

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

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.

1	FEDERAL TRADE COMMISSION	
2	I N D E X	
3		PAGE :
4	Welcome and Introductory Remarks	3
5		
6	Panel 1: Data Security Assessments	6
7		
8	Panel 2: Fireside Chat on Emerging Threats	82
9		
10	Panel 3: The U.S. Approach to Consumer Data	111
11	Security	
12		
13	Panel 4: FTC Data Security Enforcement	179
14		
15	Closing Remarks by Maneesha Mithal	244
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		

1 P R O C E E D I N G S

2 WELCOME AND INTRODUCTORY REMARKS

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

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

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

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

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

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

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

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

22 Restrooms are located in the hallway outside
23 of the auditorium.

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

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

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 PANEL 1: DATA SECURITY ASSESSMENTS

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

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

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

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

1 are going to go straight into the first hypo.

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

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

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

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

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

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

22 MR. TRILLING: Thank you.

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

1 MS. HOLCOMB: Yeah, sure. There are a
2 number of published standards to use, and I think it
3 is critical that a standard be used, both internally
4 and externally. So, for example, in this hypo number
5 1, the CISO would want to use something like an ISO
6 framework or maybe the NIST cybersecurity. You could
7 use the Carnegie Mellon Maturity Model. Those would
8 all be very useful in determining how do our risks
9 look, how mature is our security organization. Those
10 can be used, like I said, internally. They can also
11 be used by an outside assessor to understand how
12 strong the security is.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 it's basically cyber hygiene.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 lines talking about security as well as other risks.

2 So I'll stop there.

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

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

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

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

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

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

25 The Ponemon Institute put out a study now

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

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

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

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

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

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

14 MR. PACE: Let me start with the second
15 question because I think it will impact the first.
16 The information requirements for cyber insurance, 15,
17 20 years ago when cyber insurance was first offered,
18 they were actually probably the highest they've ever
19 been. Insurance is a market, and we saw the
20 information requirements necessary to be offered cyber
21 insurance actually fall.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 to Company C's ability to obtain cyber insurance?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

25 So on one hand, that can be really helpful,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

17 Tom, I don't know --

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

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

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

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

1 continues to go.

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

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

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

1 business overall.

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

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

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

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

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

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

1 includes automated tools.

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

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

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

24 (Laughter.)

25 MS. NATHER: But part of it is literally

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

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

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

17 MS. HOLCOMB: I would agree with --

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

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

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

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

15 MS. JILLSON: It's a cheeseburger.

16 MR. HARKINS: Cheeseburger, yes.

17 (Laughter.)

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

20 MR. HARKINS: Yes, exactly.

21 (Laughter.)

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

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

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

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

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

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

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

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

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

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

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

12 MS. HOLCOMB: Absolutely.

13 MR. HARKINS: Absolutely.

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

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

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

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

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

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

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

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

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

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

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

3 So let's say it would cost you a million a
4 year to have a security program and you don't get
5 breached until your second year, and it only costs you
6 \$500,000, you came out ahead. So from a purely
7 financial standpoint, it doesn't always make sense for
8 a company to go all out in addressing its security
9 risks if that incurs substantial financial risk.

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

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

1 larger ones, for that matter.

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

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

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

1 the security organization looking at priorities.

2 So this is going to be a matter of priority.

3 Yes, the assessor or the internal system, or anybody,
4 should come up with all of the problems. So whether
5 it's the heartbeat or the lungs or whatever it is, you
6 know, have the full list, but then you have to
7 prioritize them, and you want to have the right people
8 prioritizing and then looking at the cost benefit of
9 each one.

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

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

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

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

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

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

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

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

1 encryption.

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

13 I think to the earlier point on the
14 lifestyle that Wendy talked about -- I mean, I'm
15 starting to get really hungry for lunch all of a
16 sudden, I don't know why. But so many times we talk
17 about, well, PCI compliance is not enough, and we have
18 to make sure that we understand the PCI practices
19 versus the compliance to a one-point-in-time
20 attestation. So within the standard itself, it's over
21 200 requirements that are business continuity
22 practices for good security process, and being able to
23 make sure that those security practices continue to be
24 in the environment.

25 The attestation that comes from having an

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

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

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

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

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

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

25 So a critical part in scope is to make sure

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

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

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

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

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

1 risks are.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

19 MR. MCANDREW: Fourteen years in a row.

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

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

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

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

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

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

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

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

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

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

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

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

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

1 items to make sure that you continue to manage it.

