S. HRG. 115–307

CYBERSECURITY: RISKS TO THE FINANCIAL SERVICES INDUSTRY AND ITS PREPAREDNESS

HEARING

BEFORE THE

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

SECOND SESSION

ON

EXAMINING CYBERSECURITY ISSUES IN THE FINANCIAL SERVICES SECTOR, FOCUSING ON THE RISKS TO THE FINANCIAL SERVICES INDUSTRY FROM CYBERATTACKS AND CYBER THREATS AND THE READINESS OF THE FINANCIAL SERVICES INDUSTRY TO COMBAT THEM

MAY 24, 2018

Printed for the use of the Committee on Banking, Housing, and Urban Affairs

Available at: http://www.govinfo.gov/

U.S. GOVERNMENT PUBLISHING OFFICE
31–197 PDF WASHINGTON : 2019

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

MIKE CRAPO, Idaho, *Chairman*

RICHARD C. SHELBY, Alabama
BOB CORKER, Tennessee
PATRICK J. TOOMEY, Pennsylvania
DEAN HELLER, Nevada
TIM SCOTT, South Carolina
BEN SASSE, Nebraska
TOM COTTON, Arkansas
MIKE ROUNDS, South Dakota
DAVID PERDUE, Georgia
THOM TILLIS, North Carolina
JOHN KENNEDY, Louisiana
JERRY MORAN, Kansas

SHERROD BROWN, Ohio
JACK REED, Rhode Island
ROBERT MENENDEZ, New Jersey
JON TESTER, Montana
MARK R. WARNER, Virginia
ELIZABETH WARREN, Massachusetts
HEIDI HEITKAMP, North Dakota
JOE DONNELLY, Indiana
BRIAN SCHATZ, Hawaii
CHRIS VAN HOLLEN, Maryland
CATHERINE CORTEZ MASTO, Nevada
DOUG JONES, Alabama

GREGG RICHARD, *Staff Director*
MARK POWDEN, *Democratic Staff Director*

ELAD ROISMAN, *Chief Counsel*
TRAVIS HILL, *Senior Counsel*

ELISHA TUKU, *Democratic Chief Counsel*
LAURA SWANSON, *Democratic Deputy Staff Director*
COREY FRAYER, *Democratic Professional Staff Member*

DAWN RATLIFF, *Chief Clerk*
CAMERON RICKER, *Deputy Clerk*
JAMES GUILIANO, *Hearing Clerk*
SHELVIN SIMMONS, *IT Director*
JIM CROWELL, *Editor*

C O N T E N T S

THURSDAY, MAY 24, 2018

CYBERSECURITY: RISKS TO THE FINANCIAL SERVICES INDUSTRY AND ITS PREPAREDNESS

THURSDAY, MAY 24, 2018

U.S. SENATE,
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS,
Washington, DC.

The Committee met at 9:28 a.m., in room SD–538, Dirksen Senate Office Building, Hon. Mike Crapo, Chairman of the Committee, presiding.

OPENING STATEMENT OF CHAIRMAN MIKE CRAPO

Chairman CRAPO. The Committee will come to order.

Today we will hear about cybersecurity in the financial sector. Today's witnesses come from a wide range of organizations and can provide us with insight on the threats faced by and the preparedness of the financial sector when it comes to cyber.

Four years ago, this Committee held a similar hearing where I noted that a recently aired "60 Minutes" segment called 2014 "the year of the data breach."

Given the various data breaches over the past few years, most notably the Equifax data breach last year, I am not sure that 2014 still holds that title.

As our society increases its reliance on technology and becomes accustomed to immediate access to information and services from companies, the risk of—and the potential damage caused by—data breaches continually increases.

Americans are becoming more aware of the amount of information, including personally identifiable information, or PII, that is stored by companies, and there is a growing realization that this information can be stolen or misused.

The collection of PII by both the Government and private companies is something that has long troubled me. Many question how both use the data collected and how such data is secured and protected.

The collection and use of PII will be a major focus of the Banking Committee moving forward, as there is broad-based interest on this Committee in examining it.

Today we will hear from our witnesses regarding cybersecurity and about the risks to the financial services industry and its preparedness.

We have heard from many regulators before this Committee about their focus on and oversight of cybersecurity and how it is critical to the operations of companies and our markets. This is especially true for companies in the financial services space.

The financial sector itself is a main target for hackers because, as many have said, "that's where the money is."

Banks are under constant attack every day. Because of this, they and other firms in the financial services industry have devoted substantial resources to protecting information systems, and the industry is widely viewed as one of the most advanced sectors in terms of prioritizing cybersecurity.

Today I hope to learn more about: the risks to the financial services industry from cyber attacks and cyber threats; the work being done in the financial services industry to increase cyber readiness, combat cyber attacks, and increase resiliency; and what more needs to be done by the private sector and Government to help protect companies' and consumers' information.

It is critical that personal data is protected, consumer impact in the event of a data breach is minimized, customers' ability to access credit and their assets is not harmed, and the financial sector is resilient enough to continue to function despite a cyber breach at a financial sector company.

I will welcome our witnesses again but welcome. And, Senator Brown, you may proceed.

STATEMENT OF SENATOR SHERROD BROWN

Senator BROWN. Thank you very much, Mr. Chairman. Thank you for holding this hearing today.

This Committee last considered cyber preparedness of financial institutions 3 ½ years ago. Since then, sophisticated, targeted cyber attacks have become all too frequent, exposing the personal information of millions of Americans, costing our economy hundreds of millions of dollars.

Cutting corners on cybersecurity risks real harm to real people's lives. Each data breach or each cyber heist that makes the news seems larger than the one before, and after a while, we barely raise an eyebrow. But think about a family trying to get a mortgage who finds out that their credit score has been wrecked through no—they do not have knowledge about it and it has been wrecked through no fault of their own. It is clear these risks to the financial system and Americans' personal data are growing.

Today's hearing will give us a window into how the financial services sector works on cyber preparedness, fighting cyber attacks, promoting cooperation among private and public entities.

Financial institutions must work diligently not just to maintain standards set by industry and Government, but also to improve protections for financial infrastructure and customer data whenever possible. As risks increase and threats become more advanced, financial institutions and Government agencies must facilitate and encourage information sharing.

Banks certainly have the resources to invest in protecting their customers. The FDIC reported on Tuesday that banks are doing better than ever. Including the benefit from the tax bill, net bank income increased 27 percent compared to 2017. That has been consistent, in most cases double-digit profit increase over most of the last 8 years. Even without the tax benefits Republicans in Congress bestowed on the largest corporations and the wealthy, bank profits would have been up 12.6 percent from a year ago.

Record profits for banks should not just mean that top executives get bigger bonuses and the largest shareholders benefit from stock buybacks and dividends.

Banks should be investing in their businesses, whether it is cybersecurity or a living wage for their employees. I remember the average teller in this country makes $26,000 a year. Rather than lobbying to be let off the hook from rule after rule, the Nation's largest banks should focus their time and effort on securing financial infrastructure against attacks and protecting sensitive consumer data.

Law enforcement also plays a critical role in assessing and warning about cyber threats, and its ability to share sensitive cyber threat information more quickly will help combat those threats. I know there has been good work done in this area. We need to build on it. We cannot let up now. And that is why I am glad the five of you are here.

A secure and resilient financial system is the foundation of commerce and our economy. There is always the risk that cyber thieves will try to steal money and consumers' personal data or that a hostile country will seek to disrupt our financial system. We cannot risk undermining faith in that system.

It would take just one cyber attack to undermine our trust in financial institutions. Once that happens, it will take more than hearings, legislation, or policy changes to restore that trust.

I look forward to hearing all of you address these issues. Thank you all for joining us.

Chairman CRAPO. Thank you, Senator Brown.

We will now move to our witnesses and their testimony. We have with us five excellent witnesses today, and I will briefly introduce Mr. Nelson, Mr. Daniel, and Mr. Venables, and Senator Brown will then introduce our two witnesses from Ohio.

Senator BROWN. Thank you.

Chairman CRAPO. Mr. Bill Nelson is president and CEO of the Financial Services Information Sharing and Analysis Center, also known as FS–ISAC, and has held such a position since 2006. FS–ISAC is a nonprofit association dedicated to protecting the global financial services industry from physical and cyber attacks. Its members include organizations from banks, credit unions, securities firms, and insurance companies.

Mr. Michael Daniel is the president and CEO at the Cyber Threat Alliance. CTA was formed in 2014 through an informal agreement to share intelligence among Fortinet, McAfee, Palo Alto Networks, and Symantec. Prior to joining the CTA, Mr. Daniel served from June 2012 to January 2017 as Special Assistant to President Obama and Cybersecurity Coordinator on the National Security Council staff.

Mr. Phil Venables is the managing director and head of operational risk management and analysis at Goldman Sachs. Mr. Venables has been at Goldman Sachs 18 years. His first 16 years he served as Goldman's chief information security officer, or CISO, before moving into a wider role in Goldman's Risk Division. Mr. Venables serves on the executive committee of the U.S. Financial

Services Sector Coordinating Council for Critical Infrastructure Protection and is co-chair of the Board of Sheltered Harbor.

Senator Brown.

Senator BROWN. Thank you, Mr. Chairman.

It is my pleasure to introduce two Ohioans on this panel. I do not get this honor that often, so thank you.

Carl A. Kessler III is a senior vice president, chief information officer of First Mutual Holding Company, 25 years of experience in technology, 15 in banking at super-regional and community banks, of which Ohio has a number of them. While working in banking, Mr. Kessler has tackled a broad range of cybersecurity issues, from building banking websites to designing security architecture. He began his career at the Department of Defense after graduating from the Honors College at Ohio University. Welcome. And Tom Fraser, the bank's CEO, and Mr. Kessler both do a really important and crucial job serving the banks' customers in northeast Ohio. The bank is located in Lakewood, Ohio, west of Cleveland. Welcome, Mr. Kessler.

Bob Sydow is a principal at Ernst & Young and Americas cybersecurity leader. He has more than 30 years of experience working with Fortune 500 companies and all aspects of information security, data protection and privacy, identity and access management, cyber threat management, and cyber economics. I met with Mr. Sydow this week. I was impressed with his expertise in all things cybersecurity, and I was also impressed with his knowledge of all things Cincinnati Reds. While I am a Cleveland Indians fan in the other end of the State, I urge any of you that are baseball fans in this audience to at least one time go to a Cincinnati Reds opening day. It is a celebration of America's first baseball team. Cincinnati is a baseball town, and I have been to opening day half a dozen times there, and it is something, if you love baseball, you want to experience. But Mr. Sydow has promised if any of you will go, he will give you tickets and give you a tour——

[Laughter.]

Senator BROWN.——and tell you all things Cincinnati Reds history.

So thanks to the both of you for joining us.

Chairman CRAPO. Thank you, Senator Brown, and I think I will try to take you up on your suggestion. I will not take the tickets, however.

Gentlemen, we appreciate you being with us today and bringing your expertise to assist us with this issue. We will proceed in the order that you were introduced. I remind you that we ask you to keep your oral remarks to 5 minutes. You have a little clock there that is supposed to help you. And this is one of those days where we are jammed for time, hence the reason we moved the time of the hearing up. Both Senator Brown and I are a little jammed for time. So I am reminding our Senators as well that we want you to keep yourselves to your 5-minute limit, if you can do so. Actually, we will try to help you do so.

Mr. Nelson, you may proceed.

STATEMENT OF BILL NELSON, PRESIDENT AND CEO, THE FINANCIAL SERVICES INFORMATION SHARING AND ANALYSIS CENTER (FS–ISAC)

Mr. NELSON. Thank you. Thank you, Chairman Crapo and Ranking Member Brown and other Members of the Committee, for inviting me to speak today. I do not have one of the timers, so cut me off if I go over 5 minutes.

Chairman CRAPO. Well, if you hear this sound [banging gavel] that means the bell rang.

Mr. NELSON. I will discuss the topics that you mentioned already: cyber risks, efforts by the financial services industry to increase cyber readiness, and what more needs to be done by the private sector and Government to help protect companies' and consumers' information.

As you mentioned in the intro, I have been CEO of FS–ISAC since 2006 and have seen some major changes occur in the last 12 years. I think the biggest change has been the growing sophistication and volume of cyber threats and attacks.

In response, the financial services sector has made significant investment in cyber defenses and has come together as a community to back major resiliency efforts. I have also witnessed an evolution of the public-private partnership. Today the financial services industry receives tremendous benefit from that partnership that enables cyber threat intelligence to flow to the sector and improve detection, prevention, and response to cyber threats and other risks.

By way of background, you mentioned that FS–ISAC is a private sector, nonprofit organization. We have been around since 1999, and our formal mission is provided in the written testimony. If I could sum it up in maybe just a few words, it is really to protect the financial services sector.

There is an inherent strength in sharing derived from three fundamental pillars: one, the public-private partnerships; two, cross-sector sharing; and, most importantly, three, member-to-member sharing. We often think of FS–ISAC as a virtual neighborhood watch where financial institutions really keep an eye out for each other. One company's reported incident can help the entire sector respond and prevent the same attack from affecting their firm.

Driven by the direction of our membership, FS–ISAC performs a number of key critical functions: we share threat and vulnerability information; we conduct coordinated exercises, often with our Government partners; we manage rapid response communications for both cyber and physical events; we produce education and training programs; and we foster collaboration with other key sectors and with Government agencies.

We have grown rapidly in recent years. When I started, we had a little bit under 200 members. We have about 7,000 companies that belong to FS–ISAC today. These include, like you mentioned earlier, commercial banks, credit unions, but also stock exchanges, clearinghouses, brokerages, investment firms, insurance companies, payment processors, and financial services trade associations. We are headquartered in Reston, Virginia, and have expanded globally with members in 44 countries today, and we have a team of over 100 staff and consultants in eight countries across five continents. That is a long way from when I started in 2006 when we had me and about five outsourced people. That was it. So we have grown really in response to the threat.

Each day, cyber risks evolve as attacks increase. We have invested a significant amount of money, but they continue, these cyber threat actors, to target the financial services sector. Their motivation varies. It can be corporate espionage. It can be stealing money. It can be launching disruptive attacks like we saw in 2012 and 2013 against about 50 financial institutions, and even destructive attacks.

As they grow in their sophistication targeting, the primary evidence of these attacks are the types of attacks leveraged against financial institutions to steal money and disrupt. They include things like phishing; targeted email spear-phishing campaigns resulting in account takeover where they steal your money; also business email compromise which involves the compromise of legitimate business email accounts to initiate unauthorized wire transfers or ACH; ransomware attacks, we all know about that; distributed denial of service attacks, which can impede access to online services; and data breaches, which steal sensitive information.

I think the sector has really come together in a proactive manner. As a result, we have greatly expanded our products and services to our members. We have devoted a large number of resources to really tailor them to smaller financial institutions and their service providers. At the same time, we have enhanced our analysis of threats and best practices for defending against those threats.

We have expanded our exercise program, which includes an annual cyber attack against payment systems, or CAPS exercises, with thousands of participants last year, and have introduced the new cyber range program that allows members to have hands on keyboards, to gain experience to respond effectively to a real-live cyber attack. And we have improved our capability to respond to major cyber and physical incidents, including emergency member calls. The last couple, we have had over 3,000 members participate on. And we have expanded our in-person online member training programs.

In addition to these efforts, we have also created two new subsidiaries—one to add an extra layer of security for consumer accounts, and the other to reduce systemic risk. At the request of leaders in the industry, we established the Sheltered Harbor in 2016 to enhance the industry's resiliency capabilities in the event of a major disaster or event.

In conclusion——

[Laughter.]

Mr. NELSON. I provide more details in my written statement, but let me highlight four recommendations. We are encouraging regulators to harmonize their cyber regulatory requirements, leverage authorities in the Cyber Information Sharing Act, CISA, and the USA PATRIOT Act to implement more effective information-sharing programs; number three, establish cyber deterrence and response capabilities, encourage adoption of global cyber norms; and four, support efforts to develop a technology-capable workforce.

Thank you very much. Thank you for the opportunity.

Chairman CRAPO. Thank you for your flexibility. And we do read your written testimony very carefully. I want you to know that.

Senator—I mean Mr. Daniel. I just about made you one of us. That probably was a demotion.

[Laughter.]

STATEMENT OF MICHAEL DANIEL, PRESIDENT AND CEO, CYBER THREAT ALLIANCE

Mr. DANIEL. Well, thank you very much. Thank you, Mr. Chairman, Ranking Member, other distinguished Members of the Committee. Thank you for the opportunity to come and speak with you this morning.

What I think I can do is provide sort of a strategic overview of the threat context in which this industry is operating and then talk a little bit about what we have done to try to tackle the problem and where we need to go going forward.

When you look out at the landscape, because we live in a digital age, almost everything in our country is now heavily dependent upon the internet and cyberspace. And so, therefore, these threats affect all of us. But the threat is actually continuing to get worse, and it is getting worse in four ways.

One is it is becoming broader. As we create this Internet of Things, we keep hooking more and more of stuff up to the internet. And it is not just laptops and desktops anymore. It is your watch, your phone, your car, your light bulbs, a whole plethora of different devices. The threat is becoming more prevalent as more and more malicious actors, whether they are nation states or criminals, realize that they can try to achieve their goals by operating through cyberspace. The threat is becoming more dangerous as those actors are willing to undertake more and more destructive activities. If we had been having this hearing back when Bill first joined the FS–ISAC, we would have been talking a lot about website defacement. None of us talk about that anymore because that is the least of our problems.

And then, finally, the threat is becoming more disruptive. As I mentioned, with our digital dependence, as it increases, things that used to be merely irritating now pose, you know, organizational existential questions. You know, I often say that when I first started working for the Federal Government in 1995, if the network went down, we just did something else for the day. You know, we worked on our noninternet-connected computers or we held meetings over the phone or did other things. And now if the network goes down, you pretty much send your workforce home because you cannot do anything.

Now, for the financial services industry in particular, you know, they also face challenges related to both criminal and nation-state-enabled cyber theft, and those are a real problem for the industry. But it is also becoming clearer that the threat of disruption, those nation states that target the industry for the purpose of inflicting economic harm on the United States and the West is becoming a more prevalent threat as well.

