use. For example, there are these behavioral systems that look for patterns of behavior in the way that people access systems and try to identify fraud. I don't know if they're particularly effective in all cases but certainly people do deploy systems like that. So there are some options.

MS. MCCARRON: Thank you.

Wendy, I wanted to ask the same question to you. Are there other circumstances where you think that a financial institution would need to use something other than MFA that would be reasonably equivalent or more secure access controls?

MS. NATHER: Where it might be difficult is, again, for smaller financial institutions that are below the security poverty line where they're very heavily dependent on the third-party software that they're using.

For example, I have seen tax preparation companies that are using cloud-based services that use email as a poor man's multifactor authentication. In other words, you log in with your password and then it sends you an email back to your address of record with a code that you then have to type in. That's the cheapest and slowest and, you know, kind of least reliable method there.

But, again, it's what the smaller organizations are stuck with. Because the level of influence that a company has may determine whether those companies can make their third parties use multifactor authentication.

In cases where state governments, for example, have to contract to very small firms, this may not be possible at all for the very small firms that they're contracting with. It can be difficult for mid-sized companies to force those third parties, especially with certain software that can't be replaced.

You asked about whether there are any times when it's inappropriate to use MFA. And the only thing that really comes to mind is if availability is much more important than confidentiality, when you have to get access to something because of public safety.

For example, a healthcare provider once said, I would rather not see my patient dying on the gurney with their privacy intact because I couldn't get into the equipment that I need to save them. So that kind of thing could be a very good reason when

MFA is not -- either not practical, not appropriate or it needs to fail open if there's any question about whether, you know, people can get access.

Sometimes MFA may not be necessary because the risk is being mitigated by other factors. For example, I had a healthcare provider ask me how to use MFA in a sterile operating theater where you cannot sanitize any of the things that we would normally bring in for multifactor authentication. But if you're looking at the real risk scenario around that, if it's a sterile operating theater, it's probably physically secured. If you locked down the account so that it could only be accessed from the equipment inside of that operating theater, you might not actually need MFA. So there are a lot of different ways where you could put in alternatives if it really becomes too impractical.

MS. MCCARRON: And, Randy, may I ask you, can you think of any circumstances of where a financial institution would need to put a reasonably equivalent or more secure access control in place?

MR. MARCHANY: Well, the business process is always going to trump the security process. That's been my experience with this. But I think in the beginning a lot of financial services sort of shied

away from MFA because they thought it was, you know, too difficult or people wouldn't use it. And it's the seat belt problem. You know, in the ‘60s when seat belts were being mandated by the federal government, automakers rebelled. They said customers will never buy this. And then an automaker -- if I remember right, it was American Motors -- they started marketing it as a safety feature. And then all of a sudden they noticed a little uptick in their sales because, oh, it's a safety feature; I'm going to buy that.

And we've seen sort of something similar happen with financial institutions that now they're marketing this as a safety factor. This is one more piece of our security portfolio to, you know, help ensure the security of your financial data that you're entrusting with us.

So I think you're seeing that shift. Where it goes south is -- as Wendy said, is a lot of vendors, software vendors, still aren't -- haven't gotten it yet to at least provide APIs or some sort of, you know, mechanisms to allow us to hook an authentication system, two-factor or not, into their software. And so, you know, that needs to be addressed.

I think shared assessments, you know, if everybody in the industry says, hey, these vendors, their software packages support 2FA or MFA, these guys don't, I think that's a way that we can apply pressure on the vendors to kind of move into the MFA requirement with the shared assessment process.

But as Wendy said, public safety. You know, if you're a first aid, first responder, you're there, you're dealing with an accident victim or whatever, you don't have time to just say let me get my fob and, you know, jam it in there. In some cases, you don't even have time to log in. So public safety certainly would be the one time when I would be, you know, really considerate of the fact that it might not work in that environment.

MS. MCCARRON: All right. But no financial institution situations come to mind?

MR. MARCHANY: I can't think of one that would want to do that because their competitors would immediately say our version is safer. You know, and sooner or later, you know, that's going to hit their bottom line.

MS. MCCARRON: So I'd like to ask, then, about what possible alternatives there are to encryption and multifactor authentication.

So let me just start, Wendy, I'd like to ask you first. Starting with MFA, what is your view about whether IP address restrictions are a reasonable equivalent to MFA? Yes, go ahead.

