FEDERAL TRADE COMMISSION

COMPETITION AND CONSUMER PROTECTION
IN THE 21ST CENTURY

Wednesday, December 12, 2018
9:30 a.m.

Constitution Center
400 7th Street, S.W.
First Floor Conference Room
Washington, D.C.

FEDERAL TRADE COMMISSION

I N D E X

P R O C E E D I N G S

WELCOME AND INTRODUCTORY REMARKS

MR. HO: Good morning, and welcome back to the second day of the FTC's Data Security Hearings. My name is Jared Ho, and I'm an attorney with the Division of Privacy and Identity Protection.

Today, you will hear from panelists on the topics of data security assessments, the U.S. approaches to security and FTC data security enforcement. We will also feature a fireside chat between FTC Commissioner Slaughter and Joshua Corman from I Am The Cavalry.

Before we get started, I just need to remind everyone of a few housekeeping matters. First, please silence your cell phones and other electronic handheld devices. Please be aware that if you leave the Constitution Center building, you will have to go back through security training. Most of you have received a lanyard with a plastic FTC security badge. We reuse those, so please be sure to leave them with security on your way out at the end of the day.

If an emergency occurs that requires you to leave the conference center but remain in the building, please follow the instructions provided over the building's PA system. If an emergency occurs that

requires an evacuation of the building, an alarm will sound. Everyone should leave the building in an orderly manner through the main 7th Street exit. After leaving the building, you'll turn left, proceed down 7th Street, across E Street, to the FTC emergency assembly area. Remain in that area until instructed to return to the building.

If you notice any suspicious activity, please alert building security.

Please be advised that this this event will be photographed, webcast, or recorded. By participating in this event, you are agreeing that your image and anything you say or submit may be posted indefinitely at FTC.gov or on one of the FTC's publicly available sites.

Question cards are available in the hallway on the information table immediately outside the conference room. Event staff will be available to collect your question cards. For those of you participating via webcast, you can tweet using the #FTChearings.

Restrooms are located in the hallway outside of the auditorium.

Now, it is my pleasure to turn it over to Elisa Jillson and Jim Trilling who will be moderating

the first panel of the day on data security assessments. Thank you.

PANEL 1: DATA SECURITY ASSESSMENTS

MR. TRILLING: Thanks, Jared, and good morning, everyone.

During the hearing, we have heard about some of the common attack vectors involved in data breaches and some of the challenges that businesses face in addressing them. This panel will discuss data security assessments and the ways that they can help businesses address those challenges. We have an outstanding panel that includes professionals from the data security, insurance, and accounting sectors. Their bios are available in hard copy outside the hearing room and also online for those of you who are viewing the webcast.

In order, we have Malcolm Harkins, the Chief Security and Trust Officer at Cylance Inc.; Carolyn Holcomb, a Partner at PwC; Troy Leach, the Chief Technology Officer at the Payment Card Industry Security Standards Council; Tom McAndrew, the CEO of Coalfire; Wendy Nather, the Head of Advisory CISOs at Duo Security, which is now Cisco; and Garin Pace, Cyber Product Leader at American International Group, which you may know as AIG.

We will use a series of hypotheticals to help guide this particular panel discussion, and we

are going to go straight into the first hypo.

Company A was a startup ten years ago with an innovative rent-a-pet model. The company now has over 150 employees in three locations. The company had no security personnel, per se, at first and then hired a few IT jack-of-all-trades to handle aspects of security. The founder has now hired a CISO for the first time. How should the CISO assess the company's security at this point in time? How should the CISO stay on top of the company's security?

Before we jump into the specific questions posed in the hypo, I want to start off with a few basics. Tom, security assessments can encompass a range of tests or analyses such as vulnerability assessments, penetration tests, and black box tests. How should businesses use each of those tools?

MR. MCANDREW: Yeah, so there's a lot of different tests that organizations use in assessing security, and each one of them have their pros and cons. There's kind of a spectrum of technical tests going to business tests and risk analysis. Typical tests, many organizations start with penetration testing. It's a way of basically seeing what the adversary might see out there, what your digital footprint looks like, and it can be a very

cost-effective way of looking from the outside of what an attacker may see.

Some of the limitations of something like a penetration test is it may not be able to get to what we call the gooey inside. So it may have a great hard shell on the outside of the business. There might be a lot of the things wrong on the inside. A lot of times you'll balance that then with some internal testing or internal organizations that may use different knowledge of the environment. This includes doing some basic reconnaissance or knowing how the organization's designed, where the crown jewels are and giving some guidance to assess where that risk is.

I think the key here is to know that there isn't really one silver bullet in any of these tests. They all have different limitations. They all have different effectiveness and cost models, and the key is really to balance the types of tests that organizations are doing with the risks and the levels of assurance that they would like to provide back to their business managers, stakeholders, and consumers.

MR. TRILLING: Thank you.

Carolyn, what published standards do assessors use when conducting data security assessments?

MS. HOLCOMB: Yeah, sure. There are a number of published standards to use, and I think it is critical that a standard be used, both internally and externally. So, for example, in this hypo number 1, the CISO would want to use something like an ISO framework or maybe the NIST cybersecurity. You could use the Carnegie Mellon Maturity Model. Those would all be very useful in determining how do our risks look, how mature is our security organization. Those can be used, like I said, internally. They can also be used by an outside assessor to understand how strong the security is.

And it's important to use one of those so that it's really complete. You know, when you really want a leg to stand on and say, hey, I've really done a thorough assessment, it's important to use one of those well-known, publicly available, tried-and-true frameworks. So those are some good examples of ones to use.

MR. TRILLING: Malcolm, some observers have expressed concern that some assessors do not add much value and some pedal products that may offer little benefit. How can a company find quality security products in assessors?

MR. HARKINS: Well, I think we have to start

first by looking at the fact that the current model we have is inefficient and ineffective. We're throwing bodies at the problem and it doesn't scale; it's not full scope. And some of the assessment techniques also point to, in some cases, written into the standards, dated technology that we know doesn't work.

So I think when a chief security officer starts to look at that, they have to evaluate the economic incentives and the model with which they engage a supplier. Do they make more money because of the continued pain and problems that I have and the impact to my company? Or are they incentivized to actually make sure that I get to a better level of permanent security?

Now, the other aspect of these things that I have to think about -- and we talked about pen testing and all that, but if I was coming into this hypothetical, my first thing would be to go do a compromise assessment. A pen test is checking if somebody can get in. I want to know who's already in there because they didn't have security people to begin with. So I have to understand where compromise has already occurred, fix that, understand how they got in, remediate those problems. And then from

there, I have a clean slate from which to build on.

MS. JILLSON: You raise an interesting point about the incentives. So, on one hand, you could see value in having a repeat assessor relationship because that assessor begins to know the business and so can build on knowledge over years of relationship with that company.

On the other hand, if you have a different assessor each time, perhaps you have better incentives because you aren't -- the assessor won't be looking to get next year's business as well, and you get true independence, at least that's one perspective. What are your thoughts on that, the repeat relationship versus an independent look each time?

MR. HARKINS: The repeat relationship certainly gives you a level of efficiency on both sides of it. But I do think you have to look at different assessment techniques and then go through a pattern of changing the assessors. We all have individual biases, just like every framework has a bias. And that bias then will lead you to conclusions that will leave you with blind spots. And what we've continued to have in the cybersecurity space is too many blind spots.

And so for me, there's a diversity and a

rotation aspect to not only the approaches you take for the assessments, but who you use for the assessments whether they be internally or externally, because you're going to get then a different perspective and a different interpretation of the results.

MS. HOLCOMB: Maybe just to highlight, if I may, one point, I think, Malcolm, you started on a little bit, is the different types. So doing the compromise assessment and a controls assessment and a framework assessment and an attack and penetration. So maybe just to emphasize that a little bit. I think it's really critical that those all be used at different times because they'll all give you different results and different insights so that you can try to avoid those blind spots.

MR. TRILLING: Can we unpack that a little bit? So what is entailed in doing a compromised assessment? And tying it to this specific hypo, which, you know, we've laid out as a company that may not have quite as mature of a security program as some others, what would a compromised assessment entail?

MR. HARKINS: Well, I think again there's a variety of ways in which you can do it. There's some in the industry that do it by throwing bodies at it,

and they send people in to go inspect all the systems. Again, that's a highly manual process. It's cost-intensive and it takes a long time.

There's other approaches where you can utilize artificial intelligence machine learning. You can give a small organization certain scripts to run in their environment. It collects the data off of those systems. It then brings that back and you can use automation then to figure out where a foothold may have been gained and where lateral movement may have occurred and turn those things around in days so that you can start then, if there's been a compromise, in remediating that issue.

MR. MCANDREW: And if I can add to that, I think one of the -- we did some analysis and did some surveys across our customer base, about 1,500 different folks, and a common issue particularly in this hypothetical is, while I agree that, you know, A.I. and machine learning and all this stuff is happening, most of these organizations that are pretty small generally have a similar profile in that they're just starting to kind of integrate technology. They tend to have IT or a CISO-centric view in a smaller organization, which is about getting more technology and building out what they need to do. But we find

it's basically cyber hygiene.

So in basic organizations, we're typically going to find that they're not doing basic patch management. They don't have asset inventory. They don't know some of the basics and some of the advanced items, and they don't know what they need to protect. And so what we would encourage before you throw bodies or technology or people at it, start with a baseline of really understanding how the business operates, what are the risks you're trying to address, and go down that path.

So just like in a financial audit, you wouldn't go and throw a bunch of auditor technology to go identify if there's fraud or if certain things are happening, same thing in technology. Before you go down that rathole, look at some of the basics and it may be more efficient to spend more time getting some of the cyber hygiene and getting some of the automation in place before you get another report of all the items that need to be fixed.

MR. LEACH: And I could probably add to that. Because this particular hypo, I actually managed an organization that was about 150 employees, and just recall myself being able to discover in my first day on the job that no one knew where the

information was flowing. So, being in PCI Council, in our standards, we always say requirement zero is being able to identify where all this information is.

Typically, when we see data breaches, many times the organizations thought they were protecting the right assets, had the right number of bodies and the right technology in place, only to discover they just didn't do the right risk assessment to evaluate and understand where the data was flowing to begin with.

So I think it does start with that type of assessment of understanding not only where the data is, but as Carolyn said about some of those frameworks, like the cybersecurity framework for NIST, it helps identify the value and the risk for each type of asset that might be flowing through your information.

MR. HARKINS: The one thing, though, that systemically we all tend to miss and we've -- I've seen this over and over again -- is the assessment models are looked at in terms of risk to me, risk to my organization, which we need to do in order to manage our fiduciary accountabilities. But in too many cases, we're not looking at the risk to our customers or the societal risk.

Now, in this hypothetical pet example, you can aggregate probably two macro risks. The revenue risk of not having the rent-a-pet model happen and then the risk that that would incur to the organization, or you could look at it in terms of the information you're collecting on the people who are renting pets and the potential risk to them, if you manage it wrong.

And too frequently, the organizations that are responsible for managing risk are looking at risk to themselves, not the risk that they're creating for others. And that's also a common failing of the frameworks that we have.

MR. TRILLING: Wendy, I think you wanted to weigh in, and I have a specific followup question for you, as well.

MS. NATHER: Okay. Yeah, I was actually one of the CISOs who was hired for the first time for more than one organization. So I know the feeling of starting at an empty Excel spreadsheet and wondering where to start.

I agree absolutely with Tom that these sorts of basics of how the company manages IT need to be looked at, but just because they're called basic or they're fundamental doesn't necessarily mean they're

easy. If anybody looked at the Equifax report that just came out, one of the problems that led to the eventual breach was that their certificates -- one of their certificates had expired. So certificate management would not necessarily be the first thing you would think of for cyber hygiene, but it's incredibly important.

Another thing is that, according to one person who analyzed the report, the person who was scanning for the struts vulnerability did not use the right flags in the command for scanning, so they were only scanning the top-level directory. And, therefore, yes, the scan probably finished very quickly and didn't find what they were trying to find.

So it's that sort of thing that needs to be looked at above and beyond what the cyber hygiene standards are. It's all about how the company manages its IT.

MR. PACE: Jim, if I may, I just wanted to add one other thing to the idea of that first security assessment. I heard Tom mention make sure we meet the risk with the appropriate amount of mitigation. And I think just understanding the threat model is also important, you know.

Another panelist said, make sure that we understand what risks we're trying to prevent. That's a larger part of not just maybe the maturity assessment, their framework, are they using the right controls. But are the controls they're thinking about, are they appropriate for the risk they're likely to have? What is their peer group? What kind of threats do their peers see and making sure they build that into their risk assessment where their business will be impacted.

Obviously, in this hypothetical scenario, it seems like the ability to take payments and find those customers who wish to rent a pet are important, but just knowing what are the business -- the assets that impact the business the most and what are the likely risks to befall them, I think, is sometimes a lost starting point.

And at AIG, we often see clients who are often in the process of purchasing cyber insurance, and they're worried about threats that aren't necessarily the first threats they should be worried about. That can be frustrating.

MR. TRILLING: Along those lines, Wendy, in what way do assessments take into account characteristics such as the size of the business, its

maturity, the type of the business, and, as Malcolm highlighted, the types of data that the business may be collecting?

MS. NATHER: That's actually a really complex question. And the problem is that, even peer organizations don't necessarily face the same IT risks. In one of the Verizon data breach investigation reports, they determined that within the banking industry, smaller to mid-size banks actually did not share the same risk profile as larger banks. They had more risks in common with retail.

So you actually need to slice your data in many different ways to look at how old the organization is, and that determines how much legacy technology they also need to bring into their security program, whether they're geographically dispersed, whether they're publicly or privately owned, and who their aspirational role models are, not just what their peers are doing in security, because sometimes their peers are not doing a great job in security. They need to look at who they want to be like.

And I know that doesn't necessarily work for a hard-core security assessment, but it's something that companies should be taking into account, especially when they're starting with zero, as in this

hypothetical. They can only go up from here. The question is, you know, in which way and with which priorities do they want to build their cybersecurity portfolio?

MS. JILLSON: So in the interest of time, we're going to move on to the second hypo, but I want to keep some parts of the first one in mind. So actually, let's go back to the first.

So here we were talking about something of a novice company, a startup, that was coming into maturity. Hypo 2 deals with a mature company. So Company B is a mature company with an internal audit department, a large security staff, and a CISO who reports to the board. It plans to obtain new cyber insurance.

How should the CISO, the board, and the prospective cyber insurers assess the company's security? What types of information will prospective insurers request from Company B to assess its data security risks?

This time I'd like to just hand the hypo over to you and let you tackle these tough questions with one more intro question, and that is, what is the difference in the context of data security between an audit and an assessment? And when should the audit or

the assessment be internal versus external? And I leave that open to you all.

MS. HOLCOMB: I'll start with a couple comments. So an audit is to really provide financial statement users. It's defined by the AICPA. It's generally accepted accounting principles or international financial reporting standards. So that really is what an audit is all about, whereas these would be assessments.

So if we're going to look at what is going on in security, we will start with an assessment. So that would be the primary difference there. An assessment is not defined in standards. So, rather, it's defined by the user or, you know, in the FTC's cases, in the FTC orders. The orders really define what an assessment is looking for. Specifically in a few areas, it talks about has to be performed independently; it has to be performed using standards, which we've talked about a little bit; and then it also has to be, as Jim just said, based on the complexity of the business, the size, the maturity, the type of business, the time of data, all that has to be taken into account.

And I think in this example, you know, I think the best way to go about this is using the three

lines of defense. If you're familiar with that, the first line of defense really is the security team plus the business. So, everyone who's responsible, kind of on the front lines, for security. That needs to be communicated, directed, clear what the policies are, the procedures, the standards, the controls. So that's your first line of defense here.

The second line, since we've got a nice mature company here, the second line is the risk management function, which will look at risks holistically across the organization. So risk and compliance and legal, those functions all teeming together to say security risk is one of the risks that the organization faces, how does that fit in with the rest of the risks that we have, the compliance risks and the legal risks, and putting that all together.

And then your third line of defense is your internal audit function. Not all companies have that, but in this hypo, the company does. So that third line of defense now makes sure that that's all fit together; it's working well. The internal audit group, in fact, all three lines of defense, will report to the board. All right?

That would really be the leading practice is to have reports that go to the board from all three

lines talking about security as well as other risks. So I'll stop there.

MR. LEACH: I'll add to that. Looking at assessors versus auditors, I think one thing that we encourage for PCI, we qualify assessors, and the idea there is that there are more coaches and teachers rather than the enforcement. And sometimes it's very hard to do that because, for audits, you need to have a metric to which you measure yourself and be able to demonstrate that you've achieved some level of security for your third parties in that assurance.

But for the assessors, the hope is both internal and external that they're not only looking at the problem itself, but they're looking at what are different solutions to the same problem? So typically, if we look at where we were five, ten years ago or later, we were just trying to throw more security, as Malcolm said earlier, you know, more people at the problem rather than can we change the problem.

So in the payment space, in particular, that's what we've been looking at is is there ways for us to devalue what the asset is? So can we create things that are proxies for valuable information? So instead of an account number that could be lost, could

we have a dynamic token that replaces what a criminal could steal and then use for fraud?

I think the internal versus external is a critical partnership, actually, where the external is looking at have you met this metric so that you can demonstrate these security functions are working properly for your trusted third parties or partners, whereas the internal assessor can maintain that the integrity of the process continues and that security becomes a part of the culture. It's a business-as-usual practice.

And we've seen that quite a bit in just the maturity of organizations to have those security champions within each department within these larger type enterprises, so that you're not coming to a PCI or HIPAA or SOX or whatever compliance requirement that you're facing and having to scramble to meet a milestone of just having met some type of expectation, but you're continually measuring to that line. And there's organizations that -- out there that have done studies on this that demonstrate that those organizations that are committed to that type of internal assessments are actually saving their overall compliance and governance budgets considerably.

The Ponemon Institute put out a study now

several years old, but that they're looking at PCI compliance specifically and internal assessments that were done two to three times throughout the year were actually saving the organization about 55 percent on their entire budget because they were not deviating that much throughout the year.

MR. HARKINS: The one thing that I think in this hypothetical, though, we're missing and the false conclusion that I think many people jump to is the fact that a mature company, therefore, has the appropriate and mature information security program with the right controls. Just look at the Marriott breach, Anthem, Target, Home Depot, OPM, on and on and on, organizations that have been around for decades that one, on one measure, would say are mature. So why is it then that they're getting compromised left and right?

And so I think we have to not assume that a mature company actually has adequate controls. And in my view, the way in which these assessments should be done is to look at the control effectiveness. We need to understand the root cause of what control failed and then figure out how to improve those controls. If we start doing that, we'll actually drive a level of real maturation in our control designs and then drive

the right level of accountability back to the organizations, as well as the solution providers who, in some cases, sold solutions that didn't work.

MS. JILLSON: That's a nice segue to another question that's posed by this hypo about cyber insurance. So one view is that cyber insurers potentially have that kind of data about controls because they are looking across the industry.

So, Garin, could you speak to that? Do cyber insurers accumulate data that would enable them to gauge the efficacy of certain controls? And in this hypo in particular, how would a cyber insurer go about assessing this company's security?

MR. PACE: Let me start with the second question because I think it will impact the first. The information requirements for cyber insurance, 15, 20 years ago when cyber insurance was first offered, they were actually probably the highest they've ever been. Insurance is a market, and we saw the information requirements necessary to be offered cyber insurance actually fall.

The past few years, they've actually been on the way back up, but some of my copanelists worked for insurers in the -- to help assess companies' security posture before cyber insurance was offered and some of

my copanelists still do that. But I think that they would agree that the most rigorous assessment, boots on the ground, several days with a security assessor with a lot of experience, was something that was only done in the beginning. We're seeing information requirements go back up.

For a lot of the reasons I think Wendy mentioned, the information requirements will vary depending on the amount of coverage being offered, the size of the company, the industry of the company, and the type of assets they have. Obviously, someone who's taking credit cards, there are a specific set of questions that we're going to ask about how they protect those assets.

But generally, the requirements for insurance are going to ask what is the governance model? Who is responsible for information security? What type of sensitive information do you collect and how much? Information that helps the insurer understand the maximum potential loss. And then, again, what is their control effectiveness, what are their control capabilities, and how likely is the organization to detect and hopefully stop any type of incident from happening?

MR. MCANDREW: And I'll add that there's a

-- this is an exciting field where a lot of things are changing right now. The common mistake that we've seen is typically, from the experience we've seen, the purchasers of these insurance typically come from the CFO or finance group as they're running the business, and a lot of the times they may send the CISO or an IT manager a survey to fill out, and that's the extent of it.

And then what we find is post-breach or post-incident and they look at their insurance coverage, they realize that it only covered a certain amount, or as Malcolm mentioned, you know, like in some cases, they don't realize the entire risk that they had or what could have happened.

So one of the things that we really encourage folks to do is, you know, cyber insurance is a form of risk mitigation or transferring that risk. It's not a CFO function; it's not a CO function. It really is a business function and it's important to get everybody together.

The second part that's really happening here is the technology and the technology enablement to get smarter about this. So an annual assessment or sending people in or a one-time technology really is a point in time and provides some basic data, but you

will see, in my opinion, over the next couple years, much more ways to get automated data of, like we mentioned, some of the basic cyber hygiene to make sure that things are happening the right way in this model.

And I think, you know, there's a good point of, you know, this organization being a mature company, we like saying security is a journey, it's not an end point. And so organizations must constantly shuffle around where their investments are in tools, technologies, people, process, and, like Troy said, one of the biggest things that people can do is change their business model, go through a digital transformation.

We had one organization that had a thousand different locations that each one of those locations replicated millions and millions of sensitive information. And the tools and technology may tell you to encrypt it, to spend more information on to protect, but a little architecture design eliminated all that data and outsourced all that data or moved it into a different area where they could focus on that.

So there's kind of a balance that's happening right now of is it better to disperse your data and manage a larger group hoping that that's a

better way of managing security through obscurity or is it better to know where your data is and spend and concentrate more information on that? And that's where really, you know, today, where the industry is going to right now, which is don't have your data in so many different pockets, minimize that, and overinvest into those areas.

MR. PACE: So I want to build on two things Tom said and then come back to your first question about how insurance might be able to help this improve control efficacy.

So first, several insurers are using some of these lightweight external outside-in scans to try and get more objective views and assess cyber hygiene. But that's a good thing. I think the challenge is that -- you know, I agree with you that the cyber risk is fast-evolving. If you look at insurance policies, they're generally written on an annual basis, sometimes even longer periods, and it can be tough to, particularly with some of the regulatory reasons, to move that model to something where we're going to price risk more frequently. But, nevertheless, there's a lot of development being made there.

Back to the idea of can insurers help with control efficacy, it's linked to those information

requirements. The more insurers know about what a company looked like before something went wrong and then understanding what happened, what went wrong, and also understanding what do the companies look like who didn't have something go wrong, the more we can say, these are the controls that matter.

And I mentioned earlier that the amount of information requirements necessary to get cyber insurance reach their low, approximately four or five years ago, and have been on the uptick since, but we -- the insurance market needs better information to be able to analyze and then turn around to our insureds and say, these are the controls that matter. And I think that we are doing that and I think that's part of the reason the insurance market -- I know my own company is doing that, and why we're asking more questions and we're doing more analysis.

But it will be hard to do that because there was a period in the cyber insurance market where, famously, some insurers were offering insurance on the backing of four questions. We're not going to give good efficacy about these are the controls which stop the most common types of risks or these are the controls which if done this way fail, if we're only asking a handful of questions.

MS. NATHER: So going back to the question about whether internal or external assessments should be used and when, obviously, the answer is both, because external assessments or point-in-time assessments can often turn into a catch-me-if-you-can game. And that plays right into the way that some companies look at cyber risk, which is kind of the way that you think about how you're going to eat cheeseburgers until your first heart attack and then you're going to stop. And this kind of cheeseburger risk management is, unfortunately, pretty widespread today.

And the other problem is that you cannot stop eating cheeseburgers and go on a vegan diet two weeks before your doctor's appointment. That's just not how it works.

So, in order for these companies to make a lifestyle change in their security assessment, they need to be self-assessing, as well as getting external assessments, but also making a fundamental change in how they manage their day-to-day operations and their security so that it doesn't turn into a studying-to-the-test scenario. It's actually a fundamental change in how they manage security every day.

MR. HARKINS: One other thing just as a quick comment for assessors, for folks to consider, the assessment process itself actually poses a risk to an organization. If the assessor finds issues in your environment, finds vulnerabilities, and they're doing it in the aggregate for multiple companies, they're a target, because if I'm a bad guy and I can compromise the assessor, I then know all the nooks and crannies of where there's control deficiencies in their customers.

So we have to also think about that as organizations -- and as the chief security officer, when people assess me, particularly externally, I see them as a risk and I need to assess their ability to manage and protect that data. And we've certainly seen assessors get compromised.

MR. TRILLING: With that, we're going to move on to the third hypo. So Company C is a mid-sized firm that has long struggled with patch management and third-party vendor relationships. It hires a new CISO who wants to understand the scope of these problems and of the company's security generally.

How should the CISO assess the security situation? How are these persistent problems relevant

to Company C's ability to obtain cyber insurance?

So for this one, let's go straight into the questions in the hypo beginning with, how should the CISO assess the security situation at Company C?

MS. HOLCOMB: I'll start with the third-party piece, maybe, to break this down a little bit. So vendor relationships, that's a big risk these days, as you've seen Malcolm mention some of the breaches that have been caused by third parties.

So the first thing there really is to understand what's the governance program? Do we have somebody or a group of people responsible for vendor risk management? So who's that? How are they doing it? How are they understanding what the risks are?

Number two, back to understanding what data you have is understanding what vendors we have. We certainly find a lot of organizations that really don't have that full inventory together, really don't know all their vendor relationships, what data those vendors have, whether they're in the system or receiving data, you know, what that flow looks like.

Then you go down to the contract level. Do we understand what the contract language is? When does a vendor have to tell us that they suspect a breach? When does a vendor have to have strong

security and privacy controls? Do we understand what those are? After we get through the contract, then it's real monitoring and understanding what those controls actually look like. So assessing your vendors, putting them in tiers, leading practices to put your vendors in tiers according to risk. In the old days, that used to be financial risk.

Tom mentioned, you know, sometimes the CFO is doing these types of analysis, and so you might have vendors only assessed according to how much you pay them when, in fact, it really should be what is the data that they collect and how do they get it; what's the means of obtaining that data. Then once they're in those tiers, it's understanding now what are we going to do? Are we going to go onsite and do assessments? Are we going to do questionnaires? How often? Twice a year? Once a year? Once every two years? There are all sorts of permutations, but it's really understanding and putting a whole program together around these third parties and making sure that they're monitored in an ongoing way.