Now, one thing I want to hit on is actually there is a real question in here about exactly why cybersecurity is a hard problem, because at the surface of it, it looks like it should not be. After all, it is just computers and code. And so there is a question of why we simply cannot create a technical fix to this problem. But the answer is because cybersecurity is not just a technical problem. While there are technical issues about it, it is also an economics issue, a business operations issue. It is a human psychology issue. And it is a national security issue. And it is all of those things rolled into one.

Cyberspace also plays by different rules than the physical world, so a lot of our analogies for how to do things and how to actually go about securing things in the physical world do not work in an environment that is a notable network that operates at light speed, where the concepts of time and distance and proximity all have different meanings and borders than they do in the physical world.

And then, finally, this is a new environment. Stretching it to the maximum, cyberspace is barely older than me. And we have not had time yet to develop the body of law and policy and practice that we need to operate effectively in cyberspace.

Now, we have certainly made a lot of progress over the last 20 years, including particularly within the financial services industry. I certainly agree with the characterization of the industry as one of the most, if not the most advanced sector in the country. And the level of investment from the FS–ISAC to the Systemic Analysis and Resilience Center, Sheltered Harbor, the investments that this industry has made are tremendous. But I do think that there is more that we can do on both the industry side and on the Government side. I think in particular on the Government side there is a real need to look at how the Government can focus on its comparative advantage where it has capabilities that the private sector does not and leverage the comparative advantage of the private sector where the private sector has capabilities that the Government does not have.

The Government can also focus on incentivizing good cybersecurity behavior, and we could talk about that in the Q&A.

And then, last, on the industry side, I think continuing to invest and having the industry figure out how the larger institutions can help the smaller institutions that do not have the same level of capability also make progress in their cybersecurity is a very necessary step.

So, with that, I will conclude my opening remarks. Thank you very much.

Chairman CRAPO. Thank you, Mr. Daniel.

Mr. Venables.

STATEMENT OF PHIL VENABLES, CHIEF OPERATIONAL RISK OFFICER, GOLDMAN SACHS

Mr. VENABLES. Thank you. Chairman Crapo, Ranking Member Brown, and other Members of the Committee, thank you for this opportunity to testify at this hearing today. As we all know, this is an increasingly important topic.

A number of factors are contributing to increased risk across the financial services sector, and this is primarily due in many respects to the digitalization of finance and the globally interconnected nature of the system. The same trends that are increasing benefits of the global financial system are also bringing on these new and enhanced risks.

On threats, as Bill and Mike have described, we are seeing increases threats from organized criminal groups and nation states for various different motivations around the world, and it is also worth reminding ourselves that we are not just facing cybersecurity risks. We are also seeing many risks in relation to how technology has managed and provided risks from resilience issues and software errors. And so while cybersecurity is tremendously important, it is also significant and also to focus on technology risk in general.

It is critical to have shared defenses across the sector so that all institutions, large and small, can learn from each other's best practices and so that threat information can be shared among firms, reducing the likelihood that attackers can execute their strategies without response.

We have a long history of robust information-sharing processes, and as Bill describes, the FS–ISAC is acknowledged as a preeminent example of such capability. We have established tighter coupling between the major firms using the Financial Systemic Analysis and Resilience Center, the so-called FS–ARC. And also under the Department of Treasury's leadership with various different initiatives through the Sector Coordinating Council, we have also increased sector-wide resilience, including formalized sector-wide drills and exercises that have spawned other initiatives, like Sheltered Harbor—an initiative to encourage and demand institutions maintain immutable data vaults to resist cyber attack.

Turning our attention to regulators and regulation, we benefit from a number of strong regulators across the financial sector that stipulate cybersecurity and other controls that reduce the risk of major incidents. This includes regular examinations and reviews. We continue to support the need for harmonization across regulation, domestically and globally, and we commend the efforts to date from the industry and regulators and Government on the use of the NIST Cybersecurity Framework.

Notwithstanding the strong relationship between the public and private sectors, we continue to focus on improvements here, particularly around metrics to make sure that we are able to quantify the value and timeliness of the information flow between the public sector and private sector.

Despite all this coordination and response to cybersecurity threats, risk still remains, and we need to continue to be vigilant to adjust the defenses of individual firms and the sector as a whole by making sure we adopt innovative approaches to protecting customer data as well as making sure that we are protecting the services that we offer. The goal here is to reduce single points of failure and also single focal points of attack.

Finally, I would recommend all organizations that operate critical public services or protect customer data adopt strong defenses and security programs based on a number of different approaches, specifically:

Integrate cybersecurity into the fabric of organizations, from business risk management processes, strategy and product development to the foundation of how the technology is built and operated.

Second, improving capabilities amongst people, processes, and technology. There needs to be continued emphasis on the embedding of controls into critical technology products and services. We need secure products, not just security products. We should also recognize that cybersecurity risk mitigation is not solely the responsibility of designated cybersecurity professionals but is, perhaps more importantly, in the domain of leadership, risk managers, and engineers at all levels of organizations. In other words, we need more security-minded people, not just security people.

And, finally, design for defensibility. Our goal should be to design our technology and information processing environments to be more inherently defendable and resilient in the face of attacks, and we have to keep examining our global supply chains to look for security issues and avoid excess concentration risk in services and geographies.

Thank you, Mr. Chairman, for allowing me to provide this input, and I look forward to taking questions as we go through the panel. Thank you.

Chairman CRAPO. Thank you.

Mr. Kessler.

STATEMENT OF CARL A. KESSLER III, SENIOR VICE PRESIDENT AND CHIEF INFORMATION OFFICER, FIRST MUTUAL HOLDING COMPANY

Mr. KESSLER. Chairman Crapo, Ranking Member Brown, and distinguished Members of the Committee, thank you for the opportunity to testify before you today.

I will share the unique perspective of a front-line practitioner on the practical pros and cons of cybersecurity regulation, information sharing, and community bank collaboration.

Two key regulatory changes have positively improved the approach of community banks in managing cybersecurity risks. In the wake of the Dodd-Frank Act reforms, supervision of our affiliate banks migrated from the OTS to the OCC. In the last few years, FFIEC established the Cybersecurity Assessment Tool, or CAT. These changes have led to an ongoing dialogue with regulators. The CAT provides a standard way to assess risk and provides guidelines for what controls might be appropriate.

Highly trained examiners are critical. Because of the changing nature of the threat environment, an exam is never a static, check-the-box activity. It is always a dynamic conversation. My recommendation to this Committee is to ensure the consistent availability of highly trained IT examiners whose skills are in high demand in both the public and private sectors.

Another consideration for this Committee is to ensure that similar cybersecurity rigor exists among nonbank financial services companies. How do we safeguard customer data at companies that are outside the oversight of prudential regulators?

Community banks rely heavily on a network of third-party service providers. While we always maintain primary accountability for safeguarding customers' information, a significant portion of the risk lies with core processors, payments networks, and large providers.

This concentration of financial services into a few providers creates both advantages and challenges. One challenge is that the current system relies on a high degree of blind trust in the service provider with limited transparency. We depend on our regulator to examine our service providers and identify patterns of compromise and ensure remediation. At the same time, law and regulation require us to monitor the effectiveness of our service provider's controls. This opaque approach runs contrary to best practices in vendor management.

One solution might be to create a cybersecurity scorecard aggregating data from many sources including regulatory reviews. This scorecard would impact vendor selections and create positive momentum toward control improvements.

It is most critical that we have timely access to information sharing of active threats through public and private partnerships. The key for banks is that a comprehensive ecosystem of financial service providers shares threat information in real time to an entity qualified to analyze, verify, and then communicate it back digitally to our bank where we can use it to adapt our controls. We need our third-party providers to share cyber threat information quickly with industry partners like FS–ISAC, the goal being to respond in seconds or minutes rather than days or weeks.

Timely information sharing is foundational to the industry's ability to combat a cyber threat. We cannot act on information we do not have. Important questions remain regarding if, when, and how businesses can share threats. There is still a great reluctance to share information. Liability, contract, and privacy concerns are the most often cited reasons. While customer notification and privacy laws are clearly needed, simplification and modernization of the relevant laws and regulations should enable information sharing. This is a good time to re-examine the effectiveness of cybersecurity law. Certainly, any solution must guard against shifting the liability to consumers from those who failed to protect their data.

Our mutual holding company is faced every day with the challenges required to implement an information security program. We deliver that same program to our affiliate banks in a manner that they otherwise could not afford, design, or staff. In our three affiliations, we have preserved a local banking presence, improved security controls, and done so at a minimal marginal cost. This has proven a game changer for our affiliates.

In summary, the best way to protect consumers is to increase transparency and information sharing within the financial services cybersecurity ecosystem. This Committee could help move this forward by encouraging the transparency of the performance of third-party service providers. You can also help by passing legislation which further encourages information sharing so that active threats are identified and mitigated in minutes.

Thank you for the opportunity to testify before you today. I stand ready to work with you in any way that I can to protect consumers and our financial system, and I look forward to answering your questions.

Chairman CRAPO. Thank you, Mr. Kessler.

Mr. Sydow.

STATEMENT OF BOB SYDOW, PRINCIPAL AND AMERICAS CYBERSECURITY LEADER, ERNST & YOUNG LLP

Mr. SYDOW. Thank you, Chairman Crapo, and thank you, Ranking Member Brown, for that kind introduction. The Reds need help.

My name is Bob Sydow. I am Ernst & Young's (EY) Americas cybersecurity practice leader. I refer the Committee to my written testimony on details on my remarks.

Cyber attacks are on the rise. No organization, large or small, public or private, is immune to the threat. Our clients face three significant challenges: emerging interconnected technologies drive fundamental transformations and create complex third-party ecosystems; the volume, velocity, and precision of attacks; and the shortage of cybersecurity resources and skilled professionals.

EY works with clients across all sectors, and many should be commended for their efforts. In my experience, financial services, especially the largest banks, are considered best in class, not only in terms of organization and investment but also for leading engagement with stakeholders across the ecosystem.

Large banks are accustomed to higher levels of regulatory scrutiny, and their third-party risk management programs tend to be more mature and robust. But challenges remain. Today financial institutions deal with third-, fourth-, and fifth-party risk. In addition to vendor risk most institutions struggle to secure resources and talent. Experienced cyber professionals are in high demand. Often small firms turn to third-party providers to meet those needs.

There is no one-size-fits-all solution, so I will focus on three areas where EY believes risks can be mitigated: corporate governance and risk management, the AICPA Cyber Reporting Framework, and policy solutions.

Ultimately, the board is responsible for governing a company's risk appetite and providing credible challenge to management. By doing so, boards help protect investors and enhance the company's value and performance. Banks use a three-lines-of-defense risk management model. The larger ones are adopting this model for cyber. EY considers this a best practice. Increasingly, regulators, investors, and others want financial institutions to build cyber resiliency strategies into the three lines.

Another challenge is understanding and communicating about a cyber program's efficacy. While NIST and others have developed implementation guidance, there has been no means to evaluate and report on program effectiveness. This distinction is subtle but significant.

In response, the American Institute of CPAs recently developed the Cyber Risk Management Evaluation and Reporting Framework. This is voluntary and can provide stakeholders with reasonable assurance that the identification, mitigation, and response controls are in place.

No framework can guarantee against a breach, but the AICPA cyber risk model can offer an independent, validated understanding of a company's systems, processes, and controls. Unfortunately, there is no single legislative, regulatory, or market solution that can guarantee against a cyber event. Bad actors are not constrained by regulatory, liability, or jurisdictional issues let alone ethics.

Policymakers and the business community should work together to foster collaboration and improve intelligence sharing. We need flexible and harmonized policy solutions that recognize the dynamic challenge of cybersecurity and clarify conflicting directives.

We need to balance the need for compliance with a need to manage cybersecurity and protect consumers. EY believes companies that engage in good-faith efforts, establish enterprise cyber risk management frameworks, and adopt best practices should be recognized, especially relative to liability and penalty measures.

Finally, EY encourages Congress to support modernization of Government's cyber posture, to focus on developing solutions to address cyber workforce shortages, and to educate the public and help the country as a whole improve its cyber hygiene. EY's purpose is to build a better working world, and so I thank you for providing the firm an opportunity to share our views and expertise. I welcome your questions.

Chairman CRAPO. Thank you very much, Mr. Sydow.

In the interest of time, I am going to go last, if there is time before I have to leave, and so I will turn first to Senator Brown.

Senator BROWN. Thank you, Mr. Chairman.

Mr. Kessler, do you think the current baseline for protection of consumer information is adequate? Or would you like additional control over how your personal information is stored or used by financial institutions?

Mr. KESSLER. Well, I think we are all interested in knowing what is happening with our personal information. I am personally assured when I am able to receive real-time alerts of when that information is changed, when it is affected, and changes to my credit reports. I think that there are obviously opportunities to continue to share more information with our consumers in that respect.

Senator BROWN. And when there is a breach involving personally identifiable information, I assume you think it is important for a financial institution to quickly notify customers, giving them the ability to protect themselves by freezing or monitoring their credit file?

Mr. KESSLER. Certainly, we like to take—as a mutually owned community bank, we like to take all the necessary actions to protect our customers in a timely way. So, yes, we find it very important to notify the customers as soon as is practical after working with the necessary law enforcement officers.

Senator BROWN. Thank you.

Mr. Sydow, many community bank IT services are provided through large third-party service providers. Talk about the economies of scale when it comes to cybersecurity that community banks benefit from by using large service providers.

Mr. SYDOW. Well, it is a matter of resource, Senator Brown. The larger organizations can afford the staff and recruit and retain the kind of talent that you need in a cybersecurity department and the focus that they can provide. They have the resources to buy the technologies and install and implement those that a smaller organization would not have. So if a smaller bank were to use those services, they have access to cybersecurity kind of resources that they would not have if they tried to do that in-house or on their own.

Senator BROWN. OK. Thank you. President Obama in 2009 established the position of White House Cybersecurity Coordinator to work straight cybersecurity efforts across all Government agencies. President Trump recently eliminated that position. That is the position Mr. Daniel held in the Obama administration. Will that help or harm Government's efforts to make the country and especially the financial system more resilient and stronger against cybersecurity threats? Are you concerned about that?

Mr. DANIEL. Well, yes, I am Senator. I think the reason that position was created was because, as a very new policy area, we need to drive better coordination across all the different parts of the Federal Government that have a role in cybersecurity, and so I believe that having a strong leadership at the White House level is a real necessity right now.

Senator BROWN. Do you know why he eliminated it?

Mr. DANIEL. I do not. I presume that they were looking for ways to streamline the bureaucracy on the NSC staff. At least that was the statement that was given. But I am not sure of the reasoning behind it.

Senator BROWN. OK. Thank you.

Mr. Sydow, you talked about workplace shortages in my office this week and then in your testimony, and this is not really a question, but as evidenced by the look of this panel and, frankly, the look of most of us up here, as evidenced by the fact that, of the 30 largest banks in this country, there is a female CEO only at KeyBank in Cleveland. We do not really do a very good job in financial services and technology at bringing a more diverse workforce, one of the reasons, clearly, that we all face—that you and we face workforce shortages and attracting people, as Mr. Sydow pointed out. So I hope that we all pay more attention to STEM programs for women and for people of color. We will bring more qualified people in, give more opportunities, and, frankly, have more diverse perspectives in the way we all do our jobs.

Thank you, Mr. Chairman.

Chairman CRAPO. Thank you.

Senator Rounds.

Senator ROUNDS. Thank you, Mr. Chairman.

Mr. Daniel, I would like to more or less just visit with you for a little while, and I would love input from the others as well. I have the opportunity to serve as the Committee Chairman on a Subcommittee for the Department of Defense's cybersecurity. I am just curious. Along the same lines as Senator Brown has indicated, that there had just been a change in which we do not have anybody at the White House who is directly responsible for the cyber defense, I am just curious. You have had the opportunity to work at the Federal level. Now you are part of a nonprofit organization that represents a number of different financial institutions.

In February of last year, the Department of Defense's Science Advisory Board put out both a classified and an unclassified version, not very long, 26, 27 pages, explaining the need for our country to have not only a strong—the ability to attribute where attacks from outside the country were coming into the country, but it also identified that we would not have the capability to keep people out of our critical infrastructure if they wanted to get in, both organized crime organizations but also other near peer competitors, nation states.

Along with that, it indicated that for the next 10 years we would be at risk and that one of the best approaches we could do would be to make it very expensive for those organizations to get into our financial institutions—in fact, any of our critical infrastructure. But it also made the point that we had to have a very strong offensive capability as a deterrent, similar to a nuclear deterrent today.

I would like to know, right now at the financial institutions level—and you work with a number of them—do you believe that we have a model in place today on a voluntary basis, which I am in favor of, but one in which we are at the same level across the different institutions that can then be protected almost in an umbrella-like position by Homeland Security capabilities, Department of Treasury capabilities, and then we will talk about DoD capabilities. But just your thoughts on that and how they connect with the Federal responsibilities.

Mr. DANIEL. Sure. So I think you are very right that if you look at our level of digital dependence, as I talked about, and particularly in the financial services industry, clearly cyber threats are a major problem that this industry has to be dealing with. I think when you look at the nature of the threats that they face, it is going to—anybody that tells you they can give you, as several of the panel members said, a guarantee that you will not have any cyber incidents at all, they are selling you snake oil. And what you can do, however, is manage that risk and drive that risk lower, and that requires cooperation between both the Government and the private sector in some ways that we are not completely used to in the physical world. And I think it requires bringing all of the capabilities to bear both from the private sector side and enabling good information sharing and coordination and collaboration on the private sector side, but also within the Government, between, as you mentioned, the Department of Treasury, Homeland Security, Defense, State, Justice, and in between the Government and the private sector.

Senator ROUNDS. Let me bring this—because we are all going to be time limited today. Do you think the American public today thinks that with regard to their financial services, their assets, their checking accounts and so forth, do you think they believe that the Federal Government has a role to play in protecting those assets?

Mr. DANIEL. I think they do.