MS. NATHER: Yeah. I was going to say, no, please! IP addresses, we know, are not practical as -- especially as a single authentication factor. We know they can be spoofed. And, in fact, the entire zero trust security movement these days is in reaction to our realization that you cannot trust something just because it comes from a certain IP address.

Now, it used to be that IP addresses were used as proxies for geolocation. We would assume that if you came from this IP address, you must be inside the office building and therefore you were safer because you came through physical security and there were other things that happened in the background to authenticate you. But we know now that that's not safe.

And, in fact, relying on IP addresses for authentication and for trust has resulted in some really large famous breaches, including in the 2000s when government-backed attackers attacked a lot of high-tech companies including Google and took advantage of the fact that users were being trusted if

it looked like they came from inside the internal network.

So I don't recommend that at all anymore. Sometimes you still need to use geolocation as part of your authentication or access restriction because of data privacy laws based on country or that sort of thing. But we have much better technology to do that now. We have GPS-based access control that works better.

MS. MCCARRON: Okay, thank you.

Matthew, I'd like to ask you the same question. Can you share with us your view about whether IP address restrictions are a reasonable equivalent to MFA?

MR. GREEN: Yeah, I absolutely agree with Wendy. I mean, IP addresses are, you know, the burner phone numbers of the internet. Right? Anyone can just VPN to another location, use different IP addresses. It's a terrible way to try to actually authenticate people. You know, there are more sophisticated network-based attacks where you can actually, you know, pretend to be from a specific IP address, and those are more complicated to execute. But just moving around to different parts of the internet is something that's available to really the

lowest common denominator of attackers, I think, at this point.

MS. MCCARRON: And what about device or account restrictions like behavioral fingerprinting as an alternative?

MR. GREEN: You know, this is not my area of expertise, but part of the reason that I work in encryption is because there's a certain amount of certainty around encryption. If you encrypt something and you secure the keys well, it stays protected. It's sort of like putting it in a bank vault. Whereas with behavioral type of technologies where you're looking for patterns of misbehavior, you don't get that certainty. There's no mathematical theorem that says, hey, I can detect this attacker who's in your system. There is some hopeful probability it works, but I guess from my perspective the difference between that possibility it might detect somebody and the certainty that information will stay protected, there's just such a big delta between those two things, I don't feel comfortable with the probability.

MS. MCCARRON: Okay. The proposed amendments to the Safeguards Rule would permit a financial institution to use something other than encryption or multifactor authentication as long as

the CISO had approved it in writing.

So, Randy, I wanted to ask you, as the CISO of Virginia Tech, to walk us through what that would be like for a CISO to have to write a justification to approve an alternative method other than encryption or multifactor authentication.

MR. MARCHANY: Well, as Mr. T would say, I pity the fool that has to sign that paper. It's really -- I would not want to be the person to do it. In fact, if I was asked to do that, this would be my terms and conditions, is that it has to come from the board. The board is the one that has to tell me that we are willing to -- the institution is willing to accept this risk of not using it. We're going to accept it. Go ahead and you figure out a way to make this work and then sign -- you know, create that document.

But this is not a bottom-up thing. This has to come from the board down to the CEO or president or whoever and then down to us. I just would not -- I would stay away from that as far as possible.

MS. MCCARRON: Okay. And so what is the -- what would the burden be like on the CISO to have to write such a justification? What would that look like?

MR. MARCHANY: Well, we would be the scapegoat. I mean, the moment there was a breach, then all the fingers would point to us and they'd say, hey, you said this was the way to work. And I said, no, what I said was the probability is, you know, much different. But, you know, you'd have to do other types of analysis. Maybe -- you were talking about, you know, behavioral analysis, looking at certain log-in times for certain user IDs. And you can sort of do that with sort of a continuous monitoring model. There's a lot of research going on in machine learning and AI in that type of area of behavioral characteristics. But, I mean, that is so far away from where I would go. I'm not sure I'd have an alternative plan to do that.

MS. MCCARRON: Okay.

Wendy, I'd like to ask you the same question. Could you provide us with your perspective on the possible burden to CISOs of having to write justifications for using methods other than encryption or multifactor authentication? Whether this -- does this carve out -- does it help CISOs or does it help financial institutions?

MS. NATHER: There are two justifications I can think of here for why you would want the CISO to

do this writing. And one justification is presumably the CISO can attest that from a technology point of view what they're suggesting is equivalent, you know, functionally, whether it would work.