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

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

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

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

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

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

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

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

21 (Applause.)

22 (Brief recess.)

23

24

25

1 FIRESIDE CHAT ON EMERGING THREATS

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

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

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

23 COMMISSIONER SLAUGHTER: Thanks. Thank you
24 so much.

25 MR. CORMAN: We have a fire.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3 MR. CORMAN: It fluctuates. DEF CON turned
4 25 last summer, not this past one, but prior. We
5 brought two sitting Congressmen, Will Hurd of Texas
6 and Jim Langevin of Rhode Island, to DEF CON on stage,
7 and the reception was quite good, and yet, there was
8 still a backlash because of the arrest of Marcus on
9 some of the past hacking things. So it's an ebb and
10 flow of trust and distrust. The hacker community is
11 not inherently a fan of government. They think
12 government can only make things worse. And as such,
13 the Calvary gets criticism quite a bit for engaging
14 and reaching into these areas.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 unsafe, in no world should that be okay.

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

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

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

23 The problem with this is the seller of that
24 \$100 camera is not incentivized to make it safer. The
25 buyer of that camera is not incentivized to make it

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

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

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

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

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

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

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

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

1 yet internalized the costs in doing so.

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

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

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

1 cost the same as one that doesn't.

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

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

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

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

25 MR. CORMAN: They were trying to attack

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

3 COMMISSIONER SLAUGHTER: Because of the
4 internet?

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

9 COMMISSIONER SLAUGHTER: Mm-hmm.

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

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

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

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

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

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

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

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

1 That's the private sector optimum.

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

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

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

1 moving.

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

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

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

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

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

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

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

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

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

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

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

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

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

1 lack the political will to do that.

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

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

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

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

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

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

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

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

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

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

1 undermine someone's ability to defend themselves at
2 all.

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

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

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

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

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

20 COMMISSIONER SLAUGHTER: Mm-hmm.

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

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

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

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

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

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

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

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

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

4 MR. CORMAN: Thank you.

5 (Applause.)

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

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

14 (Lunch break.)

15

16

17

18

19

20

21

22

23

24

25

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

2 MR. TRILLING: Good afternoon, everyone.

3 Welcome back from lunch.

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

7 MR. COOPER: Thanks, Jim.

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

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

1 Perkins Coie.

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

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

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

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

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

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

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

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

25 So we have evolved over the last 20 years

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

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

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

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

8 So we have the federal approach, the state
9 approach, and then very important are industry
10 standards. In some ways, industry standards, for some
11 companies at least, form the backbone of their
12 security program and are much more important really
13 for them than legal requirements. For example, the
14 Payment Card Industry Data Security Standard with its
15 12 requirements, that forms a basis for the security
16 program for merchants and many others who deal in the
17 payment card space.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 back to you, Lisa, maybe.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4 MR. COOPER: Daniel?

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

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

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

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

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

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

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

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

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

1 legal protections need to look like.

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

4 MR. COOPER: Yeah, sure.

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

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

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

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

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

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

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

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

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

21 Business practice, throughout the latter
22 part of the 20th Century and into the beginning of the
23 21st Century, transformed these numbers which are, to
24 some extent, contained in publishable directories into
25 authentication credentials. That's dangerous.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 jump in?

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

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

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

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

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

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

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

1 harm was front and center there.

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

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

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

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

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

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

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

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

25 You know, insecure devices, they don't just

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 if you recognize risk of future harm.

2 Beyond that, too, I'm not so sure a lot of
3 the lawsuits are, you know, addressing the full nature
4 of the harm. I do think you need agency action to do
5 this and to really help people. I mean, there are
6 ways that you can tackle this, like create a fund so
7 if people are harmed they can get money from a fund
8 that companies that have a breach put into, and so on
9 and so forth. So there are ways around this problem.
10 But, yeah, I don't think you just completely get rid
11 of any statute of limitations and then let people sue
12 30 years down the road.

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

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

1 day.

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

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

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

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

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

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

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

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

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

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

9 MR. COOPER: Of course not the panel.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 yeah.

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

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

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

25 Also, there is no perfect security.

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

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

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

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

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

21 MR. COOPER: Janis?

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

1 wouldn't have thought that.