Senator ROUNDS. Would it be fair to say that today Homeland Security has the ability to try and notify you and Homeland Security has the ability to try and assist in the defense? But with regard to going outside, if the attribution indicates that it is coming from outside, is it fair to say that Homeland Security does not have the ability to respond offensively to stop those attacks before they actually occur?

Mr. DANIEL. Well, I think that the ability to—it is a shared responsibility on the defensive side, and that is why I say that you have got to do that good integration across all of the different parts of the Federal Government that do have both the network defense mission and the offensive mission.

Senator ROUNDS. Let me put it this way: If there had been an attack on an institution here and it was an attack—we have a bombing and so forth, everybody would assume that the Federal Government has the first role in protecting against that. Would it be fair to also say that when it comes to cyber attacks, we have a challenge in that we do not have the policy in place today to provide for that direct protection up front?

Mr. DANIEL. Well, I actually do not believe that it is possible for the Federal Government to provide that same kind of protection in cyberspace that it does in the physical world due to the way that cyberspace works. And I believe that it will always be a shared mission between the private sector and the Federal Government to achieve the level of protection that we need.

Senator ROUNDS. Thank you.

Mr. Chairman, my time has expired, but I think this is a very good meeting to start out that discussion. Thank you, sir.

Chairman CRAPO. Thank you.

Senator Reed.

Senator REED. Thank you very much. Gentlemen, thank you for your excellent testimony. Also, let me as the ranking Democrat thank and commend Senator Rounds for his leadership on the Cybersecurity Subcommittee. Thanks, Mike.

Senator Crapo, Senator Brown, thank you. This is a very important issue. One reason I think it is very important is that I have legislation, S. 536, the Cybersecurity Disclosure Act, bipartisan legislation with Senator McCain, Senator Collins, and Senator Warner, and it would simply require disclosure by public companies, which is the usual tradition of public companies, of whether they have a director who is a cyber expert or they have some other arrangement. We do not mandate what they do, but I think it is essential to have public companies particularly tell their shareholders and the markets what they are doing at the highest level when it comes to this issue of cybersecurity. And you have described all the different ramifications throughout your testimony.

But I would like to just focus for a moment, if I could, with Mr. Daniel, and that is, Chairman Clayton was here a few weeks ago, Mr. Daniel, and he said:

> I think cybersecurity is an area where I have said previously I do not think there is enough disclosure in terms of whether there is oversight at the board level that has a comprehension for cybersecurity issues. That is something that investors should know, whether companies have thought about the issues, whether there is a particular expertise on the board or not, that is something companies should know. It is a very important part of operating a significant company. Any significant company has cyber risk issues.

And my question would be: Do you agree with that sentiment?

Mr. DANIEL. Yes, I do. I think that the nature of cybersecurity right now is that we actually do need more disclosure. We have an information asymmetry, if you will, and it is hard for markets to operate efficiently when there is information asymmetry. So steps that the Government can take to enable more investors, the public, and others to have more information about how companies are tackling the cybersecurity problem I think is generally a good thing.

Senator REED. And just a quick follow-up. You have noticed, I would guess—I do not want to put words in your mouth—variable sort of attention to these details. There are some companies that have very sophisticated individuals on the Board or arrangements. There are other companies that are essentially free riders. Is that true?

Mr. DANIEL. Well, I think that this is an area where companies are still learning how to address the issue, and some industries and companies have been way more forward-leaning than others. So I do think it is true that the capability across the board varies a lot.

Senator REED. Thank you.

Mr. Sydow, again, thank you for your testimony. I was very struck with the comment:

> At Ernst & Young, we believe that boards must be educated about cybersecurity so that they are able to make appropriate decisions anchored in sound logic and data. By doing so, boards will not only be protecting shareholders, but they will be enhancing the company's value.

And, interestingly enough, the Vice Chair of the Fed, Mr. Quarles, stated:

> The idea of having a board member with cyber expertise, when I have been on boards that had a board member with that kind of expertise, that is an extremely useful—that has not just been a nice thing to have. It has been extremely useful.

So, again, the basic theme, does this make sense to have this disclosure provision so that boards have some expertise?

Mr. SYDOW. Senator Reed, thank you for the question. I have been in this role about 5 years, and I have gone to a lot of Board meetings, and I think there has been increasing importance placed on cybersecurity in those discussions, and often there is a challenge between the translation between the technical world and the business world at those meetings. And I think that is something that—a gap that needs to be closed. However, in my remarks I also said to you that there is a shortage of qualified cybersecurity professionals, especially the people that can make that translation. So as long as you have flexibility in that and allow the boards ways to get access to those kind of individuals, I think that makes sense.

Senator REED. Indeed, this legislation is not prescriptive. It is simply, "Tell us what you are doing. In fact, tell your shareholders and the markets what you are doing," which I think makes a great deal of sense.

One of the reasons, among many, as Ranking Member of the Armed Services Committee, we had the general officer in charge of TRANSCOM, all of our transportation assets, and in an international crisis, he would be responsible to move people by aircraft, by sea, all of our military personnel to get the mission done. And he just said, volunteered that he talked to cybersecurity officers and companies that have no dialogue with their directors. And I can assure you that if something happens, probably the first strike will not be a kinetic strike against the military. It will be a cyber strike against this infrastructure of movement, logistics, *et cetera.* So this is another reason why I think we really do have to have some legislation like we are proposing.

So thank you all very much, gentlemen. Thank you, Mr. Chairman.

Senator BROWN. [Presiding.] Senator Heitkamp.

Senator HEITKAMP. Thank you, Ranking Member Brown, and thank you for having this hearing. I think it is critical that we have the ongoing conversation.

A couple points to begin with. I think the American public has given up, and I think that there is a huge variance between understanding privacy and understanding cybersecurity. They are not the same thing. And, you know, so most Americans say, look, I no longer believe that I have privacy. I do not know that you can regulate this. I do not know that you can control this. But they definitely want cybersecurity.

And so one of the things that I believe as a former law enforcement official is that, you know, you can have all the most sophisticated law enforcement equipment, surveillance equipment, but you have got to teach people to lock the door. You have got to teach people to lock their car. You have got to teach people to pay attention, maybe put some surveillance equipment of their own. And so I talk about cyber hygiene and the role that cyber hygiene should play either with employees, not just, you know, at that level of the people sitting on the board, but at every level being trained and understand the challenges, but also with membership or clients or patients, what role do they play? What role do vendors play?

We all harken back to what happened with Target. The Target breach was related to a vendor and a back-door worm that came in. So how do we build better resiliency, cyber resiliency, within the community, *writ large,* within all users, so that they understand that there are simple things that they can do that will help protect the cyber system, protect our overall system, while we are looking for that iron dome—let us put it that way, that iron dome that is going to make what we do impenetrable—which, quite honestly, I am not convinced you are ever going to get an impenetrable iron dome. And I think that the fault lines are always going to be at that lower level.

So someone, anyone on the panel who wants to take on the issue of cyber hygiene and what we should be doing here to encourage it, to educate, to move this issue of every user needs to be informed on how we protect ourselves from a cyber attack as a country as a whole, kind of a "lock your door" strategy.

Mr. VENABLES. Thank you, Senator, for the question. I will go first, and then others can chip in. I think you raise an extremely important point. I think in many respects we need to focus on basic cyber hygiene to make sure the easy attacks cannot be successful so we can focus our energy on the most sophisticated attacks. And I think it is the responsibility of all companies not only to make sure their employees and their own infrastructure is protected, but also to educate those employees and to educate our customers. I think this is a partnership that we can do between Government and the private sector to educate everybody around what best practices they can do to adopt the right controls for——

Senator HEITKAMP. I really do believe, as a former kind of customer protection/consumer protection advocate, that people want the tools. They want to understand how to do this. What can we do to provide easier accessible tools to lock the door? Mr. Nelson.

Mr. NELSON. Yes, thank you. Just to give a plug for the multi-State ISAC, it is a State and local Government ISAC, and the October Cybersecurity Awareness Month, they produce every month a cybersecurity newsletter. It is weight-labeled, so you can put it on your company's letterhead, give it all to your employees. It is a great effort. It has been going on for a couple years, and we all kind of get geared up for that month in October to educate consumers.

So there are some efforts underway. It is a Government initiative, too, at the Federal level and the State level.

Senator HEITKAMP. Mr. Daniel?

Mr. DANIEL. Thank you, Senator. I also think that it is incumbent upon the industry, the cybersecurity industry, to make that cyber hygiene and the cybersecurity that you talk about as simple as possible for consumers to do. You know, for example, right now our guidance out to consumers is to have a 16-character password that is not any actual words in the English language, that has all sorts of——

Senator HEITKAMP. And, you know, for a spreadsheet full of media passwords, they are all going to be different, like really?

Mr. DANIEL. Yes. And we need to get much better at enabling people to have very simple ways to do their cybersecurity. Sort of the analogy I use is that we make it very simple for people to use seat belts when you get in a car, and we do not expect you to answer questions about whether or not you want the antilock brakes to work. And so I think we need to try to find the same, similar kinds of solutions and approaches in cybersecurity.

Senator HEITKAMP. What grade would you give us right now in terms of how protected we are in a cyber hygiene world?

Mr. DANIEL. Well, I think we are certainly better off than where we were, say, you know, 5 or 6 years ago. So we certainly have made a lot of improvements. The problem is the bad guys keep improving as well. So I think that we still have a long way to go.

Senator HEITKAMP. Just a couple more comments, if that is OK.

Mr. KESSLER. Certainly, educating all Americans, as you are suggesting, is important but a monumental task. We try to approach it by educating our internal employees not only how to properly handle customers' information but their own, and then we attempt to engage with our customers when there is an event. For example, I think where you are going is if somebody is willing to buy gift cards in order to pay the IRS, there is a problem there. And how can we communicate to folks that this is not something they should be doing?

I like the notion of a Cyber Education Month, and one of my peers here suggested including cybersecurity education in curriculums in higher education and in other parts of our academic—our normal education, which I think is a really good idea. Thank you.

Senator BROWN. Senator Cortez Masto.

Senator CORTEZ MASTO. Thank you. Thank you also. This is such an important conversation, and we have been having this, I know, on various committees that I sit on. I appreciate the discussion today.

Let me say, you know, about 10 years ago, I remember sitting with our Nevada Banking Association, and we were talking about how we guard against identity theft. Now, 10 years later, we have a proliferation of cyber threats and attacks that we had not even contemplated at that time. But I was struck, Mr. Daniel, by your comment to Senator Rounds that this cyber infrastructure is a little different and how we manage the enforcement and collectively address these issues. And it is not just Government's role to comment. It is everybody's role now to play a part in addressing the cyber infrastructure and protecting against cyber threats. And I think that is important for everybody to understand. That is the first time I have heard somebody say that. And it is. It is important because it goes back to this issue that we have been talking about. Everyone has a role in education. To me, education is the first step in prevention. But everybody has that role in education. Everybody has a role in the coordination and the information sharing. When I say everyone, from Government to the private sector, the consumer, everyone has a role, and the businesses as well. And then the workforce shortage that we have, that I have heard here as well, we can all play in this discussion.

Let me follow up on a couple of comments that were made. One of them, Mr. Kessler, you talked about the need to pass legislation that encourages information sharing. Can you go into a little bit more about that and what you are talking about? Who is sharing the information? What type of information are you referring to?

Mr. KESSLER. Sure. Thank you very much. As a community bank and a smaller institution, we would benefit from a lot of what Mr. Daniel has already talked about in terms of the sharing of indicators of threat throughout the industry. So as another bank identifies something, they would share it, and we would automatically protect against that.

There are challenges today, when I talk to my service providers and ask them are they participating with FS–ISAC, the answer is yes. Are they sharing threats in real time? I often get the answer no, and the cited reasons are they have confidentiality agreements with us, they have privacy requirements, all things that we all agree are absolutely valuable and essential, but at the same time, from my point of view, are preventing us from receiving some of that threat intelligence that would help us to further protect the customer's privacy.

Mr. NELSON. I would like to comment on that. I think one of the great things about the FS–ISAC is you can share anonymously on the portal, so I would encourage your third-party processor to get in touch with me, and we can work on that. We get legal objections all the time. A lot of times we first get involved in the FS–ISAC, you think, "Oh, my name is going to be in the paper tomorrow if I share." Well, it does not happen. We have pretty good controls around that information. It is not shared with attribution. In fact, every time there is an attack, our members are sharing online realtime. In fact, I was visiting a CISO in Charlotte, North Carolina. You can guess which one. There are a couple big ones there. And I was meeting with him, and he had to leave to go into a special meeting for an attack that was occurring. I whip out my BlackBerry or at that time I guess it was my iPhone, looked at it, and there was the alert already. I did not say where it was coming from. I knew it was from him. So it was happening that fast while they were actually in a war room handling the attack.

So it can occur. It is just getting the right people. And lawyering up is not the answer. The answer is talk to us, let us get involved in it, and it is a pretty good voluntary system. We get lots of members sharing information. We have other third-party processors that are sharing.

Senator CORTEZ MASTO. Thank you. So I would be interested in knowing at the Federal level if there is legislation that actually needs to be introduced or if it is more just communication and working together.

I know my time is running out, but we are talking a lot of acronyms here as well. FS–ISAC, can you explain a little bit more what that is? And I recognize, I come from Nevada, I am not so sure we have that type of coordination. I know it is on the coasts, but I am not sure it is happening in every single State, or there is that collaboration.

Mr. NELSON. It is happening in every State. It is happening in 44 countries. We have 7,000 companies that are members now. It was interesting. In 2014, Senator Crapo mentioned that was the year of the data breach. It was also the year that the FFIEC, which is the regulatory agencies, the banking regulatory agencies, like the FDIC, OCC, even the National Credit Union Administration, and others, put out a policy statement saying you should share information if you are one of our regulated entities, and you need to belong to FS–ISAC. We affectionately——

Senator CORTEZ MASTO. Which stands for and means?

Mr. NELSON. Financial Services Information Sharing and Analysis Center. And when that happened, we affectionately refer to that as the membership tsunami started. We had 2,200 companies join that year, and we have been growing ever since. When I started, we had 200 members in 2006, and it has just been hockey stick growth the last few years.

Senator CORTEZ MASTO. Thank you. I know my time has run out. Thank you very much.

Senator BROWN. Senator Jones.

Senator JONES. Thank you, Mr. Chairman. And thank you to all the witnesses for being here. I agree that all of a sudden everything that I am seeing up here, there is some element of cybersecurity. It does not matter what committee I am on. It touches everything. And I think you guys touched on this before I got here, and that is the cyber workforce and trying to keep pace with the demand.

In Alabama, we have got Auburn University, which has got an incredible facility. Their cyber research center, University of Alabama in Huntsville, has one. And so we are doing our share down there. But if you could, just expand a little bit on challenges that are being faced because so many industries are now competing for this workforce. And that is only going to grow, I believe. It is only going to grow.

And so what can we do, what can the industry do? What are the challenges? Is there anything that we can look at in the Senate and the Congress to try to help with increasing the workforce for cybersecurity? I will just let you guys fight it out. Who wants to answer?

Mr. VENABLES. I can go first, Senator. I think it is a really interesting question because I think while the backdrop, we have to continue to encourage STEM education at all levels to feed a solid technology and engineering workforce for the Nation. I think also we have to not just focus on having trained and dedicated cybersecurity professionals, but thinking across all sectors from whether it is business risk management through to engineering through to product design, in making sure and encouraging in some way that every part of that, whether it is vocational training, academic training, professional qualifications, have an element of thinking about cybersecurity, privacy, and other aspects of technology risk and ethics about how we use technology.

So I think while it would be very important to continue to focus on creating more cybersecurity professionals, I think most of us worry just as much about making sure that every part of our workforce, both private and public, is equipped with the skills to think about how to manage this risk as a core part of their job.

Senator JONES. That is good.

Mr. SYDOW. Senator, the other thing I think we can do is expand the pool. Right now females only represent 9 percent of the cyber workforce, and we have the same issue across technology. We need to continue to encourage young ladies to join the profession. I know at EY we do several things, Girls That Code, other things to encourage organizations to get women into the workforce. I think that would be helpful to expand the base.

Senator JONES. Right. We have done a pretty good job of that in the political world because they are all running for office this year. But I agree with you, that is incredibly important. You know, Bishop State, I was down there visiting a junior college recently, and Apple has a coding program that they are working on with the students down there. I would assume that cybersecurity is always going to be a part of that as well. So thank you.

I do not know if anybody else has anything on that, but if not, I have got one more.

Mr. DANIEL. Well, the only thing I would add, Senator, is that I also think that we need to diversify our thinking about what we mean about the cyber workforce. Just as in health care not everybody is trained up to the same level as a neurosurgeon specialist, we need to diversify our thinking about the levels of training and who does what in the workforce so that, again, we can also continue to expand that pool.

Senator JONES. Perfect. Thank you for those. Those were great answers. Thank you.

I want to kind of followup real briefly on something that I think Senator Reed kind of touched on as well, and that is the assessment of the risk, because I understand his bill to try to get more information into investors and the marketplace about cybersecurity at companies. But I am wondering if any of you think that those ought to be—you know, something about cybersecurity threats ought to be included in the risk. When a business or, in particular, for instance, a municipality is rated, bondholders often would look at a municipality, for instance, as to whether or not that bond is going to be safe because of cybersecurity. Is there a way that we should rate using cybersecurity as well?

Mr. VENABLES. I think there is a number of existing disclosures that occur particularly for public companies as part of their regular filings and risk disclosures, and certainly all the requirements to disclose if major events, particularly material events, occur.

I think there is also a lot of work in the industry where there is more and more public ratings of the outward appearance of various different companies, and certainly I think a lot of the big audit firms, as the gentleman from Ernst & Young mentioned, working with us on various different standards through the AICPA to be able to vet and independently assess the level of security and risk in those companies. I think it would be interesting to further explore how that could be married with other types of public disclosures so you get a full picture of the risk of organizations. I think it is certainly something there is a lot of activity on and probably is worth future consideration.

Senator JONES. Great. Well, thank you all very much.

Thank you, Mr. Chairman.

