

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

Tuesday, December 11, 2018
10:10 a.m.

Federal Trade Commission
Constitution Center
400 7th Street, SW
Washington, D.C.

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

I N D E X

PAGE :

Welcome and Introductory Remarks	3
Opening Remarks	5
Presentations on Data Breaches	15
Incentives to Invest in Data Security	76
Consumer Demand for Data Security	145

1 WELCOME AND INTRODUCTORY REMARKS

2 MS. JILLSON: Good morning, and welcome to
3 the FTC's hearing on data security. My name is Elisa
4 Jillson. I'm in the FTC's Division of Privacy and
5 Identity Protection in the Bureau of Consumer
6 Protection.

7 Before we get started with the substantive
8 portion of the day, I have a few announcements.
9 First, please silence your cell phones and other
10 devices. If you leave the building during the
11 conference, you will have to go back through security,
12 so please keep that in mind, especially during lunch.

13 If an emergency requires you to leave the
14 conference center but remain in the building, please
15 follow the instructions provided over the building's
16 PA system. If an emergency requires an evacuation of
17 the building, an alarm will sound. Everyone should
18 leave the building in an orderly manner through the
19 main 7th Street exit. You'll turn left and proceed
20 across D Street to the FTC emergency assembly area.
21 Remain in that area until instructed to return. If
22 you notice any suspicious activity, please alert
23 building security.

24 This event will be photographed, webcast,
25 and recorded. By participating, you are agreeing that

1 your image and anything that you say or submit may be
2 posted indefinitely at FTC.gov or on one of the
3 Commission's publicly available social media sites.

4 Question cards are available in the hallway
5 on the information tables immediately outside the
6 conference room. Ryan Hsu and Mohamad Batal will be
7 available to collect your question cards. Please
8 raise your hand and they will collect your card.

9 For those of you participating via webcast,
10 you can tweet your questions at FTC using the hashtag
11 FTChearings. Please understand that we may not be
12 able to get to all questions.

13 Restrooms are located in the hallway just
14 outside of the auditorium.

15 And with all of that said, I would now like
16 to introduce Andrew Smith, the Director of the Bureau
17 of Consumer Protection at the FTC who will be making
18 some opening remarks.

19 (Applause.)

20

21

22

23

24

25

1 last seven months.

2 So this is an excellent opportunity for
3 us to revisit policies and question old assumptions.
4 So I don't know with my disclaimer and my caveat
5 about the amount of time that I've been here at the
6 Commission, I really can't predict much, but I can
7 predict this, that data security will continue to
8 be an important priority for the FTC and that the
9 FTC will not be retreating from its role as the
10 nation's primary data security law enforcement
11 agency.

12 Digital data security has never been more
13 important to businesses and consumers. The rise of
14 online banking, e-commerce, connected homes, connected
15 cars, smartphones, and really with this, connected
16 people, digital data security becomes more important
17 every day. But hardly a day passes that we don't hear
18 about a new security breach at a major company. And,
19 of course, this morning is no exception.

20 By one count, there were more than 1,250
21 data breaches in the last year with 4.5 billion
22 records compromised. There's an old saw in the data
23 security business, I understand, that there are two
24 kinds of companies, those that have been hacked and
25 those that have been hacked but don't know it yet.

1 So what have we been doing for -- on data
2 security? Well, like many things in government, we
3 know we use the three-legged stool model. We have law
4 enforcement, policy development, and consumer and
5 business education. First and foremost, law
6 enforcement. We like to think of ourselves as a law
7 enforcement agency. That's where most of our work in
8 this area is done. We have settled more than 60 data
9 security cases on issues ranging from internet of
10 things to children's data to financial records, and
11 there's more to come. For example, in January, the
12 FTC staff will be going to trial in D-Link, a case
13 centered on IOT security.

14 Policy development. Two weeks ago, the
15 Commissioners identified -- or the Commissioners,
16 rather, testified before Congress about what data
17 security tools the FTC is using and what additional
18 tools it could use to protect consumers' data. The
19 long and short of it was that the Commissioners
20 testified in favor of data security legislation
21 with APA rulemaking for the FTC, along with civil
22 penalties and expanded jurisdiction over
23 telecommunications carriers, nonprofits, and a
24 couple of others.

25 So also in the realm of policy development,

1 we're currently undergoing a routine regulatory review
2 of our GLBA Safeguards Rule, which is one of two rules
3 that we have made and enforced with respect to data
4 security, the other being the COPPA rule. When this
5 rule was initially issued in 2002, it was
6 revolutionary in that it was risk-based and prescribed
7 a process rather than a standard or an outcome. It
8 became a model for other risk-based state and federal
9 laws, and also provided useful guidance on data
10 security for large and small enterprises alike.

11 But in the fast-changing world of data
12 security, very little stays up to date for 15 years,
13 like the GLBA Safeguards Rule has. So we're in the
14 process of revisiting that rule to determine if
15 improvements are needed. Today's hearing is a part of
16 the Commission's policy work, and the record developed
17 today will help to inform the Commission further on
18 how best to use its tools to promote appropriate data
19 security.

20 The final leg of the stool is consumer and
21 business education. So I brought along a prop. This
22 is our Cybersecurity for Small Business publication.
23 All of these materials are on our website, and that's
24 FTC.gov/smallbusiness, and that's where most of the
25 distribution of these materials is done. So these are

1 new materials intended for small businesses but really
2 can be translated to any business.

3 It includes fact sheets. It includes videos
4 on our website. It includes quizzes and similar
5 training materials for small businesses. Included in
6 here are sort of the basics of data security, physical
7 security in the NIST framework. We also address four
8 specific scams that target businesses, ransomware,
9 phishing, email spoofing, tech support scams, and then
10 we also delve into more technical issues such as
11 vendor management, cyber insurance, both first-party
12 coverage and third-party cover, email authentication,
13 web hosting, and remote access.

14 So, importantly, this campaign is cobranded
15 with NIST, DHS, and the Small Business Administration,
16 and we also got input from the National Association of
17 Insurance Commissioners. We held a series of
18 roundtables with small businesses in 2017, and they
19 all told us that they need a single unified message
20 from the Federal Government. They were -- they felt
21 as though they were getting different and sometimes
22 conflicting messages from different government
23 agencies and they wanted one single, unified message
24 with easy-to-use resources about cyber threats and how
25 to deal with them. So we responded with this new

1 business education campaign.

2 So that's a useful reminder that we're not
3 the only ones policing data security and providing
4 guidance. So you just heard about our critical
5 partnership with NIST and DHS and SBA, but, of course,
6 we also have the Department of Justice, the U.S.
7 Postal Inspectors, and other federal and state
8 criminal law enforcers who are on the beat. State and
9 federal banking, healthcare, insurance, securities
10 regulators also are policing data security and
11 providing guidance.

12 And we have our good friends and partners,
13 the state attorneys general and, of course, private
14 industry initiatives, including the payment card
15 network -- including the payment card industry data
16 security standards, as well as standards promulgated
17 by public utilities and the defense industry and
18 others.

19 Yet despite all of our best efforts, we seem
20 not yet to have achieved optimal data security. The
21 daily rash of breach announcements make it seem as
22 though all of our efforts are just a drop in the
23 ocean. How do we explain this? On the one hand,
24 maybe our current approach is working, and the
25 apparent uptick in breaches is just a result of more

1 data moving online and the greater sophistication of
2 attackers and -- or maybe more and better intrusion
3 detection and reporting of breaches.

4 On the other hand, maybe our current
5 approach to data security requires some serious
6 rejiggering. Or maybe the current approach is solid,
7 but we just need more of it and better tools to
8 achieve it. So we're here today to ask tough
9 questions about the state of data security and data
10 security regulation.

11 What are the incentives to invest in data
12 security, and are they enough? What does consumer
13 demand for data security look like? Does consumer
14 demand meaningfully drive data security investment?
15 Should we expect consumers to participate in securing
16 their own information? How can we best assess data
17 security at specific firms and how can we communicate
18 that assessment to the relevant stakeholders, to
19 executives, boards, cyber insurers, card issuers,
20 consumers, regulators? Which regulatory and
21 enforcement approaches are working? Why are they
22 working? Can they be improved?

23 And, finally, we need it take a hard look at
24 the FTC. Are our tools up to the task of identifying
25 and remedying lapses in data security? So we're going

1 to be examining these big questions over the course of
2 the next two days.

3 This morning, we'll start by focusing on
4 data breaches. Marc Spitler from Verizon Security
5 Research will present on the Data Breach
6 Investigations Report, the annual chronicle of data
7 breaches and their causes.

8 Next, Sebastien Gay from Georgetown's
9 Economics Department will describe his work on how
10 some firms internalize the cost of data breaches and
11 whether their stock prices take a hit and how those
12 firms mitigate that potential impact.

13 And, finally, Al Pascual from Javelin
14 Strategy and Research will describe some markers of
15 how data breaches affect consumers.

16 This afternoon, we'll turn to two panel
17 discussions. The first will discuss the incentives to
18 invest in data security, ranging from consumer trust
19 to compliance obligations to cyber insurance, and
20 explore how companies make those investment decisions.

21 The second panel will explore consumer
22 demand for security. During this discussion, we'll
23 hear about emerging security ratings that allow
24 consumers to compare the security of products and
25 whether we can count on consumers to shop on security.

1 Tomorrow, we'll tackle data security
2 assessments. Assessors from a variety of backgrounds
3 -- big four accounting, security boutique, cyber
4 insurance firms -- will react to a series of
5 hypothetical assessment situations. In these hypos,
6 panelists will address thorny issues, like who defines
7 the appropriate scope of an assessment, how does a
8 company with a tight budget and big problems gauge
9 security, and when to look to inside expertise and
10 when an outside perspective may be better.

11 Next, Commissioner Becca Slaughter and
12 Joshua Corman, the Cofounder of the "I am the Cavalry"
13 security initiative will talk about the current threat
14 landscape and emerging threats.

15 Tomorrow afternoon, panelists will turn to
16 policy with a pair of panels on the U.S. approach to
17 data security and FTC data security enforcement.
18 These panels will examine what regulatory approaches
19 are working, what's falling short, and how the current
20 approaches could be improved. So we have a lot to
21 cover with presenters and panelists who have thought a
22 lot about these important issues.

23 I'd like now to turn it over to Jared Ho in
24 the Division of Privacy and Identity Protection and
25 Marc Luppino in the Bureau of Economics, who will

1 start us off with a series of presentations about data
2 breaches.

3 Thank you all for coming today and for
4 helping us to think about the state of data security.

5 (Applause.)

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 PRESENTATIONS ON DATA BREACHES

2 MR. HO: Okay. Thank you, Andrew, for those
3 remarks. And good morning, everyone. We're delighted
4 to be here today to kick off the first session of the
5 day. My name is Jared Ho. I'm an attorney with the
6 Division of Privacy and Identity Protection at the
7 Federal Trade Commission. My comoderator is Marc
8 Luppino. He's an economist in our Bureau of
9 Economics.

10 We will start out this morning with three
11 presentations from our highly esteemed guests,
12 discussing the current set of data breaches and the
13 impact of those breaches on both firms and consumers.
14 First, you will hear about the trends our experts are
15 seeing. We will then have what we expect to be a
16 lively conversation with our presenters who delve
17 deeper into the perspectives on the threats to
18 consumers' personal information.

19 We will be taking questions from the
20 audience. If anyone in the audience has a question,
21 there are question cards on the table located directly
22 outside of the auditorium. Please flag down our
23 conference staff, either Ryan or Mohamad, and they
24 will be collecting those cards and passing them to us.

25 MR. LUPPINO: Okay. There are more detailed

1 bio online, but very briefly, we have Marc Spitler who
2 leads the Verizon Security Research Team. He's a lead
3 author of the Verizon Data Breach Investigations
4 Report series and is involved in the development of
5 the Vocabulary for Event Recording and Incident
6 Sharing framework, otherwise known as VERIS.

7 We also have Sebastien Gay who teaches in
8 the Department of Economics at Georgetown University.
9 He specializes in financial privacy in real estate and
10 economics research, and he's an Assistant Director for
11 Financial Analysis for the Congressional Budget
12 Office.

13 And, finally, he have Al Pascual, who is a
14 Senior Vice President for Research and Head of Fraud
15 and Security at Javelin Strategy and Research.

16 With that said, I will turn it over to Marc
17 Spitler for the first presentation of the morning.

18 2018 Data Breach Investigations Report

19 MR. SPITLER: Well, hello, everybody. My
20 name, again, is Marc Spitler. I'm here to talk about
21 the results that we found in the 2018 Verizon Data
22 Breach Investigations Report.

23 A brief history for those of you who may not
24 be as familiar with it. This is a publication that we
25 put out annually. This was the 11th iteration of it.

1 So we've been doing this since about 2008 -- really
2 about 2008-2009. And the reason that we started it in
3 the first place was we just were not seeing enough
4 real-world data being presented back out to the public
5 on what is really happening as far as cyber crime.

6 There is a lot of discussions, and people
7 that are selling various widgets and services about
8 things that you need to be worried about and wouldn't
9 it be awful if this happened. We had a lot of that
10 type of information coming to us, but what we didn't
11 really know is when people are actually suffering
12 real-world data breaches, who's behind it, what are
13 they doing, what methods are they using, who are they
14 targeting, and why?

15 And so we put out the first report back then
16 and we've started to grow it ever since. So we are --
17 obviously, me and my team are very, very fond of good
18 data sources, and we were not wanting for data this
19 year. As you can see from some of the numbers on the
20 slide there, we had over 2,000 confirmed data
21 breaches, and we had over 50,000 security incidents.
22 And we defined a security incident as an event where
23 either confidentiality, integrity, or availability of
24 an asset was compromised.

25 So people could get a denial of service that

1 takes down their website. We would not call that a
2 breach. We would call that a security incident. So
3 just a really quick definition there.

4 And, you know, our corpus is now well over
5 16,000 breaches and over 3,000 -- excuse me, 300,000
6 security incidents. So really big, splashy numbers.
7 I'm not trying to scare anybody with that. I'll try
8 to reel it back in to kind of talk about how do we
9 categorize these to be able to present something out
10 to the public that they can actually take action on.

11 When we first started this out, we had a
12 single data source. We've now grown that to over 60,
13 so we have participants from law enforcement; certs,
14 both domestic and international; cyber insurers; other
15 forensic partners. So we have a pretty good diversity
16 of data. This is not every single incident that
17 happened last year, every single breach, so we don't
18 answer questions like are we getting better or worse.
19 What we're just trying to do is find, you know, what
20 are the tactics that are being used, what does this
21 mean to me if I'm in a particular industry? Do I have
22 to look at something more often than somebody else?
23 What's most likely going to affect me? What's my
24 3:00-in-the-morning call going to be?

25 And one of the things that we had to take a

1 look at is why are these happening to begin with. So
2 when there's confirmed data breaches and it is
3 malicious, what is the mode of the adversary? More
4 often than not it's money. It makes sense. People
5 are doing this not because they -- you know, it's not
6 because of ideology very often.

7 It certainly can be for strategic advantage,
8 which would be the cyber espionage attacks that we do
9 see. But from a frequency standpoint, it's money.
10 They're going after data that can be monetized in the
11 form of personal information, payment card
12 information, card information, banking information,
13 and it's to make a dollar in some form or fashion.

14 Now, this chart behind me is about breaches,
15 and one of the more interesting trends is you don't
16 actually have to have a confirmed data breach to make
17 money anymore. One of the ways they do that is
18 ransomware. Ransomware has actually been around for
19 quite a while, but it's really started to get a lot of
20 publicity in recent years, and our data actually backs
21 that up.

22 So we are seeing within our data set an
23 increase in ransomware year over year. It doubled
24 last year, it doubled the year prior to that as far as
25 number of incidents. So the little line graph behind

1 me tells a couple of interesting stories. The first
2 one, what this is showing is what assets are affected.
3 So ransomware, a really quick definition, it's malware
4 that gets onto a system, and it will obfuscate or
5 encrypt data and then reducing obviously the utility
6 of said data and then the adversary will demand a
7 ransom that you pay and you may or may not get a key
8 to unlock that.

9 The first thing you might notice is that we
10 actually have people on this slide. And you're
11 probably saying, okay, how do you encrypt a human?
12 You don't, but where we are able to figure out how
13 malware got onto a system, if it involved some level
14 of altering of human behavior via phishing, via email,
15 we're able to note that.

16 It seemed to go down quite a bit. That's
17 really more indicative of back in 2014 when we didn't
18 have as many of these. We knew what the malware
19 vector was. A lot of these cases we're getting now we
20 know that ransomware occurred, we know what industry
21 it affected, but they didn't provide us or they did
22 not record how the malware got on there.

23 I would be absolutely willing to bet if we
24 had knowledge of every single malware vector that
25 people, because of the email being the means to get

1 in, would be much, much higher. Our data shows that
2 email is the predominant means of getting malware onto
3 networks. Not only does our incident data show that,
4 but we have a contributor that detonates millions and
5 millions and millions of pieces of malware per
6 calendar year, and their data also shows that they're
7 finding this data and they're detonating it and it's
8 coming in via email.

9 So the one line that doesn't have as sharp
10 of a drop but I think is very interesting and, you
11 know, concerning is the one that says server. And
12 it's kind of the second one there. And it's got a
13 slow rise. And, remember, this is from a percentage
14 of ransomware incidents, so the actually numbers in
15 2017, 2016, much, much higher. And when we see
16 servers being affected by this, we realize that this
17 isn't just one person, a user in your organization
18 getting ransomware, having his or her laptop or
19 workstation encrypted. That's bad. You know, no one
20 wants that on a particular day.

21 What we're seeing is that foothold is not
22 being used and encrypted straightaway. They're using
23 that to move laterally within an organization.
24 They're using it to find databases, file servers, even
25 backup servers. Then they encrypt, and now you've got

1 a much, much higher criticality event that's
2 happening. They're able to ask for a higher ransom,
3 and there's probably a higher chance that someone's
4 going to pay it because you're in a much, much worse
5 situation than if it was just a single laptop.

6 And, so, ransomware is one of the things
7 that we've have seen rise up over the last couple of
8 years. That's why I have a slide here. And we have a
9 section on it in the full report itself, so anything
10 you see here is obviously going to be available in the
11 full report and explained even more.

12 The next topic I want to kind of touch on is
13 social engineering. So the human factor, I've already
14 kind of alluded to it with how a lot of ransomware
15 gets onto systems, but we have seen a significant
16 amount of real-world data breaches begin with social
17 engineering, notably phishing, but we're also seeing a
18 rise in what we call financial pretexting.

19 Common examples of this are people in
20 finance departments getting an email from -- and I'm
21 using air quotes here -- the CEO that is saying, hey,
22 you know, we need you to pay this invoice before you
23 go home for the weekend. It has to happen now.
24 Thanks for all your hard work. And they are duped
25 into sending -- you know, basically wiring money

1 directly to the adversary.

2 Kind of like ransomware, there really wasn't
3 a data breach there. You know, they didn't
4 necessarily give them their banking information. They
5 were just flat out tricked into sending money to the
6 bad guy.

7 But we also see human resources departments
8 actually being affected by this, too. And that ruse
9 is I'm from a payroll company or you know, again, I'm
10 an executive, and I need W-2 information for all the
11 employees. So that is obviously a data disclosure.
12 They're providing this W-2 information that's being
13 used for tax fraud. Both of those kind of affect all
14 industries fairly across the board. You know, anybody
15 can be affected by that style of attack.

16 We also see social engineering phishing
17 being used by a nation state or state-affiliated
18 groups. It's how they're gaining their foothold.
19 It's how they're getting that kind of a patient zero,
20 if you will, within an organization to again move
21 laterally within a network, move deeper to find
22 ultimately their end goal.

23 As you can see, this slide is very busy.
24 There's a lot of numbers on here, and we have a
25 limited amount of time, so I will not be going through

1 each of these individually, but what this shows is a
2 breakout of different industries and some of the
3 styles of attacks that we see. And I'm focusing
4 really on the top left grid there. So, you know, at
5 the top, going vertically are some industries and
6 going horizontally are some styles of attacks, like
7 crimeware, which is financially motivated malware,
8 typically opportunistic in nature, ransomware being a
9 prime example of that. Cyber espionage, again, that's
10 going to be all about motive, who the adversary is,
11 you know, what they're after. Denial of service,
12 pretty self-explanatory.

13 Some of these other ones are self-
14 explanatory, but what you can focus on here really,
15 really quickly is, hey, some of these cells are a dark
16 shade of blue and have large numbers in them. You can
17 even squint your eyes and be able to kind of
18 understand this is a heat map. Some areas have a
19 strong level of correlation between the type of attack
20 the industries see versus others, so you know, a
21 combination which would include restaurants, food
22 service, hotels.

23 If you go down, you can see, wow, they have
24 a very, very big problem with people attacking their
25 point-of-sale environments. It makes a lot of sense.

1 They process a lot of credit cards. Cyber criminals
2 enjoy credit cards because they can make money off of
3 it, and we already saw that slide, which is what
4 motivates most people, so we see a strong correlation
5 there. So people can just take a look at this single
6 figure.

7 And there's a lot going on here. I could
8 tell two hours of stories on this, but you can begin
9 to say, hey, am I going to spend my time and my
10 resources on a problem that's affecting me at a high
11 level of frequency? Am I putting my money in the
12 right place, or am I focusing on something that maybe
13 isn't going to be as important to me because of my
14 industry and what has happened historically to people
15 like me?

16 And, again, this is all in the full report,
17 so you can absolutely review this, and you can draw a
18 lot of interesting stories from it. Again, I'll touch
19 on a couple of the tactics that are being used. We
20 talked about ransomware. We talked about some of the
21 social attacks, primarily phishing, which is, you
22 know, via email, or what we call pretexting, which is
23 really a little bit more sophisticated than just a
24 phish, which is more of a fire and forget, spring and
25 prey, if you will, type of tactic. Pretexting is

1 where you develop a dialogue. You actually have a
2 story. You have maybe done some intelligence-
3 gathering to know who the right target is within that
4 organization, but some other things are happening,
5 too. All right?

6 We see use of stolen credentials as one of
7 the primary tactics that adversaries are using. When
8 we think about hacking and when we think about the bad
9 guys and you have maybe this Hollywood vision of
10 someone, you know, in a dark room probably wearing a
11 hoodie and they're, you know, hammering away at a
12 keyboard and they finally find that way in, in reality
13 what they're trying to do most often is to phish some
14 credentials off of someone and then reuse those. Why
15 would they want to do something harder than that? Why
16 would they want to do something that could be detected
17 easier than reuse of credentials?

18 So we see a lot of attacks on single-factor
19 static authentication. And we see that used all too
20 often to protect highly critical types of data where
21 we need to have stronger authentication, not just from
22 an outside in to your network, but also even when
23 you're on your network. We need to see stronger
24 barriers between that first laptop that might be
25 infected and other areas with other deeper security

1 zones.

2 The other types of malware that we're
3 seeing, we see what's called backdoor or command and
4 control. That establishes that foothold, that's
5 persistence and allows the attacker to take hold of a
6 system and use that as their entry point, and they can
7 issue commands to it. So you can kind of see -- if
8 you took a look at some of these, you see phishing,
9 which can lead to back doors and C2s, which can lead
10 to other types of malware that will capture
11 credentials, which can lead to the reuse of that. So
12 you see how these things are not mutually exclusive,
13 but they can go in order and tell the story about how
14 attackers are really trying to go about their
15 business.

16 So that's kind of a high level of the things
17 that we are seeing. And certainly, we'll have time to
18 go over this in more detail as we go along with the
19 panel. In front of you is the URL for the full, 80-
20 plus-page report. And, hopefully, you'll be able to
21 take a look at that. And if you do have any other
22 questions, you can -- that report will also have email
23 addresses that you can actually come back and ask us
24 questions about the data, and we'll be more than happy
25 to answer those.

1 MR. LUPPINO: Thank you very much, Marc.
2 We'll now turn it over to Sebastien Gay for the second
3 presentation this morning.

4 Strategic News Bundling and Privacy Breach Disclosure

5 MR. GAY: Thank you. Marc, Jared, thank you
6 for inviting me this morning to talk about my academic
7 research on privacy breaches. I want to remind the
8 panel and the audience that I'm here in my personal
9 capacity. None of these views reflect the views of my
10 current employer on this particular topic, and I do
11 not have any ongoing research on the topic at the
12 current time.

13 Marriott, Target, Yahoo, Home Depot, and
14 Anthem, all of these firms were breached recently.
15 After the breaches, most of these firms did not
16 encounter large decreases in their stock price. Most
17 of them actually had new highs within a week of a
18 disclosure, so what could explain this?

19 A privacy breach is a short-term crisis
20 for a company. With thoughtful preparation, like
21 any other crisis, it can actually be prevented.
22 Preparation requires prevention, so let's avoid it
23 from Marc. Loss mitigation, it happened, what's the
24 bottom line, let's get the PR involved; brand
25 management, so let's restore a firm's reputation; and

1 customer relationships, which is usually what you lose
2 once you have that type of privacy breaches.

3 Remediation costs for firms that fail to
4 adequately protect consumer data can be quite large.
5 Costly lawsuits, payments for credit report
6 monitorings and actually call centers, and loss of
7 future businesses. In a well-functioning system,
8 firms would protect themselves and insure themselves
9 against those risks.

10 And, so, the paper right here was asking the
11 most important question at the time, that was could
12 firms leverage media coverage to protect themselves
13 from costly privacy breaches. So in my paper that I
14 think is available online, "Strategic News Bundling
15 and Privacy Breach Disclosures," I examine how firms
16 can build up a repository of positive news that could
17 then be used at or around the same time that a privacy
18 breach is disclosed to offset its negative effects on
19 the price.

20 So privacy breaches, as established before
21 by Marc, are unexpected and usually negative news for
22 companies and the stock market. Given their
23 unexpected nature, the effect of privacy breaches has
24 been difficult to measure in the economic and finance
25 literature. When using event studies to examine the

1 price of a stock of affected firms before and after
2 the disclosure of a privacy breach, academic papers
3 have found both a positive and a negative effect.

4 So the question here was, why could that be?
5 And so, looking at the state in which the breach
6 happened, you can look that there are discrepancies in
7 the disclosure laws. The legal disclosure time for a
8 privacy breach, depending on the state, can depend on
9 like -- can be a few days to actually a few months.
10 That potential lag raises the question of whether
11 firms strategically releasing all the news around the
12 same time as a privacy breach can attenuate the effect
13 on its stock price and then provide a softer effect on
14 its reputation and its brand name.

15 So now, let's get on to the data that was
16 used in the paper. I have a list of privacy breaches
17 that I compiled from 2005 to 2014. At the time, I
18 relied a little bit on the Verizon report, but there
19 was also no official reporting standard that was
20 adopted. So a compilation of all privacy breaches
21 ended up being a very difficult task.

22 Data validation was important, and I used
23 more than four different sources to try to find out
24 whether or not the date of a release was correct, when
25 the breach actually happened, and the number of

1 customers that were affected by the breach, as well as
2 the magnitude of the breach. The problem here is that
3 the term like "breach accounts" is very vague and used
4 a lot of times.

5 Stock prices and other data on companies are
6 available through academic resources, and the news
7 data came actually from a very rich data set that
8 compiles all other news that are available for every
9 company with a time stamp. So think about something
10 like for the data set that I had, like 13 million
11 observations.

12 The news data are classified into three
13 types -- breaking news reports, news reports, and
14 press releases. Overall, the paper contains 542
15 privacy breaches for the time period 2005 to 2014. It
16 doesn't contain all of the incidents that Marc talked
17 about because I had to match it with stock market
18 data. And the panel, as I mentioned, had more than 13
19 million observations.