MR. HARKINS: You know, to add to what Carolyn said, and I think, again, we jump as CISOs to thinking about just the security risk. There's privacy risk. There's business continuity and

disaster risk, depending upon where they fit in your supply chain and what operations they're supporting in their organizations. You have to widen it out.

And then transitioning to the patching stuff, when I assess patching, patching is both a hygiene item for managing risk, but patching also poses a risk, because you're adding code or taking away code. So you're creating a change, which creates an operational risk. So we have to think of patching not as a panacea. It's a good thing to do, but in many cases, patching can actually generate equal or greater risk to a business.

MR. PACE: So I just want to -- maybe I'll address the insurance question and then build on that. Obviously, the applicants for insurance cannot misrepresent the risk. One -- and, today, most cyber insurance markets are going to ask questions about their -- the company's patching strategy and their cadence for doing so, because it is, obviously, important to the risk.

They want to understand, for instance, their ability to inventory their software and consistently patch and then, in the event of some type of assessment of a particularly impactful vulnerability, do an out-of-band patch.

So it's going to be something that's asked about by the insurer. And I would expect, from my experience, a company who has in the past had trouble patching regularly, who has a lot of end-of-life systems, they should expect to pay a higher premium and get less favorable terms. That said, it is not an absolute exclusion. There are plenty of companies out there who are still rocking XP and have cyber insurance. They pay a higher premium. They should expect to have more questions about their compensating controls for that risk. But coverage is there.

MR. MCANDREW: To add on, I think -- so there's three -- there this is the third scenario that we've done now. What I like about this, we started with a very small one. Then we did a large organization and this is the mid-sized. We did some research into this to look at were there some common issues or strengths or weaknesses across the sorts of customers that we support. And we did find that actually the mid-sized organizations actually were the best, were in kind of the sweet spot Goldilocks zone of patch management.

So if this is the case, then it's probably a bad thing for this organization because we typically find that smaller organizations don't have the

resources. They're dealing with lots of technology. They haven't figured out how to integrate it. The medium-sized organizations have really optimized that the most as they're trying to figure it out. The large organizations, like Malcolm said, it's harder to change. They have more interdependencies. They have legacy software. So we typically find these medium organizations are more agile and able to do some of the hygiene a little bit better.

On the flip side, what we find is they're more vulnerable to phishing attempts because they don't have the policies in some of the other areas that a more mature organization may have like with badging and some of the background checks. So I think the key for this scenario is to realize maybe that patch management is a big risk. Maybe the third-party vendor management is a big risk. Maybe there's a business model risk. There is no one answer. But, hopefully, the CISO that's coming to this organization is going to bring some background and the key is to make sure that's integrated into what the business challenges are and how they want to manage their overall cyber assurance.

MS. NATHER: We can also look at the problem with patching as an ongoing symptom of the complexity

of the IT of that organization because, in general, if you don't understand all of the stacks and layers of technology that you have, you're not sure what's going to happen when you patch or there are so many dependencies that it's hard to figure out, like a Jenga tower, which piece you're going to start pulling out first before everything falls down around you.

So looking at the complexity of that IT environment and trying to simplify it, as well as improving the overall management is, you know, the underlying root cause that will probably -- could probably help with the patching problem when it's under that organization's control. When an organization is small or not influential and doesn't -- and isn't able to influence the patching schedule of software that it bought from companies that are now out of business or XP that, you know, is out of life or for equipment that was never intended to be patched, then it's in a much more difficult situation. And I think that's something where we can look on a larger level about how we can address that type of patching problem.

MR. TRILLING: Can I follow up on those points, Wendy, and circle back to some of what Carolyn said at the outset when talking about the third-party

vendors? Focusing on the company in this particular hypo being a mid-sized firm, are there additional lessons for this type of company beyond what Carolyn mentioned in terms of thinking about how to manage the risk of dealing with vendors that may be much larger than this particular company?

MR. LEACH: Yeah, I can start with that, because -- to what the fellow panelists -- talking about dependencies. When you start in the mid-sized term, I agree with what Tom was saying, that small businesses are still trying to do it in-house and, by the time they're a mature enterprise, they have some of their third-party relationships and those contracts figured out.

But for the mid-sized organizations and a lot of the breaches, as Carolyn mentioned earlier and also Malcolm, we're seeing these third-party dependencies is a growing high percentage of the risk. And so the challenge is -- and we talked about questionnaires earlier -- is how much do you trust your third party actually understands and knows the risk associated with your business?

And we've seen, especially in the cloud services area, we've seen a lot of assumptions that the third party that is managing, whether it's the

infrastructure or the software, whatever it might be, there's an assumption that that organization is doing all the things to protect my assets, my information that's processing through their environment. And the challenge we've seen in some of the compromises or just in general assessments being done is when they start to dig beyond just a questionnaire, they start to identify that, oh, my third party was PCI-compliant, for example, but they were PCI-compliant because they also process payments and they had an evaluation against their processing environment, not the processing environment that runs on that platform for my services.

So I do think that the due diligence of third parties and managing that relationship starts to become critical for these mid-sized that, for the first time, are starting to outsource and trust these third parties to manage those exercises for them.

MS. HOLCOMB: That's a great point, especially on the scope of the PCI, Troy, like you're alluding to there, because one thing that a mid-sized can do, if your vendor is the large company, then they typically have SOC 2 type reports, you know, something from a third party that could give you some assurance.

So on one hand, that can be really helpful,

because you can look at that and say, okay, did that third party independently assess that large vendor's security and privacy? But the same as what Troy said, you have to look at the scope and you have to be careful. Did it actually include my data at the right time, on the right systems? What were the findings? What were the exceptions? You really want to scrutinize that report and make sure it is useful. But it's certainly a good way for the big vendors because all the big cloud vendors get those. Most of the big organizations will get those, which is helpful to a mid-sized.

MR. HARKINS: The one thing that I think we also have to think about that I think, again, people tend to focus on is they'll think of the IT vendors, the data vendors. And the vendor risk management program should be all vendors. Your lawyer presents a risk to you. Your accountant presents a risk to you. The cleaning crew that comes in, if you have sensitive data and you have people leaving it on the desk, and you don't have a shredding program for that data, presents a risk to you.

So it has to be systemically across, in essence, all the vendors including the ones that might be managing the industrial control systems going into

a factory or the water coming in, because, again, all those present risks. They're all getting connected to devices that could be then compromised in a cyber fashion or compromised in a physical fashion, like picking up sensitive documents off of somebody's desk and taking pictures of them.

So we have to think about the vendor risk management much more broadly than, I think, typically people are focused on in the IT space.

MR. PACE: That's the point I wanted to make, to add on to the idea of, yes, a vendor might be able to manage a piece of software with more expertise than you can manage. Certainly, there's some cloud providers out there who provide software suites and they are the experts in assessing the security of it and keeping it up to date. But, from a -- I think, as a -- maybe it was Malcolm mentioned, there's also a business continuity risk and there's certainly a reputation risk. Your customers aren't necessarily going to understand when you say, well, it was the cloud provider's fault. And there's also the idea that a certain amount of aggregation and a potential lack of diversity and more complexity does create potentially more risk when you look at an entire cloud region going out.

So from an insurance point of view, when you're looking at the vendor, doing that vendor risk assessment, there's some benefits. But I think they also need to make sure we take note of the potential risks in that, you know, you're entrusting your business' ability to run on that other vendor. It's a dependency. And there's also -- you can't -- you can't outsource that liability to your customers in that reputation risk.

MS. JILLSON: In the interest of time, we're going to move on now to the next hypo. Company D starts processing payment cards for the first time. How should the company assess its risk on day one of payment processing and going forward?

And, Troy, maybe you can start us off with this one.

MR. LEACH: I think it goes to some of the principles we've already talked about. Hopefully, by day one, they've already done quite a bit of analysis as to how they're going to be processing payments and how that is going to be -- what organization departments are going to be touching that information. And, also, they've done due diligence. Most likely, they're using third parties for at least part of this processing. They're looking to see if those -- the

terminals themselves, the point-of-sale terminals or whatever mechanism they're using to accept the cards, are going through laboratory assessment.

So, at the PCI Council, we're probably more known for the PCI DSS standard for assessing the environment, but a majority of our standards are actually technical standards for the lab -- the vendors that provide all of the technology, whether it's the payment cards themselves or the point-of-sale terminals. And so, hopefully, they've done their due diligence to research to make sure that the technology they're using is being done in a way that is lab evaluated, hopefully through a PCI-certified lab. They also are looking at how they installed it.

Probably the biggest thing, especially for small merchants -- we don't know the size of Company D, but if we were to assume it's a small to mid-sized company, one of the biggest challenges we see is they think that just plugging in a terminal is a very simple act. And we've seen, especially in the small to medium-sized businesses, they bring in someone that has no technical payment security experience, and then what they'll do is they'll plug in the terminal and say, you know what, I cannot connect to my home office, so I'm going to disable the small merchants'

firewall. And then, all of a sudden, the terminal can communicate and process.

So you'd have to have someone that understands the payment and, hopefully, by day one, they're looking to make sure that they have technology that is currently certified. But they're also using people that are trained specifically in payment processing and the security associated with it.

MS. JILLSON: Can we focus, in particular, on the risk on day one versus the risk going forward? So is the PCI assessment a point-in-time assessment? What does that mean and what does that mean for security on day two when the assessment has focused at that point in time on day one?

MR. LEACH: So, I can speak to the PCI assessment a little bit, but probably turn to my colleague, Tom, that's seen thousands of these at this point in his career.

For the risk assessment for the PCI DSS standard, it's really matured over the last 12 to 14 years since its creation. And the intent has always been that there is a continuous process of securing the payment information. And that the assessment that is done is, while it might be a point-in time, say, three weeks, a two-week assessment, it is actually --

the intent is that it's evaluating the process so that when the assessor leaves that environment, three, four, five months, as the technology and the personnel change probably multiple times in that time, they have an opportunity to continue to have good security hygiene throughout that processing environment.

So for the key -- if a company is looking to add payment processing for the first time and maintain that level of high degree to a PCI DSS evaluation, what they really need to have is security champions throughout the organization, not just isolated into an IT department, as Malcolm was talking about earlier, but there are security and payment security champions throughout the organization that understand the risk and the reason why they go about doing those type of assessments.

Tom, I don't know --

MR. MCANDREW: Yeah. So, as Troy mentioned, I think one of the key parts on this is, in the beginning -- and we ran this outcome. There was a misunderstanding of just fundamentally how credit card processing or what sensitive data needed. So for example, most organizations don't ever need to actually see a credit card number. Right? The reason they're processing -- they're not in the business of

collecting credit card information and building a repository; they're in the business of selling products and getting paid.

And I remember with work in the very beginning, we would ask people why do they have millions and millions of historic numbers or all these receipts. And some of them had a misunderstanding, they said they needed that for chargebacks or they needed that for X. So one key part, as Troy mentioned earlier, is that the technology is changing very quickly, particularly in this space, for mobile, to web, and so it's important that, as this organization goes, they're aware of what they're doing. Otherwise, they might be putting all their protection on a terminal and, in this case, maybe everybody is copying those numbers when the systems go and they're putting them into a database.

Very typically, we find other systems, like marketing or other areas, where they want information for their consumers to get information and they're capturing that and they really don't need it. So one of the key items for here is to make sure that whatever they are retaining moving forward, they really understand what that is and that should be part of their PCI assessment to make sure that that

continues to go.

One of the best things I think we can do on assessors is to minimize that risk. Right? Ask them why do you have ten years? Do you really need three month? Do you need six months? Look at the data. What percentage of chargebacks do you have and is the risk that you have of keeping this worth the liability or potential liability you have?

And a second part we find is -- and this is, I think, where some of the -- as we come in from PCI or some other areas that you're providing some assurance of this process, it's very common we find that PCI is just one of 10 or 20 different types of sensitive information they're keeping. They're keeping social security numbers; they're keeping driver's license; they're keeping passports. So this then generates -- balloons into something larger to say what is the business model and how they're doing that.

So a typical part for these folks are really to focus on transferring that -- you know, taking the payment card information, understanding why they're keeping it, minimize that, and then as part of this, use that as an overall risk management structure to drive security and privacy improvements in the

business overall.

MR. HARKINS: To add on to what that Tom was saying, which I think is perfect, and coming from a company that actually I'm responsible for PCI compliance because we just launched a consumer product, and that consumer product, we're doing the payment processing with an outsource vendor. So again, getting back to the third-party risk. And then our product actually protects payment card data and some of our customers. So our product has to be PCI-certified.

So having gone through this on sides both as a -- in essence, a processor of credit cards and then a provider of protection to those environments, it's a great way to evaluate it. But I think Tom makes a great point. You have to think about the data minimization, because in some cases, the risk is larger because people are just hoarding data without really understanding do they really need it.

And then I think the other thing that I've found, having been assessed from two angles, is that the PCI DSS standards, though good, are not necessarily all that you need to do. You need to think beyond those standards and think that you shouldn't think that just meeting that standard means

that you're secure, because we've seen, day in and day out, retailers who have had PCI compliance get breached. And so you have to think about it as, in essence, perhaps, a minimum standard but not necessarily the level with which you might need to go to truly manage the risk to your company or the customers you're serving.

MR. MCANDREW: Yeah, I'll add on to that because I've heard both -- you know, we talked about auditors and assessors and what's the difference between them. There are -- about four or five years ago, there were a lot of people that were kind of on the compliance is the minimal but security is the goal, but then we'd also say, but you're never -- there's no such thing as security. And so there is kind of a lot of confusion, I think, of, well, should we really do.

And I think really the term is kind of assurance that we're looking at, is when you look at the spectrum, what level of assurance do we have as organizations to make sure that the systems are operating, we know what data we have, and we're not negligent. And that level of assurance includes technology; includes systems; it includes frequencies of assessments; it includes internal/external; it

includes automated tools.

Negligence is you don't look at that and there isn't an understanding of how you're providing that level of assurance. Negligence is not knowing what information you have and not even knowing that it exists out there. And the key organization -- these types of key programs, is every year there should be higher levels of assurance and higher levels of automation that the information is being identified, protected, and minimized.

MS. JILLSON: One more question on this hypo, and, Wendy, I want to go back to your cheeseburger example. So how do we avoid the cheeseburger problem here, that a company says, my PCI assessment is coming up soon, and so I'm going on my diet, I've been doing cheeseburgers all year, but now I'm really going to get my house in order for this assessment? How do we avoid a point-in-time assessment being a continual process of eating cheeseburgers and dieting?

MS. NATHER: Well, if you've ever tried to get somebody else to stop eating cheeseburgers, you know how difficult that is.

(Laughter.)

MS. NATHER: But part of it is literally

that if the business does not see the risk of a cybersecurity breach as more substantial than its risk of going out of business, for example, because it's been spending too much money on IT, then it is not going to adopt that new lifestyle.

And so it is a fundamental problem of getting businesses not necessarily to understand and agree with the level of risk, but to understand that there's a certain level of due diligence that they need to follow regardless of whether they believe in the risk or not. And that it has to do with, as other panelists have talked about, with obligations to their customers, to their partners, that the business risk is not just theirs to take. So we certainly need to approach it from that perspective.

MR. MCANDREW: I was just going to add on --

MS. HOLCOMB: I would agree with --

MR. MCANDREW: Go ahead. I was going to say just to add on to that, one of the big changes that we're seeing now is IT -- it's gone from IT risk to company risk to starting to become board-level risk. So the National Association of Corporate Directors is looking at 2019 and some of the surveys they found is digital or business transformation and cybersecurity or privacy are two of the three top risks that boards

have. Don't assume that boards have knowledge around cybersecurity risk. We typically find many boards have financial or business background, but they're not aware of it.

So there's a great opportunity now to make sure that there is the education from vendors, other folks in the industry, to come back. And that's a key part that we would encourage everybody to do now, is ask how is the organization informing senior management of what cybersecurity risks are happening so that they can make adequate decisions and recommendations in governance processes.

MR. HARKINS: To tie back to the hamburger and payment card and to tie what Tom said about --

MS. JILLSON: It's a cheeseburger.

MR. HARKINS: Cheeseburger, yes.

(Laughter.)

MR. MCANDREW: An incremental improvement is the hamburger, getting the cheese off.

MR. HARKINS: Yes, exactly.

(Laughter.)

MR. HARKINS: But a true story in understanding the risks to Tom's point that I had a couple of years ago with somebody in the fast food business, that they said their CEO and their board

didn't care about cyber risks. And we got into a bit of an argument, and I said, well, what are you talking to them about? No offense to the PCI and all that stuff, but they were talking to the board about payment card industry standard compliance. And I said, well, no wonder the board doesn't care. That's a revenue risk.

I go, you know, what about the food safety data? You don't own the slaughterhouse, but the only way in which you know that the hamburger meat is good is the information flow from the slaughterhouse all the way through the point of sale. What is your cybersecurity program for your food safety data? They didn't have one because they were focused on revenue risks and PCI compliance. And when I told them that if I was some animals rights whack job activist and I could muck with the integrity of that data, I could kill your costumers. And I could be an insider or an external person doing that. That was the relevant risk that then got board relevance, that then got them to understand what they needed to do.

And what we've got to do is think about, not only, again, like I said, the risk to the company, but the risk to the customers, and then put those things together. And then, I think, Tom, to your point, when

you do that, you will have the right board items. And to what Wendy said, you'll then have the right culture to then figure out how to control for the risks.

MR. TRILLING: In the interest of time, we actually are going to move on to the next hypo. Did you have something that you wanted to say quickly, Garin?

MR. PACE: One point on that scenario, one of the things I didn't hear was risk quantification, and I hope that as -- you know, to tie what Tom and Malcolm said with a bow, they are understanding how much data we are storing, and as time goes on, how much sensitive data do I have. And then you can quantify, you know, there's been enough data breaches now, there's enough sources out there to say, if you lose this amount of data of this type in this part of the world, where these regulatory laws apply, this is how much it will typically cost you.

And I think that back to the point of data is not only an asset, but it also is a potential liability, that people need to be doing that assessment. To Tom's point, you know, is it worth holding on to this credit card that I took from a customer a year ago to pay for a cup of coffee? They're not going to return that cup of coffee. Is it

worth the liability of holding it to maybe do some marketing with it or know who they are?

MR. TRILLING: So for our fifth hypo, Company E hires a penetration tester and discovers some significant vulnerabilities in systems that hold customer information, including payment card data. However, the company is going through a difficult financial time. How should the company proceed?

I want to start off by asking should the assessor make its findings, regardless of the company's ability to afford to remediate them?

MS. HOLCOMB: Absolutely.

MR. HARKINS: Absolutely.

MR. MCANDREW: I mean, I would add absolutely. But it is a consideration. I mean, I think one of the issues that we deal with in cybersecurity is there is this perception, and I think a lot of us have it, that we go around and always we find problems, and we're disconnected from what the business risks are. So while they should definitely report it and management be aware of it, should they immediately patch this? Well, I'm not sure. There might be something else that might be causing it.

Think about if this is from like a typical brick-and-mortar. This would be similar to a toy

vendor right now that has a broken window and a door that can't lock in the front. Should they immediately go out and close their shop and get the window and miss all of the shopping or do they take that risk? We don't know.

So these are the decisions that people have. So I think the importance from the security or the pen tester here is to be able to translate these vulnerabilities into what the business risks are. So in this case, if the system has a bunch of vulnerabilities, but like Malcolm said, it's an older patched system, they decided not to patch it and they've implemented some other controls around it, it may be not be as appropriate.

If it's the other scenario, you know, that Troy mentioned, and the system is directly connected to the internet and anybody at any point in time can do this, it's probably something they should immediately work on.

So I think one of the key parts for pen testing or any pen testing organization is to work on, what are the recommendations, how do they solve it, and how do you prove that you can come back in, and that organization is improving? And the second part is really asking, how did this get there? What was

the root cause analysis? Was this lack of training, lack of awareness, is it lack of people, resources? All of those things come into this.

So what I like about penetration testing, vulnerability scanning, a lot of these technical ones that you do, is they're -- I like to think of the root cause analysis. So going back to the hamburger, there you're physical. You're doing your physical with your doctor and they come in and they tell you where your heartbeat is, your blood pressure, and you have to look at all those things in context to figure out what needs to happen.

But the other great part about the doctor is that they tell you, I saw 20 people today and you're the 20th of 20 in health. That's another good symbol that maybe, you know, your internal perception may not be the appropriate one. So I think really making sure that you understand exactly how that works with other folks is critical.

MS. NATHER: So going back to the cheeseburger analogy, now we'll add some bacon on it to really raise the stakes. The problem is that from a financial point of view, if you are not -- if you know what the possible impact of a breach is, but you don't believe that it is likely, if you don't believe

that it's probable, then your financial calculation is going to be different.

So let's say it would cost you a million a year to have a security program and you don't get breached until your second year, and it only costs you $500,000, you came out ahead. So from a purely financial standpoint, it doesn't always make sense for a company to go all out in addressing its security risks if that incurs substantial financial risk.

And let's be honest, we cannot say today whether small companies can actually afford the security that we recommend for them because we can't always say necessarily how much it will cost them. So that's the other complication to this formula.

If this company does know about some vulnerabilities, that is not the same thing as saying when the breach is going to happen or whether it is going to happen. So can they buy time while they improve their financial situation and decide they're going to address the vulnerability later? It is a calculation and it may pay off for them. So that's the other dynamic that we need to address more widely is that possibility is not probability. And we don't know what the actual cost of security is going to be for some of these smaller businesses, or even the

larger ones, for that matter.

MR. TRILLING: I know that others want to weigh in and I want to add something that you may be able to factor into your comments. In your experience, do companies with limited resources tend to shy away from having assessments because of concerns they might have about their financial wherewithal to remediate them?

MS. HOLCOMB: Yeah, I'll make a couple of comments on that one. First of all, it is culture. I think we've alluded to that a few times. I was going to say we did a survey recently of 10,000 companies responding saying that only 37 percent of them feel like their board understands the cybersecurity risk within the organization. So back to board reporting.

But here, maybe even at the management level, I think one of the keys that we haven't mentioned is making sure the right people are weighing in on the decision. So leading practice is to have a steering committee, whether it is your data governance committee, your security committee, your privacy -- whatever it is called -- but some committee of folks that are from the business, from the legal aspect, from the compliance aspect, and from the security that are making this decision together, so it is not just

the security organization looking at priorities.

So this is going to be a matter of priority. Yes, the assessor or the internal system, or anybody, should come up with all of the problems. So whether it's the heartbeat or the lungs or whatever it is, you know, have the full list, but then you have to prioritize them, and you want to have the right people prioritizing and then looking at the cost benefit of each one.

MR. HARKINS: So I'm going to take probably a controversial view on this. I don't think it is a prioritization problem first. I think if you start that way, you're going to be trading off and saying, I can't afford it, so therefore, you're not going to do it.

I come from a basis and a view that innovation comes through starvation. I'm a former finance guy. Look at the total cost of controls. Look at the security controls that are in impeding the business velocity. That companies having a financial problem, they probably have solutions in place that are controls in place that are degrading computing performance. There is cost of capital. There are so many ways in which you can look to fund a security solution that is better. If you start with just going

with this or that, I don't have the money, so therefore, I can't afford this, you're limiting the solution set with which you have to innovate around.

That's also the problem I see with a lot of chief information security officers. They don't have the business acumen to look at the entirety of the business and figure out how do I optimize the business velocity, how did I optimize for the risk, and how do I actually protect to enable the mission of the business? And I think if they frame it that way, they'll have more opportunities to figure out how you do both, improve the financial situation with the company and manage the risk.

MR. MCANDREW: I think to add one important part on this, and we've seen this a bunch of times -- so I don't think what you said is particularly controversial. I mean, I agree with that. One of the common problems that we found on this is, who is the stakeholder of this report and where is it going. So we talked earlier about audit versus assessment and where this goes. If it's an IT or a CISO that's typically hiring a pen tester, they generally -- you know, CISOs are generally charged with improving security. They generally don't want to tell their bosses about all of the issues they have. Right?

More mature organizations are able to differentiate that, but it's important to realize that there may be different things that different organizations want to do. So in this case, maybe the right solution is to minimize the IT staff. Maybe the right solution is to outsource vendors. The IT manager typically is not going to do that. So in order to get this transformation that Malcolm talked about or this innovation, we have to realize that it may not necessarily be in the best interest of the IT or the business or the stakeholders today.

So critical parts of these organizations are, who's getting the information, where is that going, so that the business can make the right decision of what they might want to do, and that may not necessarily be in the best interest of every one of those employees.

MR. LEACH: And I'll add to this hypo, when we look at this, too often we rush to the technology or the people. And often for organizations that are struggling financially, it really is the process, and being able to identify are we processing payment card data, for example, in a way that is -- do we have to spend all of this time focused on the security of the infrastructure, or can we be able to turn on

encryption.

One example of an organization that was struggling financially, they didn't even know that previously, in previous leadership tenure, they had purchased tokenization and were about to -- rather than overhaul the infrastructure, which they thought they had to do because there were security flaws in the environment, they were able to devalue the data by just minimizing how they turned and changed the process and changed where the information flowed through their organization, and then started to devalue.

I think to the earlier point on the lifestyle that Wendy talked about -- I mean, I'm starting to get really hungry for lunch all of a sudden, I don't know why. But so many times we talk about, well, PCI compliance is not enough, and we have to make sure that we understand the PCI practices versus the compliance to a one-point-in-time attestation. So within the standard itself, it's over 200 requirements that are business continuity practices for good security process, and being able to make sure that those security practices continue to be in the environment.

The attestation that comes from having an

external assessor come in and confirm that these processes are in place, that is -- a lot of boards like to point to that because it's tangible. It's a piece of paper that they can hold up and say, we met this level of compliance. But the reality of security, and actually of PCI security, is that it's an ongoing process that is supposed to be part of that lifestyle. So that when you go to have that doctor checkup or that PCI evaluation, it's really just confirmation that these processes you have in place to secure this information have been in place and will continue to be in place for some time to come.

MS. JILLSON: So in the interest of time, we're going to move on to the next hypo, and for the next -- we have two hypos left. And for these, we want to switch gears a little bit and talk about FTC assessment. So under FTC consent orders, companies are required to have biennial assessments. I'm going to read this hypo and then fold in a question from the audience.