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

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

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

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

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

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

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

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

7 MR. COOPER: Okay, thanks, Janis.

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

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

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

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

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

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

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

24 MR. CALABRESE: Yeah.

25 MR. COOPER: With respect to your fines,

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

4 MR. CALABRESE: Both.

5 MR. COOPER: Okay.

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

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

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

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

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

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

1 violation, et cetera.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

25 So I think we have to think outside the box

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

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

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

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

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

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

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

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

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

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

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

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

1 would you have a more risk-based approach.

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

11 MR. COOPER: Okay, thanks.

12 Chris, I guess you get the last word.

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

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

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

22 (Applause.)

23

24

25

1 PANEL 3: FTC DATA SECURITY ENFORCEMENT

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

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

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

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

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

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

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

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

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

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

1 security practices in place.

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

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

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

1 notice. Is that a fair criticism?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

16 (Laughter.)

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

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

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

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

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

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

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

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

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

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

6 MS. PARNES: Really?

7 MR. MANNE: Say no, say no.

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

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

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

1 MS. PARNES: Yes.

2 MS. VANDRUFF: Okay.

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

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

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

1 incredibly useful to the industry.

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

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

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

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

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

12 MR. TRILLING: Geoff?

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

25 But I think it's impossible to conceive of

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

13 MS. VANDRUFF: Okay.

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

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

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

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

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

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

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

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

22 MR. HARTZOG: Worse practices.

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

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

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

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

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

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

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

1 agency put out that business education.

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

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

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

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

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

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

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

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

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

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

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

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

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

22 MR. MANNE: FTC, too.

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

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

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

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

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

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

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

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

1 necessarily going beyond what is already built within
2 Section 5.

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

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

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

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

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

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

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

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

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

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

11 MR. MANNE: Very much.

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

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

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

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

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

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

1 emerge.

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

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

1 MR. TRILLING: Woody?

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

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

25 So you file the complaint, you enter in the

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

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

21 MR. HARTZOG: Right.

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

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

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

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

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

24 MR. MANNE: Right.

25 MR. HARTZOG: But --

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

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

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

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

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

8 MS. PARNES: It's just not public.

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

11 MS. PARNES: Absolutely.

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

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

1 case enforcement in protecting consumers and providing
2 guidance to industry?

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

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

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

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

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

13 MR. TRILLING: Lydia?

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

17 MR. MANNE: Of any sort.

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

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

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

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

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

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

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

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

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

1 follow the NIST framework.

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

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

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

1 specific about things in high detail.

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

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

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

25 The statute was deliberately framed in

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

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

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

1 statement from the FTC makes clear the judicial review
2 component is essential to the way Congress arguably
3 envisioned Section 5 -- standards under Section 5
4 playing out. At least in the data security space, we,
5 to date, have had two cases -- a grand total of two
6 cases that have actually gone before a court at all.
7 And by the way, both of them basically slammed the
8 agency for not really defining what it think it's
9 enforcing sufficiently, in very different ways and,
10 you know, with some caveats and all that. But you
11 could hardly call either of them a big win for the
12 FTC.

13 MR. MCGEVERAN: Wyndham?

14 MR. MANNE: Yeah.

15 MR. MCGEVERAN: I call Wyndham a big win for
16 the --

17 MR. MANNE: Not with respect to precisely
18 this.

19 MR. HARTZOG: But it is subject to judicial
20 review, in that we have seen it, right. It's played
21 out, which is why -- I mean, we could have more of it
22 which I think we actually would agree on.

23 MR. MANNE: So that's the thing. So, again,
24 I guess my point is to say, probably at the margin
25 between rule-making and case-by-case enforcement,

1 given the statute, it makes sense to adopt a
2 case-by-case enforcement approach, by the way, with
3 all of the other stuff that we talked about for a
4 while here. But the current case-by-case approach
5 strikes me as being just crazily inefficient,
6 especially in this area, in this data security area,
7 at pinpointing where the real problems are and
8 actually getting the right companies to correct them.

9 But I agree that those are even different
10 process problems than the process problem we've been
11 talking about. This is things like -- now, maybe it
12 requires Congress, right, having a different standard
13 of proof, you know, publishing information on when
14 they're -- from closing letters. I mean, we could go
15 on. There's a lot of things that one could do that I
16 think would both make it more likely that cases come
17 before a judiciary, and even when they didn't, would
18 provide a lot more of judicial-like information, and
19 that's what's missing.