Chairman CRAPO. [Presiding.] Thank you. Senator Brown has one——

Senator BROWN. Yeah, one question. It is really a yes or no question for Mr. Kessler. You talked about how important it is to notify your customers. Did Equifax share information with you about the breach in time to help your bank's customers?

Mr. KESSLER. No.

Senator BROWN. OK. Thanks.

Chairman CRAPO. Senator Warner, just under the wire. You have got 5 minutes or less.

Senator WARNER. Thank you, Mr. Chairman, for that gracious accommodation.

[Laughter.]

Chairman CRAPO. We always appreciate you.

Senator WARNER. Mr. Venables, we have a lot of legacy IT systems that are out there. Some of the systems are still Fortran and COBOL. You know, how do we make sure, as we do upgrades—and I understand the United Kingdom just went through a complete meltdown when they tried to—one of their banks tried to do an upgrade of their system. How are we thinking through this issue as we think about 21st century cybersecurity when we have got the legacy IT systems in place?

Mr. VENABLES. Thank you, Senator. I think it is a fascinating question because one of the things in my testimony you are always keen to point out was cybersecurity is tremendously important but it is not the only technology risk society faces. We have multiple different risks, not least including how we continue to maintain and update legacy systems to make sure those are equally protected with all the new systems that we are building.

One of the things that is interesting, I think particularly most financial institutions, but I think many other large corporations have pretty exacting standards for change management, software quality assurance, standards for how they apply preventative maintenance to systems to reduce exactly that type of major project and major IT migration risk.

The other thing that I think is worth pointing out as well is while there is a tremendous amount of focus from the financial regulators on cybersecurity, there is also still an equivalent amount of focus on change management, software acquisition and development, testing assurance, major project risk management. In fact, there is a whole shelf full of FFIEC IT examination handbooks, and quite a large number of them are about project risk and major IT migration risk, and it is certainly something that I think all major financial institutions experience quite a lot of scrutiny over not just cyber, but also their IT project risk management standards.

Senator WARNER. For a lot of these systems, the legacy systems, frankly, the original software vendor may not have continued to offer those systems, have not continued to upgrade them, so there are these huge vulnerabilities?

Mr. VENABLES. I think part of the challenge, again, not just confined to the financial sector but across the world at large, is making sure you stay up to date within some reasonable window so that the older systems that may not be supported by vendors, you are not exposed to risks from those. So I think just like any other type of apparatus, you have to invest in preventative maintenance and upgrades to keep yourself within some window to manage that technology risk.

Senator WARNER. Anyone can address this, but my concern is because of the interconnectivity of all of your systems, aren't you only as strong as your weakest link? If a single—if an institution does not keep up, doesn't that make the whole system vulnerable?

Mr. VENABLES. Well, not necessarily an individual institution, but certainly what we look at through the organizations we have set up, like the FS–ISAC and the FS–ARC, and also in work with the Department of Treasury and various other initiatives, we are exactly looking for those systemwide risks that could affect everybody that may be contributed by one or more elements of that, and so we are definitely focused on systemic risk.

Senator WARNER. I think this is probably outside the scope of the whole hearing, but to me, when we do not have a single data breach notification requirement, when we have an Equifax making as gross an error as they did and no obligation to report, or even when Yahoo has hundreds of millions outside the financial system but that is not even reportable on a SEC filing, they do not think it was material enough, I do not see how these massive failures should not fall into at least the level of a material disclosure in terms of SEC filings. So what—and I think I am down to 47 seconds, the last question. Maybe I will leave it at that and just come back to you individually, because I would like to have gotten the more macro approach of how we are going to get at this.

I just came from another intel brief, classified brief. This problem is going to only exponentially grow, and I am not sure—one of the things I think particularly as we think about from both the hardware and software side, if we think about financial institutions, for example, that might be starting to purchase ZTE and Huawei equipment, you know, the vulnerabilities that we may be building into our systems because we—and this is more the intelligence community's responsibility—are not fully informing the financial sector and other sectors of some of what we now call classified problems that we have got to get out, is only going to get much, much worse.

So my apologies for getting here late, to the Ranking Member, and my hope is I will have a chance to pursue some of these conversations with you individually. Yes, sir?

Mr. NELSON. Senator, I would like to comment. We at the FS–ISAC, we are an information-sharing body, and we have people embedded at a top secret level at the NCCIC, the National Cybersecurity Communications and Integration Center, at DHS. So we are seeing some of that, and when we get—when it is relevant, actionable for a community, we are sharing it. Also, FS–ARC is a subsidiary, and, Phil, you are involved in that. They are doing it at a much more systemic level to see if there is any systemic impact. So we have some of that in place. I think we could do more.

Senator WARNER. My concern is, you know, virtually every midsized to larger financial institution around should have somebody that has got classified status and clearances because—and this is where I am trying to push on the intel side. The intel side has not been as forthcoming to the——

Mr. NELSON. We could use a little bit of help in getting more people classified quicker.

Senator WARNER. Well, the fact that there is a 74,000-person backlog is insane, and that is a national security risk that——

Mr. NELSON. I agree.

Mr. VENABLES. Yeah, we would certainly support a much better clearance process to achieve that goal.

Senator WARNER. Right.

Senator BROWN. [Presiding.] Thank you, Senator Warner.

All of us, every Senator, can submit questions to you, and the questions are due Thursday, May 31st, a week, and please, each of you, if Senators do submit questions in writing, please respond to them as quickly as you can.

This concludes the hearing. Thank you for being here today. The hearing is adjourned.

[Whereupon, at 10:43 a.m., the hearing was adjourned.]

[Prepared statements and responses to written questions supplied for the record follow:]

PREPARED STATEMENT OF CHAIRMAN MIKE CRAPO

Today, we will hear about cybersecurity in the financial sector.

Today's witnesses come from a wide range of organizations, and can provide us with insight on the threats faced by and the preparedness of the financial sector when it comes to cyber.

Four years ago, this Committee held a similar hearing where I noted that a recently aired "60 Minutes" segment called 2014 "the year of the data breach."

Given the various data breaches over the past few years, most notably the Equifax data breach last year, I am not sure 2014 still holds that title.

As our society increases its reliance on technology and becomes accustomed to immediate access to information and services from companies, the risk of—and the potential damage caused by—data breaches continually increases.

Americans are becoming more aware of the amount of information, including personally identifiable information or PII, that is stored by companies and there is a growing realization that this information can be stolen or misused.

The collection of PII by both the Government and private companies is something that has long troubled me. Many question how both use the data collected and how such data is secured and protected. "The collection and use of PII will be a major focus of the Banking Committee moving forward, as there is broad-based interest on the Committee in examining this.

Today, we will hear from our witnesses regarding cybersecurity and about the risks to the financial services industry and its preparedness.

We have heard from many regulators before this Committee about their focus on and oversight of cybersecurity and how it is critical to the operations of companies and our markets.

This is especially true for companies in the financial services space.

The financial sector itself is a main target for hackers because, as many have said, "that's where the money is."

Banks are under constant attack every day. Because of this, they and other firms in the financial services industry have devoted substantial resources to protecting information systems, and the industry is widely viewed as one of the most advanced sectors in terms of prioritizing cybersecurity.

Today, I hope to learn more about: the risks to the financial services industry from cyberattacks and cyber threats; the work being done in the financial services industry to increase cyber readiness, combat cyberattacks, and increase resiliency; and what more needs to be done by the private sector and Government to help protect companies' and consumer's information.

It is critical that personal data is protected, consumer impact in the event of a breach is minimized, customers' ability to access credit and their assets is not harmed, and the financial sector is resilient enough to continue to function despite a cyber breach at a financial sector company.

PREPARED STATEMENT OF BILL NELSON

PRESIDENT AND CEO, THE FINANCIAL SERVICES INFORMATION SHARING AND ANALYSIS CENTER (FS–ISAC)

MAY 24, 2018

Chairman Crapo, Ranking Member Brown and other Members of the Committee: Thank you for inviting me to testify at this hearing on "Cybersecurity: Risks to Financial Services Industry and Its Preparedness." My name is Bill Nelson and I am President and CEO of the Financial Services Information Sharing and Analysis Center (FS–ISAC), as well as Chairman of the Global Resilience Federation (GRF) for cross-sector threat-intelligence sharing.

At your request, I will cover the following topics:

- Current cyber-risks and threats that the financial-services industry faces;
- Efforts by the financial-services industry that are already underway in order to increase cyber-readiness, combat cyber-attacks and strengthen the industry from cyberthreats; and
- Proposed additional measures by public and private sectors to better protect companies' and consumer's information.

Before I describe these, I want to provide background about the role the FS–ISAC plays in the financial sector. Three key takeaways I would like to leave you with today:

- Despite a dynamic and ever-changing cyberthreat environment, the financial sector has invested heavily to protect the sector's assets and consumers' information from adversaries and cybercrime;
- The financial sector has collaborated effectively to enhance cyber-resilience; and
- The financial sector continues to benefit from strong public-private partnerships that enable cyberthreat intelligence to flow through the sector and improve sector detection, prevention, and response to cyberthreats and other risks.

FS–ISAC: Information Sharing to Fight Cybercrime

FS–ISAC's mission is to help assure the resilience and continuity of the global financial-services infrastructure and individual firms against acts that could significantly impact the sector's ability to provide services critical to the orderly function of the economy. As such, FS–ISAC stands front and center in the face of continued cyber-attacks against our sector. FS–ISAC shares real-time threat and vulnerability information, conducts coordinated contingency planning exercises, manages rapid-response communications for cyber- and physical events, conducts education and training programs, and fosters collaboration with and among other key sectors and Government agencies. Think of FS–ISAC as a "virtual neighborhood watch," where financial institutions help keep an eye out for each other.

FS–ISAC was formed in 1999 in response to Presidential Decision Directive 63 (PDD 63) of 1998, which called for the public and private sectors to work together to address cyberthreats to the Nation's critical infrastructures. After the 9/11/2001 attacks, and in response to Homeland Security Presidential Directive 7 (and its 2013 successor, Presidential Policy Directive 21) and the Homeland Security Act, FS–ISAC expanded its role to encompass physical threats to the sector. FS–ISAC is a 501(c)(6) nonprofit organization and is funded by its member firms, sponsors and partners.

Rapid Growth Both Nationally and Globally

FS–ISAC has grown rapidly in recent years. Today, we have about 7,000-member organizations of all sizes, including commercial banks, credit unions, exchanges, brokerages and investment companies, insurance companies, payment processors and professionals, and trade associations. We also maintain close ties with other financial-industry trade associations as well as select, trusted Community Emergency Response Teams (CERTs) and Computer Security Incident Response Team (CSIRTs), law enforcement agencies, and other information-sharing initiatives around the world.

The FS–ISAC is based in Reston, VA. Because today's cybercriminal activities transcend country borders, the FS–ISAC has expanded globally and has active members in 44 countries. The FS–ISAC has over 100 employees and consultants in eight countries across five continents.

Financial Firms Respond to a Dynamic Threat Environment

In many respects, the current threat environment feels like an "arms race," and the financial sector has done a lot to enhance its individual and collective capabilities. Each day, cyber-risk evolves as attacks increase in number, pace and complexity. The financial sector has invested significantly to detect, prevent and respond to cyberthreats and other risks. Our member firms constantly adapt to this changing threat environment. At the same time, malicious cyber-actors, with increasing sophistication and persistence, continue to target the financial-services sector. These actors vary considerably, in terms of motivations and capabilities, from nation-states conducting corporate espionage or launching disruptive and even destructive attacks, to advanced cybercriminals seeking to steal money and hacktivists intent on making political statements.

The financial sector (in addition to other critical-infrastructure sectors) is increasingly concerned about the possibility of attacks that could potentially undermine the integrity of critical data, or lead to the manipulation or destruction of data. This growing threat affects all institutions in our sector, regardless of size or type of financial institution (*e.g.,* bank, credit union, insurer, payment processor or brokerage/investment firm).

Tactics Used by Adversaries and Criminals to Target Financial Firms

There are numerous tactics that malicious cyber-actors use to target institutions, including the following:

- ***Targeted spear-phishing campaigns, which are*** fraudulent emails that appear to be legitimate. These emails trick users into supplying sensitive information such as passwords that can result in the theft of online credentials and fraudulent transactions.

- ***Destructive malware attacks*** that impact the confidentiality, integrity and availability of data.
- ***Ransomware attacks,*** which involve malware that is downloaded and used to restrict access to an infected computer (often via encryption) until a ransom is paid (often in Bitcoin).
- ***Distributed-denial-of-service (DDoS) attacks,*** which can impede access to services for extended periods of time.
- ***Pretexting,*** which is built on a false narrative and establishment of trust to ultimately initiate unauthorized activity such as wire transfers. One form of this type of scheme is known as a "business email compromise" attack.
- ***Data breaches,*** which steal sensitive information including payment and account information.
- ***Supply chain threats.***
- ***Insider threats.***

Beyond Sharing: FS–ISAC and Financial Sector Resilience

Driven by the direction of our membership, FS–ISAC performs a number of key critical functions. We share threat and vulnerability information; conduct coordinated exercises; manage rapid-response communications for cyber- and physical events; produce education and training programs; and foster collaboration with other key sectors and Government agencies. We have greatly expanded our products and services to members. In particular, we have devoted a large number of resources to expand our services and tailor them to smaller financial institutions and their service providers.

1. Information Sharing

FS–ISAC enables its members to voluntarily and efficiently share real-time threat and vulnerability information for cyber- and physical incidents. We delivery timely, relevant and actionable cyber- and physical threat information through email, web portal, telephone, and automated feed alerts from various trusted sources and our members. FS–ISAC maintains policies, procedures and controls to ensure that all threat information shared by members is properly gathered, stored, labeled and used in a manner that abides by related sharing agreements, privacy protections, circles of trust, member operating rules, regional requirements and governing laws.

FS–ISAC cooperates with members and partner organizations, including several public-private partnerships. These include facilitating information sharing from Government partners to the FS–ISAC community and assisting members in engaging Government and law enforcement members when required. For example, an FS–ISAC employee participates in the watch floor of the U.S. Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC), playing an important role in our public-private sector information and analysis sharing.

The Basis for the Community: Circles of Trust

We support numerous "circles of trust" based on roles (*e.g.,* chief information security officers, business continuity executives, payments professionals, compliance experts) and institutions (*e.g.,* asset managers, broker dealers, clearing houses, community banks, credit unions, payment processors). We host regular threat-information sharing conference calls for members and invite subject matter experts to discuss the latest threats, vulnerabilities and incidents affecting critical infrastructure. We organize and coordinate numerous regional member meetings, roundtables, workshops and other forums that allow face-to-face exchange between members.

Our largest trust circle—the Community Institution and Association Council—includes thousands of community banks and credit unions that actively share information about threats, incidents and best practices. Since 2014, over 4,500 community institutions have joined FS–ISAC. Within this Council, member discussions and participation increased 24 percent in 2017. In the last 12 months, the FS–ISAC's industry-focused webinars on numerous topics, including protections against fraud, threat-intelligence methods and cybersecurity tools, were attended by nearly 20,000 attendees.

In addition, FS–ISAC works with numerous national and State-based financial and payments organizations, including the American Bankers Association (ABA), Financial Services Roundtable (FSR), Credit Union National Association (CUNA), Independent Community Bankers of America (ICBA), National Automated Clearing House Association (NACHA) and Securities Industry & Financial Markets

Association (SIFMA), as well as card payment associations, payment processors and State banking associations.

2. Creating and Invoking Playbooks for Incident Response

FS–ISAC maintains the financial-services sector's "All Hazards Crisis Response Playbook," which outlines the processes and considerations for identifying and responding to significant threats or events. As an example of sector-wide collaboration, this playbook was developed in conjunction with many of our members and other industry associations. We also lead sector-level crisis-response coordination and manage the Critical Infrastructure Notification System (CINS) for emergency threat or incident notifications to members.

Reducing Fear, Uncertainty, Doubt Through Media Response

FS–ISAC seeks to reduce fear, uncertainty and doubt through sector-level responses on significant cyber- and physical events. The FS–ISAC Media Response Team was established in 2014, following highly visible cyberattacks that impacted the financial-services sector and other sectors like retail that were broadly reported in the press. The Team's mission is to accurately assess the actual current and potential risk of cybersecurity events (as opposed to the potential media "hype" commonly seen) and leverage the FS–ISAC brand to properly respond to media activity using a fact-based approach. The team also strives to educate reporters and the public about cybersecurity and financial-sector practices, concepts, and terminology.

3. Always Ready: Cyber-Exercises and Incident Response

Exercises are a proactive step to practice plans, find and close gaps, and better protect systems and communities. FS–ISAC began conducting exercises in 2010 with the Cyber-Attack Against Payments Systems (CAPS) exercises. FS–ISAC has since added exercises, such as drills, to test the All-Hazards Crisis Response Playbook as well as regional exercises. In 2014, we launched the "Hamilton Series" of exercises in collaboration with the U.S. Treasury Department and the Financial Services Sector Coordinating Council (FSSCC). These exercises simulate a variety of plausible cybersecurity incidents or attacks to better prepare the financial sector and the public sector for cyberattacks. They also aim to improve public-and private-sector policies, procedures and response capabilities. The "Hamilton Series" has included leaders from the U.S. Treasury Department, financial regulatory bodies, the Department of Homeland Security and law enforcement agencies. Starting in 2018, FS–ISAC added range-based cyber-exercises for more technical, hands-on-keyboard experiences to raise capability maturity levels and resiliency across the sector. Collectively, these efforts build on the strong risk-management culture within the financial-services sector, in conjunction with extensive regulatory requirements.

FS–ISAC has improved its ability to respond to major cyber- and physical events, including emergency member calls regarding new vulnerabilities and threats. The last call we had had over 3,000 participants.

4. Support for the FSSCC, Sheltered Harbor, FSARC, Regional Coalitions and Other Sectors

FS–ISAC supports several programs, either through direct funding or through subsidiary arrangements. These are outlined below.

Addressing Policy Issues: The Financial Services Sector Coordinating Council (FSSCC).