Company AA is required by FTC consent order to obtain biennial assessments. The company believes that system X does not contain any consumer personal information covered by the order, so it negotiates with its successor a scope of work that takes system X

out of review. Setting aside legal issues, what are the implications for the assessment process of this carve-out?

So I would like you all to address that question. And we also have a question from the audience that has to do with some assessments that have been submitted to the FTC, and since then, there have been revelations about certain companies' data practices and data disclosures. In hindsight, should the assessor do anything differently, given those revelations?

MR. MCANDREW: Sure. I'll tackle this. I've gone through this several times in my life. I think the key part in this scenario, or the word that I'd focus on, is that the company believed that the system didn't contain information. Right? Belief is probably not a good reason why you would want to change scope of what you're doing. So the question is: what level of assurance do they have that those systems don't contain information? Right? What tools are they using? What automation, what interviews? There's lots of different techniques. How frequently are they doing that? Was that a one-time thing they did two or three years ago?

So a critical part in scope is to make sure

that both the organization and the assessor are working together through interviews to understand the environment and where that's at. And they both want to have a high level of assurance, whereas the assessor comes in with an opinion of somebody that's been working and can identify areas that are likely to contain information, right? Transaction logs or where they've seen some errors? But they don't typically know the ins and outs of the organization and that part. They rely on the organization that they're supporting, in this case, Company AA, to tell them how they processed what they've done in the past where there have been these repositories of information. So a critical part is that they do that.

As part of that negotiation process, it's not beneficial to have a smaller scope from an assessment perspective. Right? It's beneficial to actually have it, but there is not a lot of harm in saying as part of the engagement, can we look over here or can we test certain information? So part of the limitations is a lot of times the scope tends to be the Achilles' heel of a lot of these assessments, is that the scope is incorrect. If fact, most of the time we look at it, the scope is incorrect.

Malcolm mentioned, you know, vendors before. Many of these breaches are around venders or other points, and what happens is management said, we had no idea, we had no idea that we were at this risk and this data was out there. So I kind of come back to the question, the question that I would ask management in this scenario is: what assurance do they have that their processes are adequate, that they're covering, and that they have the right level of frequency in it?

The second part is then once they have that, how are they ensuring that new processes are not being added. So another time is you do these particularly in a biennial type of assessment. A lot changes in two years in technology today. And we talked about with this insurance, one of the biggest challenges is we're trying to guess what the threats, the risks, the technologies are 18 months, 16 months, 24 months, and unlike the financial side where it's not changing all that rapidly, the technology and the risks and the threats are changing exponentially over here.

So those are the two items that the organization really needs to do, is to make sure they're not working through a belief system to contain information, and that as they're working with the assessor, to make sure that they understand what the

risks are.

The last part I would kind of add is, many times that we've done these assessments, it is important, and I would encourage organizations to have independent or one-on-one discussions with board level or senior management without the rest of the company there. We have had many of those. We've said while we were technically compliant, what were the issues that you found? And we may have found 11 months of eating a cheeseburger, two weeks that technically did something, and maybe by the letter of the law, they technically passed that point in time. How that is written in the report, the assessor will try to do the best they can.

But a lot of times, really, if you just take the assessor and say, hey, what are the top three or four things you had that are, I think, surprising, what are the areas that we should focus on, the assessor should be able to provide that information back, and that is really improving the security of the organization, not just driving compliance.

MS. NATHER: And the other issue to think about is even if system X doesn't contain that particular consumer personal information covered by the order, and system Y does, system Y may be

dependent on or may be vulnerable to system X. So system X may pose a threat to the system that actually does contain the consumer personal information. So it's not simply a matter of which system, which bucket contains the data, but how do those systems interact and is one actually potentially vulnerable to the other? And if so, it should remain in scope.

MR. HARKINS: Yeah, I think Wendy and Tom are spot-on on that. And, Tom, I can't agree with you more in the belief. We need to know, right? We have to validate the data that is in scope and where that data sits on systems -- and, Wendy, to your point -- the interdependency of systems because if you don't do that, you're going to mis-scope the whole thing.

MS. JILLSON: Carolyn, you have some experience working with FTC assessments. Could you speak to the scope issue and also the issue that the questioner raised about whether revelations post-assessment would lead you to do anything differently with the benefit of hindsight?

MS. HOLCOMB: Yeah, sure. So I think specifically with the orders, the scope, I totally agree with the belief point. I think the assessor should do its own independent validation. Because if you're the independent assessor and you're responsible

for assessing something that is within the scope of the order, the assessor should know and have its own way of determining if the scope is appropriate.

So first of all, the assessor should be independent and skeptical, and understand what the company is saying, do its own assessment, and then understand if the scope is really appropriate and if system X really should be out of scope based on everything that everybody said.

As far as hindsight, you know, I think that's always true. Right? In hindsight, things could always be better. And maybe you'll learn something that you didn't know at the time, when you originally did it. I think the point is, when you're doing the assessment, you're as skeptical as you can be. You're turning over every rock that you can think of.

You have a team, so it's not just one person; it's a group of people. You're working with a company. You're working with their external counsel. You're looking at third parties, you know, and you're looking as broadly as possible. Also going back to an earlier hypo, you're looking at what were the external other assessments that were done? Was there a PCI assessment? Was there an attack and penetration? Was

there a compromise assessment? So you're looking at all of those pieces.

And then, as you learn something new -- for example, these are two years long, and as Tom said, a lot changes. So you can still -- even within the two years, you might look back and say, oh, now I should do this because now I've learned something else. So I think that is always true.

MS. JILLSON: What does that skepticism or, as Tom put it, the level assurance look like? So is there a sense in which the assessor doesn't want to bite the hand that feeds it. So Company AA has hired the assessor to do, you know, this project, and by challenging the parameters of this project, the assessor risks, you know, endangering kind of an ongoing assessment relationship between Company AA.

MS. HOLCOMB: Yeah, certainly a reasonable question, right, when you look at incentives and that kind of thing. But I would say, you know, at least with us, as an independent assessor, we have independent standards that require all this independence. So it's no different than doing a financial audit where we have to be skeptical. That is part of having a CPA license, and we'll get our license taken away if we don't do the right thing.

So while I understand the point on an incentive, no, it's not a factor, because that's what you're required to do. Under our standards, we have levels and levels of review. So you have the assessor. You have, after that, you know, national offices, other checkers. It goes on up the line. So there is no incentive there to do the wrong thing. It is all about making sure you're as skeptical as possible and asking all the right questions so that you don't miss something because the assessor is under the gun, too, right? The assessor can really be scrutinized. So our risk is more that we're scrutinized by others than we lose some business.

MR. MCANDREW: And I'd just add as another part of it, it's about the objectivity of the assessor. So a lot of times with these external organizations, one of the key items is to bring them in early, right? So if you bring people in six months or a year before the actual assessment to kind of do a health check or mid-year check, that could be one way to mitigate the risk, where they're not going to fail, but you can identify some areas.

A second part is the communication channel. If there can be a direct channel to, like, an audit committee on a board or something like that, where

they know that they have open lines of communication and they have a responsibility to communicate with them, there are some ways to do it. What you don't want to do in this scenario is hire an external auditor that is a friend of the IT manager, that only reports to the IT manager, right? That would be bad.

So when you look at these scenarios, you're kind of looking at what is the objectivity, what's the qualification of the assessors, what level of assurance do I have that they're doing the right level of things and confidence. If you don't feel comfortable with that, you can change, you can rotate, you can bring in different people. You can ask for that. So I think the organization has a responsibility to ensure that the assessor and the assessment process they have, that they're going through, meets their level of rigor of independence, as well.

MR. TRILLING: So we're going to turn to our last hypo for the limited time that we have left for the panel. So Company BB has annual PTC DSS audits and biennial FTC assessments required by a consent order. The PCI DSS qualified security assessor and the FTC assessor identify a number of ways in which the company's security has not been consistent with

the PCI DSS or the consent order. The company takes corrective actions. What findings should the QSA and the FTC assessor make?

So I want to start off by asking, how common is this scenario currently on the PCI side and the FTC side? So let's start with PCI side first, and either Troy or Tom may want to weigh in on that.

MR. LEACH: Sure. I'll start and then I'll pass to Tom because he actually looks at assessments.

I'll say from the qualifications itself and the training that we provide to the assessors -- and something probably unique about PCI training and for the qualified security assessors, unlike some other security certifications that I have and have had for a long time, we require annual training. And so that the training itself is a test that they have to take and pass. Tom was just talking to me last night about how he loves taking the annual test.

MR. MCANDREW: Fourteen years in a row.

MR. LEACH: But one of the things that we try to emphasize in that every year is there's a lot of changes that happen in these environments. So there's a need to continually look at how these changes happen. And we've noticed -- and we can take the previous forensic data, we work closely with

forensic investigators, looking at why something may have been missed in the past. So we emphasize that all of that information should be documented.

Now, if the organization has taken corrective measures along the way and they have now become in compliance with PCI, then they can submit to their third parties, whether that is their merchant bank or whether it is another third party looking for assurance that they're doing the right things. The documentation that they receive could be dependent. They could just receive a letter of attestation, meaning that at this point in time they've corrected those actions, and it is now an environment that should have the process. Again, I have to emphasize that point.

It's not just that they've met it at one point in time, but they have the processes in place and the technology and people in place to know, as this environment evolves, they're going to be able to adjust to the new threat model that continually changes.

So the other thing that I would put there is that if they do come to a point where they are addressing issues that cannot be resolved, there are noncompliant PCI reports that do become submitted.

And that is, at times, okay, because an organization might be going through an acquisition; they might be taking on new assets at the time of their assessment, just they've not had the opportunity that the previous organization was not doing the right things.

So being able to identify and organize in a way to say we identify where the problems are and be able to improve and recognize that we have a mitigation plan for addressing these so that we will become in PCI compliance, is an important part of QSA's job.

MR. MCANDREW: So I think from the boots on the ground side, what we've seen is it would be unusual after an FTC consent to something, that a year later that there are significant PCI challenges. As Troy said, usually what we will find is there will be significant progress. And depending on the environment they may not have made it 100 percent in a year, depending on the complexity of the organization, but there should have definitely been significant progress.

And that's the important part, is that once they have the roadmap to demonstrate that they're making progress working through that and being transparent with the organizations that they're

working with of what they've done, what they've missed, what they haven't, is really key.

The biggest mistakes that we've found is there's this feeling of transparency is not good. Keeping everything in-house and then managing or trying to manage the message on the back, that's a very poor way of doing it.

The second big trend that we see now is -- and we used to deal with this in the government when we do FISMA assessments -- this kind of idea -- we used to call it a credit and forget it mentality. That you get through the process and everyone forgets about it, and three years later, you do another FISMA assessment. On the PCI one, that's a big challenge we're seeing right now. Once people get through and they think they've gotten a "green rock" or compliant report on compliance, all of a sudden management goes or the organization goes, shew, and they redirect all those resources that they had and you find that they immediately go back to the way they were at.

So once organizations get to that class or they've done the corrective item, a key item is to ensure they've got the right processes to maintain that moving forward. And that's where you can look at governance, you can look at technology, all those

items to make sure that you continue to manage it.

MS. HOLCOMB: And I think on the FTC side, one of the good points of the order is that it does require the full two years of disclosure. So every exception that's found within the two years should be reported to the FTC, even if it's been remediated. So that's the point is to say, well, for the first six months, there was an exception, and then the company remediated, and for the last 18, there was not one.

So it's full disclosure over the two years of what was every exception. Then those should also be aggregated to say, how does this compare to what the requirements in the order are? Is this enough to say that the company didn't comply, or this is a qualified report, and there are plenty of those. Right? There's always exceptions.

I'm sure that's true in PCI as well. Nobody is perfect. No company can get this straight all the time. But I think the key is disclosing every single one, making sure the company has a remediation plan for every one, and then looking at them in the aggregate to see what they mean compiled together.

MR. HARKINS: And I also think in some cases those exceptions could be because there is a better control. Because in some cases, these standards are

written towards controls that are dated, that we know don't work. So you also have to understand that and then see the compensating controls analysis to see in aggregate then, have they been consistent with the order. And they made a choice to not follow a particular defined static technology approach that was defined in the standard and do something better.

So again, we have to open that up to the potential so that people -- again, getting back to my comment -- can innovate towards better solutions and better controls.

MR. TRILLING: So unfortunately, we have reached the end of our time for this panel. I want to thank all of the panelists for a great discussion. We covered a lot of territory, and we really appreciate the viewpoints that you presented.

We'll now be taking a break for 10 minutes. We will resume at 11:15 with a fireside chat on emerging data security threats with FTC Commissioner Rebecca Kelly Slaughter and Josh Corman.

(Applause.)

(Brief recess.)

FIRESIDE CHAT ON EMERGING THREATS

MS. JILLSON: Welcome back to the FTC's Data Security Hearing. Next up on the agenda is a fireside chat on emerging security threats between FTC Commissioner Rebecca Kelly Slaughter and security expert Joshua Corman.

Rebecca Kelly Slaughter was sworn in as a Federal Trade Commissioner on May 2, 2018. Prior to joining the Commission, she served as Chief Council to Senator Charles Schumer of New York, the Democratic leader, advising him on legal, competition, telecom, privacy, consumer protection and intellectual property matters, among other things.

Joshua Corman, the Chief Security Officer at PTC, is probably best known as the cofounder of the I Am The Calvary security organization. He has also served as the Director of the Cyber Statecraft Initiative for the Atlantic Council, CTO for Sonatype, Director of Security Intelligence for Akamai, and in senior roles for the 451 Group and IBM Internet Security Systems. I'll turn it over now to Commissioner Slaughter and Joshua Corman.

COMMISSIONER SLAUGHTER: Thanks. Thank you so much.

MR. CORMAN: We have a fire.

COMMISSIONER SLAUGHTER: Yeah, we have our fire here, appropriately digital. Thanks, Josh, for being here.

So let's start with a little bit on your background, and particularly, why don't you tell us a little bit about I Am The Calvary.

MR. CORMAN: Oh, sure. So the name is both wonderful and terrible. But I had been researching the rise of Hacktivism and Anonymous. And I think many of us in the cybersecurity profession get into it because we want to be a protector, we want to do things that matter. And what I started getting tension on is we're so focused on what's right for our shareholders or our enterprise or our single organization, that we forget that there is public trust, there is public safety, national security issues.

And when I saw the rise of Hacktivism and Anonymous, I started turning my eye towards the things that no one was paying attention to. And I kept naively thinking if I could build my credibility and get into the intelligence community or into Congress or the White House, and just get the right message to the right person, the right adult in the room, they can go fix our problems. And we did that.

We got in as high and deep as you can get. We brought five hackers into Fort Meade for two days with General Alexander. We had the conversations. And what we realized is the cavalry isn't coming. No one is going to save us. And that moment was both devastating and empowering. Because if you know no one is going to come, it really challenges you to say, what am I willing and able to do.

So it took about six months later at DEF CON, the largest hacker conference in the world. We kind of did a plea to the hacker community and said our dependence on connected technology is growing a lot faster than our ability to secure it, especially in areas affecting public safety and human life. So you can either screen your darkness and keep being a pointing finger of past failure, or we could try something new. Let's lead with empathy. Let's be ambassadors and translators. Let's be a helping hand towards future success. And it was basically a call to arms that said, if you want to be part of the solution, if you try something new, if you want to work together, you personally say, I Am The Calvary, and then donate your time or research to it.

We just turned five years old. We've done significant outreach into the Food and Drug

Administration, into Congress, and the White House, internationally. And we're trying to be that voice of technical literacy and ambassador and translator from all of the knowledge in the private sector research community into safety critical industries.

COMMISSIONER SLAUGHTER: So can you give us an example of what that would mean in practice?

MR. CORMAN: So we had Jay Radcliff, a diabetic who was hacking his own medical devices, insulin pumps. He was convinced that the FDA didn't care, that people would have to die first, and he just didn't know how to connect that truth as a patient and as a researcher into policy reform. And we said, look, how about instead of just beating your head against the wall, let's try a different approach. Let's, you know, use our social skills.

So we built trust. We did engagement. We looked at this as a campaign versus fixing a single -- a flaw in a single device. And through this cross-education, we built deep trust with Dr. Suzanne Schwartz at FDA. They taught us how regulation works. We taught them how researchers do things and why. And fairly quickly, in the grand scheme of things, they started putting a lot more technical literacy into their pre-market approval. They then did the first

safety communication in history on a bedside infusion pump that was vulnerable but unpatchable, which is a story we might get back to, and started just like really treasuring the value of coordinated vulnerability disclosure and started incentivizing medical device makers to do it.

Are we done? No. But have we had material impact on turning up the cyber hygiene of the medical device cyber supply chain? Absolutely.

COMMISSIONER SLAUGHTER: So I've been around Washington, Government, policymakers for a while, and over the last five years that you described I Am The Calvary being up, and even for the time before that, one might say there has been a change. I think "hacker" used to be a dirty word in government circles. Do you think that that's still true?

MR. CORMAN: I think it is absolutely changing. Hacker equals criminal for a while. Now, I just watched a testimony from Art Manion from CERT/CC in the Senate, and both the Chairman and the Ranking Member both implicitly acknowledged the value of coordinating vulnerability disclosure and working with security researchers and were giving a hard time to intel for not doing -- embracing it well enough. It's not that it was a single day where the worm turned.

What we tried to do instead of just saying hacking is First Amendment protected free speech or we don't like CFAA, we tried to show we can play a unique role in driving public safety, in cars, medical devices, et cetera, and when we would have that conversation, towards the end they would say, well, how can we help? And we said, well, for one thing, there's a chilling effect on researchers because of CFAA and DMCA.

So we created a body of proof of the value we could demonstrate to public safety and national security, in parallel with some great work from Katie Moussouris and Art Manion on standards and [indiscernible] on the DMCA exceptions. But in general now, several parts of the U.S. Government have published disclosure programs. The FDA encourages and rewards having it in medical devices. I, myself, used a template that we designed with the U.S. Commerce Department and NTA. It's becoming something where not only is it acceptable to embrace hackers; it's actually encouraged.

COMMISSIONER SLAUGHTER: Well, let me flip to the other side of the coin. As much as government has been distrustful of hackers as criminals, I think the hacker community hasn't always seen government as

their best friend or allies. Do you think that side is changing, too?

MR. CORMAN: It fluctuates. DEF CON turned 25 last summer, not this past one, but prior. We brought two sitting Congressmen, Will Hurd of Texas and Jim Langevin of Rhode Island, to DEF CON on stage, and the reception was quite good, and yet, there was still a backlash because of the arrest of Marcus on some of the past hacking things. So it's an ebb and flow of trust and distrust. The hacker community is not inherently a fan of government. They think government can only make things worse. And as such, the Calvary gets criticism quite a bit for engaging and reaching into these areas.

COMMISSIONER SLAUGHTER: Let me pivot a little bit and sort of zoom out on the conversations that we're having here at the FTC and in the public generally. We throw around a lot of terms, privacy, security, safety. How do you think about each of those different terms, either together or separately?

MR. CORMAN: Well, for anyone who has been watching the content over the last two days, it is still very difficult to even separate privacy from security. So adding a third thing of safety or cyber safety, as we've been calling it, is challenging.

One of the ways I do this is indirectly. I tell my neighbor I love my privacy and I would like to be alive to enjoy it. Because I think if you just want to solve for privacy, you can encrypt something. If you want to solve for privacy, safety and security, you may design the system differently. You may have fewer things. You may have less attack surface. If we ever suboptimize for just one objective, we're going to be making tradeoffs and robbing Peter to pay Paul.

Now, some of these things will be zero sum. But I think narrow solutions actually work counter to our collective interests. So when I think they are partially overlapping Venn diagrams without drawing a picture -- one of the ways I put this in healthcare -- I was the congressional task force for healthcare, cybersecurity, and they wanted us to focus on preserving HIPAA intent in the precision medicine era. And I talked to a whole bunch of chief medical officers and said, you guys have more incentive to have a corpse with their privacy intact than invest in security that provides reliable, available patient care, and no one disagreed.

So our incentives incentivized things. I hope they incentivized the right things. Instead of

having an encrypted database on a device, let's make sure it has less attack surface.

COMMISSIONER SLAUGHTER: That is a chilling example to think about. And I want to use that chilling example to pivot to some other chilling examples of some large-scale attacks and breaches that we've heard about in the public. Can you talk about some examples of publicly-known attacks and the lessons that you think we can draw from them?

MR. CORMAN: Yeah. And these three won't surprise anyone, but maybe the talking points are slightly different. Chronologically, WannaCry is the one that scared me the most. But chronologically, Marai is a real gut check for us and I think -- I was thinking about it most of yesterday.

COMMISSIONER SLAUGHTER: Let me back you up. Can you just -- for people who aren't intimately familiar with the details, can you give an overview?

MR. CORMAN: Sure. So there were three attacks, the Marai Botnet was mostly low-cost, hundred-dollarish IOT, internet-connected cameras that took down the internet for a day just before the last Presidential election. The WannaCry attack happened on Mother's Day weekend a few -- two years ago now, I'm saying, and it took out 40 percent of the U.K.'s

healthcare delivery for a weekend. It had some isolated impact on the U.S.

And NotPetya was a nation state attack from Russia against Ukraine that escaped its blast radius and did significant damage to Maersk Global Shipping, about 20 percent of global shipping, Merck Pharmaceuticals had $870 million damage including contributions to our national security supply of vaccines. This is designated U.S. critical infrastructure. So that one attack of NotPetya did more damage than a hurricane. We now have single attacks with collateral damage exceeding those of a hurricane.

So those three attacks, I think, should be policy game changers, but for slightly different reasons on each.

COMMISSIONER SLAUGHTER: So tell us a little bit about why and whether you see any of them or all of them as preventable or should be preventable.

MR. CORMAN: So in the case of Marai, real quickly, these cameras had three defining characteristics. They were internet reachable, they had a fixed hard-coded password, and they were unpatchable. So I said an unpatchable device is like the lawn darts of the internet. It’s just inherently

unsafe, in no world should that be okay.

The collective might of those to be wrapped up in a botnet, I used to work at Akamai. That was the largest botnet we had ever seen for denial of service attack. It was only using 20 percent of its population and only sending about 20 percent of the traffic. So the 20th of a 20th was still too big and took out the internet for a day.

So one of the things I think there is interesting is those three characteristics I just described are most medical equipment. They're internet reachable, fixed passwords where if you change them, you void your maintenance contract, and a lot of these are unpatchable.

So those three things, I think they were scary to public policymakers, including myself, because prior to that we had said if we simply add more transparency and information to enable free market choice, then a rationally self-interested actor will act in their own interest. The whole information asymmetry thing, we're going to dampen that with more data and then they'll buy the right things.

The problem with this is the seller of that $100 camera is not incentivized to make it safer. The buyer of that camera is not incentivized to make it

safer. It's the externalities and the tragedy of the commons where other people were hurt, and that other people might be a loss of revenue for Spotify or Netflix or Amazon. It could be a denial of service on several hospitals.

So to me, that one scares us because it shows that if there isn't some minimum hygiene or, you know, seven deadly sins you cannot do and ride the internet, some minimum burden, irrespective of the size of your device or the size of your company, then the collective harm can shatter trust in the public faith in these institutions or institutional trust as Kirsten said yesterday.

COMMISSIONER SLAUGHTER: I want to put a pin in that thought about collective harm and just give you a chance to walk through the other two, WannaCry and NotPetya.

MR. CORMAN: In the case of WannaCry, what you had was a known vulnerability that Microsoft fixed. In fact, it was such a serious one, they fixed it in Windows XP. Now, Windows XP is end of lifed. Its successor Windows Vista is end of lifed and its successor Windows 7 is now on extended support. So we are multiple generations old in this. I'm not going Marie Antoinette and say, let them eat cake and get

off XP, but they actually issued a patch for this in March. Two months later, in May, there was an attack of very badly written ransomware, not targeting hospitals, did significant harm because most of the U.K. hospitals -- most hospitals, at large, were exposed, that vulnerability to the naked internet.

COMMISSIONER SLAUGHTER: Why if there is a patch out there?

MR. CORMAN: People don't patch. People aren't incentivized to patch or they don't have the resources to patch. And what we have is we've gotten drunk on the benefits of connectivity, but we haven't understood the responsibility that comes with that. You know, I had a lot of debates during the task force of, like I said, well, we can't afford it, we don't have any money. I flippantly said, if you can't afford to protect it, then you can't afford to connect it.

Like I might want to drive a tractor-trailer, I may want to fly a 747, I might want to do open heart surgery, I am not qualified to do so. And if I want to, there's a burden I need to accomplish to demonstrate that I can do that safe. And what we've done is we like the benefits of the convergence of physical and digital, but we have not

yet internalized the costs in doing so.

COMMISSIONER SLAUGHTER: Okay. So let's stick on this for a second and talk about that small hospital with these devices or the operating systems that maybe aren't patched. When you say if you -- what did you say, if you can't afford to protect it, you can't afford to connect it. Does that mean we shouldn't have small hospitals? What does that mean?

MR. CORMAN: No. I intend to give some practical advice here. It's about -- one of the core beliefs in the Cavalry is that we're over-dependent on undependable things. And when you put it that way, you have two choices. You can depend less, which means retreat, or you can make them more dependable, which takes will, money, time, political public policy change, and it's slower.

So what we're really looking to do is right size the risk and expose the true costs of these dependencies. Where it's acceptable, keep doing it? Where it's not, do something practical. So in the case of hospitals, it may not be that they can wholesale replace all their bedside infusion pumps, but it might be that when they buy the next tranche of them, they can buy one that's patchable. They can buy one that has a coordinated disclosure program. It may

cost the same as one that doesn't.

But what we're trying to do is nudge them from a prone state to a less prone state. If they're stuck with it for the next five years, it may mean disable the wireless capability and use it as a pump as it originally was intended instead of as a hyper-connected, hyper-exposed one. They could be compensating controls, but this nihilism that we can't do it perfectly, so let's not do it at all, we're absorbing significant and growing risks.

COMMISSIONER SLAUGHTER: Okay. And let's just -- the last one was NotPetya, if you'll talk about that a little bit.

MR. CORMAN: NotPetya is really scary because that's, you know, a nation-state-level adversary, Russia, attacked the MeDoc software -- accounting software in Ukraine. It escaped its intended blast radius and any businesses having a satellite office in Ukraine got hit. This included Maersk, which is global shipping, about 20 percent.

COMMISSIONER SLAUGHTER: So go back again for the nontechnophiles among us. When you say "escaped its intended blast radius," how did that happen?