20 But that doesn't mean because that's
21 missing, we should have a rule-making that essentially
22 codifies either some very specific thing that
23 shouldn't be codified or basically what we have now
24 codified doesn't --

25 MS. VANDRUFF: Well, Geoff, Lydia has

1 handicapped whether or not Congress is going to act
2 and we're not going to take any bets on that --

3 MR. MANNE: I know.

4 MS. VANDRUFF: -- because that would be
5 inappropriate here in a federal, you know, event.
6 But, nonetheless, incorporated in many of the comments
7 submitted in the NTIA proceeding was the suggestion
8 that the agency be provided with civil penalty
9 authority. Woody mentioned that our lack of civil
10 penalty authority prevents the agency from identifying
11 where on a spectrum an individual case lands. So, I'd
12 invite the panel -- and let's start with Michelle --
13 to comment on whether civil penalty authority would --
14 well, whether Congress should provide the Federal
15 Trade Commission with civil penalty authority with
16 respect to data security enforcement.

17 MS. RICHARDSON: Absolutely. And I think
18 that is something that there is more agreement around.
19 It seems actually less controversial among decision-
20 makers. It would definitely speed up compliance
21 issues and encourage entities that are holding this
22 data to take the issues more seriously. This is a
23 very strange one-bite-of-the-apple rule that doesn't
24 really exist in other areas of the law and especially
25 considering all of the other constraints, right, if

1 we're not passing a statute to rebalance the
2 three-part test or give rule-making that front-end
3 ability to fine is more important. Because that is
4 really going to be one of the biggest motivators you
5 are going to have.

6 MS. PARNES: Are we going down the line
7 here?

8 MS. VANDRUFF: Anyone who would like to jump
9 in.

10 MS. PARNES: Okay. So I actually think the
11 one-bite-at-the-apple rule makes a certain amount of
12 sense here because there was the first case that the
13 FTC brought where it applied unfairness in a data
14 security case. Prior to that, it had always relied on
15 some statement that a company made that we have great
16 security in place. This was new. It was -- and I
17 think that this is what the Commission does kind of
18 throughout in all areas. So I do think that it makes
19 a certain amount of sense in this area, as well,
20 because each case, you know, the Commission builds on
21 previous work and will be looking at issues -- at
22 security issues that were never called out before.

23 There will always be kind of that case where
24 this was never considered a problem and now it is.
25 Now, the failure to do X is not reasonable because of

1 additional learning. So I'm not certain that a civil
2 penalty is appropriate there.

3 MR. HARTZOG: I would advocate for civil
4 penalties for the reason I said before in that it
5 allows a little more sort of gradation in terms of
6 assessing just how bad a data breach is, for example,
7 and then we can sort of look back at it. And I think
8 it's also key simply for an incentives purpose, right.

9 So one of the things that I always find
10 myself sort of explaining when I travel
11 internationally is everyone says, oh, the FTC just
12 gives people a slap on the wrist. If you Google any
13 particular FTC complaint, odds are one of the news
14 complaints will describe it as a slap on the wrist.
15 Now, I don't know if it is. As a matter of fact, I
16 think in many cases it's not, but that's how it's
17 perceived. And how the U.S. system of privacy is
18 perceived matters.

19 The U.S./EU privacy shield is in jeopardy,
20 and if it falls, we better have a good plan to replace
21 it. And so I think that civil penalty authority is
22 important not just for its own sake, but also to
23 provide incentives.

24 MR. MANNE: So if you're doing rule-making
25 or regulation by case-by-case enforcement, that point

1 you just made doesn't really matter. The issue is not
2 whether there's a punishment that is, you know, sort
3 of sufficient to deter -- I mean, although that is
4 obviously important, but one of your arguments that I,
5 of course, have taken issue with being that this
6 common law data security has evolved to elucidate a
7 standard that doesn't require penalizing. And if
8 people think that that is, you know, a slap on the
9 wrist, they're actually not really understanding the
10 way the FTC works. It's not that the fines are --
11 that there isn't enough punishment.

12 But that said, my biggest problem -- I'm not
13 inherently opposed to fines, but I think that all of
14 the discussion of fines, again, is sort of putting the
15 cart before the horse. That before we give the FTC
16 fining authority, that we have to address these
17 process problems that it has because, otherwise, this
18 is just exacerbating. What I would argue is
19 insufficient notice and insufficient ability for
20 companies to determine what reasonableness requires of
21 them and insufficient evidentiary standard. So if
22 nothing else, if we're going to impose fining ability,
23 can we agree that a slightly higher evidentiary
24 standard is required, maybe even by the Constitution,
25 that approaches that of civil cases rather than a

1 reason to belief standard? Just tossing that out
2 there.