The FSSCC was established in 2002 to coordinate the development of critical-infrastructure strategies and initiatives with its financial-services members, trade associations and other industry sectors. The FSSCC works with the public sector on policy issues concerning the resilience of the sector. Members include 70 financial trade associations, financial utilities and critical-infrastructure financial firms.

FS–ISAC serves as the operational arm of FSSCC, providing operational support of FSSCC initiatives. The FS–ISAC and FSSCC have built and maintained relationships with the U.S. Treasury and Homeland Security Departments, all the Federal financial regulatory agencies (*e.g.,* Federal Deposit Insurance Corp., Federal Reserve Board of Governors, Federal Reserve

Banks, Office of the Comptroller of the Currency, Securities and Exchange Commission), and law enforcement agencies (*e.g.,* Federal Bureau of Investigation, U.S. Secret Service). Many of these public-sector agencies are part of the FSSCC's public-sector counterpart, the Financial and Banking Information Infrastructure Committee (FBIIC), which is chaired by the U.S. Treasury Department.

An Extra Layer of Security for Consumer Accounts:

Sheltered Harbor. Sheltered Harbor was established in 2016 as an LLC, operating under FS–ISAC's umbrella, to enhance the financial-services industry's resiliency capabilities in the event of a major disaster or event. The concept for Sheltered Harbor arose in 2015 during a series of successful cybersecurity simulation exercises between public and private sectors known as the "Hamilton Series."

Sheltered Harbor is based on industry-established standards and the concept of mutual assistance. Should a financial institution be unable to recover from a cyber-attack in a timely fashion, firms that adhere to the Sheltered Harbor standards will enable customers to access their accounts and balances from another service provider or financial institution. Sheltered Harbor members access specifications for common data formats, secure storage ("data vaults") and operating processes to store and restore data and receive a Sheltered Harbor acknowledgement of adherence to the specification. As of April 2018, Sheltered Harbor membership covers more than 69 percent of U.S. retail bank deposit accounts and 56 percent of U.S. retail brokerage client assets.

Systemic Risk Reduction: Financial Systemic Analysis and Resilience Center (FSARC).

The CEOs of eight U.S. Government designated critical infrastructure firms—Bank of America, BNY Mellon, Citigroup, Goldman Sachs, JPMorgan Chase, Morgan Stanley, State Street, and Wells Fargo—came together to proactively identify ways to enhance the resilience of critical infrastructure underpinning the U.S. financial system. The result was the creation of the FSARC as a subsidiary of the FS–ISAC. Shortly after the FSARC was founded, an additional eight financial institutions, including the key financial market utilities identified by the U.S. Department of Homeland Security as operators of essential critical infrastructure, joined the FSARC as member firms.

The FSARC's mission is to proactively identify, analyze, assess and coordinate activities to mitigate systemic risk to the U.S. financial system from current and emerging cybersecurity threats. This is accomplished through focused operations and enhanced collaboration between participating firms, industry and Government partners. Key FSARC functions include:

1) Identifying operational risks associated with systemically relevant business processes, functions, and technologies underpinning the financial sector (collectively "Identified Systemic Assets");
2) Developing resiliency plans to address those risks;
3) Working with critical-infrastructure operators and the U.S. Department of Homeland Security, intelligence and defense communities to deliver strategic early warnings of attack on Identified Systemic Assets;
4) Working with law enforcement agencies to disrupt sophisticated malicious actors that may pose a systemic risk to the sector over time or may be targeting Identified Systemic Assets.

Thinking Nationally, Acting Locally: Regional Coalitions. Financial institutions in more than a dozen areas participate in the "FIRST" (Fostering Industry Resilience and Security through Teamwork) movement through the formation of public-private partnerships focused on Homeland security and emergency management issues with the public sector. Each coalition provides the opportunity for members to collaborate with one another and with Government at all levels about issues of resilience and security.

FS–ISAC has established regional coalitions in the Northeast (Connecticut, Maine, Massachusetts, New Hampshire, New Jersey, New York, Rhode Island and Vermont), Mid-Atlantic (District of Columbia, Delaware, Maryland and Northern Virginia) and California (San Francisco, Fresno and Los Angeles). Through regional coalitions, FS–ISAC learns the ground truth about the local effects of crises, while the coalitions obtain national-level crisis and threat information from FS–ISAC. FS–ISAC also supports RPCfirst, an umbrella organization for all of the regional coalitions across the Nation.

Cross Sector Collaboration and Sharing

The FS–ISAC collaborates with other sectors, including the National Council of ISACs (NCI). Formed in 2003, the NCI today comprises 24 organizations designated as their sectors' information sharing and operational arms.

Last year, the FS–ISAC spun off its Sector Services division into a new standalone, not-for-profit called the Global Resilience Federation. I serve as the chairman of GRF, which is an information-sharing hub and intelligence provider. GRF develops and distributes cyber-, physical and geo-political security information among not-for-profit ISACs, ISAOs, CERTs and other information sharing communities across vital sectors around the world. The company assists in the creation and operation of ISACs and ISAOs, or, if requested, support for the expansion of existing communities. This "community of communities" was founded by charter members—FS–ISAC, Legal Services Information Sharing and Analysis Organization (LS–ISAO) and Energy Analytic Security Exchange (EASE)—and has since been joined by National Health ISAC, Oil and Natural Gas ISAC, Multi-State ISAC, Retail Cyber Intelligence Sharing Center and National Retail Federation. As a cross-sector hub that also works with Government and industry partners, GRF facilitates and supports cross-sector intelligence sharing as well as collaboration.

Regulatory Requirements and Risk Management Culture

The financial sector has historically led the way in making substantial investments in not only security infrastructure and highly qualified experts to maintain the systems, but also in driving collaboration across industries and with the Government. Financial institutions recognize that customers trust them to protect their investments, their records and their information. Individual financial institutions invest in personnel, infrastructure, services and top-of-the-line security solutions and protocols to protect their customers and themselves, and to respond to cyber-attacks. These investments protect the individual institutions and their customers, but on its own, an individual institution generally only has the ability to protect what is within its control. Financial institutions, however, are interconnected to each other, with other sectors and with the Government. This reliance on others gives the financial-services sector a unique and critical role in the cyber-landscape and requires coordinated action for the most effective response. Recognizing the cyberthreat environment continues to expand in complexity and frequency, and that individual institution efforts alone will not be enough, executives from the financial-services sector have stepped up efforts to work together.

Cybersecurity Practices Often Burdened by Regulation and Supervisory Oversight

Financial institutions are subject to comprehensive regulations and supervisory requirements with respect to cybersecurity and the protection of sensitive customer information as well as business resiliency. For example, Title V of the Gramm-Leach-Bliley Act of 1999 (GLBA) directed regulators to establish standards for financial institutions to protect customer information. Pursuant to GLBA, regulators have imposed broad information security requirements for regulated financial institutions with strong enforcement authority. In addition to issuing regulations almost two decades ago, the Federal financial regulators have issued extensive "supervisory guidance" through the Federal Financial Institutions Examination Council (FFIEC) that outlines the expectations and requirements for all aspects of information-security and technology-risk issues, including authentication, business continuity planning, payments and vendor management." Among the obligations to secure systems and protect data under GLBA and supervisory guidance, financial institutions must:

- Develop and maintain an effective information-security program tailored to the complexity of their operations;
- Conduct thorough assessments of the security risks to customer information systems.
- Oversee service providers with access to customer information, including requiring service providers to protect the security and confidentiality of information;
- Train staff to prepare and implement information-security programs;
- Test key controls, systems and procedures, and adjust key controls and security programs to reflect ongoing risk assessments;
- Safeguard the proper disposal of customer information; and
- Update systems and procedures by taking business changes into account.

Many Regulations and Standards with Which to Comply

Financial institutions must comply with cybersecurity requirements and guidance from numerous regulatory bodies depending on their charter and activities. What's more, depending on the type of financial institution, organizations may have additional compliance and nonregulatory standards; for example, institutions that handle payment information also are required to comply with nonregulatory standards, such as the Payment Card Industry Data Security Standard (PCI–DSS). This adds to the compliance burden of financial institutions, as well as that of merchants and other organizations that handle payment information.

Most recently, the FFIEC issued the Cybersecurity Assessment Tool (CAT)—an assessment tool designed to help smaller institutions, in particular, identify their risks and determine their cybersecurity preparedness. The CAT provides a repeatable and measurable process for financial institutions to measure their cybersecurity preparedness over time and aligns with the NIST's Cybersecurity Framework. In 2016, the FS–ISAC and FSSCC leveraged the FFIEC's CAT to produce a "crowdsourced" version that incorporated automation to assist financial institutions in utilizing the FFIEC document.

Recommendations to Further Protect Financial Institutions and Customers

Finally, you asked me to describe what more needs to be done by the private sector and the Government to help protect companies' and consumers' information. For many years the financial sector has been working diligently and collaboratively to make significant improvements in five major areas:

- Enhance Information Sharing
- Improve Strategic and Tactical Analytics
- Improve Crisis Management Response and Coordination
- Improve Core Components of the Cyber Eco-system through R&D
- Improve Executive Communication and Advocacy

The financial-services sector has made significant progress in all of these. In so doing, the financial sector has developed strong collaborative relationships with numerous Government agencies (including law enforcement, DHS, Treasury, and U.S. regulatory agencies). These efforts have enhanced the resiliency of the financial-services sector. We also have worked closely with other "critical infrastructure" sectors (*e.g.,* telecommunications, energy) to enhance their capabilities and to address interdependencies.

While we are making good progress, much more work needs to be done. The following are four major recommendations. Some of these recommendations were developed in collaboration with the Financial Services Sector Coordinating Council (FSSCC) and publicly released in early 2017.

1. Encourage Regulators to Harmonize Cyber-Regulatory Requirements. Given that financial institutions are subject to numerous regulatory and supervisory requirements with respect to cybersecurity, protection of sensitive customer information, business resiliency, penetration testing, vendor management, *etc.,* there is little need for additional regulation in this space. Instead, there is a need to reduce the burden of implementing regulations for financial firms. What the sector most needs now is a focused and coordinated effort among State, Federal, and global regulators to harmonize regulatory requirements. In so doing, this is a good opportunity to leverage the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

While regulatory requirements are a powerful and effective way to ensure that financial institutions have adequate controls in place, a growing challenge facing large and global financial institutions today is the need for greater coordination and harmonization among the regulatory agencies, within the United States and globally. This will help financial firms keep pace with new threats, new financial business process models, and the necessary skillsets to evaluate the intersection of those two for security and resiliency purposes. A common refrain we hear from senior executives and practitioners in large and global firms is the need for regulators to harmonize regulatory requirements at both the policy and examination levels to reduce unnecessary regulatory compliance burdens and to better focus limited resources to mitigate cyber-risks. In addition, it would help if the U.S. Congress and Administration enacted a consistent and strong data protection and breach notification law across State and national platforms.

Related to this recommendation to harmonize regulatory requirements, we also encourage Congress and regulatory rulemaking bodies to integrate cyber-risk assessment into the legislation and rulemaking processes. Hence, Congress and regulatory rulemaking bodies should weigh the implications of concentrating sensitive data that will create new cyber-targets when evaluating potential legislation and rulemaking. The potential aggregation of personally identifiable information via the SEC Rule 613 Consolidated Audit Trail or retrieving highly sensitive penetration testing and vulnerability data on regulated institutions are examples of situations where care should be taken to avoid creating new risks and creative solutions should be sought collaboratively with industry.

2. Leverage Authorities in the Cybersecurity Information Sharing Act of 2015 (CISA) and USA Patriot Act of 2001 to Implement More Effective Information Sharing Programs. FS–ISAC and others in the financial sector supported the enactment of the Cybersecurity Information Sharing Act of 2015 (CISA). CISA encourages sharing for a cybersecurity purpose and includes incentives to entice entities to share information, including protection from liability claims, exemption from disclosure laws and regulatory use, and antitrust exemption. CISA enables sharing of information including: malicious reconnaissance, methods to defeat controls or exploit vulnerabilities, security vulnerabilities, malicious cyber-command and control, exfiltration of data and other attributes related to cyberthreats.

Mandated by the Cybersecurity Act of 2015, the Department of Homeland Security (DHS) developed a system to automate the sharing of threat indicators on a machine to machine basis. This system is called Automated Indicator Sharing or AIS and was put into service in 2016; it is free to use.

AIS leverages two internationally recognized standards for sharing: One is the data standard called Structure Threat Information Expression (STIXT) and the other is the delivery standard known as Trusted Automated eXchange of Indicator Information (TAXIIT). Threat indicators include data like malicious IP addresses, email addresses associated with ransomware, phishing or social engineering attacks, known cybercriminal campaign information and much more.

Representing its members, the FS–ISAC agreed to participate in the Automated Indicator Sharing (AIS) program on a trial basis in 2016. We have engaged in numerous collaborative technical discussions with DHS and Treasury concerning the AIS program over the past 2 years.

FS–ISAC and member firms have provided direct and consistent feedback to DHS regarding the early implementations of the AIS program. This feedback includes the need for DHS to strongly structure vetting of AIS participants, the need to verify the integrity of data transmitted and received within AIS, and the importance of providing context around the information. DHS has indicated it has heard the financial sector's feedback and is taking steps to incorporate that feedback and has recently committed to delivering on improvements that add context to indicators, includes rated scoring of vetted sources, utilizes the latest version of STIX/TAXII standards, and ability for AIS recipients to screen sources and receive data only from sources that each recipient approves.

We also encourage our U.S. Government partners to improve response time and the quality of shared information and analysis and to prioritize essential "lifeline" sectors in planning and event response. Focus Federal resources to assist those sectors whose operation is fundamental to the national defense and economy, such as financial services, electric power, and telecommunications, to mitigate against cyberthreats and to help in recovery. Continued private-public collaboration is required to develop the list of cyber-defense capabilities that can be used to respond to a significant cyber-incident affecting the Nation's critical infrastructure. Ensure that the relevant members of the lifeline sectors receive the appropriate security clearances. Also, seek improvements in sharing classified information, passing clearances and collaborating with the private sector in a classified environment. Together with the communications sector and the electricity subsector, FS–ISAC led the development of a playbook for lifeline sectors, completed earlier this year. We began drilling it during Cyber Storm and the National Level Exercise and plan a Hamilton Series tri-sector exercise for it in the fall. One of the next steps involves expanding the lifeline sectors for which it would be applicable. Another is ensuring that the tri-sector playbook connects with plans the Federal Government would use during a significant incident. The U.S. Departments of Treasury, Homeland Security and Energy have seen the playbook, though further Government socialization and coordination remains.

In addition, we encourage the U.S. Government to invest further in financial services-supporting infrastructure and risk-based cyber R&D. To ensure strong investment in the cybersecurity and resiliency of key Federal organizations, processes and systems essential to the functioning to the financial services system, it's important for the U.S. Government to assign clear responsibilities and increase significantly resourcing for efforts to detect, analyze and mitigate cyber threats to the financial system. This includes a dedicated effort within the Intelligence Community and an operational-level contingency planning, indications/warnings, and exercises program. It's important to fund cybersecurity defense and R&D initiatives commensurate with the risk that cybersecurity threats pose to the Nation's security, including funding to identify risks and mitigation techniques for emerging Internet of Things (IoT) and quantum computing technologies.

Finally, we encourage the Financial Crimes Enforcement Network (FinCEN) to provide greater clarity on legal protections for financial institutions that want to share information in accordance with the USA Patriot Act. On November 30, 2016, FinCEN participated in a FS–ISAC-sponsored webinar about information sharing on suspected money laundering. This interaction helped anti-money laundering (AML)-

regulated financial institutions better understand FinCEN's views of the potential risk mitigation opportunities available by sharing information about suspected money laundering under section 314(b) of the USA Patriot Act. Since the webinar, many of the financial institution executives who participated in the webinar, which was open to all AML-regulated financial institutions, have asked for written confirmation of the information that FinCEN officials provided verbally. Financial institutions indicated that written confirmation is necessary to encourage financial institutions to leverage the authority provided under section 314(b) of the USA Patriot Act. If FinCEN provides written guidance about what suspected money laundering and terrorist financing information can be shared with an association of approved financial associations under the USA Patriot Act Section 314(b), then financial institutions that are members of an approved 314(b) sharing information association would file Suspicious Activity Reports (SARS) with more actionable information. In turn this might enhance the U.S. Government's efforts to investigate, extradite and prosecute transnational cyber criminals.

FS–ISAC provided a list of six questions and our understanding of the answers to FinCEN on numerous occasions and is still waiting for a response. FS–ISAC would like to request that FinCEN publicize the answers so financial institutions can reference these answers. This would provide financial institution executives with much needed assurances of FinCEN's views and thus encourage greater information sharing about suspected money laundering by financial institutions pursuant to section 314(b) and other U.S. laws that authorizing the sharing of suspected money laundering and suspected terrorist financing.

3. Establish Cyber-Deterrence and Response Capabilities and Encourage Adoption of Global Cybernorms. The Congress and Administration should articulate how the U.S. Government will respond to certain types of attacks and how these actions might impact the financial-services sector and other critical infrastructure sectors. The U.S. Government should also increase efforts to extradite and prosecute cyber criminals. Attacks on the financial services industry and critical infrastructure should be considered a violation of an explicit global norm; violations of this norm should be pursued vigorously. The U.S. Government should also enable and expand cross-sector, real-time and actionable cyber threat information sharing and situational awareness. The U.S. Government should also continue to engage with the global community to develop and adopt international norms of behavior that discourage targeting of financial institutions and other critical-infrastructure sectors.

4. Support Efforts to Develop a Technology-Capable Workforce. The U.S. Government should partner with the private sector and academia to develop education and training programs to meet the business needs of today and tomorrow in addressing the significant shortage of cyber security professionals and the education system in producing enough skilled cybersecurity professionals.

CONCLUSION

The financial sector has made a significant investment in cybersecurity, risk reduction and resilience. However, threats, vulnerabilities and incidents affecting the sector continue to evolve. Individual firms have responded by making significant investments in technology and risk reduction improvements at their respective companies. Collectively, the sector has made improvements in information sharing and made strides in focusing on systemic risk, mutual assistance, enhanced resiliency and consumer protection. While more needs to be done, including additional collaboration with Government and global partners, the financial sector is making good progress and on balance has invested heavily to protect the sector's assets and consumers' information from adversaries and cybercrime.