MR. CORMAN: They were trying to attack

Ukrainian companies. It happened to leak to the global footprint of Merck Pharmaceutical.

COMMISSIONER SLAUGHTER: Because of the internet?

MR. CORMAN: A single office in -- yeah, the entanglement of IT, right. So you drop a bomb in the real world, it hits the bomb target and maybe people in the vicinity of the blast radius.

COMMISSIONER SLAUGHTER: Mm-hmm.

MR. CORMAN: You drop a cyber bomb and cyber munition and it could ripple across the entire planet in ways that were not intended.

COMMISSIONER SLAUGHTER: So then let's go back to this one. So Merck --

MR. CORMAN: It hit Maersk, Merck, FedEx, a bunch of companies. One of the ones that no one talks about is Nuance, which is voice-to-text dictation, which is a near monopoly in hospitals for doctor notes and doctor orders. So doctor orders were lost or delayed and we know that delayed and degraded patient case can affect outcomes for time-sensitive procedures.

So that was a multi-week outage for a near monopoly in healthcare. So there was absolutely a calculable impact of that particular attack. What I

think that one shows is how entangled IT systems are. So we talk about -- well, even today, we talked about a small organization, a medium organization, a large organization, as if the size of the organization is the thing to focus on. Perhaps it is not the size of the organization or the size of the device, but maybe the size of the harm or potential for harm that matters most.

And it could be this tiny little and unimportant, you know, accounting software, mostly sold to one country can hit designated U.S. critical infrastructure in the form of pharmaceutical manufacturing.

COMMISSIONER SLAUGHTER: So how do we think about that? We have a lot of conversations. We've heard them here and in other places about what are the free market incentives, how do businesses balance the incentive for security, and competing incentives that they have. What's your view about how that should be done?

MR. CORMAN: I don't want to butcher Malcolm this morning, but he had a nice way of putting this. I think too much of the conversation is on what is right for my publicly-traded company or my shareholders. Of course, that's one of our optimums.

That's the private sector optimum.

But when we talk about public-private partnerships, the reason we have a public sector, among many, is there are things that are not in the private interest, but are in the collective public interest and that's where we need it. So I think he called it what's right for shareholders, what's right for customers, and what's right for greater society.

I think the way Eli Sugarman says this at Hewlett Foundation. He says there are things that -- in terms of the public-private partnership cliche, we talk about. He says there are things the private sector -- public sector can't do, but the private sector won't do. And I think we forget there is a large and growing list of things that fall on the floor. And for that, he thinks that is the role of philanthropy and altruism. I think that's one of the vacuums the Calvary's filled.

Now, we don't want to own this. What we want to do is be the error-handling routine that says when it falls between the cracks of private local optimum and a public sector policy thing that we don't have the stomach for yet, or there are tensions, or we want to be methodical, how do we quickly triage and decide which things go where so that we can get

moving.

COMMISSIONER SLAUGHTER: So I want to come back to what the public sector should do. Let's focus a little bit in the constructive advice giving way, first, on -- let's talk about the individual, the individual consumer. You're talking about some very large-scale challenges across big industries, and often businesses that don't have any direct consumer relationship, or vulnerabilities that don't have any direct consumer relationship.

So what should we, as individuals, be doing to help promote not only our own security, but the sort of global collective security?

MR. CORMAN: So indirect answer, you know, hackers tend not to like government. So I sometimes sound like I'm pro-policy or pro-regulation. I think it is the worst possible idea, except all others. In general, my philosophy on this, and I think it's a shared one and a growing one, is, in general, free markets fix themselves when you have an informed buyer or demand meeting sufficient supply.

Where it breaks down is really two things, and I think we have both here. One is information asymmetry where I don't have enough information to act on my own self interests. And to that end, some of

the advice is the -- the consumers don't yet know this, but we should start demanding more transparency, more information about security capabilities, primitives or commitments, which I can enumerate. But, in general, adding more information.

Like before we had Carfax, we knew that I might be sold a lemon. So we had lemon laws to dampen the effects of information asymmetry economically. So I've been pushing a lot for transparency, for labeling, for patching commitments.

COMMISSIONER SLAUGHTER: How do we make that digestible and comprehensible to the individual consumer who may not understand what it means to have a hard-coded password or any of those other issues?

MR. CORMAN: So some of it has to be extracted. You and I might not know the difference between a three-star crash-rated car and a four-star, but we know a four is better. So there are ways to extract this. That's part of the role of the private sector -- excuse me, the public policymakers.

COMMISSIONER SLAUGHTER: Do you think that like third-party validators have a helpful role to play in that?

MR. CORMAN: Could be. They could. We have to look for the right thing and the things that can

maintain or preserve confidence. And to Sasha's point yesterday, a lot of our advice is really bad. So we don't want to be looking at prescriptive controls or are you updating your files for AB every day. What we want to be looking for is these are complex systems. So the failure is going to be frequent. Are you prepared for failure?

One way the Cavalry did this is on our first birthday, we launched a five-star cyber safety framework. We did a similar thing called a Hippocratic oath for connected medical devices and it's five postures towards failure. They have fancy names, so I'm going to cut past those. We say if all systems fail, these things will be hacked. How do you avoid failure? How do you take help avoiding failure without suing the helper? How do you capture, study, and learn from failure, have a prompt and agile response to failure, and contain and isolate failure?

And this was really just saying we're going to have hacked cars, but when they hack the stereo, can they shut off the brakes? So we've been encouraging things like have a disclosure program, be patchable. Avoid some of the dirty sins like, you know, hard-coded passwords, things that are obviously bad every day, twice on Tuesdays. And we currently

lack the political will to do that.

So back to consumers, I think it's flippant to say consumers should do the following things because they really can't act in their own self-interest yet. But what they can start to do is start asking for or rewarding with their wallet, people who are more transparent, who do have some of these primitives, who will say we are patchable, and we commit to patching for the next three years. When you go to buy your next home router right now, which one is safer? I'm not sure I could tell. I'd like to be able to tell and maybe, slowly, as we see more attacks, people will act with their wallets.

But the other problem is -- the tragedy of the commons is the other breakdown, which is even if I act in my own self-interest and buy the one that fits the purpose for me, I can still hurt others. And to that end, I think those are the minimum hygiene things we need some public policy on.

COMMISSIONER SLAUGHTER: Well, that is a very good segue to the next question I wanted to ask, which is that these hearings generally are an opportunity for us to think critically about our own efforts here at the FTC, and the legal landscape in which we are operating.

I don't want to put you on the spot to say what the FTC should be doing differently under current law or what the laws need to change. So I will zoom out a little bit and say, in an ideal world, what would be the role of public policy? What would be the role of an agency like the FTC? Should we be setting out best practices? Should we make those legally enforceable? How should we be engaging with the hacker and security community? What burden should the Government put on companies to sort of raise this bar? Generally, how do you think the world should look?

MR. CORMAN: I would like to give you a flippant answer. I have tremendous empathy for the role we're in and the point in history we're in, and there's a fine line here. I was thinking about this last night pretty hard. NTIA Commerce Department tried to come up with voluntary best practices for labeling for patchability. And we had a whole bunch of private sector engagement and we came up with a label that said, we commit, our product is patchable and we commit to patching it for this many years.

And towards the end people said, there's no way in hell I'm signing up for that because then the FTC is going to use it against me for fraudulent claims if I change my mind, if I find a library I

can't update. So there's a bit of a catch-22 here where we want to encourage more transparency for free market choice in parts of this overall approach, but not use it as a gotcha later for the also necessary law enforcement type enforcement.

To me, I've always looked at, as a lay person, my hope, since I don't know your business and your value levers, but my hope was it looks like you really have two major things you can do.

One is -- you've already done a few times -- which is punish people for fraudulent claims, the TRENDNet camera comes to mind. Like you can't say it's secure and then not be secure. I think the response from the private sector to that, though, is don't make any claims, which I think hurts my other goal of transparency and actual information. So that's a fine line.

The other one, though, I think is interesting, if you want to play fast and loose with some of the experimentation, what would be bold. And if you don't -- if you're passing known vulnerabilities on to your customer, if you're not equipping them with a software bill of materials that allows them to know any vulnerabilities in their product, if you're not patchable, these things may

undermine someone's ability to defend themselves at all.

So there's a shared responsibility between a producer of a good and the operator/owner of a good. And in a lot of these cases, those risks are being blindly passed on. So I always thought through the broad interpretation of consumer protection there could be some minimum transparency or capabilities that are considered negligent below a certain line, whether it's defined by FTC or simply enforced as a de facto standard. I would like to see something where it's not about did you pass a regulator compliance thing with 116 controls, but are these things beyond the pale. If like you were compromised because of a fixed unchangeable password, but you sold a device that was hackable, but not patchable.

Picture a different world where it's patchable, you've supplied the patch, but the operator didn't use it. That's on them. I can see a word where we've properly placed the risk burden on those in the best place to avoid risk, and that's going to be a bit more about defining what those unforgivable sins are on the bottom end, the floor.

COMMISSIONER SLAUGHTER: Well, I think we have just a couple more minutes, so I'm going to offer

you the opportunity to get in anything that is important to share that I didn't get to ask you about, but also articulate my view that I think this ongoing dialogue between the Government and the folks in the best position to understand real security issues on the ground is going to be critical to our ability to address them.

MR. CORMAN: The optimist in me says we're getting pretty close to critical mass. I'm not advocating for any one of these particular policy moves, but this -- if you squint, there's a few common things. There was a Senator Warner bipartisan bill on IOT hygiene. It said, you must be patchable, you shouldn't have hard-coded passwords, you should have a disclosure program inviting researchers without suing them, you should use standards-based crypto, and you should be free of "known harms." Those are the avoidable harms, right, elective risks, preventable harms.

COMMISSIONER SLAUGHTER: Mm-hmm.

MR. CORMAN: It got winnowed down to maybe three things. Be patchable, don't have hard-coded passwords, and have a disclosure program. The U.K. government has a code of practice with 16 things, including those five. And the GCHQ said these

shouldn't be voluntary, these should be purchasing requirements for the country. Out of nowhere, the State of California passed an IOT law saying you should have reasonable practices that are fit for purpose for the device, but the only one they called out is fixed credentials and passwords.

So I think and hope we're getting close to some sort of minimum hygiene because that little device that has a hard-coded password and can't be remediated can do significant harm, maybe to internet "cats" and maybe to hospitals. And I think if we aren't smart, you know, this is going to be the asbestos of our time, right. You know, we put asbestos everywhere. It was cheap, fire-retardant, and you would be an idiot not to use it.

But then we look at mesothelioma and different cancers and the eventual unseen costs, and I think what we're going to look at is we should only connect things we can afford to responsibly secure and connect, not just to the person making the device or to the person consuming the device, but to these institutions because to punctuate what we said yesterday, we have to preserve the confidence of the public, the institutional trust.

To tie this to my PTC role, I guess in the

last seconds here, one of the reason I went from a Calvary public policy role into a private sector is I saw that this software was in medical devices, in factories, in high-speed rail and aviation, and I realized there's a shared responsibility here. Even if I do everything right to secure my products, if my medical device makers don't take my patches, people get hurt. And even if they take them and apply these patches, if the hospital doesn't apply the patches, people get hurt.

And there's a relay race where many of us have to change the way we do business and none of us yet have internalized that. If we're still having an argument about what's right for shareholders, we're not thinking what's right for the public safety and national security. And the true failure is any crisis of confidence in the public to trust these otherwise superior innovations and markets.

COMMISSIONER SLAUGHTER: Well, that is both very important and very dead-on for the time that we have. So I really appreciate your thoughts, your sharing them with us today. And I strongly encourage you and the Cavalry and your fellow hacktivists to continue that dialogue because I think there are willing and eager ears in the Government now, and

having our part in that shared responsibility program is really important to me personally. So thank you very much.

MR. CORMAN: Thank you.

(Applause.)

MS. JILLSON: And I just wanted to say thank you both to Commissioner Slaughter and to Joshua Corman for that interesting perspective.

We are now going to take a lunch break. We will be back here at 1:00. We have two interesting panels this afternoon, the first on the U.S. approach to data security and the second on FTC enforcement of data security.

(Lunch break.)

PANEL 2: THE U.S. APPROACH TO CONSUMER DATA SECURITY

MR. TRILLING: Good afternoon, everyone. Welcome back from lunch.

Our next panel is on the U.S. approach to data security. I'm going to turn it over to James Cooper, who will be moderating the panel.

MR. COOPER: Thanks, Jim.

It's great to be here. I'm James Cooper from the Bureau of Consumer Protection here at the FTC. I'm really happy to be moderating this panel. We've heard yesterday and beginning of today a lot about consumer incentives, the demand for data security, firm incentives to supply, what may be some of the problems and threats out there. And, now, we're going to switch gears for this panel in the next one and talk a little more about the legal approach and policy approach to problems with data security.

We have a great panel to discuss this with. I'll just give a very brief, brief introduction. Their full bios are in the program. So right next to me, Chris Calabrese is the Vice President for Policy at the Center for Democracy and Technology, where he oversees CDT's policy portfolio. Next to Chris is Janis Kestenbaum. She's an FTC alum and currently is a partner in the privacy and data security practice at

Perkins Coie.

Next to Janis is Daniel Solove. Daniel is the John Marshall Harlan Research Professor of Law at George Washington University Law School and one of the leading scholars in privacy and data security. His textbook is one that I actually use for my class and I think most people, kind of a standard in the field of privacy and data security.

Next to Daniel is Lisa Sotto. She chairs Hunton Andrews Kurth's global privacy and cybersecurity practice where she is the managing partner of the firm's New York office, and she is also the Chairperson of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee.

And then last but not least down next to Lisa is David Thaw. David is a professor at the University of Pittsburgh, where he's the author of numerous articles on law and technology. And he's also the founding faculty director of Siren Laboratory.

So we have a great panel, a nice array of knowledge. Our panel today is supposed to look at the U.S. approach to data security. So, I think, you know, before we dive in, we should actually answer the

fundamental question, kind of the base question, is there actually a U.S. approach to data security. I mean, we have the FTC; we have state AGs; we have a variety of federal legislative -- federal legislation. Do we actually have something that we can say is a U.S. approach and how would you characterize that?

So I will turn it over to Lisa to answer that, but then invite the rest of the panel to kind of jump in.

MS. SOTTO: Thanks, James. Well, we have a cacophony of data security laws in the United States. We really have many different rules. They're not uniform. They do not dovetail nicely with each other, so that really makes for a hodge-podge, a fragmented approach to data security.

The question of what security rules to apply is probably among the most vexing for senior executives today who are facing an increasingly pernicious cyber environment. So they are constantly looking for the silver bullet. And, you know, this is a question that we get all the time, what data security rules should I apply? I'll do it if you tell me what they are. But it's not that easy. In fact, we have a confusing panoply of rules.

So we have evolved over the last 20 years

from a largely unregulated environment to today a heavily-regulated environment, but a fragmented environment. On the federal level, we have the general compendium of FTC rules largely promulgated through consent orders. We also have a sectoral approach federally to data security. For example, HIPAA for the healthcare sector, GLB for the financial sector, and both -- the rules of the road for both are written by regulators. And to make matters even more confusing, under GLB, there are literally scores of regulators who have written regulations pursuant to a single law.

At the state level, a melange of data security rules. Some are open-ended and vague, others are highly prescriptive. So we have, for example, a sectoral approach at the state level that -- probably the best example is the New York State Department of Financial Services' cybersecurity regulations, really an important set of regs, and has taken off. We also have regulations for companies that do business in a certain state like Massachusetts, where if you service customers in the state, you need to comply with those regulations.

And still another approach is to regulate security by technology. And the best example there is

California's new internet of things, privacy law. And lest we forget, at the state level we have a very mature compendium of data breach notification laws. And those laws, while they, for the most part, don't include security requirements themselves, they form a critically important incentive-based tool in this space.

So we have the federal approach, the state approach, and then very important are industry standards. In some ways, industry standards, for some companies at least, form the backbone of their security program and are much more important really for them than legal requirements. For example, the Payment Card Industry Data Security Standard with its 12 requirements, that forms a basis for the security program for merchants and many others who deal in the payment card space.

And, in fact, you know, while there's no force of law to the PCI DSS, the need to comply is that much more important than law because for an entity that takes payment cards, the ultimate threat is that the ability to take payment cards will be revoked. And, of course, that's absolutely existential for a company that lives on payment cards.

We have the NIST cybersecurity framework, which while it is voluntary, while it's supposed to apply only to critical infrastructure, really does form the backbone of many -- most security programs in the country for companies of any size.

We have the ISO standard, again, a very important, well-respected 2700 series. The Center for Internet Security, 20 critical security controls, very important standard as well. So important that the California AG has said that the AG would consider bringing an action against a company that doesn't implement these controls to threaten that they didn't have reasonable security in place. In California, the legal requirement is to have reasonable security. But if you don't follow the CIS controls, then you may be deemed to not have reasonable security.

And then other industry guidelines, the National Association of Insurance Commissioners came out with a model security law last year. As lawyers, we are subject to ABA guidance also in this space, so we don't escape.

So, what is the conclusion here? The conclusion here is that we have a fragmented hodge-podge of rules. Just to put some meat on the bones, my data, the very same data elements, could be treated

with different security standards depending on whether I'm a resident of California or resident of the State of Massachusetts, depending on whether the data is held by my banker or my doctor or my grocer and, of course, that makes no sense at all.

So, you know, consumers are very confused by all of this and, of course, businesses are also left guessing. What standards do I apply? Do I focus my limited resources only on those law that have high statutory penalties? Do I focus where there is highest enforcement risk? What do we do here?

So the reality -- and what this really leads to is that most companies have just a single information security framework and they do what's best for the company for the data and for the business -- for the data they hold and the sensitivity of the data and what works, vis-a-vis, the threat that they face and, in fact, the law is largely irrelevant.

MR. COOPER: Yes, that was interestingly said. I want to follow up and maybe ask Janis, the two of you here on the panel who actually advise clients, and just drill down a little bit. And, Lisa, you've alluded to this. I thought it was interesting that you mentioned that the PCI DSS is so important and that you just kind of ended with the exclamation

point that the law matters less in some ways than some of these private agreements or privacy requirements.

So, I guess, Janis, I'd ask you, you know, do your experiences match up with Lisa's as far as counseling clients? And then out of the panoply of laws, what do you find that your clients -- you know, what's the most scary? What do they calibrate to?

And, Lisa, you can feel free to jump in, as well. But I'd ask you, as well, Janis.

MS. KESTENBAUM: Well, I think Lisa described the thicket of laws that is sort of the U.S. approach to data security very well. It is just a welter of requirements at various levels with various approaches. I mean, at some level you can look at it and say that there is some uniform, unifying theme to it, which is reasonableness. I think like everybody at some level is striving towards encouraging companies and requiring companies to have reasonable and appropriate security. But, of course, that standard is itself incredibly high level and a potentially quite vague one.

So, it is quite difficult for companies to know what to do. Lisa is exactly right and in my experience, as well. Companies, at some level, would just like the clarity of knowing what is expected of

them and that would make it much easier for them sort of to do the right thing. But nobody is really telling them what the right thing is.

In terms of what that means, like, so what do companies do in practice, I think, you know, they do sort of take it all in and they do come up with a system. They are paying close attention to things like FTC -- FTC guidance certainly plays a role as do things like the NIST cybersecurity framework. It's very influential. Obviously, they are looking at the specific requirements if a company is in one of the particularly regulated sectors. Of course, they're paying close attention to that. Financial companies are paying close attention to GLB and who their financial regulator is and what they're saying. Companies under HIPAA are doing the same with regard to that law.

But they have difficult decisions to make. I mean, I think that it's not -- in my experience, it's not so much that I think companies do make decisions like, well, I'm going to pay, you know, the FTC said X, but, gee, you know, you're also telling me that the FTC doesn't have fining power. So I'm not going to really focus in on that. I do not think that that's the way that companies make decisions.

At the end of the day, they are just looking for ways to protect the data. You know, nobody wants to be -- not surprisingly, nobody wants to be the company that is, you know, in that headline with the breach, and that may be driving things as much as anything, right. I mean, these breaches are now legion and, yet, you know, not shockingly, it's, you know, sort of one of the highest priorities of boards of directors around the countries and CEOs and as well as CISOs to avoid being the company that shows up in the headline.

MR. COOPER: Yeah, I don't know -- and I just want to follow up and maybe get -- while I have both of you here to talk about this. What is more important to firms or at least that you see? Is it the private costs of, say, being in the headline and maybe the stock market costs of that or lost customers? Or is it the potential legal exposure that comes from possible, say, an FTC or state action, or it is, you know, the private lawsuits that may come? Of course, that would be maybe related to the private costs.

I mean, if you were to kind of lay out the hierarchy of what their concerns are, I'm just curious. I've had Janis on the spot, so I'll turn it

back to you, Lisa, maybe.

MS. SOTTO: There's no question in my mind that the first number one in the hierarchy is reputational harm and the loss of consumer trust. I think, you know, there's a whole parade of horribles that follows from having to stand on your roof and raise the red flag of having had a compromise and having a vulnerability, at least potentially suggesting there was a vulnerability in your system. There is certainly a loss of consumer trust. The markets react. There are a lot of market forces at play here. Investors react. Now, we know stocks go back up after a short time. But, certainly, there is some market reaction.

Business partners get nervous. Employees get nervous. We can't forget about the employee population, as well. So there really is a host of negativity that follows a data breach.

Legal mandates, legal obligations, yes, they're very carefully considered, but I would not call them a driver in any respect. And, certainly, lawsuits are not the driver, they're not spurring any company to take any action one way or the other. They're just sort of a necessary evil, I suppose, after the fact of a breach, as are the data breach

notification laws. Although I think the breach notification laws themselves have had a tremendously important incentivizing effect on really pushing companies to solidify their data security.

MR. COOPER: Yeah, Chris, do you want to jump in?

MR. CALABRESE: I mean, while agreeing with all of that, I might caveat it a little bit. I mean, not everybody is so public-facing that they care that much about consumer trust. They don't want to be embarrassed, but they also -- I think there is a business case, not a security case, but a business case to say we're going to do kind of the lowest cost, probably fine, security and kind of hold our breath and hope we are all right. And if we're not, we'll, you know, take our licks, we'll go through the whole -we'll give you credit monitoring thing, we'll say we're sorry, we'll say these things happen and we'll kind of move on. You know, depending on the cost of security, that may be a rationale economic decision.

So I just -- while I think that data breach and the economics here are important, I also am a little concerned that that doesn't lead us down a path where we start to say, well, the market has actually

got this under control, because it's not clear to me that that's actually true. And it's certainly not clear to me that it's true for people who aren't the company, the people whose personal information is lost. I'm not sure that their economic incentives are in any way aligned kind of with the current structure.

So I know we're going to talk more about it, but I just wanted to get that caveat in there.

MR. COOPER: Yeah, yeah. Did you want to respond quickly, Lisa, and then I'll move to David and Daniel because I know they both have something to say.

MS. SOTTO: Sure. A really quick word on that. It's a good point. I wouldn't say that it's -- it can't be the only driver. But one thing that really is an economic driver is that it's not only personal information that's getting compromised, it's also intellectual property, it's M&A information, it's financial data. There's a lot of incentive to keep that safe.

MR. COOPER: So, David, I know you want to jump in and, Daniel, with your hand up, too.

MR. THAW: Yeah, I actually wanted to build on this concept of looking at it from an economic perspective. One of the things that is continually lost in the discussions of the micro and

macroeconomics of data breaches is that we're just talking about data breaches, and that ignores the proverbial health of the network conversation.

So we can run complex analyses and say, well, is it reputational harm, is it the direct costs of response, is it indirect costs after response. At what level are we self-insurancing? Trail this out about 12 levels. And I've seen so much work on this, but at -- what's missing is the larger question of, okay, well, what about the overall health of the network, or as we would say in economics, what about network effects?

What about the types of externalities that are going to come out of an infrastructure which necessarily crosses industrial sectors and which -- in which confidence is undermined not because of any one breach or necessarily a series of breaches or even an industry, industrial sector, that has been subject to more breaches than another industrial sector, but because we reached a point where the way in which we respond is not targeted towards developing a trusted infrastructure, but rather is targeted towards case-by-case breach management.

And I think that that's something that this frame, as it were, of the economic discussion fails to

capture, and I think it's something that we need to bring into the discussion earlier when recognizing what might be missing from the current state of play.

MR. COOPER: Daniel?

MR. SOLOVE: Yeah, I think a lot of these comments have been, you know, I kind of agree with you all, especially Chris. I think that your point about the fact that, you know, reputationally, companies will take a hit, but it's often a short-term hit. So many companies have breaches that pretty much everyone has a breach. So people generally start to think, well, my data is not secure anywhere no matter where it is. And I think the law -- I mean, I totally agree. It's a set of fragments, various shards of pieces here and there.

Most of the law is reactionary. It reacts upon a breach. That's when the law typically kicks in or when enforcement begins on a law that says to do various things. When companies start to wake up is after the breach, after the bad thing has already happened. The problem is the breach already is going to cause a lot of pain. The law adds a little bit more pain to already a lot that is already there from the breach. So it's not clear the law is doing a whole lot afterwards. I mean, it's certainly adding

transparency to the system from the breach notification law. You know, the agencies get to get a nice headline. We enforced against this company and now we're doing whatever.

But ultimately what we're lacking, what's not working well, is the data security is weak. Our networks are porous. They are being infiltrated left and right. Our approach is not particularly effective. It seems to be getting worse. Costs are borne by a lot of folks that -- and not all by the companies using the data. You know, consumers bear a lot of the cost and never recoup that cost. All the data out there increasing people's risk of potential future harm, which is not mitigated appropriately. And then there's what David mentioned, the network effects. There are broader effects on security across the whole system, that can have effects that aren't internalized by companies.

So I think the law is certainly shedding light on the problem and, basically, you know, kicking a bleeding horse. Beyond that, I think the law can do a lot better job in preventing breaches. And I think that takes a different way of thinking about what the role of the law should be, when the law should intervene, and what the law should do.

MR. CALABRESE: If I could just put a very fine point on --

MR. COOPER: Yeah, yeah, Chris, go ahead, sure.

MR. CALABRESE: -- one -- something that both Daniel and David said, which is that sort of the network effect, cascading effect, I think we're actually seeing the breaches are causing an erosion of what we would consider in security to be defense and depth. These individual pieces of information that get out there, if you know my boss' name, if you know my mother -- who my mother is, if you know my e-mail address, if you know specific noninteresting personal pieces of personal information, they are incredibly useful for something like a phishing attack, right, where suddenly if I have identified you as a key person in the network, I can tailor an attack to you and then -- you know, and then you get inside the system and you can do a tremendous amount of damage.