3 But, also, my sort of potential objection to
4 fining comes down to the fact, again, that we have too
5 many settlements and not enough cases being reviewed
6 by the courts, and imposition or the threat of
7 imposition of fines virtually ensures -- potentially,
8 I think, increases the likelihood of settlement. Now,
9 it doesn't have to, and I think there would be some
10 exceptions to that. But I -- you know, my back-of-
11 the-envelope sort of logical calculation here is that
12 that will increase settlements, not increase the rate
13 at -- the FTC will calibrate their fines to ensure
14 that everybody settles, that they're never too high,
15 that companies feel compelled to actually challenge
16 them in court. And that doesn't strike me as a good
17 thing.

18 So, again, my point is to say I can see the
19 logic of the finding, but I think you have to think of
20 the institutional environment in which it's being
21 implemented. And until that environment looks like
22 you want it to look, I would be really, really
23 cautious about bringing fines into the mix.

24 MR. TRILLING: Okay. So we are approaching
25 the end time for the panel. We have time for maybe a

1 few more questions. I want to pivot a little bit to
2 talking more in depth about FTC data security orders
3 with a very general question of how effective are the
4 FTC's current data security controls?

5 MR. MANNE: Does anybody have any idea? I
6 actually think this is one of the problems.

7 MS. PARNES: Well, you know, I represent
8 some companies who are under these orders and I think
9 looking at it from the perspective of, you know, kind
10 of those companies, yeah, I think those orders are
11 absolutely achieving the objective that the Commission
12 is trying to. I mean, companies that are under order
13 spend enormous resources ensuring that they are in
14 compliance with these orders. You know, my experience
15 is that the biennial risk assessments are not
16 something that, oh, we'll worry about that in, you
17 know, kind of two years or 18 months or next year;
18 this is just an ongoing kind of living process at a
19 company. They are very aware, and, typically, their
20 assessors kind of are onsite on a pretty regular basis
21 throughout the two-year period.

22 So I think that the orders achieve one goal,
23 which is making sure that companies are focused on
24 data security. Again, I don't think they can stop
25 data breaches, but that's kind of a different issue.

1 And I think, you know, Geoff, to your point,
2 I'm talking about kind of specific deterrence. I
3 don't know about general deterrence. I really don't
4 have a sense of whether these orders, you know, kind
5 of have an impact more generally on the industry,
6 although I will say companies are certainly aware.

7 MR. MANNE: So some are.

8 MS. PARNES: Yeah.

9 MR. MANNE: So the ones that know enough to
10 come to you are certainly aware. But I would guess
11 that you and people like you, that that's actually a
12 small minority of companies.

13 MS. PARNES: Yeah.

14 MR. MANNE: And from the perspective of the
15 sort of seeming a goal -- so the very specific
16 deterrence -- and, again, like in these specific
17 cases, it's valuable especially when you're talking
18 about big cases -- sorry, big companies with risky
19 data and all of that, not so much when you're talking
20 about Tower Records.

21 But, remember, you know, I think it's clear
22 that it's a regulatory agency that is regulating by
23 case-by-case enforcement instead of rule-making. So
24 the question then is whether it's effectively actually
25 regulating through the enforcement actions. And the

1 first answer to that has to be we don't know, which I
2 think is a problem because I think some effort to try
3 to figure that out would be useful.

4 But I also think that part of the answer is
5 probably not, you know, for some of the reasons that
6 we've been talking about, and I think that that's a
7 problem and I doubt that the trade-off is worth it for
8 the benefit of the specific deterrence in the specific
9 cases just because they're so few and far between and
10 not necessarily keyed to the most risky situations.

11 MS. VANDRUFF: Well, let me ask, though, how
12 would we measure general deterrence?

13 MR. MANNE: That's hard, yeah. I don't
14 know.

15 MS. VANDRUFF: Because I don't know that it
16 follows necessarily the fact that we don't know the
17 answer means that the answer is no.