20 So during the research project, a few, like,
21 patterns on the data emerged. The first one, very
22 interesting, is that not all privacy breaches are
23 reported in the news. And actually, 50 breaches that
24 were available in the sample were not present at all
25 in the news at any point in time. More than 30 to 50

1 percent, depending on the industry of the breaches,
2 were not even the target of any, like, breaking news
3 alert.

4 Two, there was a lag between the time of
5 reporting and the actual breach that can be actually
6 quite lengthy. It went from a few days to years, and
7 we may want to talk about it with, like, the panel,
8 but when the FBI gets involved and there's an
9 investigation, we can -- the time at which you have to
10 report your privacy breach can actually be extended.

11 The third one is firms are ready to announce
12 a remedy most of the times when they disclose a
13 privacy breach, so they come ready for it.

14 Fourth is only half of the privacy breaches
15 in the sample reported an actual or even estimated
16 number of records breached.

17 And fifth, the more scary one, is firms can
18 actually be breached multiple times. Some people may
19 say they don't learn. Some others may say, like Marc
20 mentioned earlier, show me the money. It happens more
21 often in the retail, finance, and insurance industry,
22 so Social Security numbers and bank accounts are very,
23 you know, valuable to hackers, so they may be more
24 willing to go back to the same source.

25 So intuitively, privacy breaches reporting

1 and media coverage can actually be thought of as some
2 sort of a tide. The paper establishes that there is a
3 sharp drop, on average obviously, in the average daily
4 negative news compared to the usual level right before
5 firms are disclosing a privacy breach. And this
6 result is all the more surprising that I'm including
7 in that number the actual release of a privacy breach
8 as a news event, so really, if you take that out, it's
9 almost -- you would get into the negative, if you
10 wanted to push that.

11 More surprisingly, there's also a decrease
12 in the amount of positive news right before and a
13 strong increase right after the disclosure of a
14 privacy breach. So this pattern seems to suggest that
15 there is an intentional timing of disclosure when
16 firms release a privacy breach.

17 So the paper runs a series of modified event
18 studies using the amount of abnormal news defined to
19 make it simple as the deviation for the mean number of
20 new stories on a given day. The idea behind it is a
21 firm like Apple has more news on a given day than
22 Colgate. So -- and I do that for both positive and
23 negative abnormal news.

24 So what you notice is that there is a
25 significant negative effect of a breach disclosure on

1 the stock price on the day and the day after the
2 disclosure, so something like 24 to 27 basis points.
3 Surprisingly, a firm that has been breached multiple
4 times sees a decreasing effect of the privacy breach
5 on its stock price. So that seems to reinforce the
6 fact that firms learn and kind of use a little bit
7 more the media's trove that they had available in
8 order to attenuate this effect.

9 But where it's very interesting is if you
10 look at the effect of an additional piece of positive
11 news story compared to the usual amount of positive
12 news on any other day, you find an effect that is 15
13 times higher, like the effect of a positive news, an
14 additional one, is 46 basis points on the day of
15 disclosure of a privacy breach versus only three basis
16 points on any other day. And this is very consistent
17 throughout the entire sample.

18 So you notice, this completely offsets the
19 negative effect of the privacy breach that was around,
20 like, minus 24. Surprisingly enough, the market
21 capitalization and the number of records breached,
22 when available, do not have any effect on the result.

23 Something interesting, too, is that the
24 result varied by industry. There's more of a negative
25 effect for financial firms than there is for just like

1 the retail industry, for example. So this could be
2 due to a strategic and sensitive component of the data
3 that the firms have got stolen.

4 So the effect of stricter disclosure laws
5 that are different in every state, as I mentioned, is
6 significant and negative. So on average, it decreases
7 the returns on the stock price by 17 basis points, so
8 this can be in a way thought of as a partial insurance
9 for the firms by knowing that if they have a privacy
10 breach disclosure, they're going to have to release it
11 to the market more quickly than in other states. So
12 this may seem that firms would actually spend more
13 time protecting themselves when there are stronger
14 disclosure requirements.

15 So in a similar manner, you find that this
16 effect is even stronger the day after the disclosure.
17 We're talking 70 basis points. So if a sample were
18 restricted to cyber attacks, because it seems to be,
19 like, the topic of this panel, instead of all privacy
20 breaches, all of our results that are mentioned -- and
21 you see that in the paper -- are stronger, like twice
22 as much of a negative effect on the release of a
23 privacy breach.

24 These results could actually be due to the
25 fact they are more sensitive information that are

1 coming out when you have a disclosure of a privacy
2 breach that is obtained through a cyber attack. To
3 give you an idea of how different privacy breaches and
4 even cyber attacks are, I ran a similar type of
5 analysis on different types of negative news to the
6 stock market. And what happened is only a analyst
7 downgrade would have a stronger effect on the stock
8 market -- on the stock price, sorry, of the firm. So
9 congressional hearings, copyright infringement, fraud,
10 industrial events, lawsuits, even product recalls do
11 not have as strong of an effect and most of the time
12 are completely insignificant.

13 So this is really, like, quickly what's in
14 the paper. You can find the paper online. And thank
15 you for giving me the time to talk about it.

16 MR. HO: And thank you, Sebastien, for that
17 insightful piece on the impact of data breaches on
18 firms.

19 Next, we're going to move over to Al, who
20 will be giving us his perspective on the impact of
21 data breaches on consumers.

22 2018 Identity Fraud Study:

23 Fraud Enters a New Era of Complexity

24 MR. PASCUAL: Thank you. So, first, I
25 wanted to thank the FTC for having me today. I'm

1 going to be sharing some research from Javelin's
2 Annual Identity Fraud Study as background. And
3 Javelin conducts a national study. We've conducted it
4 annually for nearly 15 years where we examine the
5 incidents of identity fraud affecting consumers.

6 As a definition, identity fraud is when
7 personally identifiable information is misused to
8 attain something of financial value. In essence, it
9 is financial fraud that's made possible through
10 identify theft. And for the sake of today's
11 conversation, I'm going to be talking a lot about the
12 relationship between fraud and data breaches.

13 That relationship is strong. It has
14 historically been strong, but fraud itself is
15 changing. The role that breaches are playing when it
16 comes to fraud is changing, and I think it demands a
17 change in the way that we deal with breaches and we
18 also deal with the protection of consumers' data and
19 consumers' accounts.

20 We've been following this space for a very
21 long time, the fraud space. 2017 stood out. 2017
22 was, in fact, a record year. More consumers than ever
23 before, at least as far back as we've been keeping
24 records, were affected by identity fraud, right, in
25 absolute terms and as a proportion of the population,

1 or at least U.S. consumers. That was a record.

2 The amount lost in 2017 was the highest
3 we've seen in the last four years. Now, these are
4 total losses associated with all cases of identity
5 fraud. It is inclusive of losses that consumers are
6 experiencing as well as the businesses where these
7 frauds took place. But a third piece of information
8 that I think speaks very highly of why we're seeing
9 some of these trends play out is that for the first
10 time, when we ask consumers who are affected by a data
11 breach who received a notification what kind of
12 information was lost, for the first time, we saw that
13 Social Security numbers were at the top of the list.
14 Historically, it's been credit cards and debit cards.

15 Now, we need to consider that there are 247
16 million U.S. consumers. There are 1.2 or so billion
17 cards in circulation. And, historically, cards have
18 been a high-profile target. It is typically pretty
19 easy to access data. Generally, it's poorly
20 protected, but the fact of the matter is consumers
21 were more likely in 2017 to be told your Social
22 Security number has been compromised than your card,
23 right, and that's saying something when most people
24 have about eight cards in their wallet.

25 Not only did it have a material effect on

1 the type of fraud we saw, but it's also having an
2 effect on the consumer psyche. The type of
3 information being compromised, the source of that
4 information, and that is also very meaningful. We'll
5 talk about that first, and then I'm going to move into
6 some trends around the fraud and the relationship
7 between breaches and fraud, how it's being
8 perpetrated.

9 But I wanted to start with the consumer
10 aspect. So when we're trying to measure the impact on
11 the consumer historically, you know, one of the first
12 questions has been -- well, I guess, show me the
13 money, right? You know, what's the financial impact
14 on the consumer?

15 Well, in 2017, the financial impact more
16 than doubled from the previous year. On average,
17 consumers paid out of pocket \$104, those who were
18 affected by fraud. Now, it may not seem like a lot,
19 but when you consider we had -- well, more consumers
20 than ever before, I think the total comes in somewhere
21 between \$1.5 and \$2 billion that consumers paid out of
22 pocket, so it's not an insignificant amount of money
23 that we're talking about.

24 And it's true that the median loss is
25 actually zero because many people experience card

1 fraud, but you have to imagine given the size of that
2 population and the fact that the median loss is zero,
3 how many outlier cases have to exist that pushed the
4 mean up that far in a single year? This is a function
5 of the change of the types of fraud that we're seeing
6 become quite popular, and so I'm going to dive into
7 how different fraud types are changing, but there is a
8 meaningful effect for many victims of fraud in actual
9 dollars and cents, right, so there is harm there that
10 we can measure financially.

11 When we talk about breaches, I think it's
12 important to consider that everyone in this room has
13 probably received a breach notification or seen a
14 notification in the news that indicated they may have
15 been affected by a breach. So 2017 was not unique in
16 that consumers generally had experienced breaches
17 before, right? This was not a new phenomenon for us
18 to get a breach notification, so why was it different?
19 Why has our common vernacular changed as consumers?
20 Why are we more concerned about cybersecurity? Why is
21 our mind-set changing?

22 Well, I think, first, you have to consider
23 the type of information that was compromised in 2017.
24 It was a bit different than historical, but on top of
25 that, I think what ended up happening in 2017 was that

1 there was a change in the consumer mind-set because we
2 did not have clear sight lines as consumers as to what
3 the breach meant for us.

4 Well, in the past, big breaches were
5 generally card breaches. Now, we did have, you know,
6 large breaches of Social Security numbers here, you
7 know, and there, so certainly there was OPM, there was
8 Anthem, but Equifax was unique in the number of
9 individuals that were affected and two other facts.

10 Number one, we have no control as consumers
11 over whether or not Equifax has or had our personal
12 information. Right, and that's true of all the credit
13 bureaus and a number of other companies as well, but
14 on top of that, that information that this company in
15 particular held had to do with our financial wellness,
16 so consumers were extremely concerned. They wanted to
17 know what does this breach mean for me.

18 So if you go back through the Google search
19 results and you look at the search index, what you'll
20 see is when the breach occurred, the search index goes
21 through the roof. People went online. They wanted to
22 know what does this mean for me. There was a lack of
23 understanding, a lack of awareness there despite the
24 fact that we've been breached so many times. Think
25 about the number of notifications, the number of times

1 your information has been breached in the last ten
2 years. You're not new to breaches as a consumer, but
3 consumers had more questions than they had answers
4 last year.

5 And we can see that there's an impact,
6 right, on how they view breaches and the steps that
7 organizations are taking to keep them safe. So we ask
8 a number of attitudinal questions around data breaches.
9 And one of the agreement statements that we have
10 within the survey is that data breach notifications
11 merely help organizations save face or meet their
12 legal requirements and do little to protect me. The
13 agreement with that statement grew considerably year
14 over year between 2016 and 2017.

15 Now, consider, again, your own personal
16 experience. When you're receiving a breach
17 notification, many of them look alike, right? They
18 include pretty basic information about details behind
19 the breach and information potentially about the
20 credit bureaus to contact, right, maybe even to
21 contact the FTC in the event of fraud, right, but
22 that's it. I mean, that's what we see time and time
23 again.

24 Meanwhile, that last slide shows that people
25 had a lot of questions, questions that were not being

1 answered despite getting those breach notifications
2 over and over again. So it would seem that consumers
3 do not feel as though the way that we respond to data
4 breaches, the way that organizations respond to data
5 breaches in notifying them is sufficient. They do not
6 believe it is sufficient, or at least that sentiment
7 is growing, and it has grown considerably. And I
8 think part of the reason why it has grown is because
9 consumers are more concerned about what a breach means
10 for their identity.

11 We also ask about in the study concern
12 around identity fraud, and concern around identity
13 fraud also grew considerably. Now, typically, these
14 are numbers that don't move very much year over year,
15 so this is extremely meaningful. Going back to the
16 earlier comment around the common vernacular, I think
17 as consumers we have a much more keen realization that
18 the information that's being compromised online,
19 right, in the digital space does have more severe
20 implications for our identity because we do so much
21 online and so do criminals, do so much online.

22 So when we see that our information is
23 breached and when we receive a notification, it
24 doesn't tell us enough about what that means for the
25 digital world where that information can and will be

1 misused, so we're starting to tie all these pieces
2 together as individuals, and we're seeing that
3 reflected in our data.

4 And the experiences around fraud kind of
5 back up that notion. It's not as though we're taking
6 a leap of faith as consumers. Fraud is just becoming
7 more prevalent, and we know, right, if you have been a
8 victim of a breach before, odds are your information
9 has been misused to commit fraud, so you know that
10 there's a connection there.

11 In this chart, what you'll see are two
12 different sets of bars. The blue bar is the fraud
13 rate for all consumers in any 12-month period, any
14 calendar year. The beige bar is the fraud rate for
15 consumers who were notified of a data breach. Now,
16 there's a strong correlation. There's always a strong
17 correlation every year. This is not causation
18 necessarily.

19 And there are a number of factors that push
20 that bar up and down, but the fact of the matter is
21 there is the relationship, it is very, very strong.
22 And if I included the data for consumers who did not
23 receive a notification, you'd see that the rate is
24 typically between 2 percent and 3 percent every year.
25 So there is a very, very clear relationship.

1 Now, in 2017, you may ask why did the rate
2 go down. Well, it's very simple. That number is a
3 function of the number of breach victims who
4 experienced fraud over the number of breach victims.
5 The denominator became very big in 2017. There were a
6 lot of breach victims who had sensitive information
7 compromised. Criminals simply couldn't use it all,
8 and that's why that number declined. The fact of the
9 matter is there is a strong relationship and we know
10 it, so we are more concerned.

11 So we talked about the consumers. I do want
12 to shift into how this information is being misused,
13 how it's manifesting, and I wanted to focus on, in
14 particular, a couple different types of fraud. The
15 first is account takeover. Account takeover is among
16 the most meaningful and insidious types of fraud for
17 both individuals and for organizations.

18 So what do we mean by account takeover?
19 Account takeover in this context is when a criminal
20 gains effective control of an account. They will do
21 that by changing contact information, by changing
22 passwords. Essentially separating you as an
23 individual from the organization that's servicing that
24 account. And this makes it extremely difficult for
25 that organization to ever provide that control of the

1 account back to you because they cannot discern the
2 difference between the legitimate consumer and the
3 criminal.

4 This kind of fraud has tripled. It's
5 tripled. Losses have grown considerably, and
6 incidents have grown considerably. Now, you may ask,
7 what does this have to do with data breaches. Well,
8 two things. First, criminals can leverage personally
9 identifiable information to gain access to personal
10 accounts. And, unfortunately, there are still
11 organizations that allow you to gain access to an
12 account with a Social Security number.

13 Tie that in with a bit of social
14 engineering, someone calls up the call center of an
15 organization with that Social Security number, and
16 they can typically get a customer service
17 representative to do a lot of things, including
18 providing access to the online account, resetting
19 passwords, effectively giving them a foot in the door
20 to gain control of an account, but it's not just the
21 more sensitive personal information. It's also
22 information like user names and passwords.

23 You wouldn't think generally, because we
24 place so much value on Social Security numbers, that a
25 user name and password is really valuable information,

1 but then think about how often you reuse a password.
2 Well, criminals know that, and so they breach
3 organizations. They take lists of user names and
4 passwords, and in an automated fashion, they will
5 basically use that list. They will take those user
6 names and passwords and ping sites of different
7 organizations -- banks, retailers, mobile network
8 operators, healthcare providers, insurers -- until
9 they find pairs that give them access to an account.

10 Breaches are contributing to this trend
11 along with, in essence, very poor authentication
12 controls. And I know Marc talked about it just a bit,
13 but the fact of the matter is weak authentication is
14 prolific, it's ubiquitous. We actually conduct
15 another study on authentication, and what we define as
16 strong authentication among businesses that have a
17 digital property, adoption's in the single digits.
18 Most organizations rely on a user name and password,
19 and criminals use that to advantage after breaching
20 information like user names and passwords.

21 And the other type of fraud I think that's
22 worth mentioning in the context of breaches is new
23 account fraud. For folks who work in financial
24 services or related industries, you may view this as
25 application fraud, but in essence it's where a

1 criminal takes personally identifying information and
2 opens an account as though they were the victim. This
3 type of fraud is also on the rise. This is a lot
4 easier to connect, I think, in our minds with a data
5 breach. We understand that personal information is
6 compromised; they put it into a form online; they've
7 opened an account.

8 But what I think is more interesting here
9 and is much more problematic for the consumer is that
10 the fraud itself is changing. The reason they're
11 opening accounts, using information that's compromised
12 in a breach, is changing. So you'll notice that the
13 incident rate grows, but the amount lost does not. So
14 we may view that as a good thing inherently. Less
15 money has been lost, but there's a reason why.

16 More consumers are being affected by this
17 type of fraud, but less money is being lost. And
18 that's because criminals are opening accounts that in
19 and of themselves have no monetary value. So what
20 you'll see here are the number of existing account
21 fraud victims, so consumers who have had an existing
22 account -- it could be a debit card account, it could
23 be credit cards, it could be a loan account, it could
24 be an investment account, the number of existing
25 account fraud victims who also had a new account

1 opened using their personal information.

2 Criminals value the complete identity of an
3 individual. And we're at a point where the complete
4 identity of pretty much any person in the United
5 States can be found online. And what criminals use
6 that information for is to get paid, right? So they
7 have information that gives them access to an account
8 where you may have your retirement, but they also have
9 information they can use to open a new account.

10 Why would they do that? Well, banks check,
11 organizations check, to see where money is being sent.
12 And this is just an example. There are many reasons
13 why they would, but consider if a criminal has access
14 to your account, right, that has your retirement in it
15 and they want to move tens of thousands of dollars,
16 there are going to be pretty strong checks in place.

17 And what banks and other institutions will
18 do is they will verify ownership of the destination
19 account. And there are third-party services that
20 provide that verification. Criminals know that, so
21 armed with all of your personal information, they will
22 open up a new account. It will have information that
23 matches the compromised account. So when banks go to
24 verify the destination account, it verifies and money
25 is moved.

1 And it doesn't have to be something as grand
2 or as sinister as draining a retirement account. It
3 could be something as simple as opening a Paypal
4 account to monetize a stolen credit card, to monetize
5 a stolen checking account. We've seen this kind of
6 fraud grow considerably, and criminals are
7 opportunistic. They have all the information they
8 need. Authentication controls generally are weak, and
9 identity verification is also generally pretty weak.

10 So the long and short is that there is a
11 very strong relationship between breaches and fraud,
12 and that has not necessarily changed, but what has
13 changed is the nature of the data that's being lost
14 and how that information is being misused. And for
15 consumers, we recognize that at least on a
16 subconscious level, but many of us are also being
17 affected. There are steps that organizations can take
18 to change this paradigm.

19 Unfortunately, though, not all of them are
20 regulated in the same way. There is nothing that
21 unifies their approach in keeping consumers safe,
22 whether that comes to data security or protecting
23 existing accounts or identities. And as such, we have
24 seen fraud respond and take advantage. And this trend
25 will continue until organizations improve their

1 security postures, and we are all going to suffer
2 until that comes. Thank you.

3 MR. LUPPINO: Thank you, Al. Thank you for
4 all your insights on data breaches and resultant fraud
5 that consumers experience.

6 I'll now ask does anyone have any followup
7 comments, either on your own presentation or one of
8 the presentations of the other panelists?

9 (No response.)

10 MR. LUPPINO: Okay.

11 MR. HO: So maybe we can start with a
12 question. I couldn't help but compare Al's research
13 with Sebastien's. And, so, you know, if Sebastien's
14 research suggests that firms can or do essentially
15 offset the negative consequences of a breach and, you
16 know, that suggests perhaps they're not internalizing
17 the cost of a breach and Al's research, to me, seems
18 to suggest that consumers are experiencing harms
19 associated with data breaches, so if, you know, these
20 two situations or research are correct, then, you
21 know, is there essentially a market failure? And I'd
22 be interested to hear the panelists' thoughts.

23 MR. PASCUAL: Well, I think, you know, you
24 have to consider Sebastien's comments when you start
25 talking about market failure. It does not seem as

1 though there are the proper incentives in place for
2 organizations to change the way they do business.
3 And, you know, as a result, we continue to see
4 breaches occur. And it's not as though criminals are
5 incredibly inventive. They do the same thing over and
6 over again, moving from organization to organization.
7 And, I mean, that's what keeps the folks at Verizon,
8 I'm sure, very busy.

9 MR. SPITLER: Yeah, certainly with the
10 financially motivated ones. You know, you have the
11 ability to be opportunistic because it's not
12 necessarily "I need this set of Social Security
13 numbers" or "I need this set of payment cards,"
14 whereas the ones that are looking more for trade
15 secrets, then it's going to be a lot more targeted.
16 But, yeah, as you just said, so they don't necessarily
17 need to evolve so much. It's more like, oh, well,
18 that guy raised the bar up to here. I still have a
19 lot of low-hanging fruit that I'm able to reap, and I
20 can pull that and still make money.

21 MR. PASCUAL: As far as the organizations
22 that are being affected, surely governments are
23 affected. Nonprofit organizations are affected. But
24 for businesses, I mean, what we've historically seen
25 in our data is when they think about security, you

1 know, the top motivating factors for them are whether
2 or not it's cheap and easy, right? When they're
3 making decisions about what they're using, cheap and
4 easy tend to, you know, go right to the top of the
5 list, and that seems to be incompatible with
6 protecting, you know, the needs of protecting the data
7 that they have, whether it's their own or consumers.

8 MR. GAY: So at the time when I was doing my
9 research, something was emerging, like the
10 relationship with insurance on data breaches. And you
11 could see a pattern where there was actually a
12 mismatch between people's insurance, like pure
13 insurance against data breaches, and also the amount
14 of media that they were using in order to, like,
15 alleviate any effect of data breaches.

16 So, now, I don't know if both of you guys
17 are aware about the more, like, formed market for
18 cyber insurance, for example. Because before there
19 was a real mismatch. When doing that research, people
20 didn't know what they were insuring themselves
21 against, and then insurance companies actually didn't
22 know how to price it properly.

23 MR. PASCUAL: And I think that's going to be
24 one of the forces that actually improves security
25 postures because insurance companies are and will be

1 more likely to demand better security among the
2 companies they are insuring. Obviously, there's no
3 absolute security, but if you're going to indemnify an
4 organization, you want to be sure, at least to some
5 extent, that the risk is as low as you can manage.

6 MR. LUPPINO: Do you see in the data the
7 same firms experiencing the same types of breaches
8 over time? And based on your research, what evidence
9 do you see of learning in the market by firms and
10 consumers?

11 MR. SPITLER: Yeah, so I don't know if
12 you're referring to the exact same organization --

13 MR. LUPPINO: Yes.

14 MR. SPITLER: -- the exact same breach? I'm
15 sure that happens. The interesting thing with my data
16 set is the majority of it I actually don't know who
17 the victim is. So, for example, when the Secret
18 Service provides me information on breaches that
19 they've responded to, I get demographic information
20 and I get, you know, obviously the tactics used, et
21 cetera, but I don't get who the end victim was. And
22 we don't need that for us to do our work with it, and
23 that allows us to keep the anonymity of it.

24 I'm hopeful, you know, that in a lot of
25 these cases some of these breaches -- again, they go

1 to things that aren't necessarily earth-shattering.
2 There are breaches that occur that it's a fairly
3 straightforward and simple fix that could have at
4 least broken that particular event chain. There's
5 nothing to say that they can't circle back and try a
6 new avenue, so I don't know.

7 I'm hopeful because a lot of times we're not
8 seeing what I would call highly sophisticated attacks.
9 A lot of these are very opportunistic. It's going
10 after weaker configurations, weak authentication
11 schemes, so there's a higher chance that they can
12 learn from their mistakes. And I'm hoping that what
13 my report does is allow people to learn from the other
14 guy's mistakes, so, again, but I don't have any sort
15 of hard data percentages on that.

16 MR. HO: I want to switch gears a little bit
17 and ask Al a question about one of his slides. It
18 seemed quite interesting to me that you pointed out
19 that there's a cynicism with consumers about data
20 breach notification. And so, that, to me, seems a bit
21 counterintuitive, but maybe you can sort of elaborate
22 as to sort of what you attribute to this cynicism and,
23 you know, how if -- I guess how would you improve data
24 breach notifications if this really is the case with
25 consumers.

1 MR. PASCUAL: So I think part of the
2 challenge is that we've all gotten, to my earlier
3 point, notifications before. The notifications we
4 continue to get look very much like the old
5 notifications. And in and of themselves, there's just
6 -- there's no longer any remedial value for the
7 consumer in those. They're not going to learn
8 anything new by reading the newest breach
9 notification. All they're going to learn is that they
10 were breached, in essence. I don't think they even
11 care what happened, right? In fact, there may be so
12 much spin, you know, after the breach is announced,
13 that they have a hard time making out what actually
14 happened in the first place.

15 The challenge ultimately is that for
16 consumers, we are more aware of fraud, we're not being
17 provided with anything in the event of a breach that
18 makes us feel as though we're going to be safer. And,
19 so, you're getting a piece of paper, and how many
20 pieces of mail do we all still get, right? It feels
21 very kind of perfunctory, something that has to be
22 sent to us but doesn't give us anything.

23 I don't know if changing a piece of paper is
24 going to make consumers feel much better. I think
25 it's more about providing something to them that makes

1 them feel as though they will be safer. At the same
2 time, you know, if breaches continue to occur in much
3 the same way from organization to organization, the
4 kind of information continues to be lost everywhere
5 and consumers don't feel like they have a lot of
6 control. Giving them all the identity protection in
7 the world still isn't going to totally undo their
8 cynicism, right, because a problem still exists. And
9 what am I going to do after I have five different
10 identity protection plans? I'm probably going to be
11 pretty cynical about that, too.

12 MR. HO: Anyone else have any comments on
13 that?

14 MR. SPITLER: I would probably look at it
15 kind of as from a consumer, not necessarily from the
16 researcher, but, yeah, kind of what you said, it's
17 almost like, oh, yet another form that I'm getting,
18 and I can see that you've given me a year credit
19 check. Okay, but there's nothing in here that shows
20 me or gives me any sort of confidence that you can
21 understand why it happened in the first place, that
22 you have controls that are -- what's going to be
23 different from you and from the people that work in
24 your -- your security practitioners that are going to
25 prevent me from getting another one of these pieces of

1 paper one year, two year, three years from now? So
2 you don't really get that kind of warm and fuzzy
3 feeling from them.

4 It's just more along the lines of, oh, they
5 have to do this, so here's my obligatory piece of
6 paper from them, but I'm not getting any good sense
7 of, yep, we know what happened, we've made steps, and,
8 you know, this type of thing. You don't get really a
9 good -- it's not really confident that it's just not
10 going to happen again.

11 MR. PASCUAL: A piece of paper does not tell
12 you what the risk is to you. And we cannot possibly
13 expect that every piece of paper we send out to an
14 individual is going to be customized to their risks.
15 And it feels almost like something that needs to be
16 solved, and digital is part of the problem, but I
17 think it's also part of the solution.

18 You know, having an understanding of who the
19 consumer is, where they do business, what that breach
20 could translate into ultimately as far as fraud is
21 concerned and providing them with real solutions for
22 their digital life, that is not a piece of paper.
23 That's something totally different. Right now, people
24 pay for that kind of thing. And, again, not to say
25 identity protection is a solution we need to be

1 throwing on people, but I don't think you can improve
2 the notification enough to undo the cynicism.