Every breach cumulatively allows more of that information to be out there and it allows more pieces of it to be put together. So that is something that is going to be very hard for any kind of market driven force to get it. It almost has to be a legal regime, and I think we can then talk about what the

legal protections need to look like.

MR. SOLOVE: If I can just add a fine point responsive to that, as well.

MR. COOPER: Yeah, sure.

MR. SOLOVE: Well, too often we focus -- in cybersecurity more broadly, not just the data security piece, on this piece, on this idea of inside versus outside, securing the network. And the reality of the physics of cybersecurity is that it is not three-dimensional in the way we traditionally think about physical security. I cannot emphasize that enough.

In other words, I am less worried about you getting inside my network, whatever that phrase means, than I am about whether or not I can execute some form of adversarial operation that will cause you to do something that will result in my achieving an end that I want. And I may not need to get "inside your network" to do that. So to Chris' point, if you have this information, you may just be able to get the person to get on the phone and do what you want them to do without ever "being inside their network."

So I think it's very important as we go forward that we look at, well, what does it really mean to compromise? And we move away from this idea

of building walls and toward an idea of a more, for lack of a better term, trusted infrastructure. I realize that's overused.

MR. COOPER: So I guess kind of building on this and I'll ask you, David, since I've got you and you have a computer science background. You know what is the -- the flip side, hearing what Chris was saying that, you know, each additional bit of data that gets out there adds some sort of incremental risk, but is there a flip side to it that we're already in a world so awash with data, the odds that I'm leaving aside credit card numbers and bank numbers which can be changed, but our social security number -- if the odds that whether through the OPM breach or other breaches, my data and many of our data, social security and other sensitive information is already out there.

Could you make an argument, just playing devil's advocate, that the marginal impact of an additional breach is actually kind of close to zero in the sense that it adds more data that is already out there? Again, just I'd like to throw that out to you, David, first, but let anyone react to that.

MR. THAW: Yeah, so it's an excellent question, and I think the answer is, yes, you could make the argument, but it's an argument that answers

the wrong question. Because the question that you have to ask is why is it that we're worried about a social security number or, to look at the recent Marriott breach, a passport number getting out there? And the reason that we're worried about it is because we make the mistake of using this information. And I have to give credit where it's due to my Ph.D. adviser, Deirdre Mulligan, who first advocated this I think 20 years ago.

We use this information like social security numbers, passport numbers, driver's license numbers for authentication purposes, that's similar to a password, rather than just for identification purposes, that's similar to a user ID. I don't care if someone knows my user ID at all. I do care if they know my password. I shouldn't care if someone knows my social security number because it's an identification number. That's how it was originally constituted under the organic statute. Same with passport numbers, all the credential numbers.

Business practice, throughout the latter part of the 20th Century and into the beginning of the 21st Century, transformed these numbers which are, to some extent, contained in publishable directories into authentication credentials. That's dangerous.

Adversaries love that because now they just find a way to make you "identify" yourself and suddenly they can now authenticate because too many other people have relied on it.

So I think the question to ask really is, is there a fundamental flaw in the structure of our system from a security perspective that we really need to take a hard look at redesigning before we say, well, is it a marginal cost or not? I don't think that marginal cost question is the one we need to be answering. I think we need to take the question off the table.

MR. COOPER: Janis, you look like you --

MS. KESTENBAUM: Yeah. Well, I think -- some good points there. I mean, I think it's right that to the extent that these numbers have gone far beyond their intended use and are being used to authenticate people, it can be a problem. The social security number I think is probably the one that really stands out. And I do think it's gotten better over the years. But, you know, it still is being used and that's partly why it's -- it sort of stands out as a number that, you know, you do feel maybe a little bit more worried as the consumer when you know it's gotten out there and it's I think that the state

breach notice laws key off of things like SSNs. I think that would be one that really makes a lot of sense.

But I think that that also does also kind of shed some light on the converse, which is that there is some data that this is now -- it is widely available in part because of breaches and in part because it's just data that we are using all the time and that, you know, another breach that is releasing my e-mail address or my name or my phone number, really you do have to question whether there is actually a lot of marginal damage from that or what that damage would be.

And I think that is one thing that, for the most part, again, the U.S. -- the state -- the U.S. state breach notice laws for the most part aren't triggered by the release of that kind of data, what you might just think of as like directory-type data. And I think that that makes a lot of sense.

To take it back to your opening question, James, about like is there a U.S. approach to data security, just like one simple point which is that when I think about the U.S. versus the rest of the world, I think that is something that distinguishes the U.S. I do think that in other jurisdictions that

have breach notice laws, they are more likely to key off of things like or triggered by something like even the release of just a name or an e-mail address. And I think that is one thing that the U.S. system or the U.S. state system does well because we do have the problem of breach notice fatigue. It's something that the FTC, I think, has been very good about recognizing. And I really don't know that we're helping anybody when we require companies to provide notice when some kind of lesser form of information has been compromised in a breach.

MR. COOPER: Did you want to -- I'm sorry. I saw Lisa first and then Daniel.

MS. SOTTO: I would actually disagree with that point. I think the trend globally is to put all personal information of any sort under the breach notification law, but to modify it with a harm threshold. And I think that is absolutely critical. You could have harm that results from what is a seemingly innocuous data element having been compromised, but with a harm threshold that is layered on top of a very broad definition of personal information, we get to the right place.

Because then the question that's asked is what is the harm that can be done with this data now

being out there. And I think then you get also -- you capture the cumulative effect of lots of data being out there that, again, may be innocuous in each of the data elements. But when you put it all together, there actually could be significant harm. And, of course, then we get to the really hard question of what is harm and, you know, is --

MR. CALABRESE: I thought you were going to say how do you assign liability, but --

MS. SOTTO: How do you assign -- that's a really hard question, too. The question of harm, just a few words on that. Should we think about concrete harms? Should we think about less concrete harms like harm to human dignity, harm to reputation, harm with respect to opportunities? The trend globally is certainly to go toward a broader concept of harm.

Look, we have a very mature data breach notification compendium of laws in the United States. We were first out of the box. We did a great job really of pushing that concept out there. And, now, the rest of the world has sort of evolved and I think we can take some lessons from what the rest of the world has done and modernize our compendium of breach notification laws.

MR. COOPER: Yeah, Daniel, do you want to

jump in?

MR. SOLOVE: Yeah, on a few points. One, what's the harm of having the same piece of data, you know, breached a number of times? Well, it's not just the isolated piece of data. Okay, your social security number was breached by five companies. It's what the data is linked to; it's what these records are linked to. So if I can say, hey, I've got one record, which is a social security number, your name and your address, and I've got another one that has your name and your e-mail address and something else about you, and another record with this, this and this, you can put these things together and then start compiling a dossier about people from these various shards of information and then seeing how they inter-relate. So every breach causes harm even if there's a redundancy in some of the data points that are breached.

I also wanted to echo something that David said about the social security number. Back in the time they were passing the Privacy Act in the 1970s, there was a proposal, a growing concern, this went all the way back to the '70s, that companies and organizations and others were using this as an authenticator, essentially as a password. If you know

your social security number, you must be you. This made the social security number the identity thief's best tool. It's the worst password you could possibly come up with because you can find it and you can actually get someone's social security number. They're on public records. It's not illegal to sell a social security number.

And you can find them, you know, from breaches and everywhere else, and then you can use them to gain access to people's accounts and make accounts in their name and open up credit cards in people's name and so on and so forth. So it becomes a really good tool for the identity thief.

This tool could be neutralized. I actually think the FTC actually has the power and has had the power to do this for a long time and hasn't done it. We can talk about that a little later. But I actually think this could be shut down and should be shut down. This use causes tremendous harm to people. It makes identity theft very easy for a lot of thieves and it could be stopped, even with our existing laws. It hasn't been, unfortunately. But a lot of damage and downstream harm could be neutralized if we ceased using the social security number in a profoundly dumb way, which is what we do.

A lot of the problem with data security is actually the product of certain decisions that the Government has made. You know, it's the Government's decision to stamp us with a social security number and then not put the adequate protections on that number. I think it's irresponsible. I think the idea of, okay, let's create -- you know, let's push encryption back doors and let's not -- you know, we find out about a security vulnerability, let's exploit it and not say anything about it, I mean, all these things are ways that the law actually not only fails to prevent harm from a data breach, but, in fact, it enhances the insecurity that we have and actually exacerbates the harms of a data breach. I think sometimes our laws and policies and what our Government does is the enemy, not the friend.

MR. COOPER: Well, thanks, Daniel. I want to keep you on the spot and shift our discussion a little bit. It tees off something that Lisa brought up and that we've been touching on, is harms and what I want to -- the question I want to pose to you, Daniel is, does the current approach to data security that we have adequately address harms? For example, the FTC's case about LabMD, even though the Eleventh Circuit eventually decided it on different grounds,

harm was front and center there.

You have written a lot about how the current standing doctrine has prevented or has hobbled, at least, some plaintiffs in recovering in either tort or contract for data breaches and you have an interesting paper in the Texas Law Review that has come out about that. So I just wanted to let you start off the discussion on this. What are the harms we should be thinking about and does the current legal system adequately -- is it capacious enough, are we addressing the right harms?

MR. SOLOVE: Well, I think a lot of the law's approach to harm has been to bury its head in the sand and ignore it. And ignores it for -- not all the reasons it ignores it are invalid. There's concerns about, you know, liability and cost of class actions and, you know, do class actions really help plaintiffs and other things that are legitimate concerns. But in terms of just intellectually, you know, it's a matter of theoretical coherence. Is there a harm? I think absolutely there's a harm. There's definitely a harm from information getting out there in a breach.

There is anxiety, emotional distress. A lot of courts just are very quick to say, we don't

recognize emotional distress harm at all. That's a lie. Courts do recognize emotional distress harm. Pure emotional distress harm for the privacy torts. They've been doing it for about a hundred years, in fact and there's no -- they don't bat an eyelash. So if someone takes someone's -- a nude photo of someone and posts it online and someone sues for a privacy tort, there's a cause of action. The court will not even talk or even made to question about whether or not there's a recognition of emotional distress damages only or not. It's just of course. So it's interesting in the data breach context where courts hem and haw over this and not the case in other areas. It's clearly recognized.

And, you know, future -- risk of future injury, I think more courts are coming around to this and recognizing that there is a risk. As you start to, you know, put people's information out there, you're weakening their security. And they always say, well, how do we know if there's a real harm? And I would say, okay, I'm going to sell you, you know, two post office boxes. One post office box is fine. There's nothing wrong with it. The other one, I actually -- you know, I lost 1,000 keys and I dropped them all over the place with the post office box on

it. Which post office box would you buy? Of course you're going to buy the one that isn't compromised.

And as you compromise people's privacy and security more and more by getting the information out there, you are causing a harm in addition to anxiety. Now, it's a small harm in a lot of cases and it's a risk that's not like absolutely going to be victimized, but it's a hard thing to actually quantify or to really pin it down because it's a -- you know, a lot of the more sophisticated hackers and fraudsters out there are playing the long game. They're patient, they're waiting, they're not ready to pounce this instant or tomorrow. They're gathering information and they're patient. They're kind of compiling it.

So it's very, very hard to do that, but I think the law needs to start with the recognition that there is harm and a much more sophisticated understanding of the nature of the harm. One of the things I think the FTC has done really well and I'm really -- I think should really be applauded for this, is the FTC has recognized that the harm is not just to the specific individual, that there's a larger social harm, too. It doesn't just harm a particular person, but it harms society.

You know, insecure devices, they don't just

harm the particular person that bought the insecure device. These devices can actually be utilized by hackers to harm other people. So if I buy an insecure security camera or insecure WiFi, that can be used to harm other people or bring down other sites on the internet. So there's a larger social harm out there that a lot of times is kind of underappreciated, under-remedied in the law. The FTC is the one agency that has really recognized that and has addressed that in a number of its enforcements, which I'm really glad. I think that's one area where the law is getting it right.

MR. CALABRESE: I mean, if I could just --

MR. COOPER: Oh, yeah, go ahead. Jump in, Chris.

MR. CALABRESE: So, I mean, there's so many of these and they all are real and they all sort of are uneven in terms of their impact. But, I mean, in terms of reputational harm, I mean, Amy Pascal was the head of Sony Pictures when the breach happened. And she lost her job not because of the breach, per se, but because it revealed a whole bunch of embarrassing e-mails about her. Now, she wrote those e-mails and that's on her. But there's simply no question that she lost her job and that was a powerful harm.

The OPM hack is a national security harm that we do not have any way to get our arms around. The loss of 22 million federal workers' background check information. I mean, how many other harms that resulted in or allowed is not calculable but is very significant? You know, even stifling the free expression rights of film makers, which is essentially what the North Koreans were trying to do with the Sony hack, is a harm. Right? You're trying to use that as a broader harm to society.

So I just think that the FTC had a great -- the staff recommendations were really good I thought on this in October. I mean, medical identity theft, doxing. We are now in a world where because we've pushed so many things into the digital world, we're -- like it's all there somewhere. To the extent that you think about any piece of information, which is digital, which for most of us is lots and lots of information, we're able to draw lines to, boy, that would hurt me if that came out, or, boy, if you put those things together. You know, we're seeing greater and greater use of processing power.

I'll be the first person to say big data, at least on this panel, because it seems like something that we should -- every panel should --

MR. COOPER: We all have to drink now, right? Don't we have to drink?

MR. SOLOVE: But, I mean, clearly as you start to compile all this personal information and you pull together, we already talked about the ability to use that to harm people.

So I think that a threat for -- that I hope comes out of this -- and I will talk more about this -- is, I think, a desire to have a more harmonized national law. I think these kinds of harms are some of the reasons why we need that kind of harmonized law, both to try to get at some of these harms that may not come just from economic losses, but also to allow some nimbleness as we start to see more areas where harm can be caused something like, you know, SIM card hacking, right, where it's like, oh, no, no, no. Let's everybody step back from using phone numbers and SMS messages as authentication tools because it can cause all these other harms. You need some nimbleness in being able to address that. You don't want to wait five years for everybody to kind of catch up that that maybe isn't a great idea.

MR. COOPER: Daniel, I just want to ask two follow-up questions to you, one specific and one maybe a little more conceptual. So the specific one you

mentioned with respect to the privacy torts and, you know, courts have no problem, clearly not finding -- they have no problem with standing or -- how do they come up with damages? Are they just nominal damages that are awarded or do they try to actually quantify the harm or is it --

MR. SOLOVE: Yeah, well, it will be emotional distress. They will recognize that, you know, someone suffered emotional distress and then they'll ultimately try to figure out what is the harm that somebody suffered from that, because a lot of times it is just emotional distress. Their reputation might not be harmed by the violation of their privacy, but they might still feel emotional distressed because the information that they thought was private is not private anymore. For example, the nude photo, it might not result in people not getting jobs or losing their careers, but they feel a lot of emotional distress out of it, and the courts will quantify that.

They can be very big awards. The famous -- you know, the Hulk Hogan case where a sex tape was released about him. He got millions of dollars in damages from that case. Quite a huge verdict on that. So courts, I think, are fine. And the thing that I find very odd is that courts don't even try to try to

quantify it when it comes to data security. They just reject it out of hand and just say we don't recognize it at all. It's impossible. And, yet, it is possible. I think at least try. And the courts don't seem willing to even do that.

MR. COOPER: So I think that there are two types of harm you identify as problems in dealing with data security. One was maybe the intangible type, my nude photos are out there. Number two is the inchoate harms, right? You said that the hackers are playing the long game. So, you know, for instance, you think about -- my understanding, at least the research out there, payment cards are monetized relatively quickly because they can be cancelled. As soon as you know you're part of a breach, your credit card company often will just -- or your issuing bank will take it on themselves to cancel. Even though it's very expensive, they'll go out and they'll look on the dark web and say, some of my numbers are out there, let's cancel these cards.

But the -- take, for instance, past login credentials that could potentially be used later for like a credential stuffing attack, something where you attack another system to try to gain access to a financial account, where would you draw the line on --

I mean, knowing that maybe this wouldn't happen right away, this may be something that they would hold on to, maybe something the hackers would try -- what Chris was talking about -- maybe merge it with something else they buy on the dark web and to have -- to take over accounts or have new -- create new identities. Where, though, would you draw the line temporally?

Or are firms always going to be on the hook or is it something -- is it like medical monitoring for Agent Orange that we're just going to -- or asbestos or should there be three years, two years, six years, whatever it is? Does there have to be some kind of line drawn?

MR. SOLOVE: I think obviously I think just practically, yes, you need to draw some kind of line and say, hey, you know, at some point, there's a statute of limitations. However, a lot of the cases brought can be brought on the cases of risk of future injury and people are compensated based on an increased risk at the point of time that it's a risk, even if it doesn't materialize and you compensate people for a lower amount than if it actually materialized ten years down the road. And that's a way that you can compensate for harm now, address it,

if you recognize risk of future harm.

Beyond that, too, I'm not so sure a lot of the lawsuits are, you know, addressing the full nature of the harm. I do think you need agency action to do this and to really help people. I mean, there are ways that you can tackle this, like create a fund so if people are harmed they can get money from a fund that companies that have a breach put into, and so on and so forth. So there are ways around this problem. But, yeah, I don't think you just completely get rid of any statute of limitations and then let people sue 30 years down the road.

MR. COOPER: Okay. Lisa, it looked like you wanted to jump in.

MS. SOTTO: I think we have a problem in that we don't really know how to solve this. The solution that we've been tossing out for years now is to offer credit monitoring. Credit monitoring is good where a new line of credit is being opened with a social security number that is being used by a hacker. But it doesn't do a lick of good in many other circumstances. So I think we are -- and I don't have an answer at all. But I think we're in a bit of a quandary as to what we're actually looking to solve for by creating this pot of gold at the end of the

day.

I don't know that we have actually reached a solution there as a society because I don't know that there is one because because hackers are incredibly -- attackers are incredibly nimble because they could be nation state, they could be organized crime, they could be hacktivists, they could fall into so many different buckets, we don't even know in most cases attribution, the who done it part. So we don't know what we're solving for in most cases.

MR. COOPER: And I guess related, while we're on the notion of -- the concept of harm and this is something that was touched on I think in the earlier part of our discussion is, how do you -- how difficult is it legally -- if we think about we want harm, but to attribute harm to a specific breach. So obviously, there's the big -- there's the Marriott breach and I don't know if credit card numbers were involved in that. But let's say they are and let's say tomorrow I get a ping from my bank that my credit card is being used fraudulently. How do I -- maybe in my mind I link it with Marriott, but how do I know it's just not the skimmer at my gas station, right?

And how can the -- if we are going to look at harms, how can the law deal with that? Anyone? I

need an answer. I want to solve this. We have 39 minutes.

MR. SOLOVE: I have a comment. It's not going to be the answer that you want. But I think one of the problems with looking at the question of harm this way is it feels like there's a baked-in assumption of at least some reasonable degree of homogeneity in harm across the population, the consumer population. And I'm not convinced that assumption is correct.

In other words, the type of harm that this mythical average consumer experiences, I would hypothesize is fundamentally different than the type of harm that someone who works in the defense industry, whose entire life depends on them not being impersonated not because OPM can't sort it out, but because by the time OPM sorts it out later, four years later, they've been unable to advance their career for four years in the middle of their most prime period of advancement to have a shot at what they want to do later on down the line. That's just a fundamentally structurally different kind of harm. Number one, it's highly individualized as opposed to, again, this mythical average consumer which may be less individualized.

And if the assumption is correct, if the hypothesis is correct that there is a spectrum of these harms which are structurally different in nature, then many of these solutions, I think, are very well-intentioned, but even the concepts of a fund, how do you price what that fund needs to be if the harm range is incredibly heterogeneous? How do you ask an agency to develop processes.

So let's say that the Commission were to be the agency that handled this. Well, how would it go through promulgating rules even if it has to go through the Mag-Moss process to deal with these very, very different types of situations. It can't possibly, especially given Mag-Moss, do it for every different permutation that might come along, let alone when the new one comes along. I don't know very much -- at least not as much about other sectors, about the arts and entertainment sector, but I could imagine there are people within that sector who being impersonated could undermine their career severely. And I'm sure my colleagues could point out other examples.

So when we think about harm, I think it's important to understand that redress mechanisms, it's very easy to look for one size fits all solutions, but

that may actually drive us in a situation which is net negative benefit because we're drawing away from, we're replacing the traditional ability we might otherwise have for individuals to seek individual redress through civil systems. So I think this is a much more complicated program than a lot of the -- not this panel, but a lot of the scholarly debate that I've read has identified.

MR. COOPER: Of course not the panel.

MR. CALABRESE: No. I mean, if I could sort of -- I agree with a lot of that. I might look at it slightly differently or maybe I don't. We haven't talked about it. But I guess I agree, certainly, the harm is very heterogeneous. And I don't think that's that's a reason not to attempt redress. I think it makes redress more difficult, but I think we should try.

But it does, I think, especially the point about attribution, raise the really good reality, the really good point that is a reality in this, which is that sort of the traditional tort approach of somebody gets harmed, somebody seeks damages, that's what's going to keep the system honest, is incredibly difficult in this context, both for the attribution reason, but also because the harm is so heterogeneous.

So it does sort of argue that what we need to do is have policymakers say, all right, we acknowledge there's a harm in society. We acknowledge that this security breach is causing a harm. We're going to do our best through the political process to guess at what that harm is and we're going to impose some requirements or costs, if you will, some security regulations, aimed at getting us pretty close to limiting the worst or, you know, a significant portion of that harm because we think that's good for the overall benefit of society. So I think that's -- you know, the attribution question I don't think is one that we're going to answer.

In some cases, we may be able to and especially for more egregious harms we may have to develop specialized mechanisms to do that. I mean, doxing is a good example of this, right? You can often attribute doxing harms and you really want to because they're such a dangerous information crime. But, generally, I think it just argues for a baseline law.

MR. COOPER: Yeah, quickly, Dan, and then I want to switch gears.

MR. SOLOVE: I think that's right. Harms are only one part of the equation. Part of the

importance of recognizing harm is just that there's a recognition that this does cause harm to consumers, and that recognition is not just about compensating people, but mitigating the harm.

There are a lot of structural changes to the system that can be made or things that could be done that could mitigate harm that people could experience, and those things should be done. But those things can't be done unless you first recognize there is a real harm here that we have to account for and that companies and generally, you know, governments need to internalize and realize we need to do something here. If you don't recognize the harm, then, you know, you're not really doing enough to address that harm. That harm is often being ignored.

So I think that's one importance to recognize that it's not just to focus quickly on how do we compensate, but how do we mitigate this, what do we do to address this and particularly what do we do to prevent this from happening, which I think the law is often not doing a good enough job at.

MR. COOPER: Thanks. And I think that the last comments by Chris and Daniel are a nice segue into the forward-looking part of our discussion here. We're trying to -- up until this point, we have been

really trying to assess the current state of play. But looking forward -- and I'm going to start this off with David, but certainly then open it to everyone else -- you know, if we are going to write from a blank slate, what would a data security regime look like? If we are going to build it from the ground up. While you're thinking about that, what would be the proper goal? What should -- to sound like an economist, if we are -- what's the objective function? What are we maximizing in the data security regime?

MR. THAW: So we've talked a bit about pieces of this across the panel so far. So I'm going to try to bring that discussion together into a couple of crystallized points. The first is that there needs to be effective balancing of the interests to what we are calling consumers and the health of infrastructure. And I don't think that we have an effective balancing of that in our regulatory framework right now.

The second is that too much of the current structure of our regulatory framework not only treats these as separate problems, but doesn't communicate about them. So you don't have nearly enough communication from the Department of Homeland Security, which has more recently taken a larger swath

of the so-called critical infrastructure piece of this, and with respect, the Commission, there's not enough communication there. There's not enough communication between DHS and HHS, which has the healthcare piece of this with the financial regulation.

It's getting better. Certainly. But it wasn't anywhere near where I would have wanted it to be when, for example, I was in full-time private practice. If we were starting at a hypothetical blank slate at the statutory level and Congress were saying, okay, this is interstate commerce, we're going to preempt and create a national regime, I think that regime would have to recognize that cybersecurity generally is such a multidisciplinary, such a complex problem, that any solution which purports to be a comprehensive data security regime of some type necessarily needs to be comprehensive. It needs to look across the full set of problems. This is not something for which incrementalism and experimentation is necessarily a good thing.

I think we may have learned a lot from the federalism experiment with, for example, the data breach notification laws and some of the more robust state level statutes. But we're not at a point now

where another series of experiments necessarily is the best approach. One of the reasons why I would strongly encourage the panel and the Commission to consider that is because of the way in which we think about adversarial relationships.

So if you talk to some of the, for example, national security strategic defense studies scholars, they'll tell you the last thing we want to do in cyber conflict is let adversaries know where our red line is. Because if they know where your red line is, then they know exactly how far they can walk up to it without crossing it and they're pretty much guaranteed to do that. Likewise, a great deal of how we've thought of data security or cybersecurity regimes has been in the form to borrow, Lisa, some words from your opening remarks, just tell us what to do. That feels, to me, a lot like a checklist.

Why is a checklist dangerous? A checklist is an adversary's favorite thing. They want to see checklists for cybersecurity. It makes them incredibly happy. Even the most comprehensive checklist that one of the big four accounting and auditing firms is going to apply makes an adversary happy. Because if they know that checklist -- and they'll get it -- even if you do every item on that

checklist better than the high reliability aspects of the Department of Defense would do it, the checklist tells you what you're doing and, therefore, it tells you what you're probably, if not almost certainly, not doing.

Because even in DOD, you have to deal with scarcity of resources. In the private sector, that problem is front and center in making business risk decisions. So if you have a checklist of problems, you know exactly what the organization is not doing and that's where you direct your attacks.

So how would I sum this up? I would say, first, that we need to make sure that we balance the spectrum of potential goals or harms or different types of things, areas we'd look at. Second, I would say that we need to make sure we recognize that this is a multi- or cross-exercise and interdisciplinary exercise, ensure communication among the relevant experts, and third, that we understand that a reliance on -- an over-reliance on directive regulation, a do X and Y style approach is, frankly, I think exactly what adversaries would want.

MR. COOPER: Okay. Lisa? Yeah, I see -- and let me -- can I just put something else on the plate. This may be to -- it sounds like at least

hearing Chris and David, I think, is there room for the states in this kind of hypothetical world that we're drawing or does this necessarily have to be -- if we're talking about a network as a whole or a system as a whole, does it necessarily have to be done at the national level? So I wanted to put that on the plate for everyone and then, Lisa, let you go on.