<u>Senate Committee on Banking, Housing, and Urban Affairs</u>

"Defending Against Cyber Threats: Challenges for the Financial Services Industry"

<u>Written Testimony of:</u>

Michael Daniel

President & CEO, Cyber Threat Alliance

CYBER THREAT ALLIANCE

May 24, 2018, 10:00 a.m.

Dirksen Senate Office Building – Room 538

Chairman Crapo, Ranking Member Brown, and Members of the Committee:

Thank you for the opportunity to appear before you today to discuss cyber threats to the financial services industry and how that industry is preparing to address those threats. My name is Michael Daniel and I am the President & CEO of the Cyber Threat Alliance (CTA)—an information sharing organizations that now includes [sixteen] of the world's leading cybersecurity companies. Prior to coming to CTA, I served for over 20 years in the U.S. federal government, most recently for four and a half years as Special Assistant to the President and Cybersecurity Coordinator at the National Security Council.

Let me begin my testimony by thanking the Committee for taking on this important issue. Cybersecurity threats to the financial services industry are significant and it is imperative that the industry be ready to deal with them. This Committee plays a key oversight role in ensuring that all of the financial services industry, not just the largest banks, are investing adequate resources in cybersecurity.

The Cyber Threat Landscape

We live in a digital age. This digital age brings with it incredible efficiencies and productivity, and the financial services industry has capitalized on this new technology to enhance their products and services. However, this digitization also brings new challenges and potential vulnerabilities that—left unchecked—threaten to undermine these very benefits. The highly digitized nature of the financial services industry means that cyber threats are particularly significant. Beyond the financial services industry, our economy, our national security, and our social lives all depend heavily on the Internet and cyberspace. Unfortunately, cyber threats are growing more acute in at least four fundamental ways:

1) The cyber threat is becoming broader: As we increasingly connect more and more devices to the Internet, we are making cyberspace bigger and dramatically expanding the potential attack surface. Indeed, even by the Gartner Group's conservative estimates, there will be over 20 billion devices connected to the Internet by 2020—given current numbers, reaching that total translates into adding 10 million devices to the Internet per day – that's more than 400,000 per hour. But more important than just the numbers are the kind of devices we are connecting to the Internet. They are not just desktops, laptops, or even smartphones. They are light bulbs, refrigerators, cars, thermostats, sensors, and thousands of other "things"—a huge array of different kinds of devices with different functions, protocols, and security features. This growth in volume and heterogeneity makes effective cyber defense even harder.

2) The cyber threat is becoming more frequent: The number of malicious actors in cyberspace continues to grow rapidly as hacktivists, criminals, and nation-states all learn that they can pursue their goals relatively cheaply and effectively through cyberspace. The barriers to entry are low and the potential return on investment is high. As a result, the volume and frequency of malicious cyber activity is increasing dramatically.

3) The cyber threat is becoming more dangerous: Until recently, cyber actors generally limited their malicious activities to stealing money or information, temporary denial of service attacks, or website defacements (the digital equivalent of graffiti). But

increasingly, we are now seeing actors move to much more destructive and disruptive activities. The destructive cyber attack on Sony Pictures Entertainment, the physical disruption of the Ukrainian power grid, the use of cyber-enabled information operations to influence electoral processes, and the release of the destructive NotPetya malware are examples of this trend.

For the financial services industry specifically, three key threats stand out:

- Criminal cyber-enabled theft – criminal organizations will continue to target the financial services industry to steal as much money as they can.
- Nation-state cyber-enabled theft -- A few nation-states, such as North Korea, may also engage in stealing money from financial institutions if they have limited opportunities to earn hard currency.
- Disruption – some nation-states may target the industry for the purpose of inflicting economic harm on the United States and the West. In some cases, they may see such efforts as a proportional response to Western actions; in other cases, they may want the ability to hold the financial services industry at risk in the event of escalating conflict.

4) The cyber threat is becoming <u>more disruptive</u>: as we become more and more digitally dependent, the potential impacts of a cyber incident also increase. It is becoming harder for us to operate without access to the Internet – think about how organizations now send people home if the Internet is down. As a society, what would have been a nuisance a few years ago could now kill people.

The financial services industry must contend with these threat trends on a daily basis. Criminal organizations, nation-states, and hacktivists all target the industry, so the industry can never be complacent about its cybersecurity. On the whole, it has responded faster and more thoroughly than many other sectors. Yet, despite tremendous investment over the past 20 years, the financial services industry remains vulnerable to cyber threats.

<u>Why is Cybersecurity a hard challenge to solve?</u>

At first glance, it's not obvious why cyber threats are so hard to effectively manage, whether for the financial services industry or anyone else. If it's just a technology problem, why can't banks and other financial institutions simply deploy innovative technical solutions to stop these threats? Or why hasn't the industry's investment over the past two decades dealt with the problem? The answer is that cyber threats pose not just technical problems, but also economic, psychology, and human behavioral challenges. As a result, the response to threats has to involve not just technical solutions, but economic, psychological, and human behavioral aspects as well—a much greater challenge than simply buying a new cybersecurity device or service.

In addition, cyberspace operates according to different rules than the physical world. I do not mean the social "rules" of cyberspace that get a lot of play in the media, but rather the physics and math of cyberspace. The concepts of distance, borders, and proximity all operate differently in cyberspace compared to the physical world. Therefore, our typical models for addressing certain challenges, such as border security or missile defense, simply don't work in cyberspace. In fact, trying to use them can lead us to promote inadequate or wrong policies. Developing these new models will take time and experimentation to get right.

Finally, cyberspace and the Internet are still very new, relatively speaking. From a policy and legal perspective, we have not had the time or the experience to develop the comprehensive frameworks we need to tackle cybersecurity's challenges. What is the right division of responsibility between governments and the private sector in terms of cyber defense? What actions are acceptable for governments, companies, and individuals to take and which actions are not? Answering these kinds of questions is the fundamental policy challenge for the next few years.

What has the cybersecurity industry done to address these threats holistically?

For some time, the cybersecurity industry has known that the industry's approach to the problem was not working – we were in fact losing ground to the malicious actors. In that context, leading thinkers realized that robust information sharing across the entire cybersecurity ecosystem is a necessity in achieving enhanced cybersecurity; almost every systemic improvement anyone could think of rested on better information sharing in the cybersecurity industry. Despite this obvious enabling function, though, as a society we've had trouble figuring out how to actually share useful information, do so at a speed that matters, and then to take action based on that information. Therefore, several years ago, six of the largest cybersecurity companies (Checkpoint, Cisco, Fortinet, McAfee, Palo Alto Networks, and Symantec) joined together to create the Cyber Threat Alliance (CTA). CTA is a not-for-profit organization that is working to improve the cybersecurity of our global digital ecosystem by enabling near real-time, high-quality cyber threat information sharing among companies and organizations in the cybersecurity field. CTA's membership currently includes 17 of the largest cybersecurity companies from around the world.

To fulfill its core mission, CTA has built an automated information sharing platform with the goal of enabling and incentivizing the sharing of high-quality, actionable threat information. CTA and its platform embody a major step forward in transforming shared threat information into effective preventive measures that can automatically be deployed by CTA members to their respective customers, including customers in the financial services sector. The CTA platform is not just a concept or a set of Powerpoint slides – it is a functioning system, actively working to protect its members and their customers in near-real-time. So just as the financial services industry moved beyond talking about information sharing with the FS-ISAC and risk analysis with the FS-ARC, CTA is moving the cybersecurity industry beyond talking about information sharing and actually doing it.

By enabling this near-real time sharing, we can achieve several goals:

- CTA member companies can better protect their customers and clients by gaining access to information they otherwise would not have.
- CTA can use the shared information to develop analytic outputs that enable network defenders and governments to disrupt our adversaries more systemically. For example, CTA members have begun publishing comprehensive analyses of how a particular actor carries out its activities from beginning to end; we are calling these documents

"adversary playbooks." Just as in the sports context, if we know the adversary's playbook, then network defenders can position themselves to disrupt those activities more effectively.

- CTA enhances the industry's ability to respond to significant cyber incidents when they occur by enabling both machine and human speed sharing amongst its members.

In pursuing these goals, CTA becomes a force-multiplier for other organizations, such as Information Sharing and Analysis Organizations. By facilitating technical information sharing in the cybersecurity industry, CTA enables those entities to focus on sharing information directly relevant to that industry or region, rather than chasing generic, technical cybersecurity data. Alleviating this burden on end-user companies will raise the level of cybersecurity for everyone.

Of course, cyberthreat information sharing in the cybersecurity industry alone won't solve the problem by itself. Information sharing is only effective if it results in some kind of action or change in behavior. Therefore, while information is necessary part of the cyber risk-management equation, it is not sufficient. That's where end-user companies and governments have to take action.

What has the financial services industry done to address these threats?

The financial services industry has invested heavily in its cybersecurity, especially the largest institutions. The sector is a leader in the field and is often the yard stick for measuring progress in other sectors. In particular, I would highlight:

Financial Services Information Sharing and Analysis Center (FS-ISAC) – Founded almost 20 years ago, the FS-ISAC has become the "gold standard" for ISACs. With over 7,000 members from 38 different countries, most cybersecurity experts agree that it is the most effective sector-based information sharing organization in existence. Further, it serves as the executive agent for a large number of other ISACs, such as the automotive ISAC.

Financial Systemic Analysis & Resilience Center (FSARC) -- The FSARC's mission is to proactively identify, analyze, assess and coordinate activities to mitigate systemic risk to the U.S. financial system from current and emerging cyber security threats through focused operations and enhanced collaboration between participating firms, industry partners, and the U.S. Government. Technically housed within the FS-ISAC, the FSARC is made up of the eight largest U.S. banks and takes strategic risk analysis and collaboration to a new level.

Investment in personnel and capability – The largest financial institutions have invested in significant resources to build top-notch cybersecurity teams. The cybersecurity capability of the largest banks outstrips that of some small cybersecurity companies.

Input to the policy process – The financial services industry actively participates in the policy process here in DC. For example, it contributed significantly to the development of the NIST Cybersecurity Framework, and it has developed the Financial Services Sector Specific Cybersecurity "Profile" – a document designed to show how to make the general framework applicable to the sector.

And yet for all of these positives, the industry still has some systemic weaknesses:

Rapid fall off in capability – While the handful of largest financial institutions are extremely capable from a cybersecurity standpoint, the rest of the industry is still struggling to improve its defenses. Many regional and smaller financial institutions still suffer from the same weaknesses that plague other industries. They are unable to devote the resources to procure state of the art cybersecurity capabilities and staff.

High dependence on digital capabilities – Most financial institutions simply cannot function without the Internet or cyberspace. Money is stored digitally, for the most part. Business functions run almost entirely on line. Customers largely interact with their financial institution through some kind of digitally based system, even if it's just the ATM. Therefore, the industry is highly vulnerable to disruption coming through cyberspace.

Highly interconnected business operations – In order to operate effectively, financial institutions must be connected to each other in many different ways. However, these interconnections mean that cyber incidents can proliferate rapidly across the financial sector. Further, these interconnections are often not fully understood outside of a few experts in the industry, meaning that the actual level of risk is often undervalued.

Interdependence with other sectors – Finally the financial services sector is simultaneously highly dependent on other sectors, such as communications, information technology, and energy, and a key enabler for those sectors and many others. For example, the sector cannot function without access to power. Yet, power, transportation, health care – all depend on the ability of the financial services sector to continue functioning. The result is a poorly understood yet highly interdependent ecosystem.

What should we do about these threats?

Given the trends, growing complexities, and inherent challenges of the cyber threat, is it possible to design an effective strategy to combat it? The short answer is yes – but implementing such a strategy, whether at the organizational or national level, requires a lot of work, sustained engagement, and a multi-disciplinary, risk-based approach. It also requires inter-organization coordination and collaboration, including between the private and public sectors. The financial industry has experience with similar efforts in other areas, such as terrorist finance or counterfeiting, so the industry has a good foundation from which to build.

What do organizations need to do?

From an organizational perspective, an effective cyber strategy contains several core elements:

- Making cybersecurity a C-suite and organizational priority
- Using a risk-based, data driven approach to address cyber threats
- Developing, testing, and exercising an incident response and recovery plan
- Strong internal and external coordination

Within CTA, we have identified ten steps organizations can take to improve their cybersecurity, as shown in the following diagram.

1) *Mindset: Stop treating cybersecurity as a purely technical problem* – In most organizations, cybersecurity is a topic relegated to the Chief Information Officer, the head of IT, or the geek in the server closet; senior leaders send a problem down the line and hope they never have to talk about it again. Put bluntly, this approach fails.

   Instead, organizations must frame the problem differently. First, cybersecurity is not a technical problem to be solved, but rather a risk to be managed. By adopting this mindset, organizations can harness the tools used to manage other risks, such as insurance, resilience, defense in depth, and dispersion to manage cyber risk. Organizations must stop treating cybersecurity like a castle and moat problem – assuming that if the bad guys get "in," the bad guys win and the defenders lose. Looked at through that lens, defenders will always lose because determined bad guys can always find a way in . Instead, organizations should think about goal prevention. When conducting cyber operations, all adversaries have a goal, and if you stop them anywhere short of the goal, they lose and the defenders win. By adopting this mindset, organizations can play a game that defenders can win.

2) *Senior executive time and attention*– Cybersecurity needs to be a priority in the C-suite. If senior leaders take cybersecurity seriously and make it a priority by engaging regularly on the topic, then the organization's cybersecurity will improve. If leaders don't treat it seriously, no one else will, and cybersecurity will continue to suffer.

3) *Communications* – Once an organization has adopted a risk management mindset and senior leaders are engaged, the next task is clear communication. Leaders need to communicate cybersecurity goals and expectations across the organization and enable

communication between and across different parts of the organization. For instance, the business side needs to understand a company's cybersecurity priorities, while its network defenders need to understand business priorities.

4) *A holistic risk-management framework* – In order to deal holistically with cybersecurity's non-technical aspects, you need a framework that covers those non-technical aspects. While several approaches exist, the one produced by industry under the auspices of the U.S. Government's National Institute of Standards and Technology is the premier one in the financial services sector. The NIST Framework is NOT a how-to guide for IT people. Instead, it is aimed at executives and provides a way to think about cybersecurity from a risk management perspective.

   When organizations adopt the framework, it can help them in many ways. In particular, though, it can help organizations make resource allocation decisions. For example, the highest marginal return on the next cybersecurity dollar may not be in another technical solution. It might well be in investing in a robust recovery capability, or an employee training program, or cyber insurance. By adopting a risk management framework and analyzing where they are currently weak and strong, organizations can have an analytic foundation for making those investment decisions.

5) *Performance metrics* – If we want to manage our cyber risk over time, we need some way of knowing whether our risk is going up or down. Unfortunately, current cybersecurity metrics are generally fairly limited in value. The industry has not developed a set of widely-accepted, effective set of performance measures. There are some glimmers of hope, though, and some ideas are beginning to emerge. Nevertheless, organizations should still try to measure their performance over time.

6) *Cyber incident response planning* – The hard truth about cybersecurity is that while you can get better at it, you can never drive your risk to zero. At some point, the bad guys will successfully penetrate your organization. But that doesn't mean that you have to let the intruder SUCCEED in their goals at that point. Instead, if you have a plan ready for when the bad day happens, you have the chance to thwart the adversary and deny them their objectives. And even if you can't do that, you can minimize the pain that the event will inflict and show resilience. However, you need more than a plan in a binder on the shelf: you need to practice the plan. Too many organizations have a plan that sits on the shelf, that no one knows, and then when they try to dust it off (literally), it doesn't work.

7) *Accountability* – Holding people accountable is not a new concept. But in cybersecurity, organizations often don't have the right kind of accountability. They frequently use a zero-tolerance approach. But that doesn't work for cybersecurity – you're going to find problems you didn't know you had, you will face successful intrusions, it will take more time than you would like, etc. If companies are not realistic in their expectations, people will try to cover things up. Instead, organizations should hold people accountable for managing risk effectively, identifying problems, and then fixing them.

8) *Outside expertise* – All organizations should make use of outside expertise to improve their cybersecurity. The amount of outside expertise required will vary widely depending on a company's particular circumstances. However, even the largest, most effective companies work with outside experts on a regular basis, if only to get a "second opinion."

9) *Information sharing organizations* – All organizations should join a cybersecurity related information sharing organization. First off, it's just good to know you're not in this alone. But good sharing organizations help you understand the threats better as they emerge and provide you with specific best practices to thwart the threat. Gaining a rapid understanding of the threat and how best to deal with it is crucial.

10) *Collaboration with government* – Companies should build their connections with governments outside of an immediate crisis. No one wants to be exchanging business cards during a crisis. For many companies, cooperating with law enforcement isn't always easy; fortunately, for the financial services sector, that's less of a problem. But this collaboration need extends to Homeland Security, Treasury, and the other financial regulators in order for companies to be effective.

What do governments need to do?

As with individual companies, governments can develop effective strategies to reduce and manage the threat. An effective national cyber strategy involves three core elements:

- Raising the level of cybersecurity across the global digital ecosystem
- Disrupting, deterring, and constraining adversaries' use of these tools
- Responding effectively to incidents when they occur

In developing and implementing a cyber strategy, governments should recognize that no one agency has the full range of capabilities, authorities, and perspective needed to address the challenge. Further, no government can effectively address cyber threats by itself. Instead, cybersecurity is a fundamentally shared and distributed challenge that can only be addressed through collaboration that leverages the capabilities and authorities of companies, individuals, and governments. The private sector, non-governmental organizations, and national governments will have to work together across boundaries to implement effective cybersecurity strategies. Given this situation, governments could:

1. *Focus on comparative advantage* – Governments should not try to replicate the technical capabilities available in the private sector. They should also recognize that the cybersecurity <u>technical</u> information available to the private sector cybersecurity industry is extensive, and the government is unlikely to have technical information the private sector does not. However, governments can bring unique information into the mix – such as attribution, context, and a strategic view point; this kind of information is what the private sector does not have. Governments are also able to impose costs on adversaries through public attribution, law enforcement actions, economic sanctions, diplomatic

actions, and other means. Focusing on each sector's comparative advantage will enable the collective whole to be greater than the sum of the parts.