18 MR. MCGEVERAN: Right, right. I mean, one
19 source of evidence would be the kind of study that
20 like Ken Bamberger and Deirdre Mulligan have done,
21 where they did a very careful -- well, the book
22 comparative actually, European to the U.S., and the
23 U.S. came out looking pretty good -- hats off to the
24 Federal Trade Commission and others. In terms of
25 inculcating a consciousness of the importance of

1 process in companies, not just the ones who are under
2 the orders, but also the ones who fear that they could
3 be next, I mean, you know, that's not a quantitative
4 study. That's interviews that they did with a broad
5 spectrum of privacy officials and companies.

6 But the culture that the -- and that's
7 privacy rather than specifically a security study.
8 But the idea that a responsive case-by-case
9 adjudication system of regulation can create cultures
10 of compliance in corporations, I think there is
11 evidence to support it, although I agree we need more.

12 MR. MANNE: Just really quickly, I think,
13 for example, in your paper, you -- I can't remember if
14 you say that the FTC seems to have contributed to an
15 increase in the adoption of industry standards and
16 sort of self-regulatory bodies. And I think it's fair
17 to say there's a correlation just because the FTC has
18 existed and those things have arisen.

19 MR. MCGEVERAN: Sure, many of them.

20 MR. MANNE: But we have no way of knowing
21 that there's actually a causal relationship. But that
22 would be actually something that you probably could
23 figure out because it would be a very constrained
24 group that you'd have to sort of interview and it
25 would be really great to know. And if it really were

1 happening that way, I think it would count as a huge
2 win for the FTC.

3 I just don't think we know -- that we
4 actually know that that's happening and we can't
5 assume it just because those exist.

6 MR. MCGEVERAN: I think we're agreeing.

7 MR. HARTZOG: Yeah, and I would just add --
8 I mean, if the question is are they effective -- are
9 the orders effective in preventing data breaches, then
10 the answer is obviously of course not.

11 MR. MANNE: Of course not.

12 MR. HARTZOG: Right. I mean, but that's not
13 the -- I don't know if that's the metric by which you
14 do. Here, again, I would draw from Bill's work. When
15 do you have an order over an incredibly large platform
16 that has a massive amount of data, so one of the big
17 five, one of the major tech companies, then what that
18 does then is it does encourage a much closer
19 relationship between industry and the regulator, which
20 I think is positive. So in that effect, I would say,
21 yes, it's good.

22 And then the second thing that I would say
23 that the orders seem to do well is that they are, in
24 fact, a place to test out or at least start to evolve.
25 So I'll actually push back and say that we do get some

1 sort of evolution, maybe not in the way in which you
2 talk about, but some sort of evolution. Privacy by
3 design first started showing up in the United States
4 in these consent orders, right, in these comprehensive
5 privacy programs in response to lots of these
6 complaints. So there are ways in which we can really
7 start to have these evolving conversations. So I
8 think, at least by those two measures, they would be
9 seen as effective.

10 MR. MANNE: It seems to me, by the way, that
11 you're right that we sort of tongue in cheek are
12 saying, you know, has there been more data security,
13 you know, no, clearly no, ha, ha, ha. Obviously, that
14 is, in fact, what we should be aiming at. And I think
15 it goes back to the point I think Michelle initially
16 raised about who the FTC is looking at and sort of how
17 it thinks about its role in this. I mean, if the goal
18 is, in fact, to reduce the rate or the damage of or
19 the incidents of data breaches, targeting very
20 specific company is probably really, as I said, an
21 inefficient way of doing it.

22 But looking at the companies that are
23 actually responsible for the infrastructure and
24 considering that -- like right now we all say you
25 can't stop data breaches, and that's probably always

1 going to be true, but it could be minimized. But
2 minimizing it in any real significant way I think
3 requires rethinking the security infrastructure that
4 we rely on. And I don't think anything the FTC is
5 doing is ever going to help with that.

6 And maybe that's not it's job and, you know,
7 we can talk about. But if you really wanted to effect
8 some change here, I think you would be looking at the
9 software designers, the database designers, the
10 security experts who are the ones who are -- and for
11 that matter, even more complicated infrastructure like
12 the underlying infrastructure of the internet. Those
13 are the people who are ultimately responsible for the
14 problem that we're in and they're the ones who could
15 be incentivized to fix it. I'm not saying that means
16 they should be targeted or something, but that's where
17 we should be looking.

18 MR. HARTZOG: I mean, I would agree with
19 you, but I would disagree that the FTC, broadly
20 speaking, can't do anything about that.