MS. SOTTO: I will start by -- I was going to respond to David. I'm in violent agreement with David. But to answer your question, there is no room for the states in this. Look, I think -- in my view. We have made a mistake, I think, and it just is how it all evolved in regulating security by state. Data is like water and it flows past state boundaries, past country boundaries. You know, we really need a global approach. Now, we don't -- you know, we are not king of the world, so we can't do that. But we can certainly do something here that is far preferable to what we've been doing. Regulating security by state is just not effective.

So to get back to David's points, I absolutely agree that a cybersecurity to-do list is absolutely the wrong way to go. So, you know, when we think do you have a prescriptive approach, do you take a prescriptive approach to data security or do you

take a principles-based or risk-based approach? I am very much in favor of a risk-based approach. Now, I do think businesses need some baseline foundational principles to follow. There needs to be something concrete there to say you must do this. If you don't do this, you really are not doing right by all of your stakeholders. But beyond that, setting the ceiling, I think, is a mistake.

So I would argue that a risk-based approach is exactly the way to go because businesses know what their own systems look like, what their own threat profiles look like better than anyone else, and they can respond to those. So the ceiling -- sort of the sky's the limit in protecting data. But I do think I would argue in favor of a foundational set of principles and then we go beyond with a risk-based approach.

MR. COOPER: And let me -- I'll move to you, Daniel, next. Just touching on -- keying off something that Lisa said made me think. So in the law of economics and torts, which we think about there are two ways to solve -- you can either price -- make people pay a price for bad behavior and let them make the decision, which sounds a little bit like what you're -- I don't want to put words in your mouth, but

the sense that the entities know their risk profile better than anyone else. So that would be keyed off of harm. There is some harm and we make you pay for the external harm that you caused.

The other way is to set a very, very clear standard. You have to comply with this and if you step over that, we're going to sanction you. In that case, the sanction doesn't necessarily have to be related to the harm you cause; it just has to be sufficiently high to keep you from crossing over that line. So it sounds like what you're describing, Lisa, would be kind of a mixture of those two approaches, maybe some kind of compliance baseline and then something above that.

So, Dan, I know that, you know, you wanted to speak, but I wanted to throw that out there. We think something would -- if we're thinking about setting up a new framework, would it be harms -- would it be triggered by harm and then we set a price for the harm you cause or is it better to have a compliance regime where we set standards or is it just too difficult for even the most well meaning and well informed group of regulators to set standards that maybe that approach and a compliance type approach wouldn't work. And, Lisa, you can respond as well,

yeah.

MS. SOTTO: I'm sorry, very quickly. So, look, setting standards means that we're not future proofing because the threat actors are so nimble, so creative, so audacious in what they're doing. We need to be able to be equally nimble in our response. That's why I think a risk-based approach is right. But I think a floor is useful because companies really do need some concrete guidance in what to do as a baseline matter and then some high-level principles that they also need to take into consideration. I would combine all of that with some incentives, some safe harbors, a safe harbor from liability, along with some sort of accountability regime, as well, reporting to a board or having some certification regime in place.

MR. COOPER: Okay. Yeah, well, let me go to Daniel and then I'll get back to you, David.

MR. SOLOVE: Yeah, I'm not sure the only two options are a standard or some kind of, you know, stick at the end or punishment or liability. I agree with everything Lisa said. I mean, I think the companies need some kind of concrete guidance. You don't want to turn that into a checklist.

Also, there is no perfect security.

Ultimately, it's always a balance and the balance is between a lot of different considerations. In higher ed, for example, we have academic freedom. There are certain values in higher ed, a decentralized university system where every school is its own little fiefdom, and we want to preserve that for a variety of cultural and institutional reasons. Well, that's a terrible security environment.

It's much better to have something that doesn't have all these independent arms operating where everyone is not suspicious of someone looking over their shoulder. There's security risks in that, but we're willing to take that because we value the institutional culture, and there's a choice being made. I think that organizations make a risk calculation based on risks to their reputation, risks to financial, also the culture that they want to maintain at their particular institution.

And then there's the consumer. I think that one role that regulators can do is to kind of look over that risk calculation, make sure that companies think about all the risks, that when risks are systematically undervalued and I think, to some extent, harm to consumers is systematically undervalued by the system, is to try to introduce ways

to get firms to take that more seriously in their calculation. But, ultimately, we're not going to get, you know, the absolute perfect answer. And the answer is going be different for different companies doing different things or different types of organizations doing different things. It's not all going to be the same. The amount of data securities shouldn't be the same across all the different industries across all different kinds of data. It's going to vary.

So I think the principles-based approach, but also some kind of guidance and nudging and some very carefully, thoughtfully crafted things to get companies to appropriately and better assess these risks and do this calculation more wisely, which I think we're seeing is not happening in a lot of cases. They are doing risk analysis, but not necessarily taking into account all the risks like the larger societal risks, you know, risks to consumers, that they should be. So that's where the law can make them make that risk analysis better.

MR. COOPER: Janis?

MS. KESTENBAUM: Sure. So I feel like I'm hearing a lot of things that I agree with. So maybe solving data security and coming up with a new legal regime is really not that hard. I don't know. I

wouldn't have thought that.

MR. COOPER: We should copyright the transcript of this to start.

MS. KESTENBAUM: Exactly. But I feel like I'm hearing a lot of great ideas. And, you know, to pick up on some of what David said and others have said, I think Lisa as well, you know, this notion that it should be comprehensive, that whatever our legal regime would be if we were drafting on a blank slate, we would want it to be comprehensive and I think uniform. That does argue for a single national law.

But also the comprehensiveness, I mean, let's recall that lots of different types of entities hold and should be protecting data, that certainly are businesses, private businesses, but it's also nonprofits, it's also government agencies. I think we would want to be sure that we were thinking about all of that in whatever this new system would be.

I very much agree with what Lisa has said and others have echoed about this idea that, you know, you can't have the checklist that came from David, but there should be foundational-based minimum requirements. I think that would be helpful really to everybody, to businesses, organizations, and to data subjects, to consumers. And, you know, I think that

the FTC would be a good organization to be sort of the enforcer of that regime.

I think one thing that we're looking to get is better transparency, both transparency and clarity to the companies so that they do understand at least their baseline obligations and have the ability, through a risk-based approach, to certainly go farther than that as they would be required to do. But also for consumers. I mean, I think this is something that we've been getting at and talking about a little bit throughout this conversation is, you know, how do we make sure that consumers can make decisions about what they're going to purchase and how they're going to do business with in a way that enables them to factor in data security. I don't know if that's possible or if that's just such a hard concept for us, all of us, as consumers to really operate on.

But, I think right now the states have made a great contribution to the breach notice laws. That provides a great deal of clarity and transparency -- there's no doubt about that -- and tons of incentives for companies to keep their data security right. But, you know, I think that a breach is sort of a catastrophic event. I think we do wonder about, you know, when you're buying any kind of goods or

purchase, you're just interacting with the company, you know. I don't know what the answer is, but I do think that that's something that we would want to -- I would want to grapple with in like my new data security legal regime. So I'll leave it there. But I'm hearing lots of great ideas.

MR. COOPER: Okay, thanks, Janis.

Chris, I didn't know if you wanted to weigh in and then I'll go back to David because I know he has a comment.

MR. CALABRESE: I mean, so I, too, share a lot of this agreement. I mean, I will say I'm a little leery of -- I get the checklist concern. I also get that there's a lot of small to medium enterprises who are going to have to do this and they're going to need some guidance. While I hear we don't have a checklist, I also know that we have to meet some entities where they are, especially small nonprofits. I mean, there's just a reality there.

I mean, personally my or CDT's vision of what this national law would look like is something like a clear test. So we would need reasonable policies that -- like based on the nature and scope of the information, the sensitivity of the information, the current state of the art when it comes to

cybersecurity, and the costs. So give them a test, something to shoot for, and then build in some process requirements, so not checklists.

But, you know, you've got to have a written security policy. You've got to have a point person for security. You have to identify and mitigate -- have a process for identifying and mitigating vulnerabilities, disposing of personal information, oversight, training, a breach plan. So not the answer, but making sure that everybody is going through the steps that get you to a good answer, and I think that's important.

Obviously, we're going to need -- I think the FTC would do a great job of this. I think they should have regulatory authority so they can fill in the gaps. I think that's really important. I think they're going to need some more people and some more resources because this isn't the kind of thing that you can do with the existing resources. I think there needs to be fines and that people who are not making the cut need to be able to pay an administrative penalty, and I think that's really important.

MR. COOPER: So can I -- I just --

MR. CALABRESE: Yeah.

MR. COOPER: With respect to your fines,

would you see the fines as for noncompliance with the process requirements or fines for harm from breach or both?

MR. CALABRESE: Both.

MR. COOPER: Okay.

MR. CALABRESE: Yeah, I think that there's -- I mean, the reason we have process requirements is not because we think process magically fixes everything. But if you don't even have a process, for example, for taking in security vulnerabilities in your systems, well, okay, then how are you possibly even aware of the vulnerabilities that you have? So I think that it's important to make -- if we're going to say these are the key standards, we have to hold people's feet to the fire.

Just one more, this isn't a legal issue so much as a sort of political issue. We believe in a comprehensive law. I think we think it's really important. I will say that data breach at the national level has been a quagmire for a decade. I'm not sure it's imperative that we have a federal data breach law. I think it would probably -- if it was strong, that would be good. I'm not sure that you can't do a security regime without one and I would worry about the politics of saying, oh, no, that

absolutely must happen because it's been weighed down for so long. Similarly, sector-specific laws in things like healthcare and, you know, financial services, those are entrenched industries that are very powerful and they have security regimes.

Now, am I willing to sacrifice the security benefits for all of the entities that are currently not covered in order to insist that everybody be covered by the same standards? I'm not sure that I am. But I think it's certainly a concern I would have, which would be that you would allow sort of the focus on comprehensive at all costs to obscure the value of covering many entities that are not currently covered.

MR. COOPER: Thanks. David, I know you've been waiting to jump in.

MR. THAW: Yeah. I'm in very, very substantial agreement with a lot of the comments that have been made here, and I'm really glad that Chris went before me because one of the things which ties together many of the themes, Lisa, starting with your comment, comes all the way down the line about having a baseline framework and layering process based standards on top of that and the question of is it failure to comply with the process that becomes the

violation, et cetera.

What I often describe as the best written cybersecurity law and accompanying regulations in the world, and I've never seen anything else anywhere like it, is the HIPAA security rule. Now, I want to distinguish that very quickly and very poignantly from the way it has been implemented in practice because it's been -- and if you'll forgive the very aggressive term -- it's been bastardized in practice.

But what the law requires -- and if you go back and you look at how the National Committee on Vital and Health Statistics discussed its drafting of the regulations implementing the laws is exactly what we've all been talking about almost to the letter. I spent the better part of the past decade studying this. There's an enormous amount we can learn from this in terms of if that were to have been implemented correctly, if it hadn't been checklist-ified -- that's not a word, but I'm going to try to make it one -- then what might have gone better in healthcare on the security side?

And since everyone else has offered their thoughts on this, I'll offer mine, as well. I do think the Commission has an important role to play in this regard. I think the Commission's competency in

understanding consumer protection, particularly the deceptive pieces, is that important role. I think that if the Congress is going to take this up seriously and engage in this large-scale creation, there needs to be other players at the table with adequate technological competencies and regulatory power to be able to fill in some of the gaps where the Commission just simply doesn't have that agency expertise to do it. And somewhere around out there I have a white paper floating on this, which I'll try to make percolate to the top of my website.

MR. COOPER: Okay, yeah, thanks. Let me -- maybe I'll stick with you, David, while I have you on the spot, but have everyone. You know, one thing I'm trying to drill down on here is, you know, we've heard Chris saying we should have some process baseline, Lisa talking about kind of a baseline. I don't know if you're talking about process or actually substance in the sense of the baseline. I'm wondering how much of this new regime that we're all creating right now would be ex-ante regulation in the sense that we're going to -- and I heard rule-making authority from both of you and I think, David, regulatory authority.

So do we write down rules of the process or something more and then enforce violations to those

rules or is it more in the way we have it here at the FTC, a little more harms-based or ex-post enforcement-based? So going to what -- kind of a risk-based approach, you think, okay, well, I know my -- I'm a firm. I know what my threats are, I know what my costs and prevention are. And I know that if I have a breach, I'm going to be dinged. That's a price of doing business and we'll enforce it that way.

To what extent would there be more ex-ante regulatory prescriptions in this regime versus trying to address harms through an enforcement mechanism?

MR. SOLOVE: I'm going to put my administrative law professor hat back on and say both. But more seriously, I really do mean both. I want to remind the audience and the Commission that ex-ante regulation through a rule-making process need not be prescriptive in the way we traditionally think about that. Process-based standards are ex-ante regulation. The enforcement of -- the real big piece -- there's all this low-hanging fruit in HIPAA of did you have a plan at all, did you follow your -- but the real big piece and where I think we need to get to is the adjudicatory aspect of was your plan reasonable.

There's been so little activity in that space because there's so much low-hanging fruit in --

at least in the HIPAA space of you just didn't have a plan at all or you had a plan, but you didn't follow it, or it wasn't a real plan. We have virtually no meaningful agency jurisprudence out of HHS. I'm not faulting them. They've just have been too busy with "you didn't do anything at all."

So I think you need both. And I think that's where, if there is a hypothetical cybersecurity coordinator agency, whatever that role looks like, which promulgates here's the framework -- because NIST can't do that because they don't have rule-making authority. So whoever picks up that piece. And then with respect to consumer protection, the FTC; with respect to the other relative sectors. When the Commission, meaning the FTC, comes in and says this was unfair and deceptive for reasons X and Y, part of that adjudicatory process may well involve saying you had an unreasonable plan for these reasons that are within our agencies' competence as defined by Congress. So I think the answer is it needs to be a blend of both.

MR. COOPER: Okay. I don't know, Lisa, did you want to jump in or --

MS. SOTTO: Yeah. You know, I think HIPAA really is an extraordinary model. The problem with

HIPAA, of course, is that it is so specific that it is not future-proofed and it has become rather stale. But I look to HIPAA, frankly, for all of my clients in every sector because it does -- it's a list. It's a list, right. And it's easy to follow. The problem is the future-proofing.

I do think ideally it would be good to -- what you're talking about really is auditing of companies to see whether, in fact, they've put in place a comprehensive written information security program. The reality of life is that government agencies are never going to never have enough resources to do that, so enforcement becomes event-based. Something bad happens and then there is a look back to see whether, in fact, your security program is rationale under the circumstances.

There may be a role for a private certification-type of regime where you can -- and this is -- I'm not making this up -- this is in the GDPR where there's the general protection regulation of the EU, where you can obtain a certification from a private sector agency that says you're reasonably compliant with X scheme and, therefore, you have, again, a safe harbor from liability.

So I think we have to think outside the box

here about the types -- how we can partner with the private sector to get to something I think closer to what David is arguing for.

MR. COOPER: Daniel, you want to jump in?

MR. SOLOVE: Yeah, I think it's very important that agencies play a role before the bad event times. You know, after the breach, I think a lot of times it's just the agency piling on a little bit more pain when there's already pain enough.

I think that the FTC had some early deception actions in the early aughts involving companies that promised reasonable security and didn't deliver on it, and this was pre-breach. There wasn't any breach. But the FTC went in and said, you know, we're looking. And that was great. It created a whole new front where companies are we'll wait for the breach and then we'll do something. Now, they know that an agency is looking after what they're doing. And I think that that kind of enforcement, the auditing that HHS used to be doing, but I think stopped now, all that is great.

And I think we need more involvement earlier on. That's a, I think, better use of agency resources to really drive organizations to start taking things seriously and doing things in a better way before we

see the breach happen. The breach itself is already going to cause a lot of pain and consequence that, you know, the agency enforcement after the fact often doesn't add anything that we don't already know or that the company hasn't already suffered.

I think there's also a lot of strategic enforcement that the FTC could do. I mentioned earlier, you know, the FTC can do something with the use of social security numbers as passwords. And it's very simple. The FTC enforces reasonable data security. That's a standard in the Gramm-Leach-Bliley Act. It's generally the standard that the FTC applies in unfairness and other things and other laws.

So the FTC could just say, and I think it's pretty obvious, that the uses of a social security number to authenticate identity is unreasonable. It's unreasonable data security. I don't think anyone could argue with that. It's clear as day. So why not do an enforcement and make that statement and put companies on notice, you can't do this. And I think it would take an enforcement or two and we'd start to see that practice dry up and stop, or if Congress would pass a law, but getting Congress to do anything is impossible these days.

MR. COOPER: Janis, and then Chris, if you

want to -- we've got a couple minutes left.

MS. KESTENBAUM: Yeah. I mean, I do think it's right that we want to look to have some kind of a mixture. I think of the system that we have today, at least under the FTC Act, as being the kind of harm-based approach. And I think that that makes a lot of sense. If you think about some alternatives, I mean, right now, the FTC, at least under the unfairness authority is only supposed to take action if harm has occurred and it's substantial or if it's likely to occur. And that seems like this eminently sensible standard. I don't know that we sort of want the converse. We don't know that we want the agency -- an agency like the FTC taking enforcement action if there weren't injury and injury weren't likely. Like that, to me, seems like maybe a problematic circumstance.

So I think that in the main, we want to stick with that. What I do wonder, and this, I think, does marry up well with what we were talking before about sort of what the sort of substance of this new regime would look like, of would we have something where there might be some kind of baseline foundational requirements that were fairly specific. They could be sort of substantive requirements as opposed to process-based, and then on top of that,

would you have a more risk-based approach.

And maybe along with that, you know, you would marry up those foundational requirements, if you had them, with either some kind of a penalty or some kind of an incentive to have them. I mean, there could be a safe harbor approach or if you had -- you met certain requirements that it did protect you as a company or any kind of an organization from liability. So I would want to think about all of those approaches in concert.

MR. COOPER: Okay, thanks.

Chris, I guess you get the last word.

MR. CALABRESE: Comprehensive data, privacy law enforced by the FTC, but not overly prescriptive and would benefit both society, businesses, and consumers.

MR. COOPER: That is perfect. We're zeroed out when you said that.

Anyway, join me in please thanking the panel for a lively discussion and stay tuned for the next panel on the FTC.

(Applause.)

PANEL 3: FTC DATA SECURITY ENFORCEMENT

MR. TRILLING: Good afternoon, everyone, and welcome to our last hearing panel. For those who weren't here earlier, I'm Jim Trilling, an attorney in the Division of Privacy and Identity Protection here at the FTC, and I will be co-moderating this panel along with my colleague, Laura VanDruff. We have an esteemed group of panelists here to discuss FTC data security enforcement. Our discussion will build upon comments that other participants have made earlier during two days of the data security hearing.

Let me briefly introduce our panelists in order, and their full bios are available outside the hearing room and also online. We have Woodrow Hartzog from Northeastern University; Geoffrey Manne from the International Center for Law and Economics; William McGeveran from University of Minnesota Law School; Lydia Parnes from Wilson Sonsini Goodrich & Rosati; and Michelle Richardson from the Center for Democracy and Technology.

As with our previous panels, we will invite questions from the audience. So please wave down FTC staff who will be walking the aisles if you would like to submit a question card at any point during the discussion.

With that, I'm going to turn it over to Laura to kick things off.

MS. VANDRUFF: Thank you, Jim. So at the outset, I would like to start with a topic that we focused on a lot in the last session, which was promoting data security and deterring breaches. What are effective means of doing that within industry, and Lydia, as a member of the bar on the private side, what have you observed? What is effective in terms of promoting data security and deterring breaches?

MS. PARNES: Thanks so much, Laura. And it's really -- I really appreciate the opportunity to be here.

So I think, first of all, promoting data security and deterring breaches I think are two different things. There is a difference. I mean, as the FTC has long recognized, a company can have reasonable data security practices and still experience a data breach. And from the Commission's perspective, you know, not be in violation of the law.

So I think that the FTC and others can promote data security. I actually don't think that anybody can deter breaches. They happen. They happen in the best of circumstances. So I just think kind of making that distinction is worthwhile.

I also think it's worth noting that good data security practices, and sometimes even best practices, are actually encouraged by the marketplace. So for smaller companies, you know, that are just starting, maybe they are providing -- they are service providers to larger more mature companies and they are out in the market and they typically start to take data security more seriously when they're entering into contracts with bigger players and these contracts include commitments that they have to make with respect to data security. And it's at that point where they are responding to commercial pressures from bigger players and implementing better data security practices. And I think security is also an issue when potential investors are doing diligence on security issues.

And I think we all know that the marketplace for bigger companies, the marketplace punishes companies, sometimes very, very seriously punishes larger companies that experience data breaches. There can be devastating reputational costs, impacts on the value of a company, executives who lose their jobs because of the way in which they've handled a data breach. I think, you know, all of this suggests that there are incentives for companies to have good data

security practices in place.

But, you know, I do think that the Commission plays, has played, and will continue to play a very important role in this space. I think, you know, the discussions that the FTC is having today and that they had yesterday are really a very important piece of this dialogue. It escalates the issue. One thing that I've seen in private practice is how much companies pay attention to what the FTC says. So I am confident that when a report ultimately comes out after these hearings, you know, industry will be out parsing all of the words in that report.

So, you know, I think in terms of promoting data security, pay attention to the market and also the Commission has an opportunity to use its own voice in terms of escalating these issues and talking about the importance of data security.

MS. VANDRUFF: So, Geoff, I want to follow up with you on that, that some stakeholders have criticized that too much spending with respect to deterring breaches -- and I think that Lydia has drawn an important distinction between promoting effective data security and deterring breaches, but that too much spending on security generally has been on lawyers, crises management, and providing breach

notice. Is that a fair criticism?

MR. MANNE: Yeah, I think that's right, actually. As between functions that the FTC could perform, some of which Lydia mentioned and, you know, doggedly pursuing data breach cases against companies like LabMD for a decade, I think time and resources would be much better spent on some of the other areas where the FTC has indeed spent some time, but could spend more.

So a couple things that I would point to. In addition to reducing the sort of ex-post breach enforcement approach that it currently pursues, I think it's important for the FTC to adopt or to more consistently adopt the role as a convener of information as both an entity that needs to be informed on a regular basis in order to determine how and whether it should undertake enforcement actions, but also how and whether it should potentially undertake rule-making or other activities and disseminate that information to firms out there along the lines of the sort of start with security kind of guidance. Although that's a bare fraction of what the FTC could be doing.

Even more, I think the FTC could take a leading role in convening industry groups to take

advantage of the very real market forces that Lydia just described. There is an obvious incentive out there. Companies aren't necessarily sharing data and best practices in the optimal sort of way, nor are they sufficiently informed by the FTC about how the FTC would incorporate those, how it views the legal standards and how it would view specific practices undertaken by industry self-regulatory bodies.

But that's precisely what the FTC could and should do is give an imprimatur to certain self-regulatory bodes, give them a consistent source of information about how the FTC thinks about how it interprets the law and how it would approach their sort of best practices and give companies the ability and the incentive through either, you know, a safe harbor or even potentially on the other side, a strict liability rule for noncompliance with what these entities come up with, provided they are sufficiently informed by how consumers view what companies do, how consumers view their treatment of data, and how the FTC views the law and would enforce it in that context.

MS. VANDRUFF: So, Woody, I would like to turn to you. Lydia and Geoff have laid out different views, I think, of FTC enforcement and provided

different frameworks for potential approaches to enforcement, which is really maybe -- well, let me just ask. Do you have any reactions to what Geoff and Lydia have set forth here at the outset?

MR. HARTZOG: Sure. So I think that there is ample incentive for companies to do a certain amount of investments in avoiding data breaches and certainly there are market penalties and maybe even without the threat of some sort of regulation. We might see a heavy amount of investments, but, often, I think that when we focus on a lot of the breaches -- and I think Lydia's point about the fact that avoiding breaches and having good data security are actually probably two different things.

And I think that there are strategies that the FTC might be able to take to encourage things beyond breaches, to encourage the sort of healthy information sharing that we have, and to call back to the brief panel that we had, process-based remedies. So that's going to either require a little more efforts on behalf of the FTC in terms of filing complaints, different kinds of complaints, finding new territory for the subject of their complaints, because, right now, we've been focusing pretty heavily just on the breach. We find a breach and that's

what's articulated as the harm, and we might have to sort of go beyond that if we want to really start having a fuller discussion about what data security actually is and what the goal should be.

Because we've been heading along I think in a relatively actually conservative path. I think that there's a smart reason for that. The FTC only has limited resources. It's been given a limited grant of authority and I think that it's done a pretty reasonable job in that regard. But if it wants to, I think, make the next leap in terms of broadening the theory of what constitutes encouraging and mandating good data security, I think we start needing to move beyond just focusing just on the breach and the entity that holds the data.

MR. MANNE: Can I just say one thing to bolster that? I think I completely agree with Woody, which is a really weird thing for me to say. But it is absolutely I think the case that we've fallen into this sort of mind set of the breach as the kind of central defining feature of how the FTC is currently defining standards to the extent it is and how it is pursuing in its regulation by enforcement. All of this is focused on the breach and that, as a logical matter, Woody's right, there's a limit to resources

and all that. But it doesn't really make sense.

It is not necessarily the case that a breach demonstrates the most lax security. And it seems to me that we can talk more later about the best way to do it, but identifying that, right, figuring out where the real risks are, whether there's been a breach or not, should be the overwhelming focus. Remediating after breaches is only going to, by chance, get you to where the real issues are.

MS. VANDRUFF: Well, let's talk about that for a moment. Bill, on the last panel, a number of our guests talked about the need for standards, and different panelists had different approaches. But some observers had argued that the FTC should only bring enforcement actions if there's been a deviation from industry standards. What is your reaction to that position?

MR. MCGEVERAN: Well, there's been lots of agreement across the panels today. I'll move in with some amount of disagreement and in particular with something that Lisa Sotto, who is obviously an expert in this area, but one thing she said in the last panel was about this sort of cacophony, she said, of different standards, that there were so many different kinds of rules coming from so many different

directions, which is true, but which is quite a common problem that lawyers are familiar with facing and it's not the same thing as saying that those different kinds of standards are not reconcilable.

So I would say, in response to your question, the FTC's way of defining what should be the measure of responsible data security is already now heavily informed by a pretty well-developed understanding of reasonable and acceptable and appropriate data security practices and that it's consistent in a wide variety of sectors.