2. *Incentivize good cybersecurity behavior* – This concept has been the subject of considerable thought, including in the last administration. It is often difficult to do directly, but governments do have some tools at their disposal including:

    - Strategic use of existing regulations – governments should ensure that existing regulations promote good cybersecurity behavior, not inhibit it. Most of the time, new regulation is not required; instead, agencies should focus on implementing regulations that are already on the books. This situation is particularly true for the financial services industry.
    - Support and encourage the use of best practices – Governments are often well-positioned to be neutral parties in recommending what the best cybersecurity practices really are. A good example is the National Institute of Standards and Technology's Cybersecurity Framework.
    - Increase publicly available information – the government can facilitate disclosure of information that can help customers, clients, shareholders, and other relevant parties take appropriate defensive actions, better assess risk, and advocate for improved security. Examples of such requirements could include data breach reporting, information about material cybersecurity risks on financial statements, and public acknowledgements about how a publicly traded company is assessing and managing its cyber risk, particularly at the board of director's level. Such disclosures do not assist criminals or other bad actors – they already know where the weaknesses are; instead these requirements allow market forces to operate more efficiently. These requirements should be standardized as much as possible at the national level and harmonized at the international level to the extent possible, to reduce burdens on companies and simplify reporting for consumers.
    - Enable higher value-added competition in the cybersecurity industry – From a national point of view, we want fierce, robust competition in the cybersecurity industry. But we want cybersecurity companies competing to make their products and services more effective, not solely on the basis of who has more data.

3. *Reinforce stability in cyberspace* – Governments should strive to make cyberspace a stable, reliable environment in which to conduct business. Some key tools to achieve that goal include:

- Transparency –
    - Doctrine – Governments should be clear about how and when they will use cyber capabilities as a tool of national power.
    - Capabilities – Being clear about your capabilities in broad terms
- Promoting and Adhering to Norms – Norms can put certain activities "out of bounds." Not all nations will adhere to norms all of the time, but norms can help

constrain behavior. Of course, we have to have norms that we actually adhere to – the U.S. doesn't get to be the "do as we say, not as we do" country.

- Confidence-building measures – Adapting these approaches from arms control and conflict resolution field has promise to reduce the risk of escalation due to accidents or unintended consequences.

4. *Increase resilience to cyber attacks* – If we increase our ability to weather cyber attacks and maintain operations, then the value of conducting attacks decreases. It also makes leaders feel less "trigger" happy, because they can worry less about being pre-emptive.

5. *Increase operational collaboration between the public and private sectors* – Unlike in the physical realm, governments do not have a monopoly on cyber "force" and they're not like to get that any time soon. That means if we are going to systematically disrupt our adversaries in cyberspace, undermine the criminal business model, and respond more effectively to significant cyber incidents, the public and private sectors will need to achieve better operational collaboration.

   In considering how to build this new kind of collaboration, I don't have "the" solution for what it should look like. In fact, there's almost certainly not just one solution. However, the financial services industry has gone farther down this path than any other sector, except for the Defense Industrial Base. Through the hard work of many companies and people over the past decade and a half, the financial services industry has started building the foundations for this new kind of collaboration. The Federal government has worked hard to build its capabilities across all the relevant agencies – Treasury, the financial regulators, Homeland Security, Defense, Commerce, State, Justice, GSA, OMB, and the Intelligence Community all have critical roles to play within the U.S. context. The private sector has also been working hard globally, creating new structures, like Information Sharing and Analysis Organizations, building new technologies, and creating whole new industries, like cyber incident response firms. So the good news is that we do not need to start over. Instead, we can build on the foundation laid over the last decade.

Better cybersecurity

The cyber threats we face are very serious. For over forty years, the United States and other like-minded countries have used the Internet and cyberspace to derive enormous benefits: economic growth, national security improvements, and social well-being. However, if we do not begin to effectively address the cyber threats we face, those benefits could wither. Tackling this challenge effectively will require forging new partnerships within industries, between industries, and between the government and industry. It will require organizations to adopt new mindsets and change old beliefs to reflect the realities of the modern cyber threat environment. It will require coordinated action in a manner that reinforces market forces and competition. The financial services industry is already headed in this direction, and this Committee can help keep the industry moving. The Cyber Threat Alliance is ready to do its part in this endeavor and achieve effective cybersecurity for everyone around the world.

PREPARED STATEMENT OF PHIL VENABLES

CHIEF OPERATIONAL RISK OFFICER, GOLDMAN SACHS

MAY 24, 2018

Chairman Crapo, Ranking Member Brown, and other Members of the Committee, thank you for inviting me to testify at this hearing on Cybersecurity: Risks to Financial Services Industry and Its Preparedness. I appreciate the Committee's focus on such an important issue. My name is Phil Venables; I am the Chief Operational Risk Officer of Goldman Sachs. I have been with the firm 18 years and my first 16 years at the firm I was Chief Information Security Officer before moving into a wider role in our Risk Division.

Today, I am going to provide my perspective on the cyber-threats the financial sector faces, the broader technology risk landscape, the need for shared defenses and what can be done to keep improving the security and resilience of the financial system. A number of factors are contributing to increased inherent risk across the sector including, but not limited to, the increased digitalization of financial services and the globally interconnected nature of the financial system. The same trends that are increasing benefits of a global financial system are also bringing on these new and enhanced risks.

First on threats, it will probably come as no surprise that the financial sector, globally, is targeted by a wide range of cybersecurity threats including from organized criminal groups with financial motivation as well as nation states for a broad array of reasons.

Additionally, it is worth reminding ourselves that cybersecurity is not the only risk to information or technology systems. Risks posed from software errors, misconfiguration, outages and other resiliency issues can also cause as much impact as cybersecurity events.

It is critical to have shared defenses across the financial sector so that all institutions, large and small, can learn from each other's best practices and so that threat information can be shared among firms, reducing the likelihood attackers can execute their strategies without response.

We have a long history of robust information-sharing processes, with the FS–ISAC acknowledged as a preeminent example of such capability. Additionally, we have established tighter coupling between systemically important institutions through the Financial Systemic Analysis and Resilience Center, the so called FS–ARC. In addition, the sector's coordinating council under the Department of Treasury's leadership have proved instrumental in increasing sector resilience. Formalized sector-wide drills and exercises have spawned other initiatives, like Sheltered Harbor—an approach for firms to ensure the maintenance of immutable data vaults.

Turning our attention to regulators and regulation, we benefit from a number of strong regulators across the financial sector that stipulate cybersecurity and other controls that reduce the risk of major incidents. This includes regular examinations and reviews. We continue to support the need for harmonization of regulation, domestically and globally, and we commend the efforts to date on the use of the NIST Cybersecurity Framework. Additionally, we should be watchful for unintended detrimental consequences to cybersecurity from noncybersecurity legislation or regulation.

Notwithstanding the strong relationship on this issue between the public and private sectors, we continue to examine ways to enhance coordination. For instance, there is room for improvement in the responsiveness to financial sector Requests for Information. The establishment of the DHS National Cybersecurity and Communications Integration Center (NCCIC) in 2009 created the ability to have financial sector representatives in a cleared, collaborative space working directly with partners from Government and other industries for common purpose. Collaboration, engagement, responsiveness, between and among DHS, other U.S. Government and industry partners continues to improve as relationships build and partners are better able to understand each other's information needs. We would propose that metrics be established between the Government and financial sector to quantify and validate the flow, value and timeliness of information shared between the financial sector and public sector to quantify the state of these relationships.

Despite all this coordination and response to cybersecurity threats, risk still remains and we need to continue to be vigilant to adjust the defenses of individual firms and the sector as a whole by making sure we adopt innovative approaches to protecting customer data and services as well as designing for resilience to reduce single points of failure and single focal points of attack.

Finally, I would recommend all organizations that operate critical public services or protect customer data adopt strong defenses and security programs based on, at a minimum, the following approaches:

1. Integrate cybersecurity into the fabric of organizations—from business risk management processes, strategy and product development to the foundation of how the technology is built and operated, including planning for resilience in the face of attacks. Sustaining cybersecurity is a first class business risk along with all other risks—beginning with the Board and executive leadership and through all levels of the enterprise.

2. Improve capabilities amongst people, process and technology. There needs to be continued emphasis on the embedding of controls into critical technology products and services: we need secure products, not just security products. We should recognize that cybersecurity risk mitigation is not solely the responsibility of designated cybersecurity professionals but is, perhaps more importantly, in the domain of leadership, risk managers and engineers at all levels of organizations. I would support a national program to embed cybersecurity training into all academic and professional training and qualifications: we need more security-minded people, not just more security people. I fully endorse efforts to deal with the shortage of trained cybersecurity professionals to help manage these risks, but I also note that there is a wider issue related to the productivity of the cybersecurity professionals we already have and more needs to be done by Government and industry to improve tools, processes and the orchestration of defense across multiple platforms to get the most out of those people.

3. Design for defensibility. Our goal should be to design our technology and information processing environments to be more inherently defendable and resilient in the face of attacks, and we have to keep examining our global supply chains for security issues and excess concentration risk on specific services or geographies.

Thank you again Mr. Chairman for allowing me to provide this input into this important process and we remain committed to assisting further as needed. I'm happy to answer any questions you or the other Members may have at this time.

PREPARED STATEMENT OF CARL A. KESSLER III

SENIOR VICE PRESIDENT & CHIEF INFORMATION OFFICER (CIO)
FIRST MUTUAL HOLDING CO.

MAY 24, 2018

Chairman Crapo, Ranking Member Brown and distinguished Members of the Committee, thank you for the opportunity to testify before you today. I am pleased that the Committee continues to place a focus on cybersecurity risks and their implications to the financial system, businesses, and consumers.

As Chief Information Officer of a holding company comprised of several mutual community banks, I will share the unique perspective of community banks on cybersecurity regulation, information sharing, community bank collaboration and customer transparency.

Cybersecurity Regulation

Two key regulatory changes have positively improved the approach of community banks in managing cybersecurity risks. In the wake of the Dodd-Frank Act reforms, supervision of our affiliate banks migrated from the Office of Thrift Supervision (OTS) to the Office of the Comptroller of the Currency (OCC). The OCC has been consistent and adamant in raising all bank's readiness to address cybersecurity risks. Their outreach and guidance have yielded vast improvements in the cyber posture of community banks. In the last few years, the Federal Financial Institutions Examination Council (FFIEC) established the Cybersecurity Assessment Tool (CAT) for evaluating cyber controls in a uniform way among depository institutions.

Both regulatory actions have created a firm, but fair, supervisory approach in responding to emerging threats. While some may question these changes on the grounds of cost and a "one size fits all approach," it is indisputable that regulatory oversight protects both the banking system and the consumers. We have found that the regulators apply the FFIEC CAT tool in a manner consistent with the risk a bank poses. I believe that cybersecurity defenses and monitoring systems are integral infrastructure investments akin to those community banks have traditionally made in physical security safety. I encourage this Committee to continue its work with prudential regulators on these important matters.

With respect to OCC supervision and the advent of the FFIEC CAT, I understand both the perspectives of regional banks and community banks, having served in leadership capacities in both. I am pleased regulators use the same information technology (IT) examiners and general framework at institutions of all sizes. These examiners possess a strong understanding of cybersecurity risks and the controls deployed to protect banks and consumers. For any institution there is an inherent baseline of risk and a set of fundamental controls needed to protect consumer information. The approach of using dedicated IT examiners and practices fosters continuous improvement in preventing and detecting cybersecurity threats at institutions of all sizes.

At the same time, this approach also leads to ongoing dialogue with regulators. How much risk does our community bank present? What is most critical for the protection of our bank, our customers and our financial system? How should cybersecurity investment dollars be deployed? The FFIEC CAT helps institutions frame these risk questions. First, it provides a standard way to assess how much inherent risk an institution generates. Second, the FFIEC CAT provides guidelines for what controls might be appropriate to mitigate those risks.

After completing our holding company's assessment in 2015, we concluded that our existing information security program was well-aligned to the baseline expectations of the FFIEC CAT and, in fact, exceeded them. Subsequent actions focused our cybersecurity investment strategy to attain compliance with our level of risk and to address new threats as they arise.

Prudential regulation in conjunction with the FFIEC CAT is important to our bank's cyber readiness. Highly trained examiners are critical to administering the CAT. Because of the nature of the threat environment and the rapidly evolving domain of cybersecurity controls, an exam is never a static, check-the-box activity. It is always a dynamic conversation. My recommendation to this Committee is to ensure the consistent availability of highly trained IT examiners whose skills are in high demand in both the public and private sectors.

Another consideration for the Committee is to ensure that similar cybersecurity rigor exists among nonbank financial services companies. How do we safeguard customer data at companies outside the oversight of prudential regulators?

Information Sharing

As the cyber threat landscape evolves, a critical enabler is timely access to information sharing of active threats with community banks, through public and private partnerships.

To address the Committee's question of "what more needs to be done by the private sector and Government to help protect companies' and consumers' information," we must first identify where the significant risks lie. According to the Independent Community Bankers of America (ICBA), 99.5 percent of all banks are community institutions, half of which have assets under $250 million.[1] Almost all community banks do not operate an in-house transaction processing center. In other words, most community banks do not process customer transactions in their own data centers. They rely on a network of third-party service providers to deliver banking services. While maintaining primary accountability for safeguarding consumers' information, we rely on third-party providers including core processors, payments networks, and larger banks.

Only a few core processors provide IT services, such as customer transaction processing, mobile banking, and Bank Secrecy Act/Anti-money Laundering solutions. All banks interact through networks (ATM, debit card, and ACH) which are the backbone of the payments system. Some large banks provide processing for community banks through white labeled correspondent services. Although community banks represent the largest segment of banks in number, the risks associated with technology operations are aggregated in the data centers of just a few core processors,[2] payments networks and large banks.

Clearly, this concentration of IT services provides both advantages and challenges for managing community bank cybersecurity. The advantage is that through scale, the large service providers have more resources to address cyber threats. An additional benefit could also be realized if these providers acted transparently and shared cyber threat information with industry partnerships like the Financial Services Information Sharing and Analysis Center (FS–ISAC) and with their community bank clients.

[1] See ICBA Stats & Facts available at *http://www.icba.org/go-local/why-go-local/stats-facts.*

[2] The top three core processors hold a 70 percent market-share although how much of that is conducted in their data center versus the banks' data centers is unclear. *https://bankinnovation.net/2018/02/fiserv-has-largest-u-s-marketshare-of-top-bank-core-processors/.*

Core processors are active acquirers of technology companies and continually roll out new products. Although a core processor's information security plan may be sound today, each new acquisition introduces its own risk[3] into the environment. Thus, risk is constantly shifting within a core provider, and by extension to community banks and consumers.

I know our core processor is reviewed regularly by the OCC and FFIEC. We have limited access to the results of these reviews. If a bank were in the center of a significant event like a contract renewal or if there were a security breach in the recent past, the bank can request additional information. Community banks also have access to third-party audits conducted on a core processor's controls. Such a report is limited and only communicates if a core processor's controls are deemed effective. The actual number of breaches is typically not disclosed. Thus, a community bank must trust that if there is a significant pattern of breaches, its regulator will ensure that the causes are identified and remediated. The only way to know if a breach has occurred is if the bank is directly impacted or if the breach is significant enough to result in a news story that names a bank that happens to use that same service provider. Although these third parties are the stewards of our customer's information, we have very little insight into their overall security performance. In summary, law and regulation require banks to monitor closely the effectiveness of their service provider's controls related to cybersecurity and protecting nonpublic customer information. The current system relies on a high degree of blind trust in a service provider with limited transparency. This opaque approach runs contrary to best practices in information sharing and vendor management.

To partially compensate for this lack of transparency, banks I manage use a third party to track the information security performance of critical providers. My desire is more transparency in how service providers protect our customer information. For example, one solution might be to create a cybersecurity scorecard aggregating data from many sources including regulatory reviews. Such an approach must be carefully weighed against a chilling effect on information sharing. This scorecard, properly executed by a trusted third party, would enable banks to make better choices as they select vendors and create positive momentum toward control improvements.

It is important to explain what "information sharing" and "transparency" mean to a community bank. The key for banks is that a comprehensive ecosystem of financial services providers shares threat information in real time to an entity qualified to analyze, verify, and communicate it immediately to a bank where it can be used to adapt its controls.

FS–ISAC pioneered this kind of service and our bank was an early adopter. Upon validation of a threat by FS–ISAC, critical information such as the internet address of the attacker was automatically sent to our firewalls and blocked. This solution required our bank to setup a duplicative connection. Our ideal solution involves a close partnership between banks, our third-party service providers, a trusted third party and our security provider so that threats flow immediately to us via the existing mechanisms we have in place. The goal is to respond in seconds or minutes rather than days or weeks.

The most critical factor in thwarting a cyberattack is speed. The technology continues to improve as machine learning and artificial intelligence become more prevalent. The technology though cannot act on data it does not have. Important questions remain regarding if, when, and how businesses can share threat and/or breach information. In my conversations within the industry, there is still a great reluctance to share information. Liability, contract and privacy concerns are the most often cited reasons. I would suggest this is a good time to reexamine the effectiveness of cyber security law particularly as it affects information sharing. Timely information sharing is foundational to the industry's ability to combat a cyber threat. It may be worthwhile to require that service providers share threat and breach information with an authorized, trusted third party. In consideration for this sharing requirement, this Committee could consider expanding safe harbor liability provisions for third parties who meet certain strict requirements. This would clearly enhance consumer information protections.