However, as Randy was alluding to, the probability, the risk measurement of whether this really is good enough is something that often is -- this decision is not made at the CISO level. It's made at the board level in terms of whether they're going to fund MFA or whether they're going to fund encryption and say, no, this is just too expensive; we're just going to accept the risk but make up something that sounds good and write it down.

So I personally, also as a former CISO, would much rather see -- for purposes of accountability to see that landing at the board level. Now, the other burden that would be on the CISO would be to argue the sufficiency of the exception with auditors. And in my experience that's never a good conversation because what you end up doing is not talking about whether functionally or technologically this is equivalent, an equivalent control. You're talking about whether you're really addressing risk that neither of you really agrees on.

And so a risk discussion with an auditor as

opposed to, you know, a checklist or compliance discussion, is not good. And at the end of the day, it doesn't even matter what the auditor thinks because if a breach results from this alternative use, then, again, the accountability has to go back to the board.

MS. MCCARRON: Thank you. We have a lot of questions coming in from the audience. So I will take the first one. And if you would like to answer it, just please raise your hand and I will call on you.

The first question is we've had cloud infrastructure and people working remotely from home for a long time now, relatively speaking. Why do we need to delay implementation of the Safeguards Rule to account for that?

Okay, Wendy? Or Matthew. Why don't you go first. Sorry.

MR. GREEN: Well, actually, you know, I think Wendy is the right person to answer this question. I can actually -- I think she --

MS. MCCARRON: Okay. All right. You first, Matthew, then I'll go to Wendy.

MR. GREEN: Okay. Well, I mean, you know, so the question is why should we delay. I mean, personally, you know, I'm an academic and my view is we should not delay. We should get these things out

there immediately and there should be none whatsoever.

However, I do know that, you know, at least from my perspective, a lot of the people that I work with are having a difficult time rolling out entirely new systems and, you know, making major changes in systems that are already stressed by the fact that we're in this situation that is -- right now seems a little dangerous to me; things can break.

But I'm not sure, you know, if that's exactly the best answer. So I will turn it over to Wendy for that.

MS. MCCARRON: Okay. Wendy, what are your thoughts?

MS. NATHER: My thought is that, first of all, you know, this crisis hit us pretty suddenly and there were a lot of organizations that had to scramble either to implement remote access that they didn't have before or to scale up what they had.

And I suspect that in many cases they put in the cheapest and quickest thing that they could with the expectation that this would only be lasting for a few months and then they could go back to normal. So there was probably not a lot of planning for the long-term.

Where companies are now facing the prospect

253

of, you know, this being long-term or perhaps permanent to a greater or lesser extent, they may need to think long-term about more permanent infrastructure. They may need to rearchitect what they currently have. They may need to negotiate with the cloud providers that they had to sign up with in a hurry who, again, you know, for reasons of influence may or may not be able to give them what they really need in order to comply with the Safeguards Rule. So I think all of those argue for giving them a little more time.

MS. MCCARRON: Okay. As a followup --

MR. MARCHANY: I have one thing to add to that, though.

MS. MCCARRON: Yes, please.

MR. MARCHANY: The biggest problem with the proposed regulations is that they don't take into account the limitations that an organization may have when dealing with the cloud vendor. They assume that we have complete control of logs, access and things like that which a lot of cloud vendor providers do not provide to the organization. It's our world. You want to get logs of how, you know, things are used, you have to go through our process.

And so there's a lot of things -- I mean, I

254

agree with Matt. We should do this. But as a CISO, I'm the one that's going to have to enforce it. And there's -- it's not clear. We don't -- continuous monitoring, for instance. You know, the proposed regulations say you have to be able to do a vulnerability scan on your end points. Well, in work from home, your vulnerability scan packets are not going to be going just through your network. They're going to be going to your home ISP network. And your ISP network may interpret that scan as an attack and block it or cut you off at the home because you're the one that initiated the scan.

So a lot of these things are not under the control of the institution, and that's where the weakness is in the proposed safeguards. You know, take work from home out of that picture. You still have to deal with, you know, try and to get logs from Amazon or Gmail or even Office 365 when, you know, you have to have all that stuff contractually agreed upon before you set it up.