21 MR. MANNE: It could, it could. I don't
22 think in its current process it is doing anything
23 about that. But I agree. That's why I said before,
24 you know, having the conversation, right, convening
25 those people, talking how industry standards might

1 evolve to incorporate security practices at an
2 infrastructure level, to the extent there are choices
3 incentivizing firms to adopt security experts and
4 their processes that are actually more effective than
5 others, those are --

6 MR. HARTZOG: Well, there you go agreeing
7 with Woody again.

8 MS. PARNES: I think they should --

9 MR. HARTZOG: Now you're agreeing with Woody
10 again. That's Woody's book, pretty much.

11 MS. PARNES: So I --

12 MR. MANNE: I think they can do that. I
13 just don't think the enforcement actions are doing
14 that.

15 MS. PARNES: I think the Commission could
16 also make decisions about, from a process perspective,
17 what it thinks are really good practices and, you
18 know, kind of adopt presumptions and say if you do
19 that, we are going to presume that you've got good
20 security in place.

21 MR. MANNE: And I think that would actually
22 -- I agree.

23 MS. PARNES: That, I think, would have a
24 huge impact.

25 MR. MCGEVERAN: And that's a closing letter

1 a company might be perfectly happy for that to come
2 out in public, right?

3 MS. PARNES: Right.

4 MR. MCGEVERAN: About what a good job
5 they've done.

6 MS. PARNES: Right.

7 MS. VANDRUFF: I don't want to cut this
8 discussion short, but our time is up. I want to thank
9 the panelists for joining us today.

10 It is my pleasure to introduce the Associate
11 Director of the Division of Privacy and Identity
12 Protection, Maneesha Mithal, who is going to offer
13 some closing remarks before we conclude for these two
14 days.

15

16

17

18

19

20

21

22

23

24

25

1 CLOSING REMARKS

2 MS. MITHAL: Thanks to this terrific panel
3 and thank all of you for sticking it out until the
4 end. It was a pleasure to have all of you here. I
5 think the panels over the last two days have been
6 extremely substantive and informative, and I think we
7 have several people to thank for that.

8 So I want to thank from the Division of
9 Privacy and Identity Protection, Elisa Jillson, Jared
10 Ho, Jim Trilling, who are the staff attorneys who have
11 been putting this together, along with Mark Luppino
12 from the Bureau of Economics and Michael LeGower, also
13 from the Bureau of Economics, and several folks from
14 the Office of Policy Planning. I want to thank Laura
15 VanDruff, who's been the manager on this team, and
16 also the event staff and the press office and
17 everybody else who's had a hand in putting this
18 together. So thank you, everybody. So if we could
19 give them all a big hand.

20 (Applause.)

21 MS. MITHAL: Okay. So I've been kind of
22 taking notes as this conference has gone on and I'd
23 just like to kind of point out three main takeaways
24 that I've kind of observed from the last two days.
25 Just kind of some thoughts on some of the things the

1 panelists have raised in the context of these three
2 takeaways.

3 So the first is that we need more empirical
4 data about data breaches, the threat environment, and
5 the harms to consumers. Now, we got some information
6 yesterday morning about threat vectors. We heard from
7 Verizon on their data breach report. We heard about
8 various types of harms that consumers suffer when they
9 have been victimized by identity theft. But I've been
10 struck by the fact that on many of the panels
11 following that and today's panels, as well, companies
12 talked about the need for more data on certain
13 aspects.

14 So, for example, one panelist talked in the
15 panel about investments in cybersecurity, talked about
16 there are three aspects for determining how to make
17 decisions on cyber investment, what is the value of
18 the information, what is the probability of a breach
19 and what is the productivity of the investment that
20 might avoid that breach. I think as companies are
21 considering optimal investments in data security, it
22 would be great to be able to have more information on
23 that.

24 I think in this panel we just heard about
25 how we're measuring general deterrence. Again,

1 further academic research, economic research on these
2 issues I think would be very welcome. So I think
3 that's the first takeaway.

4 The second takeaway is that there's multiple
5 sources of incentives for companies to invest in data
6 security. We heard about a number of these incentives
7 yesterday, the company's reputation, the competitive
8 disadvantage or competitive advantage that could be
9 created by better security, cost of cyber insurance
10 could be decreased by having better security, the
11 liability regime influences incentives on data
12 security. We also talked a little bit about what
13 drives investment. What are the sources that drive
14 investment in data security?