3 MR. GAY: And back to the research that I've
4 done over that sample, 2005 to 2014 data, the issue is
5 also that the states have different requirements, so
6 you end up with the key question, like which one takes
7 precedent. If you have a multistate disclosure issue,
8 then questions get raised. I don't even know the
9 answer to that, and I think it's usually very
10 contentious.

11 In terms of breach fatigue, that's also
12 something that you could find in the sample. Early
13 on, when there were not a lot of privacy breaches, the
14 effect of those breaches were higher, like I gave you
15 the average number, that was 24 basis points, but it
16 could go as high as, like, 60 or 70 basis points in
17 the early years. Whereas the closer you get to 2010
18 in the sample, then the smaller that particular
19 effect. So this is also an interesting trait, I
20 think, there are more and more breaches.

21 MR. LUPPINO: So piggybacking on this, you
22 know, if consumers are becoming more cynical about
23 things like breach notifications from companies, do
24 you see changes in their behavior, or are they
25 becoming more -- do you see anything as far as they're

1 becoming more proactive about their data security or
2 other kind of changes to their market behavior?

3 MR. PASCUAL: We track behaviors pre- and
4 post-fraud, for example. We noticed a rather
5 disconcerting trend that two or three years ago,
6 historically, when people experienced fraud, one of
7 the first things they did was, you know, they shut off
8 all their paper statements and they went online
9 because they just didn't want things going through the
10 mail. Starting a few years ago, it kind of went the
11 other way, where people, after they experienced fraud,
12 would stop banking online, like, they'd stop using
13 online services. They had a fear that that's where
14 the risk is.

15 And that's problematic because digital
16 allows individuals to do so much. I mean, obviously,
17 it obviously allows businesses to reach a wider
18 population. But, you know, that being said, we tend
19 to be very reactive as consumers, so post-fraud we see
20 people do things like get identity protection. We see
21 them, you know, step up their security posture. They
22 take advantage of two-factor authentication.

23 If you use Gmail, I mean, Google has come
24 out and said less than 10 percent of all Gmail users
25 use two-factor authentication. I mean, if consumers

1 were really demonstrating some of the concern that we
2 see in the data in their security behaviors, I think
3 the adoption of two-factor authentication with Gmail
4 and other online services just generally would be
5 higher. It's not.

6 People are concerned. I think there's just
7 a disconnect between knowing what they should be
8 doing, right, and what they're actually doing. So we
9 see them do things only after they experience fraud,
10 but beforehand, it's kind of -- there's no rhyme or
11 reason for them.

12 And I think that speaks to the fact that
13 they need more education. They need more
14 understanding of what the implications are for them
15 and what they can actually do. But as our digital
16 life continues to expand, that can almost seem, like,
17 overwhelming. We have a unlimited number of digital
18 accounts. If you have to protect your entire life,
19 that's a tall order.

20 MR. HO: Okay. So, actually piggybacking
21 on that, so if individuals only respond after
22 experiencing a breach, right, you can also think about
23 in terms of firm responses. So going to Sebastien's
24 research about market, is it possible that the market
25 is just confident that firms will take appropriate

1 measures to eliminate the vulnerabilities discovered
2 by a breach?

3 MR. GAY: So you know I cannot answer that,
4 right? So based on my research, what you find,
5 though, is there's a high likelihood that firms have a
6 store of, like, positive news that they hold on. So I
7 don't say it's something they have to release, but it
8 could be something as announcing a joint venture. It
9 could be something as simple as the nomination of
10 someone buying a particular type of widget that it
11 could wait a month or so. And you see that in the
12 data, too.

13 So if you look and do a word analysis, you
14 notice that those are the types of news that come out
15 or expectations about future earnings most of the
16 time. So this is something that is done. Whether or
17 not it is done on purpose, obviously there's no answer
18 to that, but it is just surprising that on average
19 this is the sort of result that you would find.

20 MR. HO: Did anyone have followup?

21 And, Sebastien, this is actually a question
22 from the audience. It's a followup to your research.
23 What breaches are not represented in the news that you
24 have found that you discuss in your paper? And, you
25 know, is there a trend by size or by industry?

1 MR. GAY: So I'm going to answer the second
2 part. It was already difficult with the sample to
3 have size. I mean, less than, like, 50 percent of the
4 sample had actual numbers, even estimated numbers. So
5 most of those breaches, I think currently it is more
6 often than not that we get an idea of how many people
7 have been breached. So for some breaches that were
8 not reported in the news, it was mainly a loss of like
9 a laptop, for example. Someone forgot, like, a laptop
10 on a train.

11 And that was reported on people's websites
12 but it didn't make it as a news event, and I cannot
13 recall the company, but that was that type of issue,
14 which the laptop contained personal information for
15 the people that were working at that company. It was
16 a member of HR, but perhaps because no one knows
17 whether or not it was breached, there was no report in
18 the news.

19 MR. SPITLER: I can touch on that a little
20 bit just from kind of the data that we get in. When
21 you look at -- you know, we have a category of lost
22 and stolen assets. And the two industries that are
23 very prominent in that are healthcare and public
24 sector. And we go out of our way in the report to
25 say, hey, we are not saying that I think healthcare

1 workers and people that work in state, federal, and
2 local governments lose their laptops more than anybody
3 else, but they have to disclose it when they do.

4 And, so, we have a lot of data on industries
5 that have to disclose things like that. So that's why
6 you'll see such a high level of -- you know, it is so
7 easy for us to find healthcare breaches, just even
8 using open-source methods. We don't have to worry
9 about some of our other partners providing it to us.
10 We do similar things when we look out there and we
11 look for publicly disclosed data breaches. And that
12 is part of one of the data sets that goes into the
13 full report. So there's a lot of that is tied to what
14 industry and what type of data.

15 MR. LUPPINO: Here's a question from the
16 audience. For the Javelin estimates of consumer costs
17 from breaches, who pays the costs? Is it only
18 consumer costs, or are some or all the costs borne by
19 firms?

20 MR. PASCUAL: So the larger number I shared,
21 I believe it was 16.8 billion, that is inclusive of
22 all losses. Now, consumer costs are a portion of
23 that, and there are some costs that are not
24 necessarily reflected in the larger numbers. So
25 consider that 16.8 billion is really direct losses.

1 For consumers, you have both direct losses, cases
2 where they reported fraud and an organization said no,
3 you pay it, because that can happen despite federal
4 regulations. You know, there can be cases of fraud,
5 especially new account fraud, where the consumer
6 cannot, in essence, prove that they were not
7 responsible. Right, that burden of proof practically
8 falls on the victim. But on top of that, I think
9 that's a good example to use.

10 In the case of new account fraud, I may need
11 to file a police report, so I take time off work. I
12 may need to get a lawyer. And, so, I have additional
13 costs beyond what the fraudster actually got away
14 with, and those, you know, can be borne and typically
15 are borne by the consumer. And that's still, you
16 know, a billion-dollar-plus problem.

17 MR. HO: So we've been talking a lot about
18 the cost of data breaches. And I want to move over to
19 the attack vectors for data breaches for a moment.
20 And this is in part a question from the audience, but
21 I'll sort of add a little bit to it as well. So, you
22 know, first, we've seen this increase -- you know,
23 from Verizon's report, we've seen this increase in
24 social engineering. And, so, I'd be interested in
25 hearing how phishing and social engineering attacks

1 have become -- whether or not they've become more
2 sophisticated over time and, if so, sort of how.

3 And then tacking onto that the audience
4 question, has Verizon observed any measurable
5 differences in the frequency of attacks or use of
6 particular attack vectors when accounting for
7 particular operating systems or server types?

8 MR. SPITLER: Okay. So the first question
9 kind of regarding phishing and social engineering, and
10 when we have social engineering involved, probably
11 90-some percent of the time it's actually phishing.
12 And the reason for that is it works. So we have data
13 from multiple security awareness training vendors. So
14 you hire them. They'll actually phish your users, and
15 just tell you who took the bait, who didn't, how good
16 are you doing, are you doing better than the last time
17 we did this, et cetera, et cetera.

18 And it was about a 7 percent hit rate for
19 any -- so we sent a campaign out. Of all those emails
20 that were sent out, 7 percent of them someone will
21 take the bait, so it works. And it's also very easy
22 to do. It's a very low-cost, very efficient style of
23 attack. And, you know, if it doesn't work, oh, well.
24 You'll just try to phish the next person, right?

25 And, so, that's why we continue to see that

1 coming up. It's a very good way of -- and we also
2 take a look at how networks, you know, are kind of set
3 up, right? You know, we have some web servers over
4 here, and they get direct interaction from anybody on
5 the internet. Well, how could I interact with
6 someone's workstation? Well, I can do that via email,
7 you know, and so it's a great way to try to get a
8 foothold into a corporate network.

9 Now, as far as level of sophistication, it
10 kind of runs -- it runs the gamut. You're always
11 going to see the just throw it out there, the actual
12 just phishing. Let's see who will actually take this
13 bait. You know, you will see targeted phishing
14 attacks. It's called spear-phishing is kind of the
15 terminology for it. And that's when you're not just
16 sending it out to anybody, but you're sending it out
17 to a specific person because of the rule that they
18 have. You've probably done some gathering of intel
19 via their LinkedIn -- you know, their LinkedIn pages
20 or other social media.

21 So it allows you to kind of craft a
22 narrative to make it a higher likelihood that they're
23 going to click that. Hey, oh, I think you're going to
24 go to that blank conference. Here's a PDF, you know,
25 of the agenda or some afterparties or something like

1 that. It's topical. It's not out of the blue. And
2 it's something that, you know, you'll go ahead and
3 click on.

4 And then the second part was in regards
5 to --

6 MR. HO: Just sort of the measurable
7 difference, if you've seen measurable differences in
8 the frequency of the attacks.

9 MR. SPITLER: Oh, based on operating system
10 and things like that? Often, we don't get that level
11 of detail. Now, there are certain -- you know,
12 there's certain -- you know, I'm not going to get into
13 any sort of this operating system is better than or
14 worse than that operating system. Frequently what we
15 see is not necessarily weaknesses in the way that the
16 underlying system code was developed, but we see
17 weaknesses in how people have implemented that in
18 their environment. So, you know, a lot of times, it
19 is a weak configuration, not necessarily a software-
20 coded bug, which would be, you know, specific on one
21 OS versus the other.

22 You know, there are certain types of
23 vulnerabilities that might be exploited more often
24 than others, and we've seen things like that. You
25 know, browser-based vulnerabilities are ones that, you

1 know, if you are -- those are ones that attackers like
2 to go after because they've had good success with that
3 in the past. And, again, it gets you onto a
4 particular device in the network.

5 So we will see some, you know, some
6 weaknesses exploited with more regularity than others,
7 but it is not a, you know, this OS versus that OS or
8 this type of web server versus that type of web
9 server, at least not to where I can provide any sort
10 of guidance or hard numbers on that.

11 MR. LUPPINO: This is another question from
12 the audience. To what extent is there evidence that
13 those who steal data in large sophisticated breaches
14 with Social Security numbers and full identity data,
15 how do they monetize that day-to-day? Do they do it
16 gradually, or, I mean, do they try to monetize it
17 immediately? Do we have a sense of that?

18 MR. PASCUAL: Generally, they fall into a
19 couple camps, right? You have cases where data is
20 compromised and that individual organization looks
21 simply to sell the data, right? They have no desire
22 to commit fraud in any way, shape, or form. They're
23 going to realize values by selling it on, you know,
24 the open market. So whether that's forms on the deep
25 web or on the dark web or wherever.

1 They may do some testing of that
2 information. So they'll take -- let's say they get a
3 list of user names and passwords. They'll test them
4 at big banks, right, and, you know, they'll see how
5 much money is in those accounts. In the accounts
6 where there's weak authentication and plenty of money,
7 they will price those credentials higher than they
8 will other credentials.

9 Same thing with credit cards, right, higher
10 limit versus lower limit cards. Higher limit cards
11 are worth more. Lower limit cards are worth less.
12 They'll even do things like package them up by zip
13 code because they know that banks and credit card
14 issuers will do verifications of, you know, where the
15 cards are used relative to the zip codes of the
16 owners. And, so, they'll do additional steps to make
17 the data more valuable, right, to different criminals.

18 So you have that population, and then you
19 have those who compromise the information to misuse it
20 to and actually commit fraud. Those tend to be more
21 vertically integrated organizations, so they have the
22 capability to both glean information and then to put
23 it into use, whether that's opening new accounts
24 online or even -- it's less popular today because of
25 EMV chip cards, but, you know, take card data, put it

1 on what they call white plastic, which is just kind of
2 like blank cards or gift cards, and go to the streets
3 and start using it.

4 But you tend to see more breaches are
5 committed -- the theft of personal information is more
6 likely to be committed by organizations that are not
7 planning to commit fraud. It's generally very
8 different skill sets, but you do have vertically
9 integrated organizations who will do all of it.

10 MR. LUPPINO: Thank you.

11 MR. HO: Okay. So I'd like to conclude with
12 one final question. And I'll try to combine some of
13 the audience questions with it. So we've been doing a
14 bit of discussing about the current trends related to
15 data breaches, but I think we'd love to hear what your
16 guys' thoughts are about the future of data breaches,
17 what they look like, or what you see them looking
18 like, you know, like five years down the line.

19 And, then, you know, on top of that, what
20 would be your number one advice to firms and
21 businesses for how to avoid breaches or protect
22 themselves?

23 MR. PASCUAL: So I think from my
24 perspective, breaches will continue. I think it's not
25 just going to be the personally identifiable

1 information. It's going to be anything that's not
2 nailed down, including biometric data, right, as that
3 becomes, you know, more often used for things like
4 identification and authentication. We'll see, I
5 think, a bit of a shift in tactics depending on how
6 well that data is being protected. So you'll see
7 organizations over time increasingly protect data with
8 encryption and tokenization.

9 And I don't think that wholly dissuades
10 criminals, right, so making that data, you know,
11 harder to misuse -- now they may target organizations
12 that have yet to protect data in that way more often,
13 right, rather than going after the harder target, but
14 there's always the opportunity to do things like take
15 advantage of user privileges and get access to data
16 within the network, right, that's supposedly
17 encrypted. So, you know, there are going to be steps
18 that are going to be put in place to protect our
19 information. It's not a panacea. But because
20 information always has value, personal information, as
21 well as IP, you know, business bank account
22 information, it's all of value, so breaches are not
23 going to go anywhere. This is going to continue to be
24 a problem.

25 I mean, I think you'll even see in other

1 places like Europe where more strict data privacy
2 regulations have been put in place that breaches don't
3 go away in totality. I think you'll probably see
4 fewer consumer-level breaches, but, you know, more
5 targeted attacks to get, you know, information that an
6 organization really wants to have, whether it's
7 espionage, corporate espionage, I don't think, you
8 know, something like GDPR is going to necessarily be
9 the most effective tool for moving the gauge and
10 getting businesses to better protect that information.

11 MR. HO: Anyone else?

12 MR. SPITLER: Okay, so, crystal ball, I am
13 hopeful that some of the things that we are putting
14 into place to make it harder to monetize stolen
15 payment card data, so, you know, we're still going to
16 have these breaches, but in reality the whole story
17 doesn't stop there. Granted, your work, it's what
18 happens after the breach. How are they going to make
19 money? How can we just -- this is kind of our
20 economics and how do we defend against them?

21 And then from this point, this is their
22 economics and how do we ruin this or how do we make it
23 a lot harder, like most notably with card-present
24 fraud. So he talked about, you know, being able to
25 clone cards, white plastic, things like that. If we

1 can reduce the effectiveness of that, that's going to
2 have to cause them to change their plans a little bit.
3 I could see that then putting a higher value on
4 personal information to do tax type fraud, the account
5 takeover, new-account-type fraud, if they're not
6 making the same return on their investment that they
7 were with stolen payment cards.

8 And, also, some of the monetizable events
9 that don't necessarily require a data breach. So are
10 they going to -- you know, a lot of times, things
11 aren't new, it's just kind of nuanced. So are we
12 going to have other different styles of kind of
13 ransomware type of attacks where they're going and
14 they're holding the utility and the availability of
15 something to be able to make a buck? So I'm thinking
16 that might be the way that they would go.

17 MR. GAY: Just I can only highlight
18 obviously what was in the paper, but the idea is a
19 good look at the disclosure laws by state would be a
20 thing to think about and also looking at the mechanism
21 that firms have in order to, like, attenuate the
22 impact of privacy breaches would also be something
23 that at a time I was advocating.

24 MR. HO: Well, with that, I'd like to thank
25 our presenters for their thoughtful comments on these

1 very real and impactful issues.

2 With that, we're going to be breaking for
3 lunch. There's a cafeteria located on this floor.
4 Please remember that if you leave the building for any
5 reason, you'll have to go back through security, so
6 please plan accordingly. And we will recommence after
7 lunch at 1:00 p.m. Thank you.

8 (Applause.)

9 (Recess for lunch.)

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 INCENTIVES TO INVEST IN DATA SECURITY

2 MS. JILLSON: Welcome back from lunch. Our
3 first panel discussion this afternoon will address
4 incentives to invest in data security. And we are
5 fortunate to have with us today five panelists who
6 have thought a lot about this topic. First, my name
7 is Elisa Jillson. I'm an attorney in the FTC's
8 Division of Privacy and Identity Protection.

9 Next to me is my comoderator, Mike LeGower,
10 who is an economist with the FTC's Bureau of
11 Economics. Our first panelist is Lawrence A. Gordon,
12 who is the EY Alumni Professor of Managerial
13 Accounting and Information Assurance at the Robert H.
14 Smith School of Business, University of Maryland,
15 College Park. Dr. Gordon is the author of the Gordon-
16 Loeb model, which provides an economic framework for
17 deriving an organization's level of cybersecurity
18 investment, and he will be describing that model
19 today.

20 Next to him is Matthew P. McCabe, the Senior
21 Vice President and Assistant General Counsel on Cyber
22 Policy for the insurance broking and risk management
23 firm, Marsh.

24 Beside him is Tyler Moore, the Tandy
25 Associate Professor of Cyber Security at the

1 University of Tulsa. And next to him is Sasha
2 Romanosky, who is a Policy Researcher for Rand
3 Corporation.

4 And, finally, we have Matthew Sharp, the
5 Chief Information Security Officer at Logicworks.
6 Thank you all for being here.

7 And for the audience, if you have questions
8 during the discussion, please feel free to write them
9 down on your question cards and flag Ryan or Mohamad
10 and they will collect your cards and bring them to the
11 front.

12 Now, this morning we heard some
13 presentations on the impact of data breaches, and
14 presenters discussed whether there's a market failure
15 in security resulting from misaligned incentives,
16 where companies guard data but it's consumers who bear
17 some or many of the costs of breaches of their
18 personal information. To think through this problem
19 of incentives, we'd like to take a look at current
20 incentives to invest in security.

21 So in this slide, there is a list of
22 incentives. And, so, what I'd like to do, panelists,
23 is to go down the panel and ask each of you if you had
24 to name the number one incentive to invest in
25 security, the most important incentive on this list or

1 not shown on this list, what would it be and why do
2 you think that's the case? And why don't we start at
3 the very end of the panel with Matt.

4 MR. MCCABE: Sure. Thanks, Elisa and thanks
5 to FTC for having us up. Well, I'm in the private
6 sector. And I have served in a capacity in a number
7 of different organizations and also previously in two
8 of the premier cybersecurity consulting firms in the
9 country. The conversation or my opinions are probably
10 biased by the opportunity to sit in closed-room --
11 closed-door sessions with CISOs where oftentimes I'm
12 looking to learn from the guys who, you know, have the
13 most, I'll say, street cred, if you will, the guys
14 that are leading the largest programs in the country.

15 And pretty predominantly, what I've been
16 coached to do and what I've made a career of doing is
17 starting with value creation, so competitive advantage
18 or customer demand seems to be the two that would be
19 my preferred option. However, not all security
20 investments are, you know, easily framed in those
21 contexts.

22 MS. JILLSON: And when you say competitive
23 advantage, you know, oftentimes we think of security
24 in terms of a cost center. So how do you reconcile
25 kind of that received wisdom with the notion of

1 security as actually an advantage in the marketplace?

2 MR. MCCABE: Sure. There's a number of
3 firms and it really depends on your business model,
4 but for example, at my current employer and these are
5 my opinions, not necessarily representing the opinions
6 of my employer, we have the opportunity to build a
7 value-creating or revenue-generating service offering.
8 So, for example, we have built a data loss prevention
9 service that actually expands revenues.

10 But there are other companies in -- many of
11 them are our customers, where they're inspiring
12 purchases in their organizations by differentiating on
13 their ability to protect customer information, so, you
14 know, organizations out there that provide or support
15 fintech offerings or healthtech or regtech. Many of
16 the technology-driven organizations that are looking
17 to disrupt industries often have the ability to
18 differentiate, and the way -- one of the ways that
19 they do that is by making sure that they can inspire
20 confidence in their customers, be they consumers or
21 B2B purchases, that they're going to value and treat
22 the confidentiality of information as, you know, an
23 important part of their business model.

24 MS. JILLSON: That particularly makes sense
25 where an obvious feature of the product is security,

1 so if it's a cloud provider or let's say it's a
2 manufacturer of a home security system. So security
3 is kind of at the fore of what consumers or customers
4 are looking for. Do you think that that holds true
5 where security is not such an obvious feature of a
6 product when a customer is buying shoes or a business
7 customer is buying office furniture?

8 MR. MCCABE: Yeah, I think that there's some
9 validity to the emotional responses in management that
10 happen in organizations that do sell things to
11 consumers. For example, you mentioned shoes. In my
12 background, I worked for a shoe manufacturer, so I
13 have a little bit of insight there. And, you know, no
14 executive team wants to be distracted by a major data
15 breach, and no executive team wants to lose the
16 opportunity to grow revenues because consumers don't
17 believe that their information is protected.

18 I think one of the panels earlier seems to
19 indicate, at least from a market cap perspective, that
20 that's not happening and that consumers, in fact,
21 don't behave consistent with their best interests.
22 However, that doesn't necessarily mean the dissent in
23 management teams accurately reflects that reality.

24 MS. JILLSON: Sasha?

25 MR. ROMANOSKY: Hello.

1 MS. JILLSON: Going back to this slide. If
2 you had to name the number one incentive on or off the
3 slide, what would it be?

4 MR. ROMANOSKY: I think it's a great slide,
5 first of all. And I think the incentives that you've
6 listed here are pretty super. And I think the
7 exercise of ranking them is interesting, and I think
8 as researchers what we would love most is to be able
9 to understand the marginal effectiveness of each one
10 of these.

11 You know, I look at them, and for each one,
12 I think we could have -- you know, we could spend the
13 whole day discussing it. If we look at consumer trust
14 and reputation, it's not really clear to me that there
15 really is an effect of reputation. I'm not even
16 really sure what reputation is, for example.

17 I think what people mostly mean is just
18 sales. And, so, if we think that, you know, there's a
19 loss of reputation, I think what most people interpret
20 that as just sales.

21 We heard from the panel this morning that
22 there was a loss in stock market price because of data
23 breaches. I think there's also a larger body of work
24 that suggests that, in fact, there is no effect from
25 data breaches, and if there is, it's a very short-term

1 effect and then disappears after time.

2 The story of ex ante compliance and ex post
3 liability, I think, is fantastic. I think there is --
4 there's a whole world of -- a body of literature on
5 law and economics that talks about the benefits and
6 limitations of each one of these and how can they be
7 best applied, especially in situations like data
8 breaches and privacy violations.

9 So, for example, ex ante compliance is
10 useful when the inputs are strongly correlated with
11 the outputs. So if we really believe that certain
12 kinds of security controls will reduce the harms or
13 reduce data breaches, then compliance is something
14 that we should try and promote more and more.

15 Also useful when the injurers are known --
16 or, sorry, when the injurers are unknown. If we don't
17 really have a good handle on who is causing identity
18 theft, where the breaches came from, yet there's some
19 amount of consumer harm kind of underlaying the
20 community, ex ante compliance is good. Ex post
21 liability, very clear when the harms are very
22 quantifiable and there's property damage. When
23 there's personal injury, and when the injurer is
24 known, then you can bring actions against the company
25 and recover whatever losses.

1 The ex ante compliance, better when the
2 state has more information about the kinds of harm
3 relative to the firms. The firms don't -- themselves
4 don't really collect information about which consumers
5 or employees are harmed in different kinds of way, but
6 the state, so for example, FTC or a regulator, has
7 broader information about overall population that
8 suffers some kinds of harm. Ex ante compliance can be
9 very useful.

10 If the harms occur long after the accident
11 has occurred, for example, if that continuity, if that
12 correlation is very weak somehow, compliance can be
13 very good. I'll say that, however, so all of that
14 paints a picture of how compliance could be very
15 useful in the case of data breaches and privacy
16 violations.

17 On the other hand, you know, it still seems
18 to be a case that we're not very good, we haven't
19 gotten good at understanding what these harms really
20 are. You know, we heard earlier today, losses in the
21 hundreds of dollars for consumers, average losses. It
22 still seems to be true that most people don't lose
23 very much at all, if anything.

24 And it's really kind of a failure on our
25 part, on the information security industry, that we

1 are not very good at understanding what kinds of
2 security controls really are effective. I think
3 everyone in this room and certainly experts, we could
4 all produce a list of technologies, of procedures that
5 would help in some kind of way -- two-factor
6 authentication, firewalls, intrusion detection,
7 whatever, but nobody is really able to tell us which
8 ones are more effective and by how much. We just
9 aren't there yet. We just don't have the maturity as
10 an industry.

11 Customer demand or customer demand for
12 privacy and security, so this is a story of whether or
13 not firms compete on privacy. And I think in one of
14 the previous panels from a few weeks ago, there was
15 discussion of whether or not firms actually compete on
16 privacy, on security. And there was the argument
17 that, oh, well, yes, they do, of course, because look
18 at all the money that firms have invested in different
19 kinds of features.

20 I'm not really sure that's evidence that
21 there is a demand for privacy. At best, what we can
22 do is highlight search engines like DuckDuckGo and
23 talk about different kinds of privacy-enhancing
24 technologies that exist in the marketplace. And it's
25 nice and they're there and they work, but they haven't

1 really reached that kind of market penetration, right?
2 They're certainly not competing with Google. They're
3 certainly not competing with Bing. And, so, I'm not
4 convinced that there is actually customer demand for
5 privacy. I think if there was, we wouldn't be trying
6 so hard to find it.

7 Insurance is a great field. And I think a
8 number of us could talk all day on the benefits of
9 insurance. I think that does provide, or at least in
10 theory should provide, incentive for firms. They can
11 enjoy lower premiums, they can enjoy broader coverage,
12 they can enjoy fewer exclusions in their policies if
13 they've adopted certain kinds of security controls.
14 Again, I'll point out, we don't really know what those
15 security controls should be, but, in theory, it should
16 work and it should provide incentives.

17 And that could be a win-win-win for
18 everyone. Firms are lower risk; insurance companies
19 are more profitable; and overall social welfare is
20 increased from fewer breaches.

21 So back to your question. You asked me, you
22 know, which one of these is -- you know, could be the
23 most powerful. I don't really have an answer. I
24 haven't studied that. What I can say is that each one
25 of these offers the potential for creating incentives,

1 but none of these alone, certainly from my mind,
2 really sticks out as a major force driving firms.

3 MR. LEGOWER: Sasha, so you said something
4 that I thought was interesting about reputation, and
5 essentially that in your perspective it just collapses
6 all down to sales essentially, right, that this is,
7 you know, the business' reputation in the minds of
8 consumers. But you can also think of an individual
9 executive's reputation, right? So some individual
10 executive as domain over the cybersecurity posture of
11 a firm. And there's been some high-profile incidents
12 recently where executives lost their job or had their
13 communications exposed as a result of the data breach.