And as Wendy said, if you did something in a hurry, you weren't thinking about, oh, I need to get access to email logs or stuff like that. So that's the reason why I say, you know, they need -- it needs to be delayed to address these new models. Because

255

while we may not be coming back -- you know, we may not be dropping work from home 100 percent, I think that percentage is going to stay pretty high for a long time, especially when we're still in this -- you know, is the pandemic going to affect our health thing.

Cloud-based services, you know, how does your organization get information it needs? You know, email abuse. Somebody is threatening you with email. But your email goes through Office 365 that you don't control, or Gmail, for instance. How do you get that information you need?

So that's the part that I think is a weakness in the proposed regs. The current regulations give us that flexibility. It's not as hard and concrete and set.

MS. MCCARRON: Thank you for that. There is another question coming in about alternatives to requiring encryption. The question is, would dedicated leased lines be considered an accepted alternative to requiring encryption?

So I'd like to ask the panel for their thoughts on dedicated leased lines as an acceptable alternative to encryption.

MR. GREEN: Sure, an expensive alternative.

256

Yeah, I mean, it seems like -- I mean, if your concern is the price of encryption, I mean, maybe you have a very good deal on dedicated leased lines that, you know, I don't know about. But they're not cheap. I used to work at AT&T so I have some insight into this.

I guess my biggest thinking about this is it really depends who your attacker is. If you're, you know, worried about the National Security Agency or foreign intelligence agency, the answer is, no, absolutely not because we learned a few years ago that those are not in any way immune to those kind of attackers. But even sophisticated nongovernmental attackers have in some cases shown that they have the ability to sometimes be able to access these kinds of systems. So it's risky. It depends on what the data is. If it's financial data that has value, I'd be very nervous about that.

MS. MCCARRON: Okay.

MR. MARCHANY: It could be really expensive especially if your customer base is the public. You know, how do you deal with that? I'm not going to set up a leased line to work from home or from my phone. So, you know, unless as Matt said, unless that company has got a lot of money, I wouldn't say that it would be an alternative.

MS. MCCARRON: Okay.

Wendy?

MS. NATHER: Yeah, just to pile on what all was said. Yeah, leased lines worked great in the ‘90s. I spent a lot of time doing disaster recovery with leased lines. Believe me, encryption is a lot cheaper today. It's a lot more flexible. It's a lot easier. Just, you know -- I can't think of a good reason to go with leased lines instead.

MS. MCCARRON: Okay. To followup on the question of the cost of encryption, there's a question from the audience that says Randy was just asked about the cost of encryption and his answer was technology-specific.

I would like the panel to consider the total cost of an encryption deployment: staffing to support, training of end-users and, of course, software and associated licenses. I’d like to open that up to the panel.

MS. NATHER: I would say five. The cost is going to be five. Five what? I don't know. That is one of the big problems with security, is that it is very difficult for us to price an entire solution like this. And I’ve tried several times as a research analyst. It depends so much on the geographical

distribution of the organization. It depends upon what kind of technology they have, whether they're cloud forward or not, what kind of data that they have and so on. That’s one of the big problems, is we can't tell you how much it's going to cost.

What we can say is here's a large selection of acceptable alternatives, try to pick the ones that work best for you. And in the case of pricing out what it will take for personnel who have the expertise and the time to be able to manage these solutions, again, for smaller organizations they're probably going to have to rely on vendors and cloud-based solutions where those things are built in. Just try to use the built-in versions wherever you can. But there's no escaping that somebody in the firm is going to have to at least be able to talk to that vendor about the technology and get it set up.

MS. MCCARRON: Okay, thank you.

MR. MARCHANY: Yeah, I mean, and you're right. Now, if you're talking about a support structure for your identity for authentication, you have an identity management group. You have -- for instance, we use Duo. So there’s a group that supports the Duo stuff. You know, my office looks at Duo logs but so does the help desk. You’ve got a lot

of people that are involved on the support side if you’re doing authentication for identity. If you're doing encryption for, you know, files or data streams, it can be as much, but, you know, again, it depends on what your target is.

I mentioned the Office encryption. That's the lowest common denominator. You know, it comes built in, but it's a vendor thing. You can certainly get vendor products that do the exact same type of stuff.

MS. MCCARRON: Anyone else?

(No response.)

MS. MCCARRON: I’ll move on to the next question that I have. This is a question about ransomware attacks, which as we heard earlier this morning is one of the top two types of security risks for companies right now.