15 We talked about the culture of security
16 within the firm and the ability of the CISO to
17 effectuate change within an organization. We talked
18 about customers as a potential driver of data
19 security. We talked about cyber insurance and we
20 talked about legal incentives. At the same time, I
21 think we heard today that, you know, although many
22 companies are influenced by loss of reputation,
23 consumer trust and other things, we've heard
24 situations where some CISOs have had challenges in
25 getting companies to invest in data security where

1 they say, well, if you're going to ask me to invest \$1
2 million and a breach is only going to cost me
3 \$500,000, why should I invest the \$1 million? And I
4 think that that was an interesting question raised
5 this morning.

6 And then, finally, in terms of takeaways, we
7 talked a lot about solutions today and I think this
8 probably goes without saying, but I think we all
9 talked about the fact that a one-size-fits-all
10 solution won't necessarily work.

11 Now, I think there was some consensus
12 around the idea that companies should implement a
13 process-based approach. We heard that numerous times
14 over the last two days, a process-based approach as
15 opposed to an outcomes-based approach. We heard the
16 adage that security is a journey and not an end point.
17 We also heard that the right way to do a process-based
18 approach is not to talk about how many bodies you're
19 throwing at data security, but to talk about how
20 companies are doing risk assessments, where is the
21 data, what data is it, what risks would arise for
22 consumers in the corporation if the data was
23 compromised. So, again, we heard the term "risk-based
24 approach" a lot.

25 But in addition to a process-based approach

1 to avoiding data breaches, we also heard about other
2 approaches. We heard about the idea of devaluing
3 assets for the identity thieves and other criminals
4 that get this information. A representative from the
5 payment card industry talked about tokenization and
6 the idea that if you use tokenization you'll reduce
7 the value of credit card numbers to identity thieves.
8 We talked about the fact in the old days that SSNs
9 were used as authenticators and reducing reliance on
10 SSNs can help avoid some of the harms that arise from
11 data breaches.

12 Another solution that people talked about
13 was accountability, the need for data security to be a
14 risk management approach where you have the CFO, the
15 CISO, the risk management team and others directly
16 reporting to the board on accountability issues. We
17 heard a lot about FTC enforcement. I think there was
18 some consensus that there is some role for FTC
19 enforcement, although there may have been some
20 differences in how the FTC should conduct its
21 enforcement activities. But I think there also seemed
22 to be a lot of consensus around the need for FTC
23 business guidance, along the lines of start with
24 security and stick with security and some of the other
25 projects.

1 So to that end, I have some slides that I
2 just wanted to point people's attention to some of the
3 information that we already do have out there. So I
4 think Start with Security, we've talked about a lot.
5 I just wanted to show people that this is what it is.
6 It has kind of ten lessons to be learned from our data
7 security cases. We have data security education on
8 specific topics. This one is a specific IOT. I know
9 Lydia talked about the idea of doing more reports on
10 data security and I think this might be one model for
11 that where we talk about specifically data security
12 involving IOT.

13 We have a data breach response guide and
14 cybersecurity for small businesses which really
15 focuses on businesses that don't have IT departments
16 or legal departments and are trying to do it all
17 themselves. So that's kind of the broader review of
18 some of the stuff we've done. I think that has been
19 referred to throughout these last two days. So I
20 wanted to point that out.

21 So with that, again I want to thank
22 everybody for their attendance. The comment period
23 will remain open until March 13th. So we appreciate
24 any additional comments that people might have and
25 thank you again. And if you could all join me once

1 again in giving all the panelists and participants a
2 big hand.

3 (Applause.)

4 MS. MITHAL: And thank you very much.

5 (Applause.)

6 (Hearing concluded at 4:22 p.m.)

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 CERTIFICATE OF REPORTER

2

3 I, Linda Metcalf, do hereby certify that the
4 foregoing proceedings were digitally recorded by me
5 and reduced to typewriting under my supervision; that
6 I am neither counsel for, related to, nor employed by
7 any of the parties to the action in which these
8 proceedings were transcribed; that I am not a relative
9 or employee of any attorney or counsel employed by the
10 parties hereto, not financially or otherwise
11 interested in the outcome in the action.

12

13

14

15 s/Linda Metcalf

16 LINDA METCALF, CER

17 Court Reporter

18

19

20

21

22

23

24

25