14 So can you talk a little about the extent to
15 which concern for personal reputation might drive
16 security? So we have all this research that says
17 maybe business reputation doesn't matter so much, but,
18 you know, if an individual executive's job is on the
19 line, could that make a difference?

20 MR. ROMANOSKY: Yeah, absolutely. It could.
21 I think that's a knowable thing. I would think what
22 you could do is just ask a bunch of CISOs really what
23 drives their incentives, right? That would be one
24 way, and I think we'll get at some of this, and
25 Tyler's done some great work on that, too.

1 It is also true that there aren't that many
2 situations where executives have lost their jobs
3 because of this. Certainly, in the Sony case, and the
4 Equifax, and the Target, there have been, right, some
5 embarrassment and some layoffs because of that.
6 Although, I think in some of those cases, they did
7 enjoy a bit of a golden parachute from leaving
8 afterwards, so it is possible that the threat of
9 personal reputation could drive better behavior.

10 I'm not sure I would be the best one to
11 answer whether or not -- how much that affects the
12 decision-making. I think Tyler would be better at
13 answering that.

14 MS. JILLSON: And Tyler?

15 MR. MOORE: Okay, so hi. So I think Sasha's
16 right and that each of these incentives you list I
17 think have an impact. If I were to pick one, I would
18 point immediately to compliance as being the single
19 biggest driver certainly of investment in security.
20 And when we talk to CISOs, they almost grit their
21 teeth when they say it, but it's -- you know, they
22 know that a compliance-driven mind-set to security
23 doesn't lead to the best security plan and posture,
24 but they also know that an argument for compliance is
25 the most effective in getting the budget that's

1 required. It sets the floor for what you have to do.

2 And so much of what we do in cybersecurity
3 and cybersecurity plans result from compliance
4 demands, whether it's, you know, Sarbanes-Oxley, which
5 shouldn't even necessarily have anything to do with
6 cybersecurity but it has driven an entire emphasis on
7 security among publicly traded firms or to more
8 sector-specific compliance rules.

9 So that, to me, seems to be the strongest
10 incentive to invest in cybersecurity writ large for
11 companies. It's, you know, a fairly imprecise
12 instrument, and it tends to set a floor and not a
13 ceiling, in terms of what should be achieved, so there
14 are definite downsides, but it does seem to be
15 effective.

16 A comment about all of these incentives is
17 that I do think they all have an impact. I think the
18 real question is whether or not these incentives on
19 their own are sufficient, and I would argue that they
20 are not, taken as a whole, because of the presence of
21 market failures, and, in particular, two market
22 failures: the presence of negative externalities of
23 cybersecurity and breaches.

24 So long as the harms resulting from a breach
25 go beyond the affected organization who makes the

1 security investment decision, they will tend to invest
2 less in security than would be socially optimal. You
3 know, so take the example of Equifax. The data breach
4 happened. It was bad for the company. Their C-Suite
5 got replaced. And yet the harms to consumers, to
6 broader society, to financial institutions is much,
7 much greater than what Equifax itself, on its own,
8 experienced when we view it collectively.

9 There's also information asymmetries in that
10 we -- you know, it makes -- we don't actually have a
11 good sense often of what an effective investment is,
12 sort of following on Sasha's point about, you know, we
13 have recommendations on different investments to make,
14 but we don't know how effective one particular control
15 is or not.

16 We also don't know often what the true
17 magnitudes of certain kinds of risks are. In a
18 certain sense, data breaches is kind of a positive
19 exception to that because we have had, you know, more
20 than a decade's worth of data breach requirements in
21 force. We now know arguably more about the prevalence
22 of data breaches than just about any other
23 cybersecurity threat. And, so, that has certainly, I
24 think, influenced boards and the sort of governance of
25 companies to focus on preventing data breaches because

1 it has become so visible as a result of data breaches.
2 So we see a lot more attention being paid to data
3 breaches than we might see being paid to other forms
4 of cybersecurity risk. So just the obligation to
5 disclose, I think, serves as an incentive to make some
6 investment.

7 MS. JILLSON: Matt?

8 MR. MCCABE: So I would opt for the top
9 incentive to be reputation, but I would redefine it in
10 a way that it's really reputation to your
11 stakeholders. I think that's how certainly for public
12 companies they think of it to their board and
13 ultimately to their shareholders.

14 I mean, if you think about it, you have an
15 organization that is a viable concern, hopefully a
16 highly successful organization, and you have certain
17 risks that you deal with every day. Some of it is
18 financial risk, and you have the opportunity to plan
19 for that appropriately. Some of it might be an ethics
20 risk, and you have the opportunity to put in a
21 compliance regime and to have governance over that to
22 monitor it, but cyber risk for many of these
23 companies, is kind of that unknown risk that can just
24 take your legs out from under you.

25 And I would say that all these other

1 components actually feed into the company's -- in the
2 C-Suite's ability to maintain reputation. What is our
3 relationship with our customers? Are we meeting our
4 compliance regimes? Am I limiting my exposure to
5 large liability? Am I reducing cost? These are the
6 items that all senior officers go through every day in
7 order to maximize performance. So I think from a
8 corporate standpoint at least reputation is the
9 ultimate concern.

10 MS. JILLSON: And Larry?

11 MR. GORDON: Okay, so I would say I want to
12 rename cost reduction to cost savings. I would say
13 cost reduction over cost savings because you've got to
14 think in terms of cost being implicit and explicit
15 costs. So there are explicit costs of detecting and
16 correcting; there are implicit costs. The implicit
17 costs pick up ex ante compliance, reputation effect,
18 and ex post liability. Those are a cost to a company,
19 okay, if they have a big breach or a potential cost.

20 So, really, you can wrap up three or four of
21 those right into the cost savings notion, so companies
22 look at it from that point of view, but I think it was
23 Tyler who mentioned one of the real issues is that a
24 lot of the big costs are what we call implicit costs,
25 the costs of, you know, with reputation, the way we

1 look at some stock market returns.

2 Unfortunately, these costs tend to be
3 transitory. And by that I mean they're not permanent.
4 Temporary stock prices drop down. Look at the big
5 breaches we had. You know, take a look at Target's,
6 for example. You know, their stock dropped down for a
7 few weeks, and then it comes back.

8 But on the other hand, part of those costs
9 is that there are executives who lose their jobs. The
10 CEO lost his job. The CISO, you know, chief
11 information security officer, she decided one month
12 after the breach that it was time to retire, that she
13 was planning on it any way. And we see that quite
14 often. Actually, a lot of the security officers are
15 the ones who bear the brunt, so what we have is an
16 agency problem.

17 At least from my interaction with security
18 officers, many of them, you know, they look at this
19 and say, look, we need more security because I'm the
20 one who pays the price. And from the chief financial
21 officer's point of view, he or she looks at it from
22 cost-benefit basis. So, you know, what are the
23 benefits? What's the cost? And if the benefits
24 aren't greater than the costs, we take a hit. It's an
25 operating cost.

1 So I would say cost reduction because to me
2 cost reduction includes compliance. If you don't
3 comply, you've got a significant cost. Reputation
4 effect. If you have a big breach, that's a cost to
5 your company. Ex post liability is clearly a serious
6 cost, and so you can wrap up many of these into cost
7 reduction.

8 On the other hand, I would also say that all
9 of these things are important. You know, so it's not
10 like one doesn't count, but, to me, when companies
11 look at -- corporations that I deal with, when they
12 look at security, they're thinking in terms of
13 potential costs. And they're thinking in terms of
14 there's a cost to a reputation if they have a big
15 breach. There's a cost to -- if you have a big
16 lawsuit and you lose, there's a cost to not complying.
17 There's a cost to detecting and correcting breaches,
18 so all these things I put into cost.

19 MR. MCCABE: Can I just comment on that
20 description? And, you know, this is perhaps a little
21 oversensitivity, but to kind of back up some of -- our
22 portfolio of clients and even our own company, I think
23 it's very rare that you have a CFO or a treasurer who
24 says, look, you know, you just analyze the cost, and
25 if we have to take a hit, we take a hit.

1 I just don't think that that's how companies
2 think about this problem. I think what they do -- and
3 to go off of Sasha's comment -- the hard part of this
4 is the calculus of what's the overall efficacy of
5 these protective measures. So there was a great post
6 on a White House blog several years ago about a CISO
7 complaining to Michael Daniel that, look, I spend
8 millions for security that's regularly defeated by a
9 \$500 rented piece of malware. What is my extra
10 investment in security going to yield? And if you
11 can't put a number on that, I just don't want to keep
12 throwing dollars into a pit and suffer a continuum of
13 breaches anyway.

14 So I think actually what you're seeing is
15 that there's acceptance within a lot of industries
16 that breaches are going to happen, and that you're
17 never going to be able to have 100 percent solution,
18 so you're going to have to get to a high level of
19 security but prepare for breaches anyway. And it
20 becomes more of a risk management and a governance
21 conversation.

22 MR. GORDON: Yeah, I don't disagree with
23 what Matt said. I didn't mean to be cavalier about
24 it, but take a look at the NIST 1.1 version. They
25 explicitly say the tier you want to be on is a cost-

1 benefit decision. That's what I meant. It's,
2 overall, you have to look at it from that point of
3 view. So if you look at subsequent risk management,
4 you need to look at it from a cost-benefit point of
5 view. Even NIST puts it into their cybersecurity
6 framework.

7 And NIST, when you talk about compliance,
8 the NIST framework, ever since our current president
9 said that all government agencies have to be at least
10 consistent with that, that's been one of the biggest
11 compliance issues I see, you know, to really get firms
12 to look at their cybersecurity in a more serious way
13 than they may have done in the past. But I agree. I
14 mean, I didn't mean to be -- and not cavalier about
15 it. I meant that they look at this as, you know, I
16 can't have 100 percent security, so the question is
17 how much do I invest.

18 MR. ROMANOSKY: So let me add one thing,
19 though, that I think gets lost in the discussion and I
20 don't think -- that I don't think is inconsistent with
21 what both of you have said. But that if we're talking
22 about firms and enterprises and enterprise-level risk
23 management, cyber will just -- will be -- just one of
24 the risks that they have to manage. And, so, yes, it
25 becomes a cost-benefit decision, and I think that's

1 appropriate to the extent that we can reasonably
2 quantify cost and benefits, and I'm not convinced that
3 we need to, certainly as researchers anyway.

4 We really want data, and we love data, and
5 we love analyzing data. That's kind of the fuel by
6 which we go, but in this case, it's not clear to me
7 that more numbers actually get us further ahead, but
8 the real point is that if Cyber -- if we want to
9 manage cyber, just like any other kind of enterprise
10 risk, I think what we need to do is assume that if an
11 appropriate assessment is done and it turns out that
12 cyber risks don't pose that great of a threat to us,
13 that they will be deprioritized, that the investments
14 will be deprioritized. And I think we should accept
15 that. That would be appropriate for a firm to do.

16 So when we speak of incentives, what doesn't
17 appear here, so these are all incentives for firms who
18 invest in cybersecurity. It doesn't really ask --
19 they don't really ask the question of how should firms
20 prioritize cyber relative to all of the other risks
21 they face -- tax and finance, employment, supply
22 chain, competition. The list goes on and on.

23 So one useful exercise, I think, will be to
24 understand how cyber relates in terms of risks to
25 these other areas. And, again, if it's true that

1 cyber just doesn't present itself as a great risk,
2 then it should be appropriately deprioritized.

3 MR. GORDON: Can I? I agree with what Sasha
4 said, but I'd even go further and say that from an
5 investment point of view, investments in cyber is just
6 one of the major investments companies make. And
7 companies, unless they're in business to sell
8 cybersecurity, you know, services, they can't put all
9 their money into cyber, so they have to look at this
10 as -- they look at other investments.

11 And whether we like it or not, most major
12 corporations use NPV models. They know they're not
13 precise. It's a framework. It's a framework where
14 they go through a process. And over time, you assume
15 that, you know, the results from that process will be
16 beneficial that year. You're going to have to make
17 better decisions by following, you know, a set
18 process, and I think when it comes to cyber
19 investments, it's the same idea.

20 Cyber investments are competing with all
21 other investments. I know lots of CFOs, and they tell
22 me, well, everyone comes in and wants more money, they
23 want a new product line, they want a new building, new
24 equipment. So cyber investments are competing with
25 other investments. And once you realize that, it's a

1 resource allocation decision for firms.

2 You know, for example, Target was spending a
3 ton on cyber. It wasn't like they were not spending
4 money on it. Their breach was due to outsourcing a
5 little piece of their work, so I agree with what Sasha
6 was saying, but I would just say it's more than just
7 the incentives. It's across the whole level of
8 investments, and that's the real issue. So you need a
9 process, and the process has to be somehow consistent
10 with the other investment decisions because eventually
11 someone asks you, why should I give you more money
12 rather than putting it over here.

13 MR. SHARP: So, Larry, I think Tyler brought
14 up the point. It's about who bears the brunt of the
15 outcome, the benefit of the outcome, and I think if
16 we're thinking about this in the context of
17 enforcement, which I think is a little bit the point,
18 and thinking about if there is, in fact, an agency
19 problem, meaning we make an investment that's
20 appropriate for my firm but doesn't necessarily
21 consider all of the externalities, then there's that
22 true risk of market failure.

23 And I think that's the piece that while I
24 agree there's a cost-benefit analysis and every CEO,
25 CFO, CISO is balancing the allocation of scarce

1 resources fundamentally, the broader question is how
2 do we effectively influence that for the protection of
3 consumers. And I think we've circled around
4 compliance.

5 Tyler, your research talks a lot about the
6 compliance story, and I think in many cases it has
7 helped related to, Larry, some of your research. The
8 first dollar you invest in security is going to be
9 much more effective than the tenth dollar you invest,
10 meaning there are diminishing returns. And I think,
11 Larry, your approach puts a cap on what is an
12 appropriate ceiling. And, so, then compliance drives
13 the floor, and somewhere in between I'm stuck
14 negotiating with the various executives, and I think
15 what we find that's maybe not represented here but all
16 too true is there's an element of storytelling and
17 charisma that CISOs bear the brunt of carrying in
18 order to get the adequate budgets.

19 And if I can have an appealing story, and
20 this sort of relates back to my original commentary,
21 if I sit in front of my CFO and I can expand revenues,
22 I get money. And if it is in front of that same
23 executive team and I tell a story of the world is
24 ending and no amount of investment will ever get me
25 past the ifs, not if but when, then I can get money

1 once, and that's what happened in 2014 for a lot of
2 CISOs. And then the money dried up by 2016, right?

3 MR. GORDON: Everything you said I agree 100
4 percent. So what I always talk about is revenue-
5 generating projects versus cost-savings projects. And
6 what Matt just said is exactly that point. So the
7 example I always give is something like, you know, if
8 you come and ask for a \$10 million investment in a new
9 product line that's going to generate \$20 million in
10 additional revenue, so let's just say the net benefit
11 there would be the 20 minus the 10 or the bottom line
12 goes up by 10 million, okay, you're much better off
13 asking for that than if someone comes along like Matt
14 and says, I want a \$10 million in a network security,
15 and I'm going to save you \$20 million in costs, right,
16 but you don't show any revenue growth.

17 And the name of the game for most senior
18 executives, especially if they're on stock options, is
19 revenue growth because the stock market -- there's
20 lots of evidence, the stock market moves with revenue
21 growth. So what Matt just said, I would say, can you
22 come to my class? I talk about in this class all the
23 time, exactly what you just said. And I actually
24 bring in people like yourself, chief information
25 security officers, to give examples of just what you

1 said, so thank you. I mean, that's a great
2 testimonial.

3 MR. MOORE: Larry's class.

4 MS. JILLSON: Let's move now to talk about
5 each of the incentives that's listed here. And, so,
6 the first is customer trust, and we have a question
7 from the audience about why we did not include
8 customer welfare or customer well-being on this list
9 of incentives.

10 So to what extent do you think that customer
11 welfare, well-being, collapses into trust? And how
12 much does trust matter? Does it matter if consumers
13 begin to view a certain firm as no longer trustworthy
14 on security, or do the number of breaches we've seen
15 and the fact that people keep shopping at these places
16 show that maybe trust doesn't matter that much?

17 On the other hand, does trust matter
18 particularly in certain areas? So maybe for companies
19 that have children's information, financial
20 information, health information, you know, certain
21 forms of sensitive data, where does trust matter, if
22 at all?

23 MR. SHARP: I can offer the anecdotal
24 evidence that comes out of CISO roundtable community
25 discussions. Certainly for the discussions that we

1 have inside of the roundtables, the dialogue is
2 basically customers have to trust in order for sales
3 to go up, right? So I think we end up equating all of
4 those things in a different way, whether it's
5 competitive advantage or reputation or customer trust.

6 At the end of the day, protecting customers
7 is important, but I think earlier in the session
8 previously we've seen that consumers don't necessarily
9 behave congruent with their own best interest. For
10 example, the comment about 10 percent of Gmail users
11 having multifactor enabled would lead to consumers
12 just don't behave in a way that would be in their best
13 interest because the email account is actually how you
14 can reset every other password that they have access
15 to.

16 MR. MOORE: So just the question about
17 consumer welfare, I mean, I think consumer welfare is
18 what, you know, when you're thinking about overall
19 what the social welfare should be, then obviously you
20 need to consider consumer welfare. When you're
21 thinking about firms and what's going to drive their
22 incentives to invest, their perspective is different.
23 Their perspective is on what maximizes the firm's
24 revenue.

25 If they're in a consumer-facing industry

1 where, you know, it's important that they respect
2 privacy, it's important that they gain the trust of
3 their customers, then they will act accordingly, but I
4 think it's very much not the case across the board.
5 You know, I mean, you look at the example of Equifax,
6 which is, you know, that trust should be important to
7 their business, but it was actually incidental. And
8 to a certain degree, the trust that they needed to
9 engender is with their customers, which weren't the
10 people whose data was lost.

11 So, yeah, I think firms are going to, you
12 know, in general, look at an incentive which is
13 maximizing their own interests, which may or may not
14 align with consumer welfare.

15 MR. LEGOWER: I want to jump in and move to
16 discussion about compliance and liability. I think
17 it's been brought up by most of you either explicitly
18 or implicitly that you think that compliance and
19 liability are big factors in cybersecurity
20 investments. So the question I want to pose to the
21 panel is, do these compliance considerations actually
22 encourage more marginal investment or do they just
23 sort of reallocate the investment that's already going
24 to happen?

25 In a sense, is there just -- is it a hard

1 budget constraint on what you can spend and compliance
2 considerations direct where it goes, or do compliance
3 constraints actually spur additional investment?

4 MR. SHARP: Yes. I think it's both. It
5 depends on the firm in that there are some firms who
6 are maybe a bit more sophisticated and are thinking
7 beyond just compliance, who have allocated their
8 budget, and then they realize that there's a
9 significant chunk of it that just has to be allocated
10 to dealing with compliance circumstances, and that's
11 the ideal, probably. But, then, there are other firms
12 who otherwise would select below the floor. And the
13 compliance requirements end up setting the floor, and
14 that entirely directs what they need to spend their
15 money on.

16 MR. GORDON: I think if they have a budget
17 constraint and they can't go over it, then they're
18 reallocating. And if they can get additional funds at
19 the constraint, then it's a question of trying to
20 figure out the sort of the best allocation. So it's a
21 combination. It really does depend on exactly, you
22 know, what Michael said was do they have a budget
23 constraint, right?

24 And, also, the other point I would make is
25 how are they allocating their funds currently. Are

1 they -- you know, compliance might force them to
2 reassess their allocation process, or maybe they
3 weren't at the best position from their point of view.
4 They may reallocate it. So it's those two factors,
5 you know, where are you in terms of the allocation of
6 the resources and what kind of budget constraint do
7 you have?

8 MS. JILLSON: Thinking about compliance and
9 liability together, how is investment to ward off
10 liability different from investing to meet compliance
11 obligations?

12 MR. MOORE: At the most basic level, what
13 their difference is is that you -- it's the ex ante
14 versus ex post in the sense that, you know, you have a
15 compliance rule in place because you want the
16 investment to be made to prevent the harm from ever
17 being realized in the first place.

18 And, so, if the harm is so great that it
19 cannot be easily reversed or mitigated, then you focus
20 on ex ante compliance. If the harms aren't so great,
21 then you can just assign liability and deal with the
22 fallout after the fact. When you think about breaches
23 of personal information or any breach of confidential
24 information, one of the big challenges is as soon as
25 you have this breach of confidentiality, there's no

1 going back.

2 When all of the Social Security numbers get
3 disclosed from a large data breach, there's no way to
4 undo that breach of confidentiality, and so it's a
5 one-way action. And, so, when you have situations
6 like that where the bad event has sufficient cost and
7 cannot be reversed, then the emphasis should be on
8 compliance. If, in fact, the harms aren't so great or
9 they can more easily be reversed, their effects, then
10 you can push towards liability.

11 MR. SHARP: So, I'd love to respond to that.
12 The dialogue in the cybersecurity community today has
13 largely been we've invested, perhaps overinvested, in
14 preventive controls in the network. And the reality
15 is the conversations that are happening in boardrooms
16 are about cyber resilience, acknowledging the "not if,
17 but when" sort of paradigm of thinking. And I think
18 you'll hear from some other very innovative firms that
19 are starting to drive stronger opportunities to have
20 more holistic prevention.

21 But when you look at the -- Sasha, I think
22 it was you that made a comment earlier. When we're
23 making decisions on where to invest money that we
24 don't necessarily know what the best places to place
25 those bets are, as CISOs, and I think there are some

1 nuances that we can pull out of that a little bit
2 further and say, I think just about everybody that you
3 would talk to in the security community would say we
4 need to have multifactor, we need to have patching, we
5 need to have configuration management, but every FBI
6 and Secret Security briefing that you go to talks
7 about how the overwhelming evidence is that patching
8 is not functional and the configuration management is
9 not working.

10 And, so, I think the question of we don't
11 know what to invest in is not the real issue. It's we
12 don't know how to make the organizational or process
13 changes effectively in order to achieve the ultimate
14 outcomes that we're after, and so I think there's
15 nuance in the data that you're interpreting has a
16 different nuanced outcome to consider.

17 MR. ROMANOSKY: I mean, I see those as the
18 same thing. The point is we don't really know what's
19 best. We don't know where to spend our first dollar.
20 We have a list of -- we have a bucket of technologies,
21 of processes, of things we think we should do. They
22 probably all work to some extent, but we don't know
23 where to start investing or to exhaust our budget.

24 MR. MOORE: And to your point about
25 misconfigurations, we spend all this money on

1 controls, but we don't have the people in place to be
2 able to adequately use them. I think that, at a high
3 level, is still an issue of budget, right, because you
4 need to be able to -- you can reallocate your
5 resources to people who can be trained to be able to
6 effectively use the controls that you have deployed.
7 And there is definitely a challenge there because of
8 workforce limitations and just the behavioral
9 preference to buy another service or another tool
10 rather than to adequately use the tool you have.

11 MR. SHARP: Yeah, I think the hamster on the
12 wheel starts to become the issue. We get an unlimited
13 number of vulnerabilities coming from the hundreds of
14 thousands of users in different applications. And,
15 so, no matter how good we do, there will always be a
16 percentage of users that click on phishing. There
17 will always be a percentage of applications that will
18 not be patched, and so the dialogue -- and I think
19 Matt probably can speak about this a little bit
20 further -- is shifted to we're going to accept that
21 some percentage of this can't be mitigated and we need
22 to start to actively manage the downside impact
23 through cyber-resilience investments.

24 MR. ROMANOSKY: I mean, for what it's worth,
25 I really like that point. I think -- and, again, Matt

1 can speak of the insurance policies, right? So what
2 you see in the applications and the rate schedules
3 that carriers use is to ask a bunch of questions
4 related to technical issues. There's some process
5 stuff in there, but again we don't really know, right?
6 We're asking a battery of questions that we think are
7 correlated with better security posture, but we don't
8 have any evidence to demonstrate which ones -- which
9 technologies are better and even which questions to
10 ask.

11 And I think I'm of the mind now that those
12 nuances don't really matter and what does matter is
13 the story of resilience and a maturity of processes.
14 And I think the better we are able to assess maturity
15 of processes, the more quickly we'll get at an
16 understanding of better security posture versus weaker
17 security posture, and resilience is tied into that.

18 And, so, I mean, I reject the claim earlier
19 that there are two kinds of companies, those who have
20 suffered a breach, those who don't know it. I think
21 that's a silly comment, right? It's a marketing
22 comment. It just can't factually be true.

23 But there is something to the point of,
24 look, we should accept that we will be breached. And
25 even if that doesn't happen, we should prepare for it.

1 And, so, what that means is that you establish a level
2 of maturity of processes in order to maintain
3 resilience. We accept that we start off with a level
4 of output of our firm here, that we become resilient
5 to absorb some percentage of that attack, of that
6 outage, and that we develop processes to return to
7 that 100 percent output level as quickly as possible.
8 This is this resilience triangle that people talk
9 about, and I think that's a smart way. I can't prove
10 to you, but I believe that's a smart way of reducing
11 the cost and addressing the problem.

12 MR. LEGOWER: So, I want to move on because
13 we have -- since we have Matthew McCabe here and all
14 this talk about resilience and risk management, I
15 think we would be remiss if we didn't ask Matthew to
16 talk a little bit about cyber insurance and explain
17 how cyber insurers make decisions about which policies
18 are appropriate for which companies.

19 MR. MCCABE: Sure. And I actually think it
20 moves on just as a perfect segue from what we are
21 talking about because I think that mind-set that
22 you're talking about is what industry currently has.
23 I mean, certainly, when we're going through an
24 insurance process, the process is not a checklist of
25 what technologies do you have and did you get seven

1 out of ten and therefore you scored a 70.

2 Quite frankly, the process is, you know, it
3 might start with a question of how much data are you
4 holding, what type of data are you holding, and what
5 do you do to limit your sensitive data. And, then,
6 there's the discussion back of what that process is of
7 how you appreciate what your assets are. Do you
8 really need all this data or do you have a data
9 limitation policy?

10 So cyber insurance is all about the maturity
11 of organizations. And, I mean, I guess I would reject
12 the notion that it's without basis of how to assess
13 posture of a company. It is definitely not an exact
14 science, but all reports are that the cyber insurance
15 industry is profitable and, therefore, one could say
16 that economically determined to be doing a good job
17 for assessing security with -- you know, of course,
18 there are breaches and there are claims and there are
19 exceptions that pop up, but overall on a macro
20 standard, doing very well.

21 So there's -- I would say to really simplify
22 the product of cyber insurance and maybe just to back
23 up a step, it's different from having a cyber-related
24 peril than having cyber insurance. Cyber insurance is
25 a very specific product. Cyber-related peril means

1 that I was able to hack into an industrial control
2 system, get something to blow up, and, as a result,
3 there's a property claim or there's a liability claim.
4 That's not cyber insurance. That's on more
5 traditional lines like property or casualty.

6 For cyber insurance, you're looking at a
7 bucket of three things. I've had a cyber incident,
8 and I have to pay out of my pocket to respond to that
9 incident somehow, whether in the data breach context
10 that's providing notice and providing credit
11 monitoring or credit restoration or whether that's
12 dealing with a ransomware event and restoring data or
13 replicating the actual servers or devices that have
14 become corrupted, what's often called a bricking
15 event.

16 Number two would be the liability angle,
17 and I think that there's large amount of incentive
18 that can be gained out of liability. We had the
19 conversation between compliance and liability. I
20 would look at compliance as a standard of liability.
21 But if you can actually work with liability and find
22 ways to cap liability by going above layers of
23 compliance, then you have very powerful incentive for
24 the private sector.

25 And then the third bucket for cyber

1 insurance really deals with the continuing operation
2 of a company, what we would call business
3 interruption. So if you're -- like in a NotPetya
4 event if your company's been taken down and disabled,
5 whatever extra expense you might have from that and
6 whatever income that you've lost can be covered by the
7 insurance.