Here's the self plug. So I have my newest article that's coming out in the University of Minnesota's Law Review, which you can find on my Twitter page.

(Laughter.)

MR. MCGEVERAN: I talk about this, defining the content of this duty. I looked at 14 different sources of the duty, 14 different frameworks. Seven of them legal; seven of them private, things like insurance underwriting and industry standards like the NIST and the PCI standards. Across those, you can reduce the fraction to a pretty clear set of best practices that are widely shared across those segments.

So I wouldn't say the FTC should only act when industry standards have been transgressed. I would say the FTC should and does act informed by this growing convergence and consensus around an understanding the content of the duty.

MS. VANDRUFF: That's very helpful, Bill.

Michelle, I want to ask you a related question that other observers have argued as sort of a further extension of this question about standards, that the liability should extend really only where a target has willingly or knowingly departed from industry standards. Developing that evidence for the agency would be resource-intensive both for the agency and for the targets. How should the FTC balance those considerations?

MS. RICHARDSON: I think we would be disappointed if we moved away from the reasonableness standard which has been implemented across a number of different states here at the FTC. And I think that then gets back into the question we just talked about, right, about enforcement versus trying to make systemic changes. I think that is where the future is, right. We have so much security debt, individual enforcement actions are not making up the gap that we need to, and I think you're only going to make that

gap larger if you are trying to limit enforcement to situations where you have this willful misconduct.

I would say I know people are afraid of standard setting. I think there's usually a presumption that the FTC is going to come up with something wild and crazy that no one has seen before, right. But if you go back and you compare the materials you're already putting out as guidance with NIST and BITAG and, you know, European bodies, they're very, very similar, right, if we're talking about the baselines and the same half a dozen things has been the baseline for many years now and there really is no reasonable case for not following them, especially if you're talking about entities that are sophisticated.

So we do like reasonableness. I think that is the better way to go. It's something that really scales with the sophistication of the entity, the sensitivity of the data, their choices in data processing, and it is going to be the only way legally that we can start making up for lost time.

So, Lydia, before I move on, I just want to circle back. There's been some discussion here about focusing on process instead of output instead of the results and thinking about a firm's data security practices instead of the breach, in lieu of the

breach. But, of course, to prove unfairness under our statute, as you know well, we have to show likely injury or actual injury. Should the agency be bringing actions on poor data security practices absent a breach?

MS. PARNES: Really?

MR. MANNE: Say no, say no.

MS. PARNES: No. So I think that is such a difficult question. I mean, I know that the Commission has done that. There have been cases where the FTC has taken action against a company and it hasn't experienced a breach. I think that -- I think, you know, kind of the LabMD line of kind of not the way LabMD, but the argument about injury being required and, you know, certainly the Commission's focus on looking at informational injury, I think all point to the notion -- and I think under unfairness, you need -- you do need to prove some harm to consumers.

So I think it would be -- I think on the unfairness side of it, it would be very difficult for the Commission to prevail in a case if it didn't have proof of injury.

MS. VANDRUFF: Using our existing Section 5 on fairness authority?

MS. PARNES: Yes.

MS. VANDRUFF: Okay.

MS. PARNES: Yes. Yeah, yeah, yeah. No, no no, absolutely. You know, it strikes me as maybe not -- I mean, it's not overreaching, but maybe from more of a prosecutorial discretion perspective, if a company doesn't have kind of what the Commission considers to be appropriate security, but there hasn't been a breach, the Commission may decide to take some action short of an actual -- you know, seeking an order.

It's my understanding, based on discussions with folks here, that there have been, you know, kind of countless investigations over the years, and I know there were investigations when I was here, that were closed for a variety of reasons. You know, data security investigations that were closed for a variety of reasons. Sometimes it was the company reacted very quickly. I mean, there are all kinds of reasons why the Commission decides to exercise its discretion.

That, I think, is really -- I think there's a lot of learning that you guys have that the FTC staff has on the basis of both when you decide to move forward and when you decide not to move forward. And I think that's information that actually would be

incredibly useful to the industry.

MR. TRILLING: So I think we had a couple others who wanted to comment on this line of questions. Woody, did you have some input you wanted to add?

MR. HARTZOG: Sure. So I take the point, and I think it's a good one, that under the existing way in which Section 5 has been interpreted, that it would be hard in a lot of instances to bring more complaints when they are in the absence of a obvious breach. That being said, I want to actually encourage that -- encourage more complaints or at least some sort of action in the absence of an actual breach to build upon what Dan said in the previous panel because, A, that's a way to be proactive about things, and B, if we do think that data security is process-based -- in other words, what constitutes good data security is following a procedure not just some sort of end results -- then it almost actually compels us to pursue that as a remedy.

We give tickets for speeding even if cars don't get into accidents, but presumably the reason we have speeding laws is to avoid accidents. And maybe where this comes down to -- what this throws sort of into sharp relief is the need for the FTC to have a

little bit more room to work with a larger spectrum of possible remedies or finding authority. So for example, we might consider failure to follow process in the absence of some sort explicit breach or harm. Maybe there's a smaller fine or a less aggressive sort of remedy pursued.

But I don't think it follows necessarily that we should entirely avoid some sort of regulatory involvement in the absence of a breach because it's the process that we want to actually focus on in the first place.

MR. TRILLING: Geoff?

MR. MANNE: So I'm going to finally disagree with Woody a little bit. I think, obviously, I said earlier that this sort of central focus on the breach as the central element of the FTC's enforcement and effectively rule-making processes is inappropriate, and I stand by that. I do not think that it's feasible given the extent to which the FTC has tried to define reasonableness or injury or any of the other elements, you know, duty and causation and the like, that it's bad enough that a breach itself is considered a harm. I don't think that's even tenable under the statute and with the current standards.

But I think it's impossible to conceive of

and the Court in DLink obviously thought this as well, as did the Court -- certainly the ALJ and probably the court in LabMD -- that it's impossible to conceive of a case where there isn't something closer to injury than nothing at all. But I do agree with Woody that -- oh, sorry, I should say kind of an element of this -- well, I agree with Woody that there could be something other than an enforcement action. I don't think it makes sense to pursue an enforcement action where there isn't, again, at least a breach and, honestly, quite a bit more than that. But something other than an enforcement action, of course, makes a lot of sense.

I would echo something that Michelle said, although put a strong constraint on it. I think it absolutely makes sense if anyone -- to identify sort of baseline security practices that apply to every firm across the board no matter any of the relevant characteristics you can imagine, the dimensions on which firms can vary. If there are actually identifiable security practices that would apply to all of them, there's no reason not to adopt those as a virtual requirement. But has anyone actually assessed whether that's true, whether there actually are some elements of data security that literally apply across

the board to everyone? It is totally believable to me that that is true. I just don't think anyone has actually done that yet. But the FTC should do that.

And unless and until the FTC can produce the sort of evidence that these X, Y and Z security practices should apply in every instance across the board, I don't think we should be talking about in this sort of baseline. But once they've done that, it seems to me it makes perfect sense to apply such a standard and that's where you can have liability even in the absence of a specific breach. But there's a lot that has to be done first before we get there. I think it should be done.

MS. VANDRUFF: Michelle, I'm sorry, you had -- you wanted to weigh in?

MS. RICHARDSON: Yeah, yeah. I would say, though, I think this moment we're in right now culturally is recognizing that data is different, right. And it's going to be very different than a lot of the things FTC has to deal with. And so these front-end preventive measures are going to be incredibly important. The breach is just too late, right. This is different. The data is intimate, it's immutable, it's being used to make decisions against us that are incredibly important about where we get to

live and go to school, what we pay for healthcare, right, and it's irrevocable often after these breaches. After it's out there, you can't make people whole. It is not like giving someone their money back or giving them a new car. So we have to accept that we have to conceptualize the risk and the remedy differently here.

I'll say, you know, I'm forgetting my number, but there is an excellent NIST document that recently resurfaced, NIST OR NTIA that tried to list all of the different standards, even internationally, and the status of where different industries were with implementation. And it was actually pretty well all over the map.

MR. MCGEVERAN: If I could just jump in. So, I mean, I'll agree with you up to a point, Michelle, but I'm not sure that does makes data different in the sense that Woody was talking about before, where a lot of times stepping away from the constraints of Section 5, as it exists right now to some degree, or at least thinking about interpreting it perhaps in ways that we could discuss, but looking back at data security as a problem, if the bridge falls down, the immediate public reaction is where were the inspectors before the bridge fell down.

And approaching breaches as a necessary condition of an action or an investigation, which I know is not quite what you're saying, Geoff, but, you know, we need to be thinking about a preventative and process-based model. If that cannot be accommodated within the boundaries of Section 5 -- I'm not sure that's true; I think maybe it can be -- but if it can't, then we have to think about whether Section 5 is enough.

MS. VANDRUFF: Well, I'd like to -- we're running a little bit short on time, but I did want to follow up on one issue that Geoff alluded to. He said that there should be room for the FTC to take action other than enforcement actions. We received a couple questions from the audience about whether the government entity, unnamed, could do pen testing, penetration testing, on private companies and then name and shame, whether that's a possible avenue.

Geoff, I'll put that to you since you raised the alternative.

MR. MANNE: Penetration testing, and then I didn't hear what you said.

MS. VANDRUFF: And name and shame. So presumably, if the results were poor, if a company had vulnerabilities on their public-facing systems,

whether a government entity, again the questioner did not put it to be that necessarily the FTC could identify those companies, or then the questioner also says maybe then the government entity could demand remediation.

Alternatively, we also received another question from the audience about the role of closing letters, FTC closing letters specifically, where -- and the purposes that those serve. And I'd invite you to address both of those questions from our audience.

MR. TRILLING: Can I actually add, to further complicate it --

MS. VANDRUFF: Okay.

MR. TRILLING: Very related for people to think about, with any of these ideas that are different than bringing enforcement actions and maybe deciding to commence an investigation after a breach, given the potential cost to the businesses involved and the cost to the FTC and the allocation of FTC resources, how should the FTC go about deciding who it would be examining?

MR. MANNE: So let's see. With respect to the closing letters, I suspect you may find near unanimity here that -- I think Lydia's already said this -- that there's -- it is at least as important to

know why the FTC is not bringing cases as to know why they are bringing cases. Honestly, the FTC's doing a terrible job telling us why they're bringing the cases they're bringing, and I think they need to do a better job there.

But, you know, since Dollar Tree -- I don't think there's one case since Dollar Tree where we had a closing letter, and that closing letter said nothing. Dollar Tree was the last closing letter I can think of to say anything useful. We haven't had those. I think it would be immensely valuable and really no small cost -- no cost to the FTC since that information is already provided by the staff.

It is -- sort of to segue to the name and shame kind of question, I agree that it's not absolutely clear that closing letters should identify companies by name. I think that's worth considering, because there is obviously a potential reputation hit just from the fact of an investigate, even if it was closed. But that seems like a small hurdle to jump. I mean, sometimes it will be harder than others, but definitely something to consider. And sometimes it might actually make sense to reveal the name.

With respect to other mechanisms, I think we're sort of jumping the gun. I think the real

problem, the real concern I have with enforcement, the real concern I have with other approaches is the same reason that I'd like to see, at the very least, closing letters and that is I don't think that the FTC has enumerated either the way it views the statute and what it actually means by reasonableness nor how it will apply to the facts in a range of cases. To put it differently, I don't think that the FTC has provided fair notice in the vast majority -- for the vast majority of firms.

And thinking about even other remedies that would still key off this same kind of amorphous reasonableness standard that really doesn't tell you much, seems in a way not much better than the enforcement process, except it might cost a little bit less and, therefore, at least be less wasteful. Again, I think the place to direct efforts is to establishing these sorts of standards, making it very clear, identifying whether there are clear safe harbors and also clear -- what's the opposite of a safe harbor?

MR. HARTZOG: Worse practices.

MR. MANNE: Worse practices that could -- I think would require Congress, right, and potentially lead to statutory damages completely in the absence of

a breach. But one has to do that assessment first. One can't just say, well, hey, you know what, good password practices seem like something everyone should do. Reasonable password practices.

That's not enough guidance to impose statutory fines for people who don't follow good password practices, especially when you consider that those best practices, the things that NTIA is pointing to, that NIST is pointing to, these are things that relate to the most sophisticated parties in any particular area and that's fine and I think it's actually is appropriate to hold them to higher standard. And, in theory, a reasonableness approach could address that. I would query whether any of the FTC's actions have ever talked about the sophistication of the parties and their knowledge of data security and ability to implement those practices. But that seems like it should be discussed.

But those standards are something that you would expect sophisticated players to comport with, but it's not clear that a small retailer, who is just trying to make sure they don't run afoul of the law and protect their customers, I don't think it's necessarily the case that we should assume them not

following the state of the art practice is an inherit violation. That's the sort of thing that I think the FTC really does need to hash out because I don't think it's clear where that line is drawn, for example.

MS. PARNES: So if I can -- thank you. This is, I think, really interesting. I mean, I completely agree that the Commission has a role well beyond enforcement and has impact well beyond enforcement. If the only way the Commission was able to kind of make a point was by bringing a case, I think the agency would be severely constrained because it just, as people have mentioned, does not have the resources to kind of solely focus on enforcement.

I also think, kind of taken together with that, I think the overarching standard needs to be a reasonableness standard. It is impossible to have a standard that is specific because data security changes so quickly. What makes sense kind of today may not in a year. But kind of beyond that, it's really interesting. The Commission has provided guidance about kind of like the difference between the nature of data security required for a mature company and the nature of data security required for a small business. And I think -- although you guys can correct me if I'm wrong, I think I was here when the

agency put out that business education.

But business education -- and the Commission does fabulous business education and regular blog posts on data security and the start with security work that the Commission has done has been super-impressive. But even with all of this information that goes out there, I don't think that it has had the same impact, for example, as the FTC's privacy report. That was a game changer for companies. It moved the needle significantly with respect to how companies think about privacy.

And I think that -- and I think the Commission needs that kind of effort on data security. Maybe it touches on standards, but I'm not thinking of it in like really kind of like developing an FTC version of a NIST standard or ISO standard. I'm thinking of it more in terms of, you know, an FTC version of kind of what -- the kind of guidance, meaningful guidance and detailed guidance that the Commission gives in its reports. And I think it has -- did first this kind -- the major privacy report and then filled in on more than an annual basis on, you know, kind of different aspects of privacy.

I would think that is a worthwhile investment for the Commission in the data security

area, a kind of major effort that really sets out data security requirements for companies in a report. And then, you know, the agency kind of comes back to that on maybe an annual basis and updates it, and in the course of that is convening industry players, certainly academics who think about this, but security experts, I mean, people who really know this field and who can address it on an annual basis. And I think that those reports really could move the needle in terms of actions that industry takes.

MS. RICHARDSON: Can I just actually jump in here really quick just to say, you know, I think we don't want to wander too far in worrying about what very small businesses do with their security because they rely on a very small handful of big players, right, who are service providers and software providers and platforms. If those handful of companies are making important decisions, it is going to trickle down, right. Because really when you're the small business on the other end, you're only making a handful of decisions, right. You're dealing with the controls offered by your service provider, your e-mail provider.

So the idea that these sorts of standards can't scale, I don't know if that's right, that might

be somewhere else where the FTC can work with some of these larger entities to make these systemic changes, right, because that's, I think, what we keep talking about at CDT is how do we get back to systemic changes that move the burden from individual users back to the people who are best able to address the problems. That could be everything from e-mail authentication software to purpose specifications and registries for connected devices, things like this -- you know, if there's a commitment to it from some of the big actors, it would really make huge changes in the ecosystem.

MR. MANNE: You know, I totally agree with that. I'm just pointing out that the cases the FTC has pursued have been, at best, at very best, mixed on that score. It seems almost self-evident that, yes, clearly you should be going after addressing the potential problems with the people who are literally designing the security systems, not the Tower Records who are implementing them or the small car dealership in Georgia whose name I forget or BJ's or LabMD or any of a number of other companies, at least not first or -- and at least in a very different way.

But I completely agree that if there was a lot more -- it would help if a lot more attention was

paid to those who are actually clearly sophisticated parties and who are literally designing the important elements of the security infrastructure that everyone is using, it seems like low-hanging fruit.

MR. TRILLING: Could we go to Bill and then Woody?

MR. MCGEVERAN: So plus one on that. I mean, look at the PCI, the Payment Card Industry, standards that target essentially the behavior of large intermediaries that have a lot of influence and, you know, your mom-and-pop shop that you're rightfully concerned about is primarily, just as Michelle says, engaging in the services of a few providers for the card reader that's sitting on the store counter. And it's a much larger, more sophisticated entity that's actually making sure that that's compliant with PCI.

I would also point out the PCI standard is itself an industry-created, contractually-enforced type of structure that has been, often by name, just sort of absorbed into a lot of law and a lot of states talking about data security.

MR. MANNE: FTC, too.

MR. MCGEVERAN: So that's a -- and the FTC, that's right. So you can see in that, I think, a model for a process where industry is leading in a

sincere sophisticated way developing some guidance that then government actors can rely on and hold those companies legally accountable for complying with them.

MR. HARTZOG: So I was getting ready to disagree with Geoff and then he went and said the thing that I agree with again. But he knows that we disagree on the general sort of way in which the reasonableness standard has been filled in by the FTC. I'll leave it to Bill to fill that in because I actually second the great article that he wrote on that.

But I would argue and I would agree with the panel that the reasonableness approach is the right approach precisely because it's flexible, precisely because it allows for that sort of variation. And then the point that was just made, which I think is a really important one and one that we should emphasize, which is that -- and it actually goes to your second question, which is how should the FTC go about allocating its resources in terms of complaints and who should we target.

And I think that the answer has to be, at least in part, some of the larger -- some of the actors in the larger sort of data ecosystem that contribute to the vulnerabilities that then lead to

breaches that haven't yet been targeted. And so the FTC, in a few complaints, has started to develop a means in instrumentalities theory about those that create technologies that are then used as a means of data breaches or those that build technologies in an unreasonable way that facilitate data breaches, but not necessarily the data holder or the data collector and it might be a different actor. So I would encourage that sort of allocation of resources.

And another thing to think about is the role of some of the vendors that have indeed popped up that are offering services not just to small companies, but to large companies, monitoring services, these data security companies that employ algorithms in AI to help spot vulnerabilities and flag possible problems.

In my talks with a lot of my computer science colleagues, one of the things that they've noted is that sometimes there are some wild claims getting made by some of these vendors about the efficacy of some of these programs and people naturally rely on some of these wild claims and it turns out that the FTC -- that going after wild faults and misleading claims is right in the FTC's wheelhouse. That would be a way, I think, to expand the FTC's approach to data security without

necessarily going beyond what is already built within Section 5.

MR. TRILLING: I want to see if we can synthesize some of the comments that have been made so far. So several people have expressed support for a reasonableness standard being the right approach for enforcement and Michelle, in particular, mentioned that reasonableness is calibrated to characteristics of the particular business, such as the size and complexity of its data operations, the type of data that it's collecting. How do we synthesize support for reasonableness standard with some of Geoff's criticism about the desire from some stakeholders for the FTC to provide more notice about what's expected?

So for example, even with a closing letter, Lydia highlighted that security knowledge and tools that are available to address vulnerabilities can change in a year, they can change more quickly than that. What should a closing letter look like if that's the solution or what other solutions might there be that might provide more guidance without failing to take into account that what's reasonable for one business at one point in time with the data that it collects may not be a checklist or even be

effective guidance for another business six months later that collects entirely different data sets?

MR. MANNE: It seems to me that it's very clear that to the extent that the FTC talks about the characteristics of the different companies that have factored into its settlements, that for the most part it essentially, correct me if I'm wrong or misremembering, essentially mentions that and then says, taking account of the size and complexity of the business, we feel X. It does not actually explain the thought process. The aspects of its complexity of its business or its size or anything else and how it specifically relates to its feeling that given those things, those actual characteristics, they translate into a feeling that whatever particular security practices were insecure.

What I'm trying to get at is, it is not the identification of particular security practices being unreasonable which indeed can change and, of course, changes from company to company, is the kind of information that people need. It is the way in which the FTC connects those kinds of facts, those kinds of characteristics to what it views as being reasonable security. I would just note -- and, again, I would like someone to do this analysis, but it's totally

possible that this is accurate, that virtually every data security settlement the FTC has entered into has been -- I don't want to say identical, but really, really, really, really similar. And, yet, they've applied to companies of vastly, vastly different characteristics.

So, now, it is possible that indeed the right approach for the FTC to take to every one of those cases is identical, that have a more comprehensive program, a 20-year consent, I mean, all of the elements of the settlements. I don't think that it's -- I don't mean to be totally dismissive to say that can't be the case, but I don't think the FTC has done anything to demonstrate why, indeed, given the vast variety among all of those companies, that what should result -- the appropriate settlements that result from those are virtually identical. I don't think anyone here could tell you why the FTC thinks that that's appropriate.

Again, I don't mean to say that it's not, I mean to say the FTC has never told us why it is. This strikes me as basically the fundamental problem with this reasonableness approach, is that it is not that it's lacking in the specificity of the actions in any given case that are not reasonable, that's actually

often pretty clear from the complaints and the settlements, it's lacking in the reasonable for any company that is not identical to that company to understand how it needs to act, how it needs to proceed in order to make sure it doesn't run afoul of the law.

MR. MCGEVERAN: So this is where the process-based phrase that a number of people on this panel and the previous one have sort of stated comes into play, right. I mean, so --

MR. MANNE: Very much.

MR. MCGEVERAN: -- what is reasonable for one company will be different than what is reasonable for another precisely because the appropriate risk assessment that we would hope each of these organizations will have done for themselves will have identified levels of risk scaled to their resources, scaled to the sensitivity of the data they hold and so forth.

If what reasonableness really ends up being at its core is an expectation of authentic risk assessment, a systemic response to those risks in the form of a compliance approach that's articulated that you can explain to the FTC should they ask you what you were doing to prevent problems. And, you know, I

think a small number of sine qua non architectural requirements, best practices and some worst practices that can be identified pretty clearly from consent decrees, but it's really much more about systems Thank about checklists, of course. And I think that is -- by definition, inherently going to be scalable.

So the thing that you are objecting was identical in different consent decrees was the identical statement that you should go and do what's appropriate for your company. And that, I think, is, by definition, scalable.

MR. MANNE: But that doesn't tell you anything. Do you think the FTC has done that? I mean, I agree with you, but I don't think the FTC has said anything about -- for example, looked at a company's risk assessment and said, hey, you did an effective risk assessment or an ineffective risk assessment and decided that your security was appropriate given that risk assessment because then it would be forced to say something like, we're going to hold you liable because your math is wrong. I think that's what they should actually be doing.

MR. MCGEVERAN: That's one reason I heartily agree with both of you about closing letters, because I think that would be a natural place for that to

emerge.

MS. PARNES: So, right. I mean, it seems as if -- and I agree with the premise that what you're talking about is kind of making a connection between the reasonableness standard which I think in the orders is kind of reflected and you have the process provision, you have to have a comprehensive data security program, making the connection between that and what actually happened with this company. I think that FTC complaints tend not to do that. They are very factual, they are not at all analytical.

Putting my private practice hat on, I think that most companies would object to revealing -- to having the Commission reveal that kind of information. I think it would probably end up kind of being potentially a real roadmap for how kind of bad guys might be able to take advantage of a system. But I do -- so even though I'm not certain how that could happen in an individual case, I do think at like a bit -- take it a bit higher than the individual company. I think that same analysis can be done without talking about the specific facts of this company. And that's where I think there's just kind of huge value in sharing that learning in some kind of -- like in reports.

MR. TRILLING: Woody?

MR. HARTZOG: So I want to push back a little just because -- I mean, I take Geoff's point there is a sort of lack of diversity in the orders that come out, right. So maybe one of them says there should be a comprehensive security program and one of them says there should be a comprehensive privacy program. But they ultimately -- a lot of them end up looking relatively the same. But it's not the orders I think at all that we should be looking at; it is, in fact, the complaints.

I would agree that the complaints need to be -- it would be helpful if they were more factually detailed. But if you're going to go with the reasonableness approach, I think that one of the things that we could all benefit from is more of it, right. So there's more closing letters, which I would also agree with, though I understand the concerns about that. More complaints. And here's where the lack of not just resources, but the lack of finding authority really gets in our way because what it does is it limits the ability of the Federal Trade Commission to really provide a sort of spectrum of wrongdoing because it's really binary, right.

So you file the complaint, you enter in the

identical consent order. Of course the consent orders are going to be the same because we want to encourage some sort of baseline responsible behavior, so it would be sort of weird to say, you know, you could have an okay privacy program, but, you, you have to have a comprehensive privacy program.

MR. MANNE: I think there are a lot more dimensions of this, though, that need to be taken into account, like, for example, the extent to which settlements are resulting, which would only be increased if there was finding authority instead of litigation. Look at, by the way, the Eleventh Circuit's LabMD opinion, which specifically points to the orders and says these are insufficient. I fear the FTC making more specific orders for exactly the reasons we've been talking about, but it's very clear that at least one court thinks that the current approach, which takes basically sort of a vague set of standards like you have a comprehensive security program --

MR. HARTZOG: Right.

MR. MANNE: -- and arguably applies it to very different facts is woefully insufficient, and it's because they don't actually make that connection.

There's just -- one final thing I have to

point out is this multidimensional thing. Why not a higher standard of proof like as is common in all civil cases, a preponderance of the evidence standard instead of a reason to believe standard, both for issuing a complaint and even more importantly for adopting a settlement?

The purpose of which would be both to give some incentive for parties to challenge and actually go to court where actual common law can be made and where we can actually learn something and also for the Commission to understand that it probably has to provide some more information to reach this higher standard lest -- and I think it's important that third parties have a -- like a Tunney Act -- something like a Tunney Act for FTC data security settlements with a preponderance of the evidence standard and an opportunity for third parties to intervene and challenge the FTC's assertion that the settlement is in the public interest and basically -- you know, virtually the language from the Tunney Act.

MR. HARTZOG: Well, yeah, I mean, the more of this we get, the more filled in the standard will then become, right.

MR. MANNE: Right.

MR. HARTZOG: But --

MR. MANNE: Without it, I think you're just doing the same thing you've been doing, which isn't really providing a whole lot of information.

MR. HARTZOG: Well, yeah. I mean, I think that it seems as though some of this is really -- if you want a reasonableness standard than you sort of have to accept the thing that come with a reasonableness standard, which is a lot of inherent ambiguity. Even under optimal circumstances, if I spend the entirety of my torts class talking about reasonableness and we play the game, like how little could we change this factual scenario and switch the liability results.