The questioner has asked the panel, should the proposed GLB Safeguards Rule go farther and also require secure air-gapped backups of information to minimize the impact of a ransomware attack? To me, this seems as important as multifactor authentication and encryption.

MR. MARCHANY: I’m going to jump into this one first.

MS. MCCARRON: Please do.

MR. MARCHANY: The best defense against a ransomware attack is your backup system. If you get hit with a backup -- with a ransomware attack, blow away your -- the affected machines and restore it from your most recent backups. That's the most effective means to do so. You may lose a day's worth of work but I’d rather lose a day’s worth of work than the entire, you know, cake. So our infrastructure, you know, for ransomware is very, very specific.

Another thing is when you look at a lot of ransomware attacks that hit organizations, what gets encrypted in the ransomware attack is not just a file structure on my computer. It's a file share that I had with someone else. And we typically leave that file share open, the permissions open, to anybody that has access to that.

If you manipulate the permission so that only this working group has access to these files and this big common file share, that does limit -- I mean, you're not going to prevent the damage but you're going to limit the damage that can be done. That's why we say use a separate account if you're using your home computer because most ransomware these days that we’ve seen does not require administrative privilege to do its damage. It just operates on that.

So if Wendy and I have an account, and Matt, the three of us have accounts on my computer and Wendy gets hit with ransomware, there's a good chance it's only going to encrypt her files and leave our files alone. So you can do some proactive stuff to limit the damage. But the number one thing is backups.

MR. GREEN: Yeah. So, I mean, certainly the question is whether we should require this. I mean, I guess one of the nice things about ransomware today is that if you don't protect yourself against ransomware the way that Randy said, the consequences are you're in big trouble and, you know, maybe your users are in big trouble only in the sense that you can't service them anymore. But at least their data isn't spread across the internet. Right? It's lost.

If ransomware evolves into the kind of thing people have been concerned about where it's actually exfiltration where information is not simply encrypted but is actually stolen, it's much more challenging to do. But if that were to happen, I guess maybe the calculation would change.

Right now I guess, you know, the calculation that people are making is do businesses -- should we require that businesses protect their own operations,

or do we want to have rules in place to just require them to keep confidentiality of user data? And so these are really two things. I believe in protecting the confidentiality of user data and I also think people should voluntarily protect their data so it doesn't get destroyed. But I don't know personally whether we need to mandate that.

MS. NATHER: Yeah. The question of ransomware is, as Matt just said, you know, partially a confidentiality issue, especially if that data is exfiltrated and the attacker is threatening to expose it. But it's also an availability issue. And, of course, we saw that with NotPetya and other, you know, more recent ransomware attacks.

And the problem is that simply having available an air-gapped backup is not necessarily going to solve the whole problem. There are some problems that are much more difficult to solve like the level of connectivity needed amongst healthcare providers who have to be able -- again, for safety reasons, for health reasons, have to be able to share data widely and allow connectivity that, you know, is based on software that they do not control; that they can't rewrite; that they can't say stop using SMBv1.

You know, so, again, when we get into what

can we realistically enforce, we can enforce some solutions but not all of them that we would need to address ransomware. Is enforcing some of it better than -- you know, better than nothing? Possibly. It depends on how the regulations are crafted. And I leave that to wiser heads.

MR. MARCHANY: Well, and I think we just sort of all agreed that, you know, this is not enforceable. I mean, the primary vector that triggers the ransomware attacks is the end-user. You know, they click on something. So I don't know how they would -- how you would word a requirement in the regulations to prevent a ransomware attack.

MS. MCCARRON: Right. We have another question from the audience. In an earlier presentation today, it was mentioned that CISOs perhaps shouldn't be risk acceptors but they should be those who say yes or no; that a risk is mitigated as to the process or as a technical change.

So does that seem like something that is likely to be incorporated into the updated rule, that the board of directors or executives are the level of risk accepters?

MR. MARCHANY: Well, that would be nice. No, I've never accepted -- the only thing I accept

risk for is the data that I'm the data owner of. My job -- and this is from my predecessor; he set this standard. My job is to provide technical advice as to whether the risk that, for instance, Wendy as CEO wants to accept. I would give her technical advice saying, yes, the method that you want to address the risk looks good from a technical standpoint, but I'm not the one that's going to say you shouldn't accept the risk or you should accept the risk based on anything else other than the technical stuff.

MS. MCCARRON: Okay.