8 But I will say for the product itself, as
9 cyber risk has grown, the product and what it covers
10 expands more and more every day. And I think that
11 it's become -- look, the overall market for protective
12 technologies in the United States alone is in the
13 neighborhood of \$115 billion according to Gartner
14 Research. The overall amount of cyber insurance,
15 global premium written, according to Betterley, is in
16 the neighborhood of \$5 billion.

17 So are those exact numbers? No, but they
18 can give you a pretty good estimate of where we are
19 from how much we've invested in protective security to
20 coming on the scale of we're realizing it's really a
21 management process. We're never going to be able to
22 protect everything, so how resilient are organizations
23 responding to cyber threats and recovering from them?
24 And if you look at our industry, they have started to
25 turn to the risk transfer part where the take-up of

1 cyber insurance has been in the neighborhood of 20
2 percent to 30 percent for four or five years now.

3 MS. JILLSON: So how should we think about
4 cyber insurance? Is it properly thought of as an
5 incentive to have better security because companies
6 want better premiums and coverage, or should we think
7 of it more in terms of it is simply a risk transfer
8 mechanism? And is there a moral hazard problem with
9 cyber insurance?

10 MR. MCCABE: So in reverse order, I would
11 say no, there's not a moral hazard problem because I
12 don't think that companies are spending on insurance
13 in order to accept the fact that they have known
14 defects. I think what they're doing is realizing that
15 they can't spend their way out of this problem, and
16 they're taking it on as another risk management
17 strategy.

18 When the NIST framework was being developed,
19 part of President Obama's executive order required
20 three different agencies -- Commerce, Treasury, and
21 the Department of Homeland Security -- to publish
22 reports on incentives. And cyber insurance was the
23 only one common to all three. And that seems like a
24 very odd thing because it's an expenditure. And you
25 don't really view an expenditure as something to

1 incentivize better controls.

2 But I think in the mature sense, if you're
3 thinking, look, if I'm going to have cyber insurance
4 as part of my overall risk management strategy, then
5 my ability to perform good security is going to be
6 realized on the insurance side as well with declining
7 premiums and with hopefully favorable terms. It's
8 basically the investment of confidence by the
9 underwriters. So I think that it's a function of
10 leading companies in the right direction.

11 Look, if all cyber insurance did was
12 transfer the risk financially, that would be valuable,
13 but the truth is that it's helping companies to
14 develop risk management response policies. It's
15 helping companies assess their overall cyber posture.
16 It's becoming ingrained in the whole cyber risk
17 management approach throughout enterprises.

18 MR. MOORE: And I would just add, so to
19 build onto some of your comments, I think -- I mean,
20 fundamentally, there is risk transfer. That's a core
21 part of the product, but there are these potential
22 additional benefits that you can get, one of which is
23 this idea that if you have someone -- an organization
24 that comes to you and buys this risk transfer, then
25 ideally they're thinking about the overall risk

1 management process. So that means they're already
2 mitigating and spending significant amounts on
3 mitigation and realize that they also want to do some
4 transfer as well.

5 There's also this fact that the insurers go
6 through this process of evaluating clients and
7 ensuring that you are spending enough on mitigation.
8 So if you want to get a reduced premium, then you need
9 to take certain steps and show that you've taken it,
10 so that's definitely a benefit.

11 In terms of the moral hazard question, I
12 would say it's not really a concern now. In
13 particular because most companies cannot fully insure
14 the potentially unbounded scope of what a cyber
15 insurance loss could be. Frequently, companies say
16 that -- large companies are not able to necessarily
17 even buy as much coverage as they might even want to,
18 and so there are still relatively low caps on the
19 amount of coverage you can get. And so, worst-case
20 events go way beyond what tend to be covered, so
21 that's one thing.

22 The final point I'll make is that the
23 existence of data breach notification obligations
24 through these state laws has really helped bootstrap
25 the cyber insurance market for reimbursing costs

1 surrounding data breach. So, you know, and the fact
2 that there is this obligation to disclose creates the
3 obligation for companies to have these costs and then
4 make them go ahead and apply for -- get insurance and
5 file claims.

6 Other forms of cyber insurance -- or other
7 forms of cybersecurity and cybersecurity risk, there's
8 still a calculation as to whether or not you'd
9 necessarily even want to file a claim with your
10 insurer because you might then have to publicly report
11 it. And so that's an example of the policy
12 intervention of data breach notification enabling
13 cyber insurance.

14 MR. ROMANOSKY: Can I ask? So, Matt, you
15 made one comment that was curious. You said -- tell
16 me if this is wrong. Insurance companies are
17 profitable, therefore, we are able -- that shows that
18 we are able to properly assess risk.

19 MR. MCCABE: It shows that these companies
20 who have been writing cyber risks for 10 to 15 years
21 and making profits on it are doing their business
22 well.

23 MR. ROMANOSKY: I guess that's the part I
24 don't understand. So the more profitable the company
25 is, the better it shows that they're able to assess

1 the risk. So the profitability comes from having
2 premiums, issuing premiums but suffering no claims.
3 Right, if there are no claims, then the firms -- the
4 carriers can be most profitable.

5 MR. MCCABE: Oh, no. They have claims.
6 What they're trying to do is assemble a portfolio of
7 diverse companies.

8 MR. ROMANOSKY: Oh, I see.

9 MR. MCCABE: They're trying to -- well, I
10 mean, we can go back to 101 and explain the insurance
11 industry, but there's undoubtedly the profitability of
12 an insurance company in writing cyber portfolios is
13 testament to how well the job they're doing.

14 MR. ROMANOSKY: But that profitability comes
15 from diversification of the portfolio as opposed to
16 being able to better -- as opposed to being perfectly
17 able to assess the cyber risk.

18 MR. MCCABE: There's no perfectly to
19 anything in the world. Government decisions are never
20 made in a continuum of perfection. Educational
21 decisions are never made in a continuum of perfection.
22 Economic models are never drawn up in a continuum of
23 perfection. What there is is an assessment of what
24 maturity of organizations are. And it's not just
25 diversification. It's an evaluation of security

1 posture.

2 If an insurance company spots a potential
3 insured that has flagrant weaknesses and a lot of
4 exposure, the market will recoil. And as a result,
5 the prices for premium of that company will go up.
6 And to your point, the amount of limits out there
7 for that company will be less. I think that is a
8 completely appropriate market response for cyber
9 assessment.

10 MR. SHARP: Can I just -- let's say you have
11 -- and this is a common thing -- a billion-dollar
12 company, 3 percent of revenue spent in IT and 10
13 percent of that being spent in cybersecurity. So a
14 billion-dollar company could be spending \$3 million a
15 year in a security program. That company may choose
16 to insure to protect against a breach of something
17 like 5 or 10 million records. That policy would cost
18 somewhere between \$30,000 and \$60,000.

19 Let's say that you double it. Let's say
20 that you triple it. If it's \$150,000, the incentive
21 to me or to my team to really build a \$3 million
22 program in order to reduce \$50,000 off of my insurance
23 doesn't make sense. So I find some -- so my personal
24 experience -- and this could be an anomaly -- is
25 that's not a dialogue point in any of the discussions

1 that I'm having with any of my peers nor with my
2 executive team.

3 And then the other thing that I would offer
4 is -- and I don't know that your firm -- your firm may
5 operate differently, but I've been in a couple of
6 rounds of purchasing this cyber insurance, and the
7 brokers come in and they bring a group of folks to ask
8 some questions. And, categorically, the questions are
9 insufficient to tell really what's happening, so it
10 seems or it would appear, if I'm extrapolating, that
11 we're doing assessments similar to demographic
12 assessments in like car insurance where you say -- you
13 look and behave in a particular way.

14 You're 20 years old. You're a male. You
15 live in this area code. And, therefore, we're going to
16 classify or price this policy in a particular way,
17 which is different than the more informed version of
18 plug this thing into your car and we'll measure your
19 accelerations and decelerations and the way that you
20 actually behave on the road.

21 And, so, it looks like the questions that
22 are asked are more targeted towards mitigating or
23 adequately litigating, not paying an insurance claim.
24 And it looks like the instruments that we have to
25 measure cyber liability are dramatically insufficient,

1 just from -- that's my perspective, and I know that
2 that could be different than your perspective.

3 MR. MCCABE: Well, the instrument to measure
4 cyber liability has got to be data on what's been paid
5 out before. And we are certainly at nascent days of
6 the standard of care. Now, as far as coming in and
7 asking what those questions are, one of the things
8 that we should be aware is that there are more and
9 more tools that are becoming available to underwriters
10 to actually assess risk, but you're right, unless
11 you're within the footprint and doing a forensic
12 assessment, you're not really going to know what's
13 going on.

14 But the fact is that from a macro
15 standpoint, are they looking at different sectors and
16 companies within that sector and being able to judge
17 them one over another from the survey they get, the
18 questions for followup, some kind of external data
19 analysis? You get a decent picture for the purposes
20 of insurance. Now, is that going to stop cyber
21 attacks? No, but we're not stopping cyber attacks.
22 We're managing cyber risk. We're helping industries
23 become more resilient.

24 MR. GORDON: Can I say one --

25 MR. LEGOWER: In the interest of time, I

1 think we have to move on, but you'll be happy to know
2 that we're going to hand the mic to you. So we're
3 going to turn now to the mechanics of how companies
4 actually make decisions about investing in security.
5 And to start us off, I'm going to ask Larry to explain
6 the model that you've developed for cybersecurity
7 investments.

8 MR. GORDON: So you want me to click this?

9 MR. LEGOWER: You've got your slides here.
10 Yeah, there you go.

11 MR. GORDON: Oh, okay. So I think of this
12 as a framework. I'm not lost in the mathematics.
13 There's a lot of mathematics that underlies it. So
14 the framework is very simple. It's a process where
15 you look at -- I think it was Matt who mentioned with
16 the cyber insurance that you look at companies, you
17 want to know what data you're trying to take care of,
18 what's the value of it.

19 So the first thing you want to do is figure
20 out what data you're trying to protect, what's the
21 value of it, and the value of it is in terms of how
22 much could you lose, you know, the cost to you. So
23 that's part of the value.

24 Okay, and then the other thing is what's the
25 probability of a breach. And then, lastly, is how

1 effective are your investments, the productivity of
2 investments. So it's three very simple aspects to the
3 process. One is, you know, what's the value of the
4 information you're trying to protect, what's the
5 probability of having a breach, and what's the
6 productivity of the investment.

7 And, so, without going through mathematics,
8 you look at those three things. You can develop a
9 grid like you see in the middle. They have the chart.
10 The chart on your left-hand side, all it's basically
11 saying is exactly -- I think it was Matt or somebody
12 else mentioned that if you put more money into
13 investments, the first dollar you get more out of it
14 than you get the second, so the value of the
15 investment is -- the benefits are increasing at a
16 decreasing rate. And that's really all the left-hand
17 chart says, but it also says there's an optimal amount
18 to invest. I don't know the optimal amount. It would
19 change for every company.

20 And no matter what you think, it is ex ante,
21 ex post, it's probably not going to be the right
22 amount, but what I would argue is following some sort
23 of a rigorous process over time, taking into
24 consideration what the others here on the panel were
25 saying, that resilience and looking at what I consider

1 control, seeing how you did at the end of the period,
2 so you make these decisions ex ante and ex post. You
3 evaluate it, and then you move into the next phase, so
4 it's a continuous feedback process, and that's the
5 intent.

6 The nice thing about that middle grid there
7 is to suggest that you could come up with a grid and
8 look at how much you think you might want to invest
9 in different databases. I'm a big believer in
10 segmenting databases. So you can look at how much
11 to invest in databases, but the nice thing about it
12 is you can do a simulation around it. So you don't
13 like my probabilities that I threw in? Throw in a
14 whole bunch of your own and do a probability
15 assessment.

16 You could also -- you know, the value of the
17 information, no one knows exactly the value in terms
18 of what you're trying to protect and what you could
19 lose, but you could do a simulation around that. So
20 that's the whole idea.

21 The last little picture on the right-hand
22 side, all that's saying is that it started off as an
23 academic model. It was originally published in a
24 computer science journal with a lot of mathematics.
25 And eventually I kept saying to my coauthor, Marty

1 Loeb, and actually one of the other papers we wrote,
2 Joe Lay (phonetic) who's actually sitting in the
3 audience, we actually came up with an example, and we
4 tried to show how to use the process.

5 And to my surprise, the Better Business
6 Bureau picked it up and actually put it in a 2017
7 report and recommended it to all small businesses in
8 North America to think in terms of this framework.
9 Again, not using -- you know, not getting caught up in
10 the actual numbers, per se, but it's a process that
11 you go through and you figure out, you know, the value
12 of your information, the probability of a breach, and
13 what do you get for additional investment, so what's
14 the productivity of investments. And, so, that's all
15 that slide shows.

16 MR. LEGOWER: I think you had another slide.

17 MR. GORDON: I have another slide. I can
18 just -- you know, I've actually -- you know, it's
19 something Michael asked about. This one was about
20 incentives and government incentives. And it really
21 got to the issue of, you know, what can the Government
22 do in terms of giving incentives. Most incentives
23 that were in the slide that Elisa had before were
24 really things from the firm's point of view.

25 So the Government's been looking at lots of

1 incentives. You know, they give tax incentives,
2 grants and so on, but it's not that obvious that
3 giving incentives, okay, will increase security. One
4 of the problems is we don't really have a clean
5 measure of security. So all this little slide is
6 supposed to show is that you can show very easily that
7 the Government -- if a firm was already allocating
8 their funds in an optimal manner, then government
9 incentives, which would shift their allocation if they
10 have a budget constraint -- Michael's point -- would
11 shift it away from a better solution.

12 On the other hand, if they can increase
13 their budget, then government incentives would tend to
14 increase the level of security, so that's the bottom
15 line of what's on there. That was -- actually, I
16 should mention that the first -- can I go back on
17 that?

18 MR. LEGOWER: Oh, yeah, go ahead.

19 MR. GORDON: Yeah, how do I go back?

20 MR. LEGOWER: The red button.

21 MR. GORDON: This one?

22 MR. LEGOWER: Yeah.

23 MR. GORDON: Okay, so I should mention, the
24 model, when we originally developed it, we were being
25 supported by NSA. And -- going forward -- that's

1 okay.

2 And DHS actually was very interested in what
3 kind of incentives we could give to the private sector
4 as a Government, you know, to increase security, and
5 so we looked at some of the issues. And this was one
6 of the things that we talked about in our report.

7 But there's no absolute. I'm not lost in
8 the mathematics. I think the mathematics gives you
9 insight, and then, actually, you know, looking at a
10 process.

11 MR. LEGOWER: So, I want to follow up. So,
12 you know, the first picture here, the declining
13 function -- or, sorry, the function that's increasing
14 at a decreasing rate, that's the productivity of
15 investments.

16 MR. GORDON: Right.

17 MR. LEGOWER: So, I think Sasha was alluding
18 to this earlier, that, like, nobody really knows the
19 shape of that function to some extent, right? And
20 it's a big component of, you know, where the optimal
21 point on that curve is, is what that curve looks like.
22 So does anybody -- Larry, you can start us off, but
23 does anybody have ideas on, like, how we can maybe go
24 about estimating what that curve looks like?

25 MR. GORDON: So we originally -- what we

1 looked at was different -- we called them security
2 breach functions, so we looked at different
3 productivity functions of investments, okay? And
4 based on a couple of broad classes of investment
5 productivity functions, we were able to show that
6 there is an optimal level, and it's much less than a
7 lot of people think. It's, you know, roughly one-
8 third of the expected loss. Mathematicians around the
9 world started to say this is nonsense. I got emails
10 saying this is voodoo economics, and then eventually a
11 mathematician in Russia and one in France around the
12 same time said these guys stumbled on something that's
13 more powerful than even they realized. He was right
14 for me but not my colleague. He knew it was right.
15 Okay?

16 So Marty Loeb, who's not here, I went to
17 Marty, and said, maybe the guy's right. These were
18 math professors, and he says -- and we did look at
19 different productivity functions, but you can find
20 some that it doesn't work. All that graph is intended
21 to show is there's diminishing larger returns to
22 levels of investments. You know, you put in -- you
23 know, if you look at your opportunities, you should be
24 able to get more for the first million than for the
25 second million, whatever investing in. If it's a

1 smaller company, more for the first 10,000 than you'd
2 get for the next 10,000.

3 And, so, ever since the Better Business
4 Bureau came out and recommended the framework --
5 again, they recommend the framework. They don't say
6 get lost in the mathematics. I've had lots of small
7 companies come and talk to me, and I talk about the
8 framework. You know, it's a process. You're better
9 off to use some formal process than just, you know, ad
10 hoc, poof, some number out of the air. And you're
11 never going to get them right, and one big breach and
12 the whole thing falls apart.

13 MR. SHARP: So, the folks with Rich Seiersen
14 and Doug Hubbard did some additional research that I
15 think complements and maybe contradicts in some
16 places, but what they were able to do is start from
17 the foundation that there is a way to make calibrated
18 predictions about things that we can't measure today
19 or have been unsuccessful because we don't have the
20 adequate information to measure today.

21 And I think the other thing that they
22 highlighted was that there's some false thinking out
23 there stemming from statistical illiteracy around how
24 much data you need to come up with functional models.
25 But at the end of the day, what is true is using

1 calibrated assessments with folks who have expert
2 judgment, you can get fairly accurate estimates of
3 probability. And I think using that information with
4 a properly calibrated expert you can actually get
5 fairly accurate estimates.

6 But to -- I forget was it Sasha or you,
7 Tyler, the validation that this is, in fact, the
8 appropriate curve or this is the best model, I don't
9 think we have empirical evidence to support that part,
10 right?

11 MR. GORDON: I agree completely. So I
12 should just tell you, we had a consulting firm in D.C.
13 -- I won't mention the name -- said, let's take your
14 model and we'll go to all of our clients, and we'll
15 bill you out at a high rate and you'll get a great
16 consulting fee. My response was, what, are you crazy?
17 Any number we give them is not going to be the right
18 number, but you're better off to go through a process.
19 Let them try -- each firm is different, and exactly
20 what Matt said, with the right experts in the firm,
21 they can -- it's better than just pulling numbers out
22 of the air.

23 And over time, I would argue, the same way I
24 would argue for net present value models, I would
25 argue that they're better off doing it that way than

1 just ad hoc be pulling numbers out. And I think, you
2 know, what our other Matt said was that even the
3 insurance companies, you look at what kind of
4 information you're trying to protect, what is it
5 you're doing. You know, and so it's a formal process.

6 And, so, even though you may have thought
7 I'm going to come in here and try to sell you on the
8 mathematics, I'm not. You know, I understand -- there
9 is some real mathematics underlying this.

10 MR. MOORE: And I think in some sense the
11 question is, like, you know, the question may have
12 been, you know, how can we collect data to maybe, you
13 know, best validate what this model is. I think maybe
14 that's not the right question. I think the real
15 problem that we face is that we don't have data on
16 effectiveness of controls, right?

17 And, so, we maybe have some point estimates
18 of the likelihood of different categories of security
19 events like breaches and how they could vary by
20 sector, but what we have very little insight right now
21 onto is how effective these particular security
22 controls are or even this class of security controls
23 are against these kinds of threats. And if you were
24 to increase your investment in this control or across
25 these suites of controls, how would that reduce your

1 expected losses? And we just have no idea.

2 Okay, I think I've been provocative enough
3 to elicit a disagreement, but the -- I would argue we
4 don't think we have a good sense of what the -- you
5 know, what the true cost of an attack is and, more
6 importantly, how effective certain defensive
7 countermeasures are. And I think part of the reason
8 why is I think there is just not a lot of interest
9 among the vendors and designers in the cybersecurity
10 industry in providing this. And it's hard to do. I
11 think it's very hard to do, but it's also not
12 something that they're interested in providing, and so
13 I think fundamentally that's something that we need to
14 make more progress on if we're going to get more
15 effective security investment. Now Sasha?

16 MR. ROMANOSKY: Yeah, so, yeah, that's true.
17 So I was initially -- I probably sounded very critical
18 of the insurance industry, and I don't mean to be. I
19 probably was when I initially started doing some of
20 this research, that, you know, oh, my God, we all turn
21 to insurance companies because we think that they
22 should have the perfect answers for everything and
23 they should be these wonderful seers that can provide
24 perfect investments.

25 And, so, I started looking at these rate

1 schedules and saw that, look, this is not quite great.
2 But the reality is that even I wouldn't know how to do
3 a completely accurate assessment, right? I can give
4 you a good idea of what to look for, but even I
5 wouldn't be able to do that. And I think they're
6 trying, right? So, you know, you can see the
7 evolution of these policies evolving over time, and I
8 think that's a good thing.

9 I do think that they provide the only
10 opportunity to get at exactly the kind of data that we
11 really want, right, exactly the kind of answers that
12 we want to understand, which is what kinds of security
13 controls matter and by how much. And they have that
14 through the claims data. And this isn't rocket
15 science, right? All this takes is a little bit of
16 statistics, a bit of a regression.

17 So you can imagine in your head a
18 spreadsheet, where all of the rows represent the cyber
19 policies that a carrier has or a group of carriers
20 have, right, so every policy. The columns -- the
21 first column represents whether or not a claim has
22 been filed, yes or no, say in the past 12 months. And
23 all of the other columns represent properties of those
24 firms, the industry, the size, number of employees,
25 and then answers to the security questionnaires, what

1 kinds of controls they actually had.

2 And you just run a regression, and you get
3 an answer. And maybe it's not a perfect answer.
4 Maybe you don't -- maybe not everything is
5 statistically significant, but you start to get at a
6 sense of here are the kinds of processes, procedures,
7 security controls, whatever, that actually matter and
8 then predict in a statistical way of affecting whether
9 or not a breach occurs and a claim has been filed.
10 Right? That's it. It's nothing more sophisticated
11 than that.

12 Yes, there are issues with data and data
13 cleaning, and do we have the right kinds of questions
14 and whatever, but that is one way -- that is the only
15 way that I know of to be able to get at a way to
16 validate this model and get at very useful kinds of
17 questions.

18 MR. SHARP: And I would just say there may
19 be some sampling bias. Having worked at a couple of
20 firms and actively participated in a process of
21 helping companies respond to data breaches and other
22 kinds of security compromises, I think it's very rare
23 that those data breaches actually get publicly
24 disclosed, so I would say, you know, fewer than 2 or 3
25 percent, if I had to put a number on it.

1 And, so, I think the information that we do
2 have that would come out of the insurance folks should
3 be properly caveated to take into account that there's
4 a set of drivers that cause people to disclose and not
5 all data compromises or security incidents or what
6 have you are effectively represented in the data that
7 the insurance companies have.

8 MR. ROMANOSKY: Dude, my research is full of
9 caveats. I have no problem with caveats. But that
10 doesn't mean it can't be done.

11 MR. SHARP: Sure.

12 MR. ROMANOSKY: That we can't try.

13 MR. SHARP: Yeah.

14 MS. JILLSON: So firms are reporting that
15 they are spending more money on cybersecurity. Do you
16 think that even if we don't know necessarily what
17 controls are the best in particular instances if we
18 don't have that kind of data, can we look at kind of
19 overall spend to get a rough sense as to the security
20 at an organization?

21 If you're coming -- if you're looking at it
22 from a regulator's perspective or if you're coming
23 into an organization as new security personnel or on a
24 consulting gig, can you look at that rough spend and
25 get some sense as to likely security?

1 MR. GORDON: If you had the number, that
2 would be great. The problem is firms don't report how
3 much they spend on cybersecurity. I've got about ten
4 studies. I'm sure everyone else who does research in
5 the area has about ten studies waiting to go if they
6 had that kind of a number. In fact, I actually --
7 when I testified in Congress, I actually said one of
8 the things that would be great if we could have is
9 somehow have firms report how much they actually
10 invest in cybersecurity.

11 MR. MCCABE: It's a really common metric for
12 when you're applying for cyber insurance, how much,
13 but it's also very difficult to ascertain because it's
14 not necessarily a clean budget item. You have cyber
15 investment in a lot of different disciplines.

16 MR. GORDON: They're giving you private
17 data. That's not publicly available.

18 MR. MCCABE: No, it's confidential.

19 MR. GORDON: Yeah, that's what I mean. It's
20 hard to --

21 MR. MCCABE: Yeah, it's not in their 10-K.

22 MR. GORDON: Yeah, right. That's what I
23 meant.

24 MR. MOORE: I mean, there's definitely
25 going to be correlation. I think that -- I think

1 the correlation is going to be very noisy. And,
2 furthermore, because we have these problems about
3 information asymmetries, about the quality of
4 investments, we have these systematic -- systemic
5 problems that will make it very, very noisy. That's
6 what I'd say.

7 MR. SHARP: So there are some sources of
8 data like Gartner and Forrester and IANS and other
9 folks who do aggregate benchmark data and then share
10 that functional data. I mean, it's a part of every
11 CISO's pitch deck for whether you're getting more or
12 less funding. You include it when it helps you and
13 you don't when it doesn't.

14 MS. JILLSON: All right, let's turn now to
15 another slide. So this is a polling question, so I'd
16 like to ask this question to the panel. So who
17 provides or should provide incentives to invest in
18 data security? And to a certain extent, this overlaps
19 with where we started our discussion.

20 So A, culture, which could be security
21 professionals, executives, or boards.

22 B, customers or consumers.

23 C, cyber insurance.

24 D, law, whether the source of that is state
25 statute, state of breach litigation, federal agencies.

1 Or E, other. Or you can choose some
2 combination thereof.

3 So let's run down the panel and hear each of
4 your answers. And let's do the reverse from last
5 time, so let's start with Larry.

6 MR. GORDON: It's simple. A through D and
7 probably add E, also. You can come up -- you know,
8 there's no one incentive. That's what -- you know, we
9 started off with incentives. There's no one
10 incentive. I know one thing, the SEC certainly has
11 now become very interested in cybersecurity risk,
12 starting in 2011 when they came out with their
13 disclosure guidance from the Corporate Finance
14 Division; then in 2018, when the Commission came out
15 with a statement on cybersecurity risk and then in
16 2018, on top of that, when the Enforcement Division
17 came out with internal controls, accounting internal
18 controls should take into consideration email
19 breaches. And I think these are all incentives. And
20 I think every one you got listed there, as I look at
21 them, you know, you can pick one, but I think they're
22 all important. I think they're all important. I'm
23 copping out on you, but I really -- I believe that.

24 MR. MCCABE: Yeah, for D, I don't really
25 look at things like litigation and mandated compliance

1 regimes as an incentive. I view that as the other
2 side of the coin. An incentive should really be
3 about, okay, other than meeting my bare minimum
4 compliance requirements, what are my interests in
5 going above that model? And there's a lot of ways to
6 achieve it, as Larry said. I mean, I think what you
7 really do it for is A and B. You do it for your
8 corporate reputation, and you do it to make sure that
9 you have customer trust and that you're going to have
10 that good faith and that good name, but I think that
11 there's a lot of mechanisms in which the Government
12 can participate to provide incentives.

13 I would give as an example from the
14 terrorism world the Department of Homeland Security's
15 Safety Act, which gives litigation protections for
16 companies that are able to demonstrate that they have
17 security that is more likely than not to deter a
18 terrorist incident. You can apply for Safety Act
19 protection. Things like that I would consider more of
20 an incentive rather than the Luca Brodsky incentive of
21 you've got to do this.

22 MR. MOORE: Okay, I will do a variation on
23 what Larry said, and I'll give you a rank ordering.
24 So I think ideally it would come from the customers
25 and consumers. And in the cases when you can get

1 that, when the consumer demands sort of naturally
2 align, let's go with that, that's great.