MR. MANNE: But in torts, in torts and reasonableness you have duty, causation, proximate and actual cause, but I think, in particular, duty and causation are lacking from the FTC's process. So I agree that there is inherent uncertainty in a reasonableness standard and I'm not suggesting that that -- you know, for the same reason that I do think negligence works in a tort context. I don't think that's the inherent problem.

I mean, the problem is that because of the standard of review and because of the absence of judicial review, even though it seems pretty clear to

me that the statute requires demonstration of causation at the very least, and if you're going to adopt a reasonableness approach, I think you have to identify what the duty is that's being breached. I don't think either of those is regularly, if ever done, and -- I'm sure they do it. This is the thing. I'm sure that it's done, right?

MS. PARNES: It's just not public.

MR. MANNE: I'm sure that they have -- the staff issues a memo that outlines all of this.

MS. PARNES: Absolutely.

MR. MANNE: It's just that no one gets to see it except the staff. And I agree with you completely, Lydia, whether that information gets released in specific cases or in some much, much more detailed aggregated form than the -- I agree with you useful, but not doing this -- business guidance, like Start with Security, it has to be released or else we're never going to know how FTC is actually viewing these things that we do get in courts in negligence cases.

MR. TRILLING: So Michelle closely related to these issues about providing a different type of guidance or signaling to industry. Would data security rule-making be more effective than case-by-

case enforcement in protecting consumers and providing guidance to industry?

MS. RICHARDSON: Absolutely. And I think the disagreements you're hearing now about how to resolve these questions of specificity and clarity, the obvious answer is rule-making and getting to APA rule-making, right. And I think that's on the table at this moment. I think there's going to be a serious effort to pass privacy legislation next year and that everyone is talking that there will be a security component of it. Whether that will pass, there's still a lot to be seen in the scope of rule-making. But I think that's exactly what we need at this moment to speed up systemic changes here that we need before it is too late.

I think we feel that this is the only way that we're going to rebalance data interests between everyday users and the companies who are building who are building this system on any reasonable time frame and in a way that actually makes sure that people who are responsible for the systems and able to make informed decisions are actually doing so.

I think we could maybe like a two-year time limit on it or something that would make sure that there would be implementation time, and it would give

the clarity to companies that they're asking for. And, I mean, I am sympathetic because in our work that we have been trying to talk about privacy and data security legislation, you're constantly being whipsawed between that is too vague, and then you write something, well, that is too prescriptive, and you're really just in this Goldilocks of data security where nothing is ever right.

And, hopefully, with the rule-making, though, you can be as detailed and sophisticated and context-oriented as you want there and, you know, raise all boats here for all of us.

MR. TRILLING: Lydia?

MS. PARNES: Yeah. So I don't think that any legislation will be passed. You know, I've lived in Washington too long.

MR. MANNE: Of any sort.

MS. PARNES: The Commission has supported the lowest-hanging fruit, data breach notification legislation, for at least 15 years and nothing has happened. And the debate on the Hill will always be preemption versus no preemption and I do not think there will ever be agreement on that.

But if there was, what would a rule say? I mean, it's -- would a rule say, you know, you have to

have two-factor authentication because if it does, it will be out of date, or will it say you have to have reasonable security and will it kind of track GLB and kind of have -- be process-oriented in a way that I think raises issues under LabMD about enforceability. So I don't see a rule in this particular area kind of addressing the concerns.

I also kind of think that if you are -- it's interesting to me, if you're talking about reasonableness and that's kind of like the violation is you didn't have reasonable procedures in place, it seems unreasonable to me to impose a civil penalty. I mean, you know, if you violate kind of a specific rule, you called five million people who are on the do-not-call registry, that's easy, you know. That is very specific. It is appropriate to impose a civil penalty.

I think all of the FTC's rules really are very clear about what you've done wrong. And the problem that I have in thinking about a security rule-making is that I just don't see how it gets there, to be that specific.

MR. MCGEVERAN: I mean, I've written before about responsive regulation in this space, which is the law from Ian Ayres and John Braithwaite, which

lots of agencies do all the time, whether they call it that name or not. You know, it's like a pyramid and you start at the bottom thinking about the kind of -- things like start with security, things like guidance and business education, and you move up the pyramid towards something like penalties at the top.

And the idea is not that the penalties are used with frequency or carelessly, the idea is that they're, you know, William Douglas, the Supreme Court Justice, was one of the first heads of the SEC and he called his civil penalties the shotgun they I keep behind the door. It's well oiled, but I hope not to use it. And so having some penalties as a component of that, but really focusing on case-by-case adjudication that takes on board some of the criticisms you've made, Geoff, about more specificity in detail, but thinking about it in that cooperative, collaborative, drawing on industry wisdom way, I feel like that is going to be more likely to get us to a place of clarity than a regulation.

MS. RICHARDSON: Well, and -- I probably should have mentioned this the first time, but I think where the clarity comes from is not just the process, but the outcomes. This is what people like about the NIST framework. And, obviously, you can't just say go

follow the NIST framework.

MR. MCGEVERAN: Well, you could, actually. That wouldn't be bad.

MS. RICHARDSON: It's that there's a process, there are outcomes and you have a menu of controls and you have incredible flexibility about how to get there, right, the outcomes. So if you marry those two things, you give both the clarity and guidance of ways to meet the end goal and the flexibility, though, to meet the business model. I mean, I think we also need to just accept that giving ourselves the task of writing a technology law that will apply perfectly to every scenario, every outlying case forever and ever amen without amendment is an impossible task. It is not fair to put it on the FTC in this critical moment because that is not how we judge any other area of law.

MR. HARTZOG: So just to jump in, I want to agree with Bill here and I do think that rule-making authority would be useful and I do actually think that it would end up being a reasonableness statute. I think that all of the evidence that we've seen shows us that that's exactly where we would end up and I think that that's largely okay. I think that it would be a really bad idea to really start getting pretty

specific about things in high detail.

The virtue of reasonableness is that it can be responsive to this large thing. And, ultimately, if that's what we're going to do, I think that the point of reasonableness is not necessarily to convey entirely the specific standard, but one of the sort of virtues or costs of a reasonableness test is who gets saddled with the uncertainty of compliance.

MR. MANNE: Yeah, I want to point out that because -- even though I think that the current approach to case-by-case enforcement is seriously problematic and lacking, that doesn't mean that a rule-making approach is necessarily better. I think we can't forget that the statute that the FTC is enforcing is an unfairness statute, right. I just want to read a couple of sentences from the unfairness statement. This is the FTC actually doing a really fantastic job explaining why a sort of straight rule-making approach is really problematic here.

So the present understanding of the unfairness standard is the result of an evolutionary process. By the way, this is also why the common law of data security is problematic because it's also not an evolutionary process.

The statute was deliberately framed in

general terms since Congress recognized the impossibility of drafting a complete list of unfair trade practices that would not quickly become outdated or leave loopholes for easy evasion. That task was assigned to Congress, subject to judicial review -- also not happening -- in the expectation that the underlying criteria would evolve and develop over time. As the Supreme Court observed, the ban on unfairness "belongs to that class of phrases which do not admit a precise definition, but the meaning and application of which must be arrived at by what this Court elsewhere has called 'the gradual process of judicial inclusion and exclusion.'"

I don't think they're wrong about that. It's not to say rule-making is inherently inconsistent by any stretch, and I think there are certain aspects of rule-making, certain things that the FTC could do by rule-making that could be helpful here. I don't think those have clearly been identified. But trying to implement data security standards at large by rule-making, I think, under the authority granted by a statute that requires it to ensure that conduct is fair, is inherently inconsistent with the statute.

I do also think, though, it's inconsistent with the current sort of approach as that very

statement from the FTC makes clear the judicial review component is essential to the way Congress arguably envisioned Section 5 -- standards under Section 5 playing out. At least in the data security space, we, to date, have had two cases -- a grand total of two cases that have actually gone before a court at all. And by the way, both of them basically slammed the agency for not really defining what it think it's enforcing sufficiently, in very different ways and, you know, with some caveats and all that. But you could hardly call either of them a big win for the FTC.

MR. MCGEVERAN: Wyndham?

MR. MANNE: Yeah.

MR. MCGEVERAN: I call Wyndham a big win for the --

MR. MANNE: Not with respect to precisely this.

MR. HARTZOG: But it is subject to judicial review, in that we have seen it, right. It's played out, which is why -- I mean, we could have more of it which I think we actually would agree on.

MR. MANNE: So that's the thing. So, again, I guess my point is to say, probably at the margin between rule-making and case-by-case enforcement,

given the statute, it makes sense to adopt a case-by-case enforcement approach, by the way, with all of the other stuff that we talked about for a while here. But the current case-by-case approach strikes me as being just crazily inefficient, especially in this area, in this data security area, at pinpointing where the real problems are and actually getting the right companies to correct them.

But I agree that those are even different process problems than the process problem we've been talking about. This is things like -- now, maybe it requires Congress, right, having a different standard of proof, you know, publishing information on when they're -- from closing letters. I mean, we could go on. There's a lot of things that one could do that I think would both make it more likely that cases come before a judiciary, and even when they didn't, would provide a lot more of judicial-like information, and that's what's missing.

But that doesn't mean because that's missing, we should have a rule-making that essentially codifies either some very specific thing that shouldn't be codified or basically what we have now codified doesn't --

MS. VANDRUFF: Well, Geoff, Lydia has

handicapped whether or not Congress is going to act and we're not going to take any bets on that --

MR. MANNE: I know.

MS. VANDRUFF: -- because that would be inappropriate here in a federal, you know, event. But, nonetheless, incorporated in many of the comments submitted in the NTIA proceeding was the suggestion that the agency be provided with civil penalty authority. Woody mentioned that our lack of civil penalty authority prevents the agency from identifying where on a spectrum an individual case lands. So, I'd invite the panel -- and let's start with Michelle -- to comment on whether civil penalty authority would -- well, whether Congress should provide the Federal Trade Commission with civil penalty authority with respect to data security enforcement.

MS. RICHARDSON: Absolutely. And I think that is something that there is more agreement around. It seems actually less controversial among decision-makers. It would definitely speed up compliance issues and encourage entities that are holding this data to take the issues more seriously. This is a very strange one-bite-of-the-apple rule that doesn't really exist in other areas of the law and especially considering all of the other constraints, right, if

we're not passing a statute to rebalance the three-part test or give rule-making that front-end ability to fine is more important. Because that is really going to be one of the biggest motivators you are going to have.

MS. PARNES: Are we going down the line here?

MS. VANDRUFF: Anyone who would like to jump in.

MS. PARNES: Okay. So I actually think the one-bite-at-the-apple rule makes a certain amount of sense here because there was the first case that the FTC brought where it applied unfairness in a data security case. Prior to that, it had always relied on some statement that a company made that we have great security in place. This was new. It was -- and I think that this is what the Commission does kind of throughout in all areas. So I do think that it makes a certain amount of sense in this area, as well, because each case, you know, the Commission builds on previous work and will be looking at issues -- at security issues that were never called out before.

There will always be kind of that case where this was never considered a problem and now it is. Now, the failure to do X is not reasonable because of

additional learning. So I'm not certain that a civil penalty is appropriate there.

MR. HARTZOG: I would advocate for civil penalties for the reason I said before in that it allows a little more sort of gradation in terms of assessing just how bad a data breach is, for example, and then we can sort of look back at it. And I think it's also key simply for an incentives purpose, right.

So one of the things that I always find myself sort of explaining when I travel internationally is everyone says, oh, the FTC just gives people a slap on the wrist. If you Google any particular FTC complaint, odds are one of the news complaints will describe it as a slap on the wrist. Now, I don't know if it is. As a matter of fact, I think in many cases it's not, but that's how it's perceived. And how the U.S. system of privacy is perceived matters.

The U.S./EU privacy shield is in jeopardy, and if it falls, we better have a good plan to replace it. And so I think that civil penalty authority is important not just for its own sake, but also to provide incentives.

MR. MANNE: So if you're doing rule-making or regulation by case-by-case enforcement, that point

you just made doesn't really matter. The issue is not whether there's a punishment that is, you know, sort of sufficient to deter -- I mean, although that is obviously important, but one of your arguments that I, of course, have taken issue with being that this common law data security has evolved to elucidate a standard that doesn't require penalizing. And if people think that that is, you know, a slap on the wrist, they're actually not really understanding the way the FTC works. It's not that the fines are -- that there isn't enough punishment.

But that said, my biggest problem -- I'm not inherently opposed to fines, but I think that all of the discussion of fines, again, is sort of putting the cart before the horse. That before we give the FTC fining authority, that we have to address these process problems that it has because, otherwise, this is just exacerbating. What I would argue is insufficient notice and insufficient ability for companies to determine what reasonableness requires of them and insufficient evidentiary standard. So if nothing else, if we're going to impose fining ability, can we agree that a slightly higher evidentiary standard is required, maybe even by the Constitution, that approaches that of civil cases rather than a

reason to belief standard? Just tossing that out there.

But, also, my sort of potential objection to fining comes down to the fact, again, that we have too many settlements and not enough cases being reviewed by the courts, and imposition or the threat of imposition of fines virtually ensures -- potentially, I think, increases the likelihood of settlement. Now, it doesn't have to, and I think there would be some exceptions to that. But I -- you know, my back-of-the-envelope sort of logical calculation here is that that will increase settlements, not increase the rate at -- the FTC will calibrate their fines to ensure that everybody settles, that they're never too high, that companies feel compelled to actually challenge them in court. And that doesn't strike me as a good thing.

So, again, my point is to say I can see the logic of the finding, but I think you have to think of the institutional environment in which it's being implemented. And until that environment looks like you want it to look, I would be really, really cautious about bringing fines into the mix.

MR. TRILLING: Okay. So we are approaching the end time for the panel. We have time for maybe a

few more questions. I want to pivot a little bit to talking more in depth about FTC data security orders with a very general question of how effective are the FTC's current data security controls?

MR. MANNE: Does anybody have any idea? I actually think this is one of the problems.

MS. PARNES: Well, you know, I represent some companies who are under these orders and I think looking at it from the perspective of, you know, kind of those companies, yeah, I think those orders are absolutely achieving the objective that the Commission is trying to. I mean, companies that are under order spend enormous resources ensuring that they are in compliance with these orders. You know, my experience is that the biennial risk assessments are not something that, oh, we'll worry about that in, you know, kind of two years or 18 months or next year; this is just an ongoing kind of living process at a company. They are very aware, and, typically, their assessors kind of are onsite on a pretty regular basis throughout the two-year period.

So I think that the orders achieve one goal, which is making sure that companies are focused on data security. Again, I don't think they can stop data breaches, but that's kind of a different issue.

And I think, you know, Geoff, to your point, I'm talking about kind of specific deterrence. I don't know about general deterrence. I really don't have a sense of whether these orders, you know, kind of have an impact more generally on the industry, although I will say companies are certainly aware.

MR. MANNE: So some are.

MS. PARNES: Yeah.

MR. MANNE: So the ones that know enough to come to you are certainly aware. But I would guess that you and people like you, that that's actually a small minority of companies.

MS. PARNES: Yeah.

MR. MANNE: And from the perspective of the sort of seeming a goal -- so the very specific deterrence -- and, again, like in these specific cases, it's valuable especially when you're talking about big cases -- sorry, big companies with risky data and all of that, not so much when you're talking about Tower Records.

But, remember, you know, I think it's clear that it's a regulatory agency that is regulating by case-by-case enforcement instead of rule-making. So the question then is whether it's effectively actually regulating through the enforcement actions. And the

first answer to that has to be we don't know, which I think is a problem because I think some effort to try to figure that out would be useful.

But I also think that part of the answer is probably not, you know, for some of the reasons that we've been talking about, and I think that that's a problem and I doubt that the trade-off is worth it for the benefit of the specific deterrence in the specific cases just because they're so few and far between and not necessarily keyed to the most risky situations.

MS. VANDRUFF: Well, let me ask, though, how would we measure general deterrence?

MR. MANNE: That's hard, yeah. I don't know.

MS. VANDRUFF: Because I don't know that it follows necessarily the fact that we don't know the answer means that the answer is no.

MR. MCGEVERAN: Right, right. I mean, one source of evidence would be the kind of study that like Ken Bamberger and Deirdre Mulligan have done, where they did a very careful -- well, the book comparative actually, European to the U.S., and the U.S. came out looking pretty good -- hats off to the Federal Trade Commission and others. In terms of inculcating a consciousness of the importance of

process in companies, not just the ones who are under the orders, but also the ones who fear that they could be next, I mean, you know, that's not a quantitative study. That's interviews that they did with a broad spectrum of privacy officials and companies.

But the culture that the -- and that's privacy rather than specifically a security study. But the idea that a responsive case-by-case adjudication system of regulation can create cultures of compliance in corporations, I think there is evidence to support it, although I agree we need more.

MR. MANNE: Just really quickly, I think, for example, in your paper, you -- I can't remember if you say that the FTC seems to have contributed to an increase in the adoption of industry standards and sort of self-regulatory bodies. And I think it's fair to say there's a correlation just because the FTC has existed and those things have arisen.

MR. MCGEVERAN: Sure, many of them.

MR. MANNE: But we have no way of knowing that there's actually a causal relationship. But that would be actually something that you probably could figure out because it would be a very constrained group that you'd have to sort of interview and it would be really great to know. And if it really were

happening that way, I think it would count as a huge win for the FTC.

I just don't think we know -- that we actually know that that's happening and we can't assume it just because those exist.

MR. MCGEVERAN: I think we're agreeing.

MR. HARTZOG: Yeah, and I would just add -- I mean, if the question is are they effective -- are the orders effective in preventing data breaches, then the answer is obviously of course not.

MR. MANNE: Of course not.

MR. HARTZOG: Right. I mean, but that's not the -- I don't know if that's the metric by which you do. Here, again, I would draw from Bill's work. When do you have an order over an incredibly large platform that has a massive amount of data, so one of the big five, one of the major tech companies, then what that does then is it does encourage a much closer relationship between industry and the regulator, which I think is positive. So in that effect, I would say, yes, it's good.

And then the second thing that I would say that the orders seem to do well is that they are, in fact, a place to test out or at least start to evolve. So I'll actually push back and say that we do get some

sort of evolution, maybe not in the way in which you talk about, but some sort of evolution. Privacy by design first started showing up in the United States in these consent orders, right, in these comprehensive privacy programs in response to lots of these complaints. So there are ways in which we can really start to have these evolving conversations. So I think, at least by those two measures, they would be seen as effective.

MR. MANNE: It seems to me, by the way, that you're right that we sort of tongue in cheek are saying, you know, has there been more data security, you know, no, clearly no, ha, ha, ha. Obviously, that is, in fact, what we should be aiming at. And I think it goes back to the point I think Michelle initially raised about who the FTC is looking at and sort of how it thinks about its role in this. I mean, if the goal is, in fact, to reduce the rate or the damage of or the incidents of data breaches, targeting very specific company is probably really, as I said, an inefficient way of doing it.

But looking at the companies that are actually responsible for the infrastructure and considering that -- like right now we all say you can't stop data breaches, and that's probably always

going to be true, but it could be minimized. But minimizing it in any real significant way I think requires rethinking the security infrastructure that we rely on. And I don't think anything the FTC is doing is ever going to help with that.

And maybe that's not it's job and, you know, we can talk about. But if you really wanted to effect some change here, I think you would be looking at the software designers, the database designers, the security experts who are the ones who are -- and for that matter, even more complicated infrastructure like the underlying infrastructure of the internet. Those are the people who are ultimately responsible for the problem that we're in and they're the ones who could be incentivized to fix it. I'm not saying that means they should be targeted or something, but that's where we should be looking.

MR. HARTZOG: I mean, I would agree with you, but I would disagree that the FTC, broadly speaking, can't do anything about that.

MR. MANNE: It could, it could. I don't think in its current process it is doing anything about that. But I agree. That's why I said before, you know, having the conversation, right, convening those people, talking how industry standards might

evolve to incorporate security practices at an infrastructure level, to the extent there are choices incentivizing firms to adopt security experts and their processes that are actually more effective than others, those are --

MR. HARTZOG: Well, there you go agreeing with Woody again.

MS. PARNES: I think they should --

MR. HARTZOG: Now you're agreeing with Woody again. That's Woody's book, pretty much.

MS. PARNES: So I --

MR. MANNE: I think they can do that. I just don't think the enforcement actions are doing that.

MS. PARNES: I think the Commission could also make decisions about, from a process perspective, what it thinks are really good practices and, you know, kind of adopt presumptions and say if you do that, we are going to presume that you've got good security in place.

MR. MANNE: And I think that would actually -- I agree.

MS. PARNES: That, I think, would have a huge impact.

MR. MCGEVERAN: And that's a closing letter

a company might be perfectly happy for that to come out in public, right?

MS. PARNES: Right.

MR. MCGEVERAN: About what a good job they've done.

MS. PARNES: Right.

MS. VANDRUFF: I don't want to cut this discussion short, but our time is up. I want to thank the panelists for joining us today.

It is my pleasure to introduce the Associate Director of the Division of Privacy and Identity Protection, Maneesha Mithal, who is going to offer some closing remarks before we conclude for these two days.

CLOSING REMARKS

MS. MITHAL: Thanks to this terrific panel and thank all of you for sticking it out until the end. It was a pleasure to have all of you here. I think the panels over the last two days have been extremely substantive and informative, and I think we have several people to thank for that.

So I want to thank from the Division of Privacy and Identity Protection, Elisa Jillson, Jared Ho, Jim Trilling, who are the staff attorneys who have been putting this together, along with Mark Luppino from the Bureau of Economics and Michael LeGower, also from the Bureau of Economics, and several folks from the Office of Policy Planning. I want to thank Laura VanDruff, who's been the manager on this team, and also the event staff and the press office and everybody else who's had a hand in putting this together. So thank you, everybody. So if we could give them all a big hand.

(Applause.)

MS. MITHAL: Okay. So I've been kind of taking notes as this conference has gone on and I'd just like to kind of point out three main takeaways that I've kind of observed from the last two days. Just kind of some thoughts on some of the things the

panelists have raised in the context of these three takeaways.

So the first is that we need more empirical data about data breaches, the threat environment, and the harms to consumers. Now, we got some information yesterday morning about threat vectors. We heard from Verizon on their data breach report. We heard about various types of harms that consumers suffer when they have been victimized by identity theft. But I've been struck by the fact that on many of the panels following that and today's panels, as well, companies talked about the need for more data on certain aspects.

So, for example, one panelist talked in the panel about investments in cybersecurity, talked about there are three aspects for determining how to make decisions on cyber investment, what is the value of the information, what is the probability of a breach and what is the productivity of the investment that might avoid that breach. I think as companies are considering optimal investments in data security, it would be great to be able to have more information on that.

I think in this panel we just heard about how we're measuring general deterrence. Again,

further academic research, economic research on these issues I think would be very welcome. So I think that's the first takeaway.

The second takeaway is that there's multiple sources of incentives for companies to invest in data security. We heard about a number of these incentives yesterday, the company's reputation, the competitive disadvantage or competitive advantage that could be created by better security, cost of cyber insurance could be decreased by having better security, the liability regime influences incentives on data security. We also talked a little bit about what drives investment. What are the sources that drive investment in data security?

We talked about the culture of security within the firm and the ability of the CISO to effectuate change within an organization. We talked about customers as a potential driver of data security. We talked about cyber insurance and we talked about legal incentives. At the same time, I think we heard today that, you know, although many companies are influenced by loss of reputation, consumer trust and other things, we've heard situations where some CISOs have had challenges in getting companies to invest in data security where

they say, well, if you're going to ask me to invest $1 million and a breach is only going to cost me $500,000, why should I invest the $1 million? And I think that that was an interesting question raised this morning.

And then, finally, in terms of takeaways, we talked a lot about solutions today and I think this probably goes without saying, but I think we all talked about the fact that a one-size-fits-all solution won't necessarily work.

Now, I think there was some consensus around the idea that companies should implement a process-based approach. We heard that numerous times over the last two days, a process-based approach as opposed to an outcomes-based approach. We heard the adage that security is a journey and not an end point. We also heard that the right way to do a process-based approach is not to talk about how many bodies you're throwing at data security, but to talk about how companies are doing risk assessments, where is the data, what data is it, what risks would arise for consumers in the corporation if the data was compromised. So, again, we heard the term "risk-based approach" a lot.

But in addition to a process-based approach

to avoiding data breaches, we also heard about other approaches. We heard about the idea of devaluing assets for the identity thieves and other criminals that get this information. A representative from the payment card industry talked about tokenization and the idea that if you use tokenization you'll reduce the value of credit card numbers to identity thieves. We talked about the fact in the old days that SSNs were used as authenticators and reducing reliance on SSNs can help avoid some of the harms that arise from data breaches.

Another solution that people talked about was accountability, the need for data security to be a risk management approach where you have the CFO, the CISO, the risk management team and others directly reporting to the board on accountability issues. We heard a lot about FTC enforcement. I think there was some consensus that there is some role for FTC enforcement, although there may have been some differences in how the FTC should conduct its enforcement activities. But I think there also seemed to be a lot of consensus around the need for FTC business guidance, along the lines of start with security and stick with security and some of the other projects.

So to that end, I have some slides that I just wanted to point people's attention to some of the information that we already do have out there. So I think Start with Security, we've talked about a lot. I just wanted to show people that this is what it is. It has kind of ten lessons to be learned from our data security cases. We have data security education on specific topics. This one is a specific IOT. I know Lydia talked about the idea of doing more reports on data security and I think this might be one model for that where we talk about specifically data security involving IOT.

We have a data breach response guide and cybersecurity for small businesses which really focuses on businesses that don't have IT departments or legal departments and are trying to do it all themselves. So that's kind of the broader review of some of the stuff we've done. I think that has been referred to throughout these last two days. So I wanted to point that out.

So with that, again I want to thank everybody for their attendance. The comment period will remain open until March 13th. So we appreciate any additional comments that people might have and thank you again. And if you could all join me once

again in giving all the panelists and participants a big hand.

(Applause.)

MS. MITHAL: And thank you very much.

(Applause.)

(Hearing concluded at 4:22 p.m.)

CERTIFICATE OF REPORTER

I, Linda Metcalf, do hereby certify that the foregoing proceedings were digitally recorded by me and reduced to typewriting under my supervision; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were transcribed; that I am not a relative or employee of any attorney or counsel employed by the parties hereto, not financially or otherwise interested in the outcome in the action.

s/Linda Metcalf
LINDA METCALF, CER
Court Reporter