MS. NATHER: Yeah, I would say that the level of risk is a long ongoing discussion between the CISO and their management. And a lot of it has to do with probability. And with financial institutions, the ones who are very, very good at quantifying risk on a financial level can sometimes approach a level of quantifiable risk in security that makes everybody happy at that institution.

But looking at it from the outside, it can be difficult to say, well, I believe that technologically speaking this will mitigate 48.5 percent of the risk that we just agreed on. You know, that is very, very hard to do.

And the decision as to whether to accept the

265

risk, I believe, is ultimately a business one because mitigating that risk can cost money, effort, time. It can be an opportunity cost where the business is not moving forward on something else because they’re having to remediate something. And those sorts of decisions, including reputational risk, are not the sorts of things that the CISO can or should be making in my opinion.

MS. MCCARRON: Okay. Thank you.

So those are the rest of the questions from the audience. So I would like to wrap up by asking you all to just do a quick speed round, your lightning last thoughts on encryption and multifactor authentication that is in the proposed amendments to the Safeguards Rule. I would like to give everybody just about one minute to summarize or provide any additional thoughts. I’d like to start with Matthew, please.

MR. GREEN: Well, I mean, first of all, I think that we're in a great time when we’ve reached the point where we can actually mandate that encryption be used. I mean, years ago -- I’ve been in this field for 15, you know, 20 years now, I guess. And, you know, encryption used to be this exotic thing that was very, very difficult to use, very expensive

266

and not really feasible for securing information security systems. And we've reached the point where now it is something that’s come to be and we can actually build well. So I’m really happy about that.

And the same thing goes for MFA. We’ve reached the point now where we know that passwords do not work well. They are just simply not by themselves enough of an authentication feature. And fortunately there are a whole bunch of companies and inventors that come up with ways to make this better. And we're actually winning. I would say if you look at the overall progress of attackers versus defenders, the defenders -- when these systems are used and deployed, the defenders can win.

And now having those systems deployed is really the last final challenge. And I think that’s, you know, what’s great about these rules, is they start to make that happen. So that's it.

MS. MCCARRON: Thank you.

Randy, may I ask you for your final thoughts on encryption and multifactor authentication for today?

MR. MARCHANY: Yeah. I mean, certainly with encryption, as Matt said, it's become more commodicized, you know, now that it's not a big deal

267

from a financial standpoint.

As far as MFA goes, I always tell people, I say, look, when people push back, I said, you've been using two-factor for at least 15 years now. It's called an ATM card. And so when they -- when you hit them with that, they go, oh, okay, I got you. And so we've been doing this type of stuff over time, as Matt said. And I think it's finally gotten into the public psyche that these are good things to do. So it makes perfect sense to have these requirements in the Safeguards.

MS. MCCARRON: Thank you.

And, Wendy, may I please give you the last word?

MS. NATHER: Please, thank you. Yes, as Matt and Randy have both pointed out, we have a lot more options, a lot more technologies today than we did before that are making both of these solutions, both encryption and MFA, easier to use, more flexible, in some cases cheaper, and we should be encouraging their adoption wherever possible.

Having said that, we need to maintain the flexibility in the enforcement to allow for situations and environments where the organization can't necessarily rebuild everything from scratch. They

268

have to work with what they've got.

And, also, at the same time, we can’t be absolutists about finding the perfect solution and enforcing the perfect solution because that may not necessarily be practical. We just have to make sure that organizations are not using the equivalent of a decoder ring from a cereal box to solve -- you know, to mitigate their risk problems. But I believe we can do that today.

MS. MCCARRON: Thank you very much. I want to thank Matthew and Wendy and Randy so much for your time and for your expertise. Thank you very much for a very informative discussion. We appreciate it.

So this concludes the GLB Safeguards Rule workshop. I wanted to thank everyone for tuning in and for listening and for all of your excellent questions during the course of the workshop today.

If you have additional questions or any written comments, they may be submitted online at regulations.gov, any written comments related to the agenda topics or any of the issues discussed by the panelists of the workshop today. So please file any written comments that you have by August 12th so they can be considered as part of this rulemaking.

Again, thank you all very much for your time and your attention today, and the workshop is concluded. Have a nice afternoon.

(Hearing concluded at 4:31 p.m.)

CERTIFICATE OF COURT REPORTER

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

s/George Quade
GEORGE QUADE, CERT