3 It doesn't always work out. And when it
4 doesn't work out, you better hope that the companies
5 themselves have a culture to make the right
6 investments and to do the right thing. And if that
7 doesn't -- and one of the ways in which that could be
8 magnified is through cyber insurance in that it can
9 provide sort of an outside perspective to sort of
10 validate what you're doing and also provide some sense
11 of, you know, what the true cost of insurable events
12 are, so that sort of can magnify, you know, a company
13 whose culture is already in the right place.

14 But, then, I think the last step has to be
15 the law, and I think because you're not going to get
16 complete coverage from just those first three because
17 of the presence of the market failures I talked about
18 earlier.

19 And in terms of what the law can do, I think
20 the law can do steps to remedy those actions. In
21 particular, try to mitigate the information
22 asymmetries by collecting and disseminating data that
23 would enable us to evaluate security controls more
24 effectively, for example, by having increased
25 disclosure about cybersecurity risks, some of which

1 we're already seeing through the SEC guidance, as
2 Larry alluded to.

3 You know, litigation, as a stick, in the
4 event of companies that just are not acting in good
5 faith. And, so, that's the order in which I would put
6 it. I think you need them all. There you go.

7 MR. LEGOWER: That's kind of interesting.
8 It seems like you're implying that the law should sort
9 of act as a force multiplier for the first three.
10 It's like you should give information to consumers so
11 that consumers can direct incentives. You should, you
12 know, impose liability so that cyber insurance has
13 teeth and things like that.

14 MR. MOORE: Absolutely. I'm a believer in
15 capitalism. I think, you know, when you have to have
16 government intervention, it needs to be in order to
17 make private markets work better.

18 MR. ROMANOSKY: Yeah. So I think D
19 starts -- provides the floor, right? It's a
20 compliance, the statutes, the enforcement actions,
21 it provides the floor, and then comes from customers.
22 So to the extent the customers actually care about
23 firm behavior, they have an opportunity to drive
24 things. I don't see that happening, right?

25 We had a discussion earlier about the extent

1 to which firms invest and respond to -- whether or not
2 firms compete on privacy and security. And I don't
3 think investment in different kinds of technologies
4 provides you that answer, and I don't really see that
5 much of a market for it anyway. It's an old problem,
6 and we've talked about it a lot, but I don't see it
7 changing.

8 I think the firm -- the board -- I don't see
9 much of an impact from A, right? The board's going to
10 respond to costs and different threats, and those
11 costs are going to come from consumer behaviors. And,
12 again, if the consumer behavior isn't there, if, like,
13 that pressure isn't there, they're not going to
14 respond.

15 And the same with cyber insurance. Right
16 now, you know, I just don't see it as having a great
17 opportunity for driving incentives.

18 MR. SHARP: Yeah, I'm remarkably aligned
19 with what Sasha shared. The law and the compliance is
20 driving the floor. And for those folks that are
21 looking to be checking the box, that helps pull them
22 back into reality and do the right thing, but for
23 those folks that have come to the conclusion that
24 cyber resilience makes sense, then you have a
25 combination of customer demand in a culture that's

1 driving the story forward. And I think that cyber
2 insurance is a part of an overall risk management
3 strategy, but I don't see that as an incentive,
4 frankly, at all.

5 I think when you think about drawing up the
6 laws, it's important to consider we have organizations
7 with varied business models. That means different
8 margins and ability to invest in things. And we also
9 have a different size and scale of organizations, and
10 so, not that this is news to you guys, but what that
11 means is that you have an entire set of "check the
12 box" customers that we encountered in my consulting
13 days quite frequently that would benefit a lot from
14 increasing the floor.

15 And then I think what you find on the top
16 end is compliance can be disruptive and redirect
17 investments in unhealthy ways. So for example, we
18 help people move to the cloud. When people are in the
19 cloud, the technology behaves very differently, but
20 the rules and the compliance standards are written in
21 ways that make us have to jump through additional
22 hoops in order to solve things in ineffective ways
23 when we can get stronger security outcomes using new
24 technology paradigms, so I just would also put that on
25 the docket.

1 Compliance certainly does, for those more
2 innovative and secure firms, actually create a drag,
3 and that's an unfortunate reality.

4 MS. JILLSON: I want to thank all of the
5 panelists for their time and their insights. We are
6 now going to take a 15-minute break. We'll start back
7 here at 2:45 with a panel discussion of consumer
8 demand for security.

9 (Applause.)

10 (Recess.)

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

1 CONSUMER DEMAND FOR DATA SECURITY

2 MR. HO: Okay, good afternoon, everyone, and
3 welcome back to the third session of the day on the
4 consumer demand for security. Again, my name is Jared
5 Ho, and I'm an attorney in the Division of Privacy and
6 Identity Protection. I'm joined by Mark Luppino, an
7 economist in our Bureau of Economics.

8 We'll start out this session today first
9 with a presentation from Justin Brookman from Consumer
10 Reports on the standards that Consumer Reports uses to
11 evaluate security.

12 Then we'll kick it off to a moderated
13 portion of our panel with a polling question. As with
14 previous panels in the morning, there will be event
15 staff walking around with question cards. If you have
16 a question, please flag one of them down. They will
17 collect the cards and pass them up for us to read.

18 And with that, do you want to give
19 introductions?

20 MR. LUPPINO: Sure. I'll briefly introduce
21 our panelists. To my left we have Justin Brookman,
22 who is the Director of Consumer Privacy and Technology
23 Policy for Consumer Reports Advocacy.

24 Michael Higgins is a 30-year veteran of the
25 information security industry and has previously

1 served as the CISO for NBC Universal, The New York
2 Times, and LexisNexis.

3 Wiley Hodges is a Director in Product
4 Marketing in Apple.

5 Kirsten Martin is an Associate Professor of
6 Strategic Management and Public Policy at George
7 Washington University School of Business.

8 And Rick Wash is an Associate Professor at
9 Michigan State University in the Department of Media
10 and Information, where he codirects the Behavioral
11 Information and Technology Lab.

12 With that, I will turn it over to Justin.

13 MR. BROOKMAN: Thanks. Can I have the
14 clicker?

15 Thank you. So I was asked to give a little
16 presentation on what we're doing at Consumer Reports
17 around demand for security. So, first, just a couple
18 words about Consumer Reports in general. I think most
19 of you all know we test lots of stuff, right? We have
20 8 million members now, test about 7,000 products a
21 year. I think generally we're recognized as
22 independent and expert and data-driven in the advice
23 and information we make available to folks.

24 A few years ago, though, I think we started
25 to recognize that we really weren't capturing all the

1 elements, all the lot of modern products, especially
2 connected in smart products. So we started to think
3 about how can we start to do tests and evaluate
4 products and services for things like privacy, for
5 things like security, for things like ownership,
6 right? Do we even own our products anymore? Do we
7 have the right to resell them, the right to repair
8 them? Things like interoperability. I have a bunch
9 of smart things in my house. Will they talk to each
10 other? How do you give and evaluate points to
11 products based on that sort of thing.

12 And, so, the Digital Standards, a project we
13 launched a couple of years ago, originally Consumer
14 Reports sitting down with some partner organizations,
15 ranking digital rights, who's part of New America, the
16 Cyber Independent Testing Lab, and Disconnect Me makes
17 privacy tools like the Disconnect ad blocker, and
18 started to think, okay, if we're going to evaluate
19 products based on privacy and security, what are the
20 criteria, what are the elements that we're going to
21 look for.

22 And, so, we published this document online.
23 It's available if you search for the digital standard.
24 It articulates things like, you know, product support
25 over time, control of your information, what do the

1 policies say. It's an open-source document. It's
2 available on GitHub. We're constantly reevaluating it
3 and looking at it and tweaking it. I'm going to spend
4 some time in the document on Friday, making some
5 suggestions based on some of the testing we've done so
6 far. So if you have ideas and you want to take a look
7 and think about some of the things that we suggest and
8 make some suggestions for refinement, we would
9 certainly appreciate that.

10 And, so, I wanted to talk just a little bit
11 about some of the actual elements in the standard for
12 things that we look at on data security. So use of
13 encryption, is data transmitted encrypted on the
14 device, is it encrypted in transit? Ideally, we would
15 look to see if it's encrypted in the cloud server
16 side, but that's hard for us to evaluate.

17 Commitment to support periods, a really
18 important thing for us. Right now, there's not a lot
19 of information available to folks about how long. If
20 I buy a smart TV, will it be supported for 5 years, 10
21 years, 20 years, 1 year, no year. Not a lot of
22 information available about that.

23 When I was here at the Federal Trade
24 Commission a couple of years ago, we did a report on
25 smart phones, how long smart phones are supported for.

1 Found just a vast, wide range of practices, right?
2 Some super expensive flagship phones just didn't get
3 any support, were vulnerable to attack straight out of
4 the box. Some phones got supported for, like, years
5 and years and years. Right now, not a lot of
6 information for folks about that.

7 Resistance to attacks, there are certain
8 penetration tests we can do in our labs about things
9 to see if things are vulnerable to certain common
10 types of attacks, and can we do that ideally without
11 violating the Digital Millennium Copyright Acts?

12 Passwords, again, obviously the passwords
13 should not be passworded out of the box, but do they
14 support long passwords, do they allow cut-and-paste
15 from password managers, do they have a bug bounty
16 program, so they allow/encourage third-party
17 researchers to come and say, hey, we found this
18 problem on your site, a process for taking those sorts
19 of things into account.

20 Security oversight, do they have a security
21 oversight program? Again, hard for us to test. We
22 may not be able to have a lot of visibility into that,
23 but there may be some indicia we could look at as
24 representing that they have with a program in place.
25 Do the updates happen automatically? Even if a

1 product is supported, it's not going to do a user a
2 lot of good if my router software is available on
3 Router.com but doesn't come to my device, maybe give
4 credit for automatic updates that are pushed to the
5 device.

6 On the other hand, what if they're bundled
7 with functionality updates as well? There is recently
8 criticism of Epson for bundling security updates with
9 updates that actually impinged upon someone's use of
10 the products, so how do we consider that? Multifactor
11 authentication, something that can in some cases be
12 useful for security.

13 Best build practices, is the product not
14 overly complicated, is it not overly reliant on third-
15 party code and libraries, which might introduce some
16 fragility into the system? Are folks told about
17 changes if my password's changed, will I be told about
18 it by email or some other service?

19 And, then, are updates authenticated, is it
20 actually authenticated from coming from the server or
21 from the manufacturer? This is just a handful of them
22 that I thought it would be useful to kind of, like,
23 walk through what we're thinking. There are more on
24 the site and that we're trying to operationalize in
25 some of our testing.

1 And, so, the goals of this should be
2 obvious. Right now, there's not a lot of information
3 readily available to folks in the marketplace about
4 privacy and security practices, so if folks do want to
5 make security-conscious choices, this will empower
6 them to do so.

7 At least as important is kind of pushing the
8 supply aside as well. Right now, I think a lot of
9 companies don't have accountability for dodgy
10 practices. They kind of skate by on ignorance of
11 folks knowing what's going on. If we give a company a
12 low rating, they get mad at us. They take these
13 things seriously. They'll call us and complain and
14 occasionally sue us. So if we can introduce some
15 degree of accountability for practices that -- I think
16 we've all seen in the security space a lot of, like,
17 common practices are actually just things that could
18 easily be remedied.

19 Certainly a lot of FTC's data security
20 practices are things that really should have been
21 captured but somehow they just skated by on. I think
22 the Equifax security breach, which was reported on in
23 the Senate oversight hearing the other day showed
24 things again that really should have captured from the
25 beginning. If we can push folks on the supply side to

1 think more about these things in advance, I think
2 that's good for the ecosystem.

3 And, so, I'm going to walk through a couple
4 slides about, you know, how we've been doing this, how
5 we've been kind of like building out our program,
6 originally just looking at kind of -- occasionally
7 things like apps, like so investigative journalism
8 type things. Here's an app we looked at called Glow,
9 which is a woman's fertility app. It has access to
10 super-sensitive information about folks, and we dove
11 into it and found, like, a lot of sort of security
12 vulnerabilities. Again, things that could have easily
13 been addressed. Passwords could have been changed by
14 attackers. Attackers could get access to pretty
15 sensitive stuff without being authenticated.

16 In this case, we did responsible disclosure,
17 went to the app manufacturers, explained at length all
18 of our findings and concerns, and before we published,
19 we got them to address them. But this is how we first
20 started thinking about how do we apply the digital
21 standard in practice.

22 Then, last year, we did an expose on some
23 smart TVs on data security and privacy. On security
24 again, we didn't see any of these companies promising
25 to update software, provide security support for any

1 period of time. So consumers had to kind of go in
2 hoping and guessing.

3 We found a couple of security
4 vulnerabilities in the Samsung and Roku TVs.
5 Attackers would be able to change channels and put on
6 objectionable content and put the volume to 99.
7 Again, more nuisance type stuff, but things that
8 probably should not be possible to be done. I know at
9 least in the case of Samsung, they agreed and did
10 actually update their software to address the
11 concerns.

12 On the privacy side, just recently I worked
13 on a -- at the Federal Trade Commission as well, a lot
14 of smart TVs have the capacity to watch what you're
15 watching, so they will take snippets of what you're
16 watching and send it back to the lab, and then they
17 can kind of build out a pretty dense behavioral
18 profile about all the things that you do on your
19 television.

20 I think because of the FTC's work on the
21 Vizio case, they all kind of asked for permission,
22 they all push you through some screen where you had to
23 press okay. Varying ways of doing that, varying
24 degrees of how good that was. Again, from Consumer
25 Reports' perspective, you know, how do we evaluate

1 user design like this, how do we give points for how
2 big the okay is and where the skip or don't or say no
3 button is. So definitely a concern for us about how
4 to evaluate on privacy, but also for security choices
5 as well.

6 And, now, more recently we started to
7 actually translate these into Consumer Reports
8 ratings. So this is one from a couple of months ago.
9 We looked at some mobile peer-to-peer payment
10 services. Fortunately, to avoid any awkwardness in
11 this panel, Apple ended up doing quite well in this
12 evaluation. You can see we look at things like we
13 might look at otherwise like authentication, is there
14 customer support. Do folks -- but then two of the
15 five categories that we have are also on data privacy
16 and data security.

17 And ApplePay is actually very thoughtfully
18 designed to actually limit the amount of information
19 that Apple itself ever collects by any transaction to
20 limit the way that any information could be used for
21 identity theft in the future. So in this case, Apple
22 did really quite well on both privacy and security.

23 The other companies, you know, getting in.
24 It's hard to test, right? I mean, the information
25 could be sold or leaked or used on the back end

1 without a lot of visibility. And to us, we had to
2 rely in large part on the disclosures they make, and
3 some of the companies reserve pretty broad rights to
4 do lots of stuff with your personal information. So
5 in this case, they ended up scoring not as well. And
6 these were things that were incorporated in the
7 overall score.

8 Some of the challenges that we're
9 confronting so far. So, one, we actually have to rely
10 on documentation in a lot of cases, and it's often not
11 really illuminating. You all have looked at privacy
12 policies. Privacy policies today are not really
13 designed to convey meaningful information to folks.
14 They are compliance documents that are designed to
15 evade liability. So if you're actually trying to look
16 at what companies are doing on privacy, it's actually
17 hard to tell. Even if you had the time, like I do, to
18 review privacy policies for a living, it's hard to get
19 a lot of information about it.

20 Right now, we don't have a lot of
21 information about how long products are being
22 supported, like I said. I think we'd like to build
23 that out over time if, in fact, Samsung washing
24 machines get updated longer than others. Would you
25 want to be able to say that? That could go into some

1 sort of reliability type metric that could be
2 incorporated into ratings overall.

3 Right now, we don't have that. Right now,
4 there's not a lot of ground troop we can point to.
5 Even trying to go back in time and try to figure out
6 how long the products have been supported is actually
7 quite challenging but something that we're committed
8 trying to figure out. Some things it's really tough
9 to test. You know, do we have to compile every
10 software system? I mean, even if we could, it's
11 actually quite challenging and expensive to do that,
12 and then there are lots of things we can't, like,
13 again, anything server side, we don't have any insight
14 into. There, we have to rely on the documentation.
15 Like I said, there's not enough information that we
16 would like.

17 And, then, you know, how you translate a set
18 of tests to a constantly evolving set of product
19 buckets. You know, products are different. They may
20 have different threat models. They have access to
21 different types of information, so access -- you know,
22 information on the phone is very different than on a
23 smart TV. And, so, how do you do that sort of
24 changing and testing at scale?

25 You know, scores are going to be subjective.

1 You know, we try to make them as objective and
2 repeatable as possible, but you're going to, you know,
3 identify 12 out of a handful of criteria that we're
4 trying to compress into a fairly narrow set of
5 information, and how do you do that reliably and
6 fairly?

7 How do you give points for vulnerabilities
8 that they actually patched? Like the example of Glow,
9 we looked at like -- we found, like, a bunch of
10 different vulnerabilities. And, so, if the company
11 says, okay, we patched them all, give us a perfect
12 score, like how do you take into account what may have
13 changed? And, like -- and things change overnight,
14 right? I mean, a software update can change
15 everything radically. It might not even be a software
16 update. It could just be some interface change. It
17 could be a policy change; it could be a practice
18 change that we don't have any way to check for.

19 And, so, how do you -- again, if you're
20 testing 7,000 products, not all of which are connected
21 but more and more are, how do you set up systems to
22 keep track of them over time and to make sure the
23 scores are accurate.

24 And then, you know, just in closing, I think
25 this may -- I think this will probably transition to

1 some things that the panelists are going to talk
2 about, that I think the demand-side approach is
3 incredibly important and providing more information is
4 essential. I don't think it can entirely solve the
5 problem.

6 So, one, like, you know, not all security
7 threats are felt by consumers, right? If my smart
8 refrigerator is being used to DDoS Jared, I may not
9 care, right? It's not affecting me, so I'm not really
10 incentivized to price that into my smart TV or smart
11 refrigerator choice.

12 Folks sometimes have trouble assessing
13 security risks. One, this is complicated stuff. A
14 lot of folks don't necessarily understand all the
15 security ramifications from a connected or smart
16 device. Even if they did, consumers are not
17 necessarily great at assess tail risk, right? This is
18 a essential part of behavioral economics. People
19 underprice risk, which is why, you know, we made the
20 policy choice to mandate seatbelt use in cars.

21 Testing will provide imperfect data. We
22 don't have access to everything, so we're trying to
23 input more information into the marketplace, but it's
24 not as precise as -- you know, this company is
25 providing \$13 worth of security. It's necessarily a

1 lot more "lossy" than that.

2 And attribution is going to be -- is always
3 going to be delayed and if at all possible in the
4 security space. If my information -- if I'm subject
5 to identity theft five years down the road, they may
6 not know that it was X company's practices that did
7 that five years ago. So there's definitely some kind
8 of disconnect between my market choices there.

9 So for these reasons, I think it's kind of
10 essential that information's important but we probably
11 -- we definitely need policy enforcement as well, so
12 encourage the FTC to encourage what it's been doing
13 under Section 5 but ideally with a dedicated security
14 statute, too.

15 And with that, I'll turn it back to you all.

16 MR. HO: Great. And thank you, Justin, for
17 that presentation. And I know that we'll be returning
18 to questions about the tools available for consumers
19 to comparison shop based on security later on in our
20 discussion.

21 But, first, I want to turn to a polling
22 question. And it's really more of a scale than it is
23 a polling question but so in our last panel, it was
24 suggested that, you know, some folks were not entirely
25 convinced that there is a consumer demand for security

1 or that perhaps that consumer demand isn't quite there
2 yet. And I think that this spectrum or this polling
3 question sort of gets to that.

4 And, so, you know, I'd like to sort of ask
5 our panelists sort of what their thoughts are on the
6 consumer demand of security and sort of where you
7 think that we fit on this scale. You know, on one
8 end, you know, is security important to -- is security
9 important to consumers and who bears sort of the
10 responsibility for security? Do they expect that
11 firms bear the responsibility solely or do they
12 understand or appreciate that it's a shared
13 responsibility between firms and themselves?

14 You know, is it a moderate sort of
15 appreciation or demand for security, or do folks feel
16 as though consumers don't expect security in the
17 products or some, you know, other category?

18 So why don't we start with Rick, and we can
19 go down the line.

20 MR. WASH: Sure. I really like this
21 question. There's a logical option that's actually
22 missing. It says firms are responsible; there's a
23 shared responsibility. The third logical option is
24 that consumers are entirely responsible, and that's
25 actually not an option in this, and I think that's a

1 good thing.

2 So my opinion, in my experience and in my
3 work, I found I think B is the closest, that people
4 seem to really think that security is important.
5 People I talked to, they spend a lot of time trying to
6 figure out, especially as they use consumer devices,
7 as they use apps and websites, they try to figure out
8 what they can do to help security.

9 They often see it as a balancing act between
10 what it is they're trying to accomplish and what the
11 security goals are. I hear a lot of end consumers
12 talking to me about how they are told something that
13 they're supposed to do about security, such as don't
14 write down your passwords, and then they realize that
15 they can't get their -- they can't accomplish their
16 goals if they actually follow the security advice that
17 they've been given, and they spend a lot of time
18 trying to find a middle ground.

19 So it's not that they're just going to
20 ignore the security advice; it's that they're going to
21 try to find a similar advice that they could give
22 themselves that they feel accomplishes the similar
23 security goals but still allows them to get their work
24 done. And, to me, that's a real sign that they think
25 security is really important, but they see it as kind

1 of a shared responsibility. They don't know -- they
2 know that they don't know everything about security.
3 They look to advice from experts and advice from
4 people like the FTC to try to figure out what they
5 should be doing, but then they have to adjust that
6 advice to whatever situation they're in and what their
7 life is like.

8 And that adjustment process is the really
9 hard part, and I think that's where things are getting
10 lost a little bit right now. So I would say B.
11 People mostly think it's important, but they see it as
12 a shared responsibility between themselves and the
13 firm.

14 MS. MARTIN: So I agree with you,
15 especially around when we think about at the
16 workplace. I wonder about consumer-facing products
17 if it isn't closer to A and that they don't see
18 themselves as being a point of vulnerability to a
19 larger system. I think when we're at the workplace
20 and we have to not write down our passwords and we
21 have to have two-factor identification and all the
22 academics get really mad and they don't want to do it,
23 but we kind of understand that this is part of the
24 larger system, that we have to do it to keep our
25 system safe.

1 And I don't know that they see it as a
2 shared responsibility when they set security on their
3 refrigerator or they might see it on my phone and I
4 don't want my phone to be hacked and made into a brick
5 but not as a part of a larger system. Similar to when
6 in -- not that they shouldn't. They should see it as
7 part of a larger system, but I'm not sure that they
8 do.

9 Interestingly, we do think of that that way
10 around regular security with, like, the ideas of see
11 something, say something, that we're all points of
12 vulnerability in a larger system, but when it comes to
13 cyber, that messaging doesn't come through. There
14 isn't that constant vigilance. So I would put us at
15 A.

16 MR. HODGES: I think I would want to get a
17 hybrid of some of these, of course. I want to pick
18 and choose because I think that the concern about
19 security is uneven. I think that consumers tend to
20 place a high value on security in situations where
21 they understand that there are security implications
22 of the decision they're making. So one of the most
23 salient examples being exchanging payment credentials
24 of some sort because they've been conditioned to
25 expect that that's a security moment in their lives.

1 But I actually believe that they don't
2 understand always the implications of other things
3 that are at least equally important to security. For
4 example, I think updating software is a very important
5 part of security, and it's something that I think the
6 vast majority of consumers don't necessarily have a
7 firm grasp of in terms of its implications.

8 And, so, I think that they sense importance
9 to it in certain situations, and in others, they have
10 absolutely no idea. It might be the externalities
11 that were referred to earlier, of, you know, why does
12 Bob care if his smart TV, you know, is DDoS-ing Mary's
13 network. And at the same time, I think that there are
14 situations also where that risk to themselves and
15 other situations becomes more visible. So in the
16 news, there may be something.

17 So at a moment in time, I think a consumer
18 may have a great awareness of security and a great
19 demand for it, but I think on average, on any given
20 day, it's kind of an uneven thing.

21 MR. HIGGINS: I guess I'll be a little bit
22 of a naysayer here. I think there's an F here.
23 Present company excluded, I don't think the consumers
24 really think it's important at all. And I say that
25 with a lot of background information with what the

1 consumers are doing. I think they are more concerned
2 about that large-screen TV being able to be 4K or play
3 Amazon than they are about the security that's
4 imbedded in the TV to prevent Amazon seeing what
5 they're watching.

6 I don't think Best Buy, if you go to a Best
7 Buy tech employee he'll ever -- he's answered any
8 security question probably in the last month about the
9 security of a particular 4K TV. I just don't think, I
10 think -- and it's based upon what Justin said, the
11 externalities. We've made security violations of
12 consumers to be painless. We have made the fines for
13 stealing a credit card \$50, and nobody ever charges
14 that to the consumer for losing his credit card
15 because they're afraid they'll cancel their credit
16 card and go to a different credit card carrier. So
17 they move around.

18 We've made -- banking fraud was so pervasive
19 a few years ago before the nine federal agencies got
20 together and mandated every bank had to institute two-
21 factor because each bank was afraid because if they
22 instituted and put security in the consumers would
23 rebel and go to another bank. So I think we wish that
24 consumers were more important and more concerned about
25 security, but I think their actual feet on the street,

1 what their behavior is telling us is, sure, if you ask
2 someone as they walk by, do you think security's
3 important on your smart thermostat you have at home,
4 of course they're going to answer yes. But do you
5 think they asked the question when they were buying it
6 about what it's doing, where it's reporting, who is
7 seeing the data out of it? I just don't think actions
8 are speaking much louder than words in my opinion.

9 MR. BROOKMAN: Yeah, I think that's fair. I
10 mean, I was inclined to kind of come down in between
11 on moderately important because I think people
12 generally, as to privacy, they have a vague sense of
13 there are things out there that could attack them, but
14 I think when they're buying a smart TV, they're not
15 thinking of it because they're not aware of what any
16 possible risks could be, right?

17 I mean, when we did our story on smart TV
18 privacy, people were very surprised, like, oh, it
19 never occurred to me my TV might be listening to what
20 I would do. It never occurred to me that if I type in
21 my credit card information on my TV, that if it's not
22 encrypted, that it could be attacked.

23 So I think generally in the connected world
24 people have a vague sense, like, yeah, this stuff's
25 important. Being able to make individual choices,

1 which is why we're trying to provide some more
2 accountability for it is actually quite difficult.

3 On the whose responsibility, I think that
4 this -- this I feel more firmly that I think people
5 expect it to be taken care of for them just because,
6 you know, the firms are the ones who are the experts
7 here, right? If I plug in my new smart hub home at
8 home, like I don't know, what should I be doing.
9 Nothing occurs to me as a consumer about what should
10 be done.

11 I expect that that's part of the product
12 that I bought, that the experts will have put in place
13 systems for authentication, systems to address all the
14 things that we looked at. I mean, a consumer is not
15 going to know whether there's a bug bounty program,
16 right? So I think it's part of the default
17 expectations that this is a responsibility of the
18 company.

19 MS. MARTIN: Can I just add -- I was just
20 going to say, I think there's two different things
21 going on here. One is, is it important to them; and
22 the other is do they trade on it in the market. And
23 those are two completely different questions to ask.
24 So is it important to me that my oven doesn't combust
25 and catch on fire? Absolutely. Do I ask if it's

1 going to combust and catch on fire? No. I just
2 assume it's not going to do that.

3 And, so I think that there is just an
4 assumption, and I'm not saying that this is correct,
5 there needs to be greater understanding by the
6 consumers, but that's why they're so surprised when we
7 ask them, did you know that Amazon is getting access
8 to this data? Did you know that the data aggregators
9 are sniffing up all of your information? Those are
10 privacy violations. Do you know that this was a
11 security violation? And they're like, no, I would
12 never have been okay with that.

13 So I do -- I think that they think it's
14 important, but they just assume like other certain
15 product features that the firm is taking care of it.
16 And, so, they aren't trading on it in the marketplace.
17 So that would explain their behavior, and yet they're
18 still shocked and upset when they find out there's
19 been a security violation.

20 MR. HO: So, Kirsten, that's actually sort
21 of a great segue into sort of our next conversation
22 slide on the tradeoffs. What are the other factors
23 that consumers are -- that might be considering and
24 that might go into the demand question.

25 But before we get there, so it looks like we

1 have, you know, a panel of highly esteemed guests, and
2 we have one A -- it looks like we have one A, one B.
3 Justin, I think you're more on the C line, and then we
4 have an E. So, you know, we can sort of see that
5 there's a wide range of sort of thought on this issue,
6 and so I think this next slide might sort of get us
7 into the conversation as to you know, why is there
8 this discrepancy, are there other factors at play.

9 You know, there certainly are. You know,
10 you flip on -- you know, you turn on the paper, you
11 read an article, and there's a security incident
12 almost every single day. What is the reason for
13 consumers buying, you know, poor security products?
14 Does it have to do with any of these factors on the
15 list?

16 And with that, I'll turn it over to Mark.

17 MR. LUPPINO: So, I mean, another prism that
18 you can think about this is kind of the prism of
19 product design, right, on the firm side. So how do
20 firms balance these competing concerns of consumers
21 that are kind of listed on the slide with concerns
22 about security? And the way they do that, is that
23 consistent with consumers' true preferences. And is
24 it useful to think about this problem in these terms
25 of tradeoffs? We can start with Justin.

1 MR. BROOKMAN: Well, I don't design products
2 for a living so I was going to someone who does.

3 MR. HODGES: Okay. I'll hop in since I do
4 design products for a living. I think, you know, one
5 of these strikes me as kind of a strange outlier, and
6 I know it's weird, it's top of the list, cost, because
7 I don't know that -- I think Justin even mentioned it
8 earlier. Like a consumer doesn't really understand
9 the \$13 worth of security. And, frankly, that
10 unevenness I mentioned also is reflected in what our
11 customers demand. So we have some who actually demand
12 a great deal of security from us, others who demand
13 none at all, and we need to meet everyone somewhere
14 that we can all be comfortable with.

15 All these other things are tradeoffs against
16 one another, though, and in general, our experience is
17 that we see the highest utilization and most
18 satisfaction with security features that are automatic
19 or nearly automatic, and our experience is that we
20 improve security outcomes and we nudge or make
21 invisible things that are good security practice.

22 So great examples are, you know, we found a
23 few years ago that less than half of our users were
24 setting passcodes on their phones, and that was a not
25 good thing because that's a foundational element of

1 security. And when we did a little -- honestly, not
2 much, it didn't take long to figure out what was going
3 on -- a little research, we found out they were
4 unlocking their phones on average 80 times a day, and
5 that kind of presented to us exactly why they weren't
6 setting passwords on their phone, the friction.

7 And, so, that's directly what led us into
8 looking at biometric authentication, our touch ID
9 feature, and later face ID really reflect that desire
10 to make something that's a much more natural and fluid
11 way of interacting with the device and still
12 preserving, you know, some amount of security,
13 hopefully a very good amount.

14 We also see this with things like two-factor
15 authentication. We rolled out various forms of two-
16 factor authentication for Apple ID, for example, many
17 years ago, and the adoption was abysmal. And part of
18 that was on us because we didn't really work to make
19 it seamless and transparent. Now, if you're migrating
20 from device to device, people don't actually realize
21 this, but very often they're actually effectively
22 setting up a two-factor authentication system and
23 installing tokens on their devices and all kinds of
24 things, and it's happening completely behind their
25 backs.

1 In some ways, I don't love not being
2 transparent about security, but as a marketing person,
3 I would love to trump it, what it's doing for you, but
4 also the fact that sometimes we don't love the idea of
5 not being fully transparent with our customers what's
6 happening, but at the same time, we've found that
7 that's where we get often the very best outcomes from
8 a security perspective.

9 So I'd say usability is probably the king
10 here, productivity along with it, and functionality
11 very nearly. I think latency is an odd one. I think
12 it may apply more to things like e-commerce situations
13 and things like that. From our perspective, what we
14 see is that various technical innovations are
15 continually removing any sort of computational or time
16 cost of the security feature. So we're not really
17 seeing that being nearly as big a factor.

18 MR. HO: And, Wiley, just to follow up. So
19 this slide is framed as tradeoffs, suggesting, you
20 know, one or another approach, but some people have
21 suggested perhaps it's more of like a scale or a
22 spectrum. And, so, you know, whereas the cost might
23 be a factor, there might be sort of a solution, so you
24 don't need to give up security for, you know, any one
25 of these things. And, so, how does sort of Apple

1 approach that on any of these factors?

2 MR. HODGES: Well, I think the answer varies
3 with the specific aspect of security. And, so, I
4 think a lot of it is an approach. You could call it
5 an iterative approach basically, where we will try
6 something that we think is encouraging a good security
7 behavior, we'll measure its effectiveness by looking
8 at uptake and the way our customers employ it, and we
9 will look at how we can improve that outcome as we go
10 forward.

11 Usually, what we see is that users are
12 prioritizing what I would call productivity or
13 usability above almost everything else. It's the
14 convenience that really governs their behavior, and so
15 like I said, building things that are automatic or
16 invisible really is what gives us the best outcomes.

17 There are some situations where we won't do
18 that. A good example today still is software update,
19 where we want there to be some affirmative user action
20 associated with it, in part because we think it's a
21 moment that a consumer should have some control over,
22 but we also want to strongly encourage that moment to
23 happen because we believe there's immense security
24 value in doing that.

25 So sometimes we're balancing that ourselves

1 to look at maybe it's a little more inconvenient this
2 way, but we also want the consumer to have a sense of
3 control, because that also goes to building trust with
4 the consumer, which we think is an important part of
5 having them, you know, have a sort of constructive
6 security relationship with us. So when we ask them to
7 do something, they might believe it's for a very good
8 reason.

9 MR. WASH: So in addition to that, I really
10 like the point you made about how there are some
11 things that when we can, it's really great if we can
12 just kind of automate security. In an ideal world, it
13 would be awesome if we would just say, hey, we made
14 this secure, you don't have to do anything, you don't
15 even know about it, but in practice, there's a lot of
16 things that where the users and the consumers have to
17 be involved in the security aspects.

18 It's interesting that you brought up
19 software updates. I've actually done a lot of work on
20 software updates. And one of the things that --
21 there's an interesting, really clear tradeoff around
22 security and then usability because software updates
23 often change functionality.

24 And, so, if I -- and often the security ones
25 do because they're preventing something happening that

1 shouldn't be happening, but then they change the way
2 things work. And if you start changing things
3 underneath people, they can get upset. And, so, there
4 is actually an intentional choice that consumers end
5 up needing to make about how to trade off security and
6 software updates. And that comes up in a lot of
7 different security situations where you can't just
8 entirely remove the user from the security decision.

9 Authentication is another one that you came
10 up with, which is, like, there's no way to remove the
11 user entirely from authentication. That wouldn't be
12 authentication anymore. And, so, we have to get the
13 users involved and the consumers involved in these --
14 in a number of these situations, and that's where
15 we're running into the real challenges.

16 You said it's somewhere between productivity
17 and usability, and I agree. A lot of times, when I
18 talk to consumers about how they think about security,
19 the answer is -- they don't answer with the security
20 answer. They tell me why they're trying to --
21 something they're trying to get done. So they look at
22 their phone and they don't see a screen, they see this
23 is how I talk to my mom at night. And that's the
24 important thing, is they want to be able to accomplish
25 these things in their life that have meaning for them,

1 and the security is the ability to do that.

2 And, so, they see security as an enabling
3 feature when they can and try to figure out how to use
4 it. And I've heard that over and over again.

5 MR. HIGGINS: I think over the years, over
6 the last decade or so, we've done, and Apple has led
7 the way on it in many instances, we've done a good job
8 at making security the formal setup. You're secure
9 when you set up a machine; you're secure when you set
10 up a router, but routers for more than a couple
11 decades came preloaded with a user name and password,
12 and you had to actively go in and change it. You had
13 to make a step and change that password and user ID to
14 do it.

15 And if you had that selection and didn't
16 do it, well, it still worked. In fact, you just
17 plugged it in and it worked. It was a great router.
18 Unfortunately, there was no security to it, and
19 everybody that knew that user name and password could
20 get into your router and do all sorts of bad things to
21 your life. But it took us a decade or more -- more --
22 to convince the router manufacturers that, yes, that
23 would impact usability for about a microsecond as
24 people were setting up their routers, that they have
25 to select a password, even if it was weak, we thought

1 a different password than the default was better than
2 nothing. Not much better than nothing, but better
3 than nothing.

4 So I think it comes down to productivity
5 with the users. I can't agree more. You know,
6 usability for the user is the principal. When we set
7 up New York Times online, I was there when we were
8 setting that up online, we set it up with a very low
9 threshold for password when you first logged into your
10 account. You're allowed to have multiple users in
11 your account so that you could have your child logging
12 in from college and using and reading the New York
13 Times online. Or your husband could, on the way -- on
14 his iPad on the way to work, as well as you sitting at
15 home.

16 And we slowly -- we call it boiling the frog
17 -- but we slowly started adding security functionality
18 and reduced the threshold to the accounts being
19 misused. There was no harm to the consumers because
20 consumer protection was one of our caveats when we set
21 it all up. But the protection to the IP, the
22 intellectual property, the news every day was
23 important and we started tightening that down over
24 time to the point where it's ten times more robust
25 today than it was when it was first rolled out.

1 And we did it over time because it was
2 usability. If we had put that level of restrictions
3 on those accounts, those first few days months and
4 weeks of when we did it, users would have never
5 adopted it. They would have gone to the next online
6 newspaper and used their services because they didn't
7 have that inherent level of security on. So it's
8 important. It's a balance for a company to make.

9 Usability is always going to be king, but
10 you've got to trade -- you've got to balance that with
11 security and understand that people, in spite of
12 themselves, still need to be protected, and especially
13 in their procedures. So I applaud what Apple's done
14 over the years. You have to now physically turn off
15 your little PIN number on your phone. You have to
16 make a positive action and say, no, I don't want
17 security where it used to be; no, I want security.

18 And everybody, I guess, in this room would
19 say I want that security and I want that privacy.
20 But, you know, now it comes default and you have to
21 actively say, no, I don't want it. And I think that's
22 a big step forward for the industry.

23 MR. BROOKMAN: These balances are things
24 that we're having trouble -- we're thinking about when
25 we're trying to evaluate services, right? So if we're

1 giving someone a score for security, do we -- you
2 know, is it most secure, or is it most reasonable
3 secure under the circumstances, right? So if you have
4 like a phone that doesn't connect to the internet, you
5 know, that's pretty secure, right, but how do you take
6 into account the other issues?

7 I mean, I know, like, we were looking at
8 home security cameras the other day, and one service
9 doesn't have cloud storage. It all goes locally. And
10 as a privacy advocate, I'm like, that's awesome, like
11 just have it stored locally, and they can never get
12 their paws on it, but, then, again, that has, like
13 usability. Like if you're, you know, somewhere else,
14 like it may introduce other security elements as well,
15 as we heard about security elements of home servers.
16 So how to balance these things.

17 Like the example you come up with automatic
18 updates, like I said, like automatic updates, like,
19 are -- are -- get points, right. They are something
20 that we look to, but the elements you articulated are
21 also exactly right, like, there should be some
22 consumer agency and control over that, and so there's
23 maybe some degree of friction saying, yes, I
24 understand the security update is appropriate, so
25 maybe that should be actually -- maybe you should say

1 the push plus okay is the optimal result. And, so,
2 trying to balance them into either overall scores or
3 even just security-specific scores is tricky.

4 MR. HO: Okay. Rick, I'd like to sort of
5 discuss a little bit more the consumer aspect of, you
6 know, consumer expectations. And you've written a
7 fair bit on this. And I'd also be interested in
8 hearing what the other panelists have to say, but
9 maybe you can start us off with sort of your research
10 on the issue of information asymmetries. Is that
11 something that exists in the security context and, you
12 know, how do we resolve that asymmetry? Is it simply
13 through more education, or is education not enough?

14 MR. WASH: That's a really good question.
15 So there are two parts to that question. Do the
16 information asymmetries exist and how do we resolve
17 that? Well, one of them is easier than the other.

18 Yes, I definitely think the information
19 asymmetries exist. There's a lot of information out
20 there and it's really interesting, it's in different
21 places. We did a project where we were looking at the
22 kinds of information that was available to consumers
23 about computer security, about cybersecurity issues.
24 And one of the things we found, we looked at three
25 different possible sources of information. One was

1 the kind of security advice that you see mostly coming
2 out of the tech industry and places like the FTC or
3 the FBI about how to protect yourself.

4 We looked at news organizations. And then
5 we also looked at a collection of kind of stories that
6 individual consumers have been telling to each other
7 about cybersecurity issues. And what we found
8 surprisingly was that there was very little overlap in
9 the kinds of information that they were talking about.
10 So a lot of the advice from the experts seemed to
11 really focus on threats and countermeasures.

12 So what's the problem, and so, like, what is
13 kind of technical aspect of the problem. So
14 authentication, someone could log in as you, and then
15 how do you deal with that. You have a strong
16 password. Interestingly, those kinds of -- that kind
17 of discussion almost never appeared in the news or
18 amongst the security stories.

19 The stories that people were telling to each
20 other focused a lot more on why -- who was doing this
21 and why were they doing it. That's actually really
22 interesting because currently, the way we're talking
23 about cybersecurity doesn't really focus a lot on who
24 the attackers and the perpetrators are and why are
25 they doing this.

1 And, so, I went into that a little bit
2 deeper to try to understand why is it that people and
3 a lot of consumers seem so interested in kind of
4 sharing speculations about, like, why would someone
5 walk into my account as me. That was a really big
6 issue that most of the discussions and the news
7 stories didn't really talk about, and the answer was
8 because they were trying to make these tradeoffs.

9 So as they kind of live their life, there
10 are these tradeoffs come up, like do I have a stronger
11 password and then have more trouble remembering it?
12 Do I write it down? There's all kinds of tradeoffs to
13 get made as they try to live their lives, and they're
14 trying to understand these tradeoffs, and so to do
15 that, they have to kind of envision the types of
16 attacks and the types of problems that they possibly
17 run into.

18 And, so, they really needed to know, right,
19 if someone got into my account, who would that be and
20 what would they do, because that really matters. If
21 it's my kid sister getting into my account and making
22 fun of me, that's a lot different than someone from
23 another country getting in and stealing lots of money,
24 right? Those are very different outcomes, and I would
25 probably make different decisions based on that.

1 And, so, trying to understand why people or
2 why these attackers were attacking things and what the
3 process was and how do these security decisions
4 actually then influence and prevent those attacks was
5 really important. When I talked to people about two-
6 factor authentication, for example, right now, I hear
7 a lot of people know what it is, they know they're
8 supposed to do it, but they don't understand how it
9 helps. And that's the thing that I'm not seeing a lot
10 in a lot of the consumer education materials right now
11 is, all right, why is this a good thing? If someone
12 was going to try to break into your account, like, why
13 would two-factor authentication actually help stop
14 them?

15 And once I start explaining it to them,
16 where we've got a study we're doing right now where
17 we're actually just sharing stories with people of
18 ways that two-factor authentication stops an attack,
19 and that seems to be very motivating, we're hoping --
20 that's what we're studying -- we're looking at an
21 experiment right now to try to figure out to what
22 extent that it is motivating, but that seems to be one
23 of the key aspects is this information asymmetry and
24 not what the security features are but why they work
25 and who they help protect against and what kinds of --

1 and what things -- what things in my life they help
2 protect me against.

3 So that also speaks a bit to the security
4 education. I do think security education is very
5 important. In my experience, the problem isn't
6 related to motivation. Lots of people say they're
7 concerned about security, and they seem like they
8 really are, but they're trying to make these tradeoff
9 decisions for themselves and their lives. And they
10 feel like they don't have the correct information that
11 they need to do that.

12 And that seems to be a lot of the problem
13 that I'm running into, and that's why it may seem like
14 people aren't making security decisions when they go
15 and buy a television, but it's partially because they
16 don't understand, okay, what does it mean. If Amazon
17 has my TV viewing, what does that mean? What could
18 they do with it, how would that harm me? They don't
19 understand that. And usually there's actually good
20 answers to that, but that's not part of what we're
21 talking about when we teach people about security.
22 And that is, I think, one of the challenges that we're
23 trying to, that at least my work is trying to address.

24 MS. MARTIN: I think you pointed out there's
25 like the scope-of-the-problem information asymmetry,

1 which is kind of -- which they're trying to talk about
2 why would someone do this in general, what types of
3 harms could befall me or everybody else with the
4 cybersecurity incident, anything along those lines.
5 And then there's like another level of when I buy this
6 thing, what level of security am I getting, or when I
7 make this update or don't make this update, like the
8 very transactional information asymmetry, that happens
9 a lot of times in the marketplace where they can't
10 trade on something. They can't trade on it if they
11 don't know about it.

12 And it's interesting because I think -- if
13 we think about the flow of information in general, you
14 have security incidents, which is an adversary, an
15 outsider coming in, and taking information, but you
16 also have privacy, which was mentioned before. That's
17 the firm just telling stuff, right? That's a
18 different thing altogether. That's not an outsider
19 coming in. That's the company is saying I think other
20 people should have access to your data, I might get a
21 little money on the side, but this is how we're going
22 to have -- I'm going to commit a privacy violation.

23 We have a ton of trouble giving that
24 information on the privacy side of consumers so they
25 can say I want to use an Apple device versus an

1 Android device, like we can't -- it's really
2 difficult. The companies have a hard time putting
3 that level of detail in a digestible form to say I
4 want to compete on privacy. It's just a difficult
5 thing to do right now.

6 We really have that problem on security,
7 because I just think that the companies themselves
8 don't always know where security vulnerabilities are.
9 It's hard to conceptualize and explain to people. And
10 that's actually where Consumer Reports does a ton of
11 work because when you have a marketplace with the
12 information asymmetries, branding and, like, putting a
13 little sticker on that says Better Business Bureau,
14 Consumer Reports, those types of things is a signal
15 from a trusted source that's kind of a standard market
16 solution to a major information asymmetry, not in the
17 scope of the problem like you're talking about, which
18 is more of cybersecurity professionals should just
19 start making PSAs on, you know, like if you see
20 something, say something, do you use two-factor
21 authentication of take your password, you know, they
22 should just make those types of things.

23 But this idea of if I can't figure it out
24 myself, I look for a trusted partner to put a stamp of
25 approval and say the equivalent of Intel Inside, or

1 this has been -- this meets a minimum security
2 threshold, and that take the burden off the consumer.
3 And I'm not sure that the consumer can ever be
4 expected to understand what factors are important,
5 because think about what they would need to know.
6 What factors are important, which Consumers Reports
7 had a bunch of professionals trying to figure that
8 out, and they had to just come up with ideas. What
9 criterium is success, and does this product meet that
10 criteria. That's a lot. You know what I mean?

11 And, so, I almost think it's inherent to the
12 problem that we're going to have information
13 asymmetries and we need to not put the responsibility
14 on consumers to buy the right product but look to
15 companies to say, look, this is the minimum standard
16 of security, this is best practices, this is just what
17 we do. Or another one is Consumer Reports comes in,
18 or someone like that, and says, this is the minimum
19 standard, how do they do on that criteria. And that's
20 the work that they do, I would say.

21 MR. HODGES: Yeah, so we're obviously trying
22 to provide more information to the marketplace about
23 the range of behaviors. But I do think -- I mean, it
24 is also a role for policy here to say what the actual
25 minimum is, right?

1 MS. MARTIN: Right.

2 MR. HODGES: I mean, this is something that
3 you talked about earlier, that consumers buy
4 something, they kind of just expect it to work. It's
5 like the analogy of, like, you don't expect your
6 fridge to explode, right? By that same token, there
7 are some reasonable expectations when you buy
8 something that there's some implied warranty that is
9 going to work, it's going to have some degree of
10 support going forward.

11 And, so, I know the Federal Trade Commission
12 has done a little bit of work on this area, like,
13 they've done warning letters against -- I know Revolve
14 was a smart hub that was bought by Nest, and Google
15 bought them, and it was kind of connected to
16 everything in your house, and it relied on server
17 support to work. And then one day, I guess Google was
18 like, we have too many smart hubs, let's just shut
19 this one down. But someone had, like, paid 300 bucks
20 for it 18 months before and it just, like, turned off,
21 right?

22 And in that case, the Federal Trade
23 Commission said, well, no, they sent them a warning
24 letter, saying, okay, because you're giving everyone
25 their money back, we're closing this case, I think the

1 implication being, like, at some level that does
2 become deceptive or unfair. And, again, as we're in
3 the space right now where there are absolutely zero
4 norms around support length, right?

5 I mean, at some point I think the FTC may
6 need to step in and say, okay, if this particular
7 device is vulnerable to lots of attacks, consumers are
8 being attacked, we see so many IOT products out there
9 that have just dire support practices, the FTC at some
10 point is going to have to step in and use their
11 Section 5 authority to say -- to at least put some
12 barriers in the road about what's forbidden.

13 MR. HIGGINS: Well, most of this, most of
14 the businesses, I think almost all the businesses now,
15 have a set of standards from a security perspective
16 that they abide by, even within the products that
17 they're developing. And there's -- I mean, in fact,
18 some of the jokes about standards, they're so great
19 because there are so many to choose from, but, you
20 know, that's the challenge of a business trying to set
21 up its practice.

22 Usability, as I said, is the bottom line,
23 but oftentimes, that is at a tradeoff. They trade it
24 off and they trade off security for it, especially as
25 a fledgling company, because they want to grab market

1 share quickly, as fast as possible, and really I think
2 those are danger zone people. An established company,
3 I think overall, there's a growth aspect that happens
4 at some point. They get enough users behind them,
5 they have enough of a reputation, they have enough of
6 a brand name, and they embed security.

7 If they haven't done it before, that's when
8 they get serious about it, but it is a tradeoff in the
9 early days. Do you hire a new programmer to build
10 more usability functions, or do you hire a security
11 guy? You know, they trade that off every single time
12 as a young company. Most big companies, because they
13 do have these standards they have to abide by, are
14 following the rules -- for the large point, are
15 following the rules and are doing the right thing in
16 building security into their overall processes.

17 That's not to say privacy because I think, I
18 don't know about you, but, you know, one of the great
19 topics around the turkey table this year was how many
20 people had ever read a complete privacy document,
21 privacy statement on any service or product from
22 beginning to end on any product or any service they've
23 ever bought. And the answer was nobody at the table
24 had ever done it. In fact, most don't even get
25 through the first page because it's just convoluted

1 lawyer-speak. It's more litigation prevention than it
2 has anything to do with a declaration of their
3 privacy.

4 And, so, most people don't know what's in
5 those documents and they don't know what the data that
6 they're giving the company is for. It's very secure.
7 They're sending it back to the host company very
8 securely, and they're protecting it, but then what
9 happens to it, nobody has any idea.

10 So I think the overall perspective and the
11 overall industry is run on a risk level, and more
12 importantly than anything else, companies are trying
13 to protect their brand and trying to protect their
14 reputation to be able to stay in business.

15 MR. LUPPINO: Thank you. We have a question
16 from the audience. Currently, demand-side incentives
17 for firms regarding security seem to be mostly back-
18 loaded. Consumers leave due to a breach instead of
19 being front-loaded. Consumers purchase based on
20 security.

21 Is it important to push front-loaded
22 incentives or are back-loaded incentives sufficient
23 and how to be -- and how would it be best to push
24 front-loaded incentives for consumers?

25 MR. HIGGINS: I'll take a shot first, I

1 guess. From a front-loaded standpoint having been in
2 Corporate America for quite a while now, I'm telling
3 the salespeople to sell security as a feature doesn't
4 go over really well. They want to talk about the
5 usability, the functionality, the interoperability,
6 the resiliency. They want to talk about every
7 feature. Security is in there. If you ever looked at
8 a website for a product, if security is mentioned on
9 that product at all, it's way at the bottom of the
10 list. So it is back-end-loaded.

11 I think selling a product up front from a
12 security perspective is an uphill battle today, and it
13 goes to some of the security training that we don't do
14 to normal consumers and infusing a security awareness
15 in the general population that they should be asking
16 those questions. So I think it is back-loaded, and
17 that's the way it's going to be until we can change
18 business practices.

19 MS. MARTIN: Well, one question is which
20 market actor, I know the name of it is consumer
21 demand, but I'll just say, I could see three -- I used
22 to say two, but now I'll say three different market
23 actors that could exchange money for security, right?
24 Consumers, which I think we've all identified issues
25 with expecting security to be something that's traded

1 in the marketplace of consumers. The other place that
2 we look at businesses that have to get money is from
3 stockholders, so public companies or investors and
4 they can demand. And that's why probably it's being -
5 - you know, there are some policies around it through
6 the SEC, is because if you're a publicly traded
7 company, there are certain obligations of disclosure
8 that you have to explain so that stockholders can
9 understand the risk you're taking around
10 cybersecurity.

11 And the other one -- and that's -- so that's
12 front-loaded in some ways. Like, you're saying I need
13 to prove to you to get your investment as to what, so
14 you can invest in me if I meet some sort of minimum
15 threshold that you've identified, and especially for
16 institutional investors, they could look at that.

17 And, then, finally, insurance companies. I
18 mean, those are other market actors that you have to
19 then front-load that decision to prove to them and
20 they will trade on securities. So I know we're
21 talking about consumers, but consumers are just -- and
22 you could have -- there could be all sorts of market
23 actors that actually are more likely to only do
24 business with you if you meet a certain security
25 threshold than consumers.

1 So if you're a target supplier now, I bet
2 you they're going to be much more, you know, focused
3 on the cybersecurity of their suppliers than they were
4 prior, you know what I mean? Like, so I would just
5 say there's more than consumers for market actors.

6 MR. BROOKMAN: Absolutely. Yeah. I would
7 say, I mean, a couple things. So, one, some more
8 requirements around transparency, right. A couple
9 states have laws saying that you have to have a
10 privacy policy, but they don't actually have to say
11 what's in them. So privacy policies tend to be, like,
12 super vague, like, yeah, we collect data and do stuff.

13 But if there is, like, a -- but if there's a
14 requirement, say, that you have to do -- you know, you
15 say X, Y, and Z in the policy, that allows maybe not
16 consumers sitting around the table, but allows folks
17 like us, allows folks at the FTC, it allows the press
18 to introduce some degree of accountability in there
19 for practices.

20 I mean, I do think it could be a good thing
21 to push more companies to make affirmative promises of
22 support going forward. You know, we're starting to
23 see more of that around mobile phones, right? You've
24 seen a number of Android devices promise to support
25 periods for two or three years. And we have some more

1 expectations that, you know, desktop systems are going
2 to be supported for a longer period of time. We don't
3 have norms in IOT, I think. You know, some policy
4 initiative to get folks to say that out loud in
5 advance I think would help move the market in a good
6 way.

7 You know, companies committing to data
8 minimization up front, I think the example with
9 ApplePay is a real good one, you know, Apple going out
10 of its way to say, hey, we're not getting this. And
11 this actually is one of the more prominent selling
12 features of ApplePay. I mean, you don't often see a
13 white paper link to the main page on security
14 protocols on the product description page, which I
15 think is a really positive thing.

16 And, then, like, I think there used to be
17 just more questioning in advance, like do we really
18 need to connect this to the internet? Like, a friend
19 of mine, like, bought a washing machine and, you know,
20 she spent, like, an hour getting it to talk to the
21 router. And, like, I can imagine some peripheral use
22 cases, yeah, if you want to, like, start the cycle on
23 the way home so it's not going to get moldy, and so
24 you don't have to start it in the morning, so, yeah,
25 there's some mold minimization, like smell issues.

1 But, like, by and large, like, I personally
2 would pay more money for a washing machine not
3 connected to the internet. And, so I think there's
4 been this big, like, panglossian, and let's connect it
5 all in Silicon Valley and other manufacturers. I hope
6 we're starting to rethink a little bit.

7 MR. WASH: So my work is mostly on the use
8 side more than the sales. So I think the premise of
9 the question is that security matters more during use
10 than at the sales point, than the initial point. And
11 I think that's right, but my work is mostly on use, so
12 that could just be because I study use.

13 But one thing that I've noticed, especially
14 on the use side, is that there are different -- that
15 security matters differently for different types of
16 products and different types of information. The
17 contrast that I like to draw is when I talk to people
18 about financial losses, such as stealing your credit
19 card, people seem to believe that, like, this is
20 something that if someone steals my money, I can get
21 it back. The banks are doing a pretty good job of
22 giving me my money back.

23 However, something very different to compare
24 that against would be photos of my kids. If someone
25 steals and deletes the photos of my kids, there is no

1 way that anyone can give that back to me. And, so,
2 the people that I've talked to seem to treat those
3 situations very differently. And, so, you may look at
4 something and see security, but it depends on how the
5 consumers are thinking about what is it protecting,
6 and that actually might lead to slightly different
7 answers in different segments.

8 MR. HIGGINS: But that goes back to the
9 question you asked earlier, why? Why is someone going
10 to try to steal pictures of my kids, so they're much
11 more freer to put that data out on the cloud in their
12 instance because they think, well, nobody's going to
13 go after it because why would they go after it.

14 MR. WASH: Yes.

15 MR. HIGGINS: So, you know, again, it goes
16 back to harm and risk issues, their own assessment,
17 it's a risk.

18 MR. HODGES: I would add, I think there's
19 this other interesting challenge, you know? I totally
20 agree with what Rick said and with what Mike just
21 said, that, you know, these stories are a big part of
22 how consumers inform their behavior. In essence,
23 they're kind of doing threat modeling, but back to
24 information asymmetries without a lot of information,
25 and --

1 MR. HIGGINS: Structure.

2 MR. HODGES: -- right, yeah, and structure
3 and formal methodology, all these things. But,
4 ultimately, I think one of the challenges is always
5 what can I do about it, because I think when you look
6 at how do I prevent the loss of my photos, it's not
7 immediately evident to every consumer every time what
8 the right answer might be. And, so, I think one of
9 the challenges is understanding, what are the actions
10 or steps I could take, even if I fully understand the
11 threats and concerns. I think in that sense, front-
12 loading this a bit would be super helpful in helping
13 consumers understand that there was at least a
14 purchase decision they could make.

15 To Justin's point, I would also pay more for
16 a new appliance that was not internet-connected. I
17 don't know if you've heard the Betteridge's law of
18 headlines, anything that ends with a question, the
19 answer is no. I think that should be true of IOT
20 generally. But that said, you know, we don't have a
21 choice necessarily. And, so, I think one of the
22 interesting challenges is giving customers a
23 constructive choice they can make in a sense that they
24 can actually take an action.

25 MR. HO: Maybe we can follow up on that,

1 given Rick's comment about how consumers treat
2 different types of information differently. And, so,
3 if there is a market or, you know, different tools,
4 security features available to consumers, you know,
5 what tools should apply in which instances? You know,
6 take multifactor authentication, for example, as a
7 consumer feature. Should it be applied across the
8 board or in what instances do you protect information
9 versus balance friction?

10 Anybody here? Mike or Wiley, do you want to
11 start?

12 MR. HODGES: I might jump in. I would say
13 one of the big challenges is always going to be making
14 it work. It goes back to the usability tradeoff,
15 right, and actually what Justin said about, you know,
16 you can have the phone that doesn't connect to
17 anything, it's not much of a phone. So we're always
18 finding ways to trade off. And, so, for instance,
19 with two-factor authentication, you know, one of the
20 fundamental questions is is it always going to work?

21 I mean, there are actually situations where
22 I would argue you should never use two-factor
23 authentication because a loss of the second factor
24 might lead to the complete loss of the data underlying
25 it, like your photos, for example. So those kind of

1 things need to be built into the way you consider, and
2 requiring it everywhere would be a pretty ill-advised
3 policy in that sense.

4 I think customers are also going to be
5 challenged with things like interoperability. You
6 know, we can introduce the greatest security feature
7 ever. If the entire industry doesn't use it or some
8 critical number of players don't use it, it really
9 doesn't matter. And, so, I think one of the
10 interesting challenges remains how to provide
11 widespread access to some of these kind of things,
12 particularly around authentication, which remains one
13 of the thornier problems, I think, to solve in a way
14 that helps consumers without putting too much friction
15 in the process.

16 MR. HIGGINS: Yeah, I'd have to agree. I
17 won't even comment. I'll just let Wiley's statement
18 go.

19 MR. WASH: I would agree, also. To repeat
20 something I said, I'm not a product designer, but I
21 study how people use a lot of these different
22 products, and I think there's a role for giving people
23 choices and for designing different products
24 differently. So I completely agree with you.

25 There is also a role for providing

1 appropriate information and for providing kind of
2 nudges or defaults that are appropriate. So I really
3 like the examples that Mike and Wiley were talking
4 earlier about how -- like defaulting to locking your
5 phone and having to make -- take explicit actions to
6 make it so that you don't have a PIN number on your
7 phone. That seems like it makes sense. It still
8 gives people the flexibility, but it kind of defaults
9 to being secure.

10 And, so, I think having those kinds of
11 expected best practices seem valuable, though while
12 still providing some control to end-users to make
13 those tradeoffs in security decisions.

14 MR. BROOKMAN: Yeah, I mean, I'm generally
15 skeptical about efforts to make privacy protections
16 contingent upon sensitivity, but I think in the
17 security space it definitely makes sense. I don't
18 want to have to get a six-digit PIN to open my
19 refrigerator. I think that would be, like,
20 suboptimal, and I would not want to rate that highly.

21 MR. WASH: So I also have -- I was just
22 thinking about another study that I did that -- about
23 -- it was about software updates, but it actually said
24 something interesting about defaults, also. One of
25 the things that's been interesting about looking at

1 software updates over time is that we've automated the
2 software updates more and more so that if you go back
3 20 years, you pretty much had to click manually to go
4 even look to find out if you had them and then do
5 another click or two to install them. Now it's much
6 more automated. And it's been a slow process over the
7 years of getting more and more automated.

8 And as we looked at this over the years, one
9 of the things that we were noticing was we can't
10 automate all updates. There's always a few that are
11 kind of important enough that it's not -- we can't
12 automate that. And people who had more experience
13 doing software updates were better able to make those
14 security decisions, and that as we automated it more
15 and removed it from the user, it seemed like almost
16 that they had been learning less about software
17 updates and were actually having more trouble.

18 MS. MARTIN: Atrophy almost.

19 MR. WASH: Yeah.

20 MS. MARTIN: Your ability atrophied.

21 MR. WASH: The way I like to think about it
22 is if you have a range of problems from easy to hard,
23 if you remove all the easy ones, the only ones left
24 are the really hard ones, but you don't have the
25 ability to learn from the easy ones. And that was

1 actually an interesting -- so there's a consumer
2 education, so product design is related to consumer
3 education in really interesting ways.

4 MR. BROOKMAN: Yeah, I'd like to echo the
5 point I made earlier about -- with the security
6 updates and the potential for being combined with
7 updates that potentially impinge upon functionality,
8 right? So EFFQs, Epson putting in functionality to a
9 security update, that would make it harder to use
10 third-party ink cartridges, right, and so that has --
11 and there's like similar practices.

12 You know, Facebook accused of using phone
13 numbers provided for two-factor authentication for
14 text spam or for targeting ads, right? And, so, how
15 do you -- how does the FTC discourage companies from
16 lending -- from misusing information or permissions
17 provided for security updates? I mean, I think,
18 again, at some point, this may exist, may violate
19 existing law, but otherwise, there may be some
20 guidance the FTC can give to identify those sorts of
21 things as bad practices.

22 MS. MARTIN: So that is interesting because
23 you could imagine a company that misuses the security
24 updates and then uses it for a privacy violation,
25 which is what you just described, as really

1 undermining what we would call the institutional
2 trust in security or online or information security
3 in general, you know? And that would be -- and
4 because a lot of times, security violations and
5 privacy violations both hit my trust in a firm, but it
6 also makes me distrust everything.

7 And, so, you can -- we do studies that
8 show institutional trust will go down significant
9 percentage points after hearing stories about privacy
10 violations or, separately, stories about security
11 violations. And, so, you can -- and public policy
12 actually comes into play to preserve institutional
13 trust on a fairly regular basis. I mean, that's one
14 of the places where we don't let it up to firms -- we
15 don't let firms decide if you're going to allow
16 insider trading or not.

17 We take that off the table, and we say, no,
18 no, no. We're telling you you can't because that
19 undermines the institutional trust in banking. And,
20 so, you can imagine the penalties for abusing a
21 security update to be worse than just, you know, the
22 standard privacy violation that you would have because
23 of that institutional trust.

24 MR. BROOKMAN: Fully agree.

25 MS. MARTIN: That's interesting.

1 MR. LUPPINO: Thank you. Changing gears
2 slightly, what types of security requirements have
3 seen the greatest buy-in from consumers, which have
4 seen the greatest amount of pushback, and why is this?

5 MR. HODGES: I mean, from my own experience,
6 I would say the use of biometric authentication
7 represents the greatest single success we've had in
8 security and has the greatest buy-in by far. I talked
9 about less than half of users setting passcodes. By
10 the way, to use these features, you have to set a
11 passcode, like that's sort of the carrot and the stick
12 we have, is it will be easy, but you got to give us a
13 passcode first.

14 And we went to basically, I think, recently,
15 you know, high 90s compliance with setting passcodes.
16 So it was a pretty profound shift. And that's one of
17 the greatest successes, but it comes back to also
18 being associated with convenience, right? We can
19 essentially put in place a security technology that
20 removes friction, you know, improves convenience,
21 that's great.

22 And the other for us actually has been
23 multifactor authentication for our Apple ID accounts.
24 You know, we had tried doing this a fairly
25 conventional way and found it didn't work very well.

1 We've instead tried to make it as seamless as
2 possible, and, once again, we found that by doing
3 little nudges into it, like encouraging users to do it
4 during the setup process, for example, we're getting
5 much, much higher compliance. And the key is the cost
6 has to be low for the compliance to be high. I think
7 that's really the net we see in every case.

8 MR. HIGGINS: And I would add probably the
9 one that doesn't get noticed a lot is the sleep
10 function on the phone. It saves battery, it keeps
11 your phone on forever, you know, you can get to a
12 charge station before you need to charge your phone
13 again, but what it provides you is physical security.
14 You have to have your password. You have to have your
15 thumb print in order to open the phone again. And,
16 so, a lot of the old attacks of leaving the phone at
17 the bar and someone picking it up and walking away
18 with it and just being able to get into it have gone
19 away because the phone is in sleep mode and can't be
20 broken into.

21 So there's a lot of inherent security that
22 goes back to the concept that security needs to be as
23 transparent as -- not as transparent as translucent as
24 possible. It needs to be -- users just can't see it.
25 If they don't see the security happening but you're

1 providing them security, and a lot of big corporations
2 do a very good job of providing that security for
3 their product or service, if you're doing that, then
4 the security is being used by a lot of users.

5 If you're not doing that and you're making
6 it intrusive into their daily operations, something as
7 simple as, you know, yes, you have to multifactor into
8 things that you've never multifactored into before,
9 you have to enter a PIN for doing certain things, it
10 becomes intrusive and people will find a way or find
11 another service that they don't need to use that
12 service. So it's all about usability and
13 functionality at the end of the day for the consumer,
14 I believe.

15 MR. WASH: So I like your example of the
16 biometrics. Before that, I would say passwords were a
17 really successful security technology. I don't know
18 anyone who doesn't have at least one password, so that
19 is a security and a technology that pretty much
20 everyone uses.

21 MR. HIGGINS: I've got a four-year-old
22 granddaughter. I don't think she's got one yet.

23 MR. WASH: She might, actually.

24 MS. MARTIN: Yeah, That's true.

25 MR. WASH: But another thing to think about

1 the translucency that's really interesting is one of
2 the challenges that a lot of the security instances
3 that I come up with is, is there seems to be a really
4 big difference between taking positive actions and
5 recognizing things that are present versus trying to
6 notice when security's not there.

7 So one of the really big challenges that a
8 lot of security has had is when -- if security is
9 there and there's some kind of indicator that says,
10 look, there's security here, but then sometimes that
11 goes away. It's really, really difficult to notice
12 when something's missing, and it requires a lot more
13 expertise in understanding what's going on and why
14 that might or might not be missing than it is to
15 notice that something is present.

16 And, so, that is a -- it's a really big
17 difference, and a lot of the -- as we make security
18 defaults, we're seeing this more where there is
19 defaults to security but then sometimes -- like if
20 someone turned off the PIN number on your phone and
21 you didn't know it, how long would it take you to
22 realize that? That's a hard question, and actually I
23 don't know the answer to that question.

24 But that kind -- so there's different types
25 of security about present versus absence that actually

1 seems to make a big difference for people's ability to
2 recognize and make decisions based on that.

3 MR. HIGGINS: A good example of that would
4 be the lock, the SSL lock.

5 MR. WASH: The SSL lock, yes.

6 MR. HIGGINS: When it's not there and you're
7 -- how many people go to websites now and you just
8 expect that any kind of PCI transaction is in a secure
9 session, and when it isn't, how many people really
10 notice it isn't?

11 MR. WASH: Yeah, there's been some research
12 that says very few.

13 MR. HIGGINS: And our DLQ tools and the
14 companies find it when it isn't.

15 MR. WASH: Right.

16 MR. BROOKMAN: The friendly part is going to
17 make browsers make choices to really highlight that
18 and to kind of really push people aggressively to
19 using SSL. On the biometric side, I would point out
20 that I think they have been fairly effective, and I'm
21 a big fan of them when deployed correctly, but
22 obviously, like biometrics are incredibly sensitive,
23 and I think the -- I think Apple and some of the other
24 leading manufacturers have been very careful to make
25 sure the data is stored locally, on the device,

1 potentially in a secure element.

2 But I think you could run into problems if,
3 like, a biometric database gets leaked and then I
4 think you run into this problem -- some of the
5 problems Kristen talked about, how you ruin it for
6 everybody. But kind of -- and more directly there if
7 people can access the raw files of people's
8 fingerprints, so while I think biometrics can be very
9 useful, I also want to caveat that with some concerns
10 about, yes, as long as it's done right.

11 As far as ones that I think people have
12 pushed back on, I might as well give a shout out to
13 companies that make you change your password every two
14 months. That's something that I know a lot of folks
15 have found to be frustrating. I know when she was
16 chief technologist here, Lori Cranor wrote a good blog
17 post about why this is actually bad security practice,
18 and in addition to I think recent compliance costs can
19 actually create more of a corpus of information if
20 hacked that could actually make it easier to guess
21 passwords.

22 So that's something I know that a lot of
23 consumers that we talk to like rebel against and I
24 think is probably, hopefully, is getting to the point
25 where it's no longer recognized as an optimal security

1 practice.

2 MR. LUPPINO: So, actually, following up on
3 that, what is the scope of third-party services such
4 as password managers some of the security burdens on
5 consumers?

6 MR. HODGES: I mean, my own perspective is
7 that there's a lot that they can do potentially. I
8 mean, you know, obviously, we have our own password-
9 management features that we deliver, but also have
10 some really great password management apps that run on
11 our platform, and, in fact, we just recently did some
12 work in our latest OS releases to help them integrate
13 better with the system, but I'm sorry to say I don't
14 think that market has proven very large.

15 I think, you know, going back to sort of
16 what's consumer demand for security looking like,
17 well, look at the market for VPN services, password
18 managers, and products along those lines and, you
19 know, it's there, there's clearly some interest, but
20 it's not immense, and it's nowhere near the size of
21 the market for 4K TVs, for example.

22 MR. BROOKMAN: There's not immense, but I
23 think they're both growing, right?

24 MR. HODGES: Yeah.

25 MR. BROOKMAN: I think there's probably

1 adaption to both, and like -- and then you look at
2 something like ad blockers, which are another third-
3 party tool, and the use of ad blockers is, like,
4 getting a lot -- has close to, like, 30 percent. And,
5 again, that's free, right, and so that's maybe one
6 element as part of it, but I think there is growing
7 market for privacy in general that does include third-
8 party tools. Again, it's not all the solution, but I
9 think the trend lines are positive.

10 MR. WASH: One challenge with that is
11 integration. So a lot of tools are difficult to
12 integrate with. Apple's a great example in that they
13 just recently in one of the more recent versions of
14 their operating system allowed the third-party ad
15 blockers to use some of the operating system features,
16 and before that, they were a lot harder to use.

17 There's still a lot of services out there
18 that don't allow third-party integration and that I
19 think limits the abilities of third-party tools to
20 solve that. And, so, that in some ways the lack of
21 integration limits the market.

22 MR. HIGGINS: I think you're right there.
23 When you're dealing with consumer products from that
24 perspective, your product that you just developed,
25 your third-party product that you just developed has

1 to work with an infinitesimal number of configurations
2 and systems out there, from PCs to mobile devices to,
3 you know, to network and devices. It's just -- it's
4 all over -- and you have to keep them -- hopefully you
5 maintain support for all of them.

6 So you can't just sell a product out and
7 say, okay, it's only going to work for this version of
8 this because your market's going to be that much
9 reduced when you realize that there are people out
10 there that are on -- let's see, I think I heard the
11 record was something around 32 versions old on an
12 Android device. You know, it's, like, crazy. And how
13 can you build a consumer product that is sufficient
14 from a security perspective on something that old?

15 MR. HODGES: I will add to that, just to put
16 another little tone of maybe -- I'll call it news, not
17 bad news or good news. As a platform vendor, there's
18 this interesting balance and tradeoff we have to make,
19 which is to provide entry points for people who build
20 these kinds of third-party products like ad blockers
21 and like password managers while simultaneously not
22 creating so much new surface area that we are
23 presenting great opportunity for attackers, which
24 we're always concerned with. And, so, that's a tricky
25 balance and definitely one that we struggle with on an

1 ongoing basis.

2 MR. HO: Okay, I'd like to use the balance
3 of our time to shift gears and talk about tools that
4 consumers have available to comparison shop and shop
5 based on security. So Justin talked about this a
6 little during the beginning with his presentation, but
7 I'm curious to hear what other folks think. You know,
8 is there a market for consumers to shop based on
9 security?

10 MR. HIGGINS: I think consumers comparison
11 shop everything. You know, they do comparison
12 shopping, they're -- all the time. Some of them, my
13 relatives, use CNET, use Consumer Reports all the
14 time. I mean, I think there is a market for the
15 ability to not only look at standard functions,
16 usability features to it, but it's more important now
17 as consumers are becoming better educated, and there
18 is a small subset that are, as they become more
19 educated on what privacy protections that particular
20 product has.

21 Again, in house, I was looking at
22 Thanksgiving, and one of the questions I asked was how
23 many people in the family were using some sort of
24 Alexa-like product in their home, that had bought the
25 device to ease their use of some of the IOT devices

1 they'd gone out and purchased. And the ones that were
2 not using it were concerned for privacy issues. They
3 had read the news articles about how it's always
4 listening and they can't trust it yet and all sorts of
5 issues around security and privacy.

6 Maybe that was my influence, hopefully, but,
7 you know, the ones that weren't looking at a function
8 -- or were using them were using them from a function
9 of they did their research and they did -- and they
10 felt comfortable and they trusted the brands that they
11 were buying. So I think overall there is a good
12 market for those types of research, and the more the
13 better.

14 MR. BROOKMAN: I'll reiterate the point I
15 made earlier about, you know, I think there's more
16 that can be done. I think given that there's not a
17 lot of affirmative requirements to make information
18 available, to make products testable, and actually in
19 some ways it's getting more difficult to test products
20 in some ways.

21 I know this is a conversation we had at one
22 of the PrivacyCons that the FTC hosted a couple of
23 years ago, that sometimes it's actually getting more
24 difficult for researchers to peek under the veil to
25 see what's happening, and then, like, beyond that,

1 we're seeing some companies actually kind of going out
2 of their way to affirmatively, like, actively
3 frustrate testing. And, so, again, this is an area
4 that potentially the FTC could bring some more actions
5 on.

6 You know, like, I think the Volkswagen case
7 was an example when the FTC did bring action, that
8 trying to fool regulators in terms of testing
9 emissions in the lab, trying to look for the specific
10 testing conditions. But they may need to go farther
11 than that because I think there the representation's
12 based on, you know, statements to regulators that,
13 hey, we're compliant with X, Y, Z. You know, we may
14 need -- and this is a comment I made at the previous
15 hearing on artificial intelligence, but, you know, we
16 may need to expand the concept of deception to
17 include, like, you know, tricking not just consumers
18 but tricking testers, tricking user agents, tricking
19 the Safari browser, tricking other things that aren't
20 quite exactly consumers but are still as software and
21 other things kind of intermediate more and more on the
22 information we get and may need -- we need to expand,
23 you know, what we consider to be adding misinformation
24 to the marketplace than currently in the FTC tool set.

25 MR. HO: And, so, Justin just mentioned some

1 challenges, and, you know, he also certainly mentioned
2 some during his presentation, you know, update
3 frequencies, it might be sort of difficult to look
4 under the hood. What do you guys think about those
5 challenges? Are there others that you didn't mention?

6 MR. HIGGINS: Well, just on website use, I
7 mean, there are commercial products available for
8 companies to buy where you can see the number of and
9 the types of places that your employees go to and rate
10 those websites based upon the types of everything from
11 its privacy rules to its contract use for how it
12 should be used, the user agreement that you click on
13 as you go onto the websites, to the security of the
14 website itself. And those are available commercially,
15 but they're largely not available for consumers.

16 It would be really great if some of those
17 tools out there would be available for consumers so
18 that just mere surfing could take on a brand new
19 activity so that they could look at it and say that,
20 yes, if you go to that site and you use that site for
21 this following action, you know, they fully understand
22 what they're doing when they go to that site and the
23 privacy that they're giving up when they go to the
24 site.

25 So almost to me, those commercial companies

1 that are doing it for commercial businesses should be
2 doing it for consumers, but there just isn't a market
3 yet for it. They can't figure out how to make a
4 business plan that could sell this to consumers, but
5 if they could, I think it would be a great step in the
6 right direction.

7 MR. HODGES: I would actually add that I do
8 think transparency remains a struggle in determining
9 these things, and, you know, vendors may be opaque for
10 good reasons, like they want to simplify a message and
11 make it easy for someone to understand or for evil
12 reasons. And it actually, like, reminded me of this
13 when I was thinking about it. I actually have seen a
14 consumer tool that's a plug-in for the web browser
15 that actually does a similar thing. And about 80
16 percent of the websites it marks as insufficient
17 information to judge.

18 MR. HO: Thank you.

19 MR. WASH: So if I have a second. One of
20 the things that I've observed is people seem more
21 willing to talk to each other, and there's a lot of
22 word of mouth than I've seen in the past. And that
23 seems to be increasing. So when I first started doing
24 research with end users, I would hear worries about
25 talking about security would make them seem like they

1 were a tinfoil hat type of person. Now, I have no
2 problems finding lots and lots of people who have
3 heard multiple stories from other people about
4 security issues, and they find them interesting, and
5 they share them with their friends and they talk a lot
6 more.

7 And, so, I think there are cultural changes
8 going on about willingness to talk about security with
9 other people that are really important. I mean, Mike
10 just talked about having a security discussion with
11 his family over Thanksgiving dinner, which seems like
12 a very normal thing to happen now, and 20 years ago,
13 I'm not sure would have been seen as normal.

14 MS. MARTIN: I think one small thing that
15 would just be an issue in the future is we've come up
16 with lots of solutions about the architecture and how
17 it can solve security and usability problems, how we
18 can have nudges to help people along, make it seamless
19 to the user around security, how we can actually give
20 better notice, and there's this effort to kind of
21 explain to people why security's important, whether or
22 not we disclose it to the SEC or to our investors or
23 our consumers or our suppliers, and they're really
24 good about it.

25 I think the more work that's done in that

1 area, the more it's hard to understand the answer
2 around privacy, which is there's no way to explain
3 this, it's too complicated. There's no solution that
4 will ever be mutually beneficial. So that answer
5 around the flow of information when there's an
6 outsider versus when it's the actual firm selling the
7 information or access to it, it sounds disingenuous.
8 They've tackled a harder problem in some ways.

9 And, so, you could see the arguments of
10 looking at those things and saying if you solve this,
11 now go solve that, you know, go solve privacy. Or if
12 it's hitting institutional trust in the similar way if
13 we're regulating security minimums, you could see them
14 turning around and saying, okay, now do privacy. So I
15 think even though they are very different, they're
16 different actors, they're related in a way that you
17 could see them regulated in a similar way.

18 MR. HODGES: No, I mean, I totally agree
19 with you, Kristen. The one thing I would note is
20 sometimes they are actually very much in opposition.
21 And, so, a great example is that, you know, laudable
22 as PCI and its related requirements are, it actually
23 requires Apple as a company to collect information on
24 customer transactions that we'd actually rather not
25 possess or not hold onto.

1 MS. MARTIN: Yeah.

2 MR. HODGES: And, so, I think there are
3 cases where we see that well-intentioned security
4 policies actually can be very much intentioned with
5 the -- what I think are the best outcomes for privacy
6 for end users.

7 MR. HO: Well, thank you for those last
8 comments that do very well in tying security with our
9 hearing in February on privacy. But with that, I'd
10 like to thank our panelists for their thoughts in this
11 conversation surrounding the consumer demand for
12 security, and I'm delighted to turn the time over to
13 Jim who will give closing remarks. Thank you.

14 MR. TRILLING: Good afternoon, everyone.
15 I'm Jim Trilling, another attorney in the Division of
16 Privacy and Identity Protection here at the FTC. I
17 want to just briefly, on behalf of the Federal Trade
18 Commission, thank all of our panelists for the
19 excellent discussion today and also thank both our in-
20 person audience and our online audience.

21 We look forward to continuing the discussion
22 tomorrow. The panelists today have highlighted a
23 number of issues that we'll be discussing more in-
24 depth tomorrow. We'll be beginning at 9:30 back here
25 at the Constitution Center with a panel on data

1 security assessment. That will be followed by a
2 fireside chat between FTC Commissioner Rebecca Kelly
3 Slaughter and Joshua Corman, who among other things is
4 a cofounder of the "I am the Cavalry" security
5 initiative

6 That will be followed by a panel on the U.S.
7 approach to data security, and we'll wrap up the day
8 with a panel on FTC data security enforcement, and
9 then closing remarks by Maneesha Mithal, who leads the
10 FTC's Division of Privacy and Identity Protection.

11 With that, thank you again for coming, and
12 we'll see you tomorrow.

13 (Applause.)

14 (Hearing adjourned.)

15

16

17

18

19

20

21

22

23

24

25

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

CERTIFICATE OF REPORTER

I, Linda Metcalf, do hereby certify that the foregoing proceedings were digitally recorded by me and reduced to typewriting under my supervision; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were transcribed; that I am not a relative or employee of any attorney or counsel employed by the parties hereto, not financially or otherwise interested in the outcome in the action.

s/Linda Metcalf
LINDA METCALF, CER
Court Reporter