Community Bank Collaboration

I would like to share a few unique and not-so-unique actions we have taken to help protect our customers. Established in 2015, our mutual holding company was founded on the belief that strong independent banks play a vital role in our

[3] In April, American Banker ran this story "BankThink Banks are from Mars, fintechs are from Venus: Bridging the matchmaking gap" by Terry Ammons which does a good job of representing the risks of a fintech acquisition; available at *https://www.americanbanker.com/opinion/banks-are-from-mars-fintechs-are-from-venus-bridging-the-matchmaking-gap*.

communities. As Ohio's largest independent, depositor-owned entity, we are faced every day with the cost, complexity and capacity required to implement an effective information security program. We believe that our holding company model leverages these capabilities with our affiliate banks in a manner that they otherwise could not afford, design, or staff. In our three affiliations we have preserved a local banking presence, improved security controls and done so at a minimal marginal cost for the holding company. This proves the cost savings for individual small banks is a game changer. We believe this is a real, practical example of the kind of collaboration envisioned by the OCC in their January 2015 paper "An Opportunity for Community Banks: Working Together Collaboratively."[4]

Customer Transparency

Finally, when talking about transparency and information sharing, we tend to focus on companies and Government entities. In all instances however we need to put the consumer at the center of this discussion. We are encouraged by the ability of technology to empower our customers. For example, many of us receive real-time alerts regarding our debit cards or when our credit report changes. I know this hardly seems to address "what more needs to be done," but keep in mind it's always about improving the speed at which we can detect and react to a threat. Giving consumers the tools and access to information makes us all safer.

Transparency and information sharing with the consumer is paramount. A key challenge for banks is the complexity of customer notification and privacy laws that exist today. While clearly needed, the simplification and modernization of the relevant laws and regulations can enable information sharing and therefore enhance consumer protections. Certainly, any solution must guard against shifting the liability to consumers from those who failed to protect their data.

Conclusion

Key takeaways:

- Continue supporting the regulatory review process and the FFIEC CAT
- Encourage transparency regarding the effectiveness of the security programs of the third-party service providers in our financial system including nonbank entities
- Review the effectiveness of current cybersecurity law with a focus on information sharing
- Review how the existing complexity of customer information and privacy protections laws may be slowing down the exchange of critical threat information
- Encourage community banks to collaborate
- Engage and empower the customer as a valued part of the cybersecurity solution

The best way to protect consumers is to increase transparency and information sharing within the financial services cybersecurity ecosystem. This Committee can help move this forward by encouraging the transparency of the performance of third-party service providers. You can also help by passing legislation which further encourages information sharing so that active threats are identified and mitigated in minutes.

Thank you for the opportunity to testify before you today. I stand ready to work with you in any way that I can to protect consumers and our financial system and look forward to answering your questions.

---

[4] *https://www.occ.treas.gov/publications/publications-by-type/other-publications-reports/pub-other-community-banks-working-collaborately.pdf.*

Testimony on "Cybersecurity: Risks to Financial Services and Its Preparedness"
Bob Sydow
Principal and Americas Cybersecurity Leader, EY

Committee on Banking, Housing and Urban Affairs
United States Senate
May 24, 2018

I. Introduction

Thank you Chairman Crapo and Ranking Member Brown for inviting me to testify today on behalf of EY. My name is Bob Sydow, and I am a principal at Ernst & Young LLP (EY), which is the US member firm of the global EY network. I lead the EY Americas Cybersecurity practices, have more than 30 years of experience in the cybersecurity field, and have helped build the EY Cyber and Technology practices. Throughout my career, I have worked with Fortune 500 companies on all aspects of information security strategy transformation, cyber risk management, data protection and privacy, identity and access management, cyber threat management and cyber analytics. My current responsibilities include oversight of EY's Cybersecurity practice, which provides assessment and security transformation services across all sectors in the Americas. The EY global network features a Cybersecurity practice spanning 150 countries and more than 7,000 practitioners.

The EY Cybersecurity practice benefits from our unique market position given the work we do within the financial services industry and across all sectors, which make up the modern day cybersecurity ecosystem. Today, I am pleased to testify and address any questions you may have about the state of cybersecurity in the financial services industry, including risks and threats to the sector and economy overall, efforts underway to increase cyber readiness against attacks and what more the public and private sector can do to better protect the economy, companies and, of course, consumers.

We have truly entered a transformative age where businesses are trying to stay one step ahead of the rapid pace of disruption. In doing so, many of our clients look to EY for fundamental end-to-end business transformation strategy and implementation. While transformations can involve everything from supply chain to customer experience, the driving force enabling this change is technology.

However, every new door opened and opportunity presented by innovative technology presents new risks, many of which are cyber in nature. It has never been more difficult for organizations to map and protect the digital environment in which they operate. Digital transformation has created entirely new industries and business models, for example by removing intermediaries in retail shopping and streamlining payment processing. It has triggered the downfall of American corporate giants and created unprecedented connectivity that is nothing short of a revolutionary force, with interdependencies at a scale we've never seen in history.

This is certainly true for the financial services sector, where some of the largest entities can have more than 70,000 third-party vendors connecting into their systems. I can tell you today that the financial services sector is considered the leader among all others when it comes to adoption of cybersecurity best practices. This is true not only in terms of organization and investment, but also in terms of leading engagement with stakeholders across the ecosystem. The industry is not without challenges, and there is variation among firms. For example, while the largest banks have considerable resources dedicated to cybersecurity risk management, smaller entities often struggle with costs and access to talent. That is not to say these organizations are not committed to cyber risk management or do not take the issue seriously. Cyber breaches and associated losses are not good for business, and when a company's business model depends on customer trust, a cyber event can be even more disastrous.

Trust, after all, is the bedrock of financial services firms and audit firms like EY. Building value successfully by using emerging technologies in the financial services sector demands a thoughtful balance. A focus on preventing cyber threats has, at times, delayed or impacted firms' digital innovation efforts, which can be a challenge in such a highly competitive market. Consumers' rapid adoption of disruptive emerging technology offerings reflects the way financial institutions create solutions that combine transparency, capability and personalization to meet customers' needs on their own terms. At the same time, they are building trust with customers in ways not previously achieved.

Those new solutions come with new threats. Crucially, the many benefits of technology, such as the processing power of the cloud, are also accessible to criminals. Firms that successfully introduce cutting-edge technologies need to infuse cybersecurity risk management practices throughout the entire development life cycle to identify and mitigate new risks as they emerge. This shift in mindset from thinking about cybersecurity as a cost of doing business to seeing it as a growth enabler is not easy, but it is the only viable path forward.

II. Global trends overview

In understanding cyber readiness within the financial services sector, it may be helpful to establish a baseline of comparison. Many US-based businesses, regardless of size, operate globally. As such, it can be helpful to review global cyber trends. For 20 years now, EY has conducted its Global Information Security Survey (GISS) across all sectors to investigate the most important cybersecurity issues facing organizations today.[1] The EY GISS captures the responses of nearly 1,200 participants in 60 countries across more than 20 sectors. Some of the key findings in this year's survey results reflect several of the challenges businesses throughout the economy are struggling to resolve, including with respect to investment, talent and organizational structure. For example:

- 89% of respondents say their cybersecurity function does not fully meet their organization's need
- 75% of respondents rate the maturity of their program to identify new vulnerabilities affecting their technologies as very low to moderate
- 35% describe their data protection policies as ad hoc or nonexistent
- 12% have no breach detection program in place

[1] The 20th EY Global Information Security Survey captures the responses of nearly 1,200 C-suite leaders and information security and IT executives/managers, representing many of the world's largest and most recognized global organizations across 60 countries. The research was conducted between June-September 2017.

- 43% of respondents do not have an agreed upon communications strategy or plan in place in the event of a significant attack
- 57% do not have, or only have, an informal program for gathering intelligence on new threats that could impact the company
- Only 4% of organizations are confident that they have fully considered the information security implications of their current strategy and that their risk landscape incorporates and monitors relevant cyber threats, vulnerabilities and risks

Digital innovation is also transforming the financial services sector — enabling firms to create new products and services, enhance access and experiences for customers, strengthen controls and drive down costs. As banks and other financial services firms define their digital strategies, their operations are becoming ever more integrated into an evolving and, at times, poorly understood cyber ecosystem.

The EY GISS results from banking and capital markets sector respondents, which were significantly weighted toward middle and small market financial services firms (82% of respondents were under $10 million in revenue), also highlight some challenges:[2]

- 85% of respondents say their cybersecurity function does not fully meet their organization's need
- 48% do not have, or only have, an informal threat intelligence program
- 54% of organizations still keep cybersecurity reporting mostly within the IT function
- 12% feel it very likely they would detect a sophisticated cyber attack
- 43% of boards have sufficient cybersecurity knowledge for effective oversight of cyber risks

In a representative comparison, data from the 2017 global EY/Institute of International Finance (IIF) bank risk management survey, which is far more representative of trends at the larger institutional banks, found that cybersecurity has become the number one concern among boards of directors and chief risk officers (CROs) for those institutions:

- 77% of CROs at the largest banks view cyber as their number one risk priority; up 26% from the prior year
- 57% of board directors view cyber as their number one risk priority; up 9% from the prior year[3]

While an individual bank's specific cybersecurity spend is proprietary, the amount of investment by the largest banks is orders of magnitude higher than those downstream, again in large part

[2] 14% of the nearly 1,200 respondents of EY's 20th Global Information Security Survey are from the Banking and Capital Markets sector

[3] "Eighth Annual EY/IIF bank risk management survey, Restore, rationalize and reinvent: a fundamental shift in the way banks manage risk," EY/IIF 2017, https://www.iif.com/system/files/ey_iif_bank_risk_management_survey_2017_restore_rationalize_reinvent_003_13_oct.pdf

because of access to resources. Forbes recently reported that two of the largest banks are spending an estimated $500 million a year each on cybersecurity.[4]

III. <u>Threats and vulnerabilities</u>

Given the prevalence and frequency of attacks throughout the ecosystem and against all organizations, the rapid integration of technological advances is a focus for many of EY's large banking clients. The Global Association of Risk Professionals published a report estimating that attacks and breaches cost businesses $445 billion every year.[5] Data grabs, ransomware attacks, processing disruptions and intentional modification of data can cost a business the trust of their customers, intellectual property and proprietary data. A cyber-related event also has the potential to have a significant effect on an organization's ongoing business operations, reputation, market valuation, financial position, operating results and compliance with laws and regulations.

Attackers may be either indiscriminate or highly targeted, attacking large and small organizations, and are pervasive in both the public and private sector. They are well camouflaged, and exposing attackers requires cybersecurity defenses that identify the threat, even when it adopts the colors of its immediate environment. Against this backdrop, organizations must consider resilience in the context of different categories of threat, which can be broken into three basic threat vectors:

1. Common attacks can be carried out by unsophisticated attackers, exploiting known vulnerabilities by using freely available hacking tools, with little expertise required to be successful.
2. Advanced attacks typically are carried out by sophisticated attackers, exploiting complex and sometimes unknown ("zero-day") vulnerabilities by using sophisticated tools and methodologies.
3. Emerging attacks focus on new attack vectors and vulnerabilities enabled by emerging technologies, typically carried out by more sophisticated attackers performing their own research to identify and exploit vulnerabilities.

Responses must be multilayered and focus on repelling the most common attacks, while also including more nuanced approaches to deal with advanced and emerging threats. As some of these attackers will inevitably breach the organization's defenses, there must also be focus on how quickly they are detected and how effectively breaches are managed.

In terms of common methods of attacks, point of access solutions remain a key element of cybersecurity response and resilience. Tools to help manage these attacks include antivirus software, intruder detection and protection systems, consistent software patch management and encryption technologies that protect the integrity of the data even if an attacker does gain access to it. Employee awareness and cyber hygiene are also crucial to frontline defense, which means changing norms to establish a cyber-minded culture throughout the organization. Of those

---

[4] "A Lack Of Cybersecurity Funding and Expertise Threatens U.S. Infrastructure," *Forbes*, 23 April 2018, https://www.forbes.com/sites/ellistalton/2018/04/23/the-u-s-governments-lack-of-cybersecurity-expertise-threatens-our-infrastructure/#4803c19149e0

[5] https://www.garp.org/#!/risk-intelligence/all/all/a1Z40000003NYkb

surveyed in the 2017 EY GISS, 68% of financial services respondents considered a careless member of staff as the most likely point of access of the attack.

To defend against advanced attacks, organizations must understand that some attacks will eventually breach their defenses and gain access to the system. As a result, it is critical to plan for and establish controls to identify and contain intrusions as quickly as possible. A Security Operations Center that sits at the heart of an organization's cyber threat detection capability is an excellent starting point and can provide a centralized, structured hub to coordinate all cybersecurity activities. Many such centers are moving beyond passive cybersecurity practices (i.e., waiting for a cyber event to be detected) and focusing on deliberately planned and continuously executed internal campaigns that seek to identify and remove hidden attackers and defeat likely threat scenarios targeting the organization's most critical assets. Even though such approaches have become a leading practice among the largest banks, 65% of financial services respondents to the EY GISS do not have a Security Operations Center — in large part because of resource constraints.

Preparing for and developing responses to combat emerging attacks requires an organization to accept that the nature of some threats will be necessarily unknown. Innovative organizations are imaginative about the nature of potential future threats and are focused on building agility into their cybersecurity approach so they are able to move quickly when the time comes. Organizations with good governance processes underlying their operational approach are able to practice security-by-design, i.e., building systems and processes able to respond to unexpected risks and emerging dangers.

Resource and budget constraints

The incredible pace, not only of technological innovation but also the evolving nature of the threat, necessarily means that there will always be more work than there are resources. While the largest banks have significant budgets dedicated to cybersecurity, many of the regional, midsized and community banks have far more limited resources. Many in the industry are focused on how to best maximize cybersecurity return on investment. At the same time, the latest technology and sophisticated risk management processes are only as effective as the workforce necessary to implement and operationalize them.

As a result, experienced cybersecurity professionals are in exceedingly high demand. The unemployment rate for these individuals is virtually 0%. According to cybersecurityventures.com, there will be an estimated shortfall of 3.5 million professionals in the global information security workforce by 2021.[6] While studies range slightly, a 2017 report estimated a shortfall of 1.8 million unfilled positions in the U.S. cybersecurity workforce by 2022.[7]

As companies continue to identify their needs and capability requirements, the war for talent will only become more acute. Sectors (i.e., financial services and technology) and regions (i.e., east

[6] https://cybersecurityventures.com/jobs/

[7] "2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk," Frost and Sullivan

coast and west coast) that are most attractive to workers are more often able to hire the top talent, which leaves potential gaps elsewhere in the ecosystem.

The cybersecurity environment also demands "life-long learning" through skills developed on the job. It is not enough for a cybersecurity professional to rely on standard classroom experience, conferences, or earning a certification. They must be able to tap into skills acquired over their career. A seasoned, cybersecurity professional is honed over time through on-the-job experiences, exposure to various situations (e.g., incident response), simulations and mentorship.

In reality, cybersecurity capabilities are needed throughout the organization and should not "live" only within the IT function. Truly differentiated cybersecurity professionals understand the business environment in which they operate, are able to convert cybersecurity threats into business implications and then into business strategy/operations. They can translate highly technical jargon into executive-level conversations. This capability is needed in the boardroom, in senior management and across business functions.

Vendors and supply chain management

As noted previously, while the largest companies can afford to build Security Operations Centers, many organizations try to overcome budget constraints by contracting out security functions, such as:

- Threat detection and response
- Vulnerability management (e.g., patching)
- User identity and access management
- Data protection and privacy

Ironically, even though vendors can help provide solutions to some of the resource constraints, third-parties inherently create additional risk. Any single entity can be a potential threat entry point, which may cause a ripple effect across the enterprise or industry. Whereas, traditionally, organizations thought of cybersecurity as a function to protect their own vulnerabilities, they often stopped short of considering the risks to the systems and data that is accessed by the third parties. Heightened regulatory and market focus have continued to put pressure on financial institutions to account for how other companies use and protect their data and manage sustainable operations, especially for critical services.

Because banks are subject to a higher level of regulatory scrutiny, their third-party risk management programs tend to be well established and more mature and robust than other financial services firms. However, as new cyber-related regulations are established and the risk related to these relationships are better understood, other organizations have begun taking steps to mature their programs.

For example, the New York State Department of Financial Services Cybersecurity Regulation required financial services firms to implement rigorous third-party cybersecurity risk management policies and procedures across the full life cycle of the relationship with third parties based upon the third parties risks to the organization..[8] The European Union's (EU)

[8] EY's *Overview of the finalized Cybersecurity Requirements from the New York State Department of Financial Services (DFS)*, EYGM Limited, February 2017

General Data Protection Regulation (GDPR) puts the onus of specific privacy requirements in the hands of the organizations and their third-party vendors collecting, storing and processing personal data. Firms subject to the GDPR will have to demonstrate their compliance with the requirements by May 25, 2018. The GDPR includes incredibly challenging requirements, such as the right to be forgotten, data portability, 72-hour breach notification, data privacy impact assessments and privacy by design. While this is being driven abroad, it significantly affects US companies offering goods or services to EU residents or those with an establishment in the EU.[9]

IV. Cyber risk governance

The board's role in fostering a cyber minded culture

At EY, we have found that directors serving on financial services boards receive a steady stream of news about cyber attacks, and most have received multiple briefings from their executive teams if not by federal national security officials. The primary challenge that directors and their firms grapple with is how to keep pace with fast-changing cyber risks in terms of the vulnerabilities or the new sources of risk that they create. Keeping up with known threats and vulnerabilities is difficult enough, but the scope of unknown cyber risks seems much larger than other, more traditional risk domains.

Directors appreciate that cyber attacks and breaches carry potential material risks and may now go beyond a profit motive to one associated with destroying data, manipulating systems and/or data, or incapacitating systems. A 2018 Council of Economic Advisors report highlighted that, of more than 1,900 breaches reported in 2016, almost 25% of breaches were in the financial services industry.[10] Hence, from a risk perspective, financial services boards understand both the potential impact and probability of cyber attacks are on the rise. EY has found that the most effective boards are implementing more robust cyber risk governance in five ways:

1. *Establishing and assessing cyber risk management maturity:* Boards need to understand the maturity of their organizations' approach relative to evolving industry and regulatory trends. Focusing on the chief information security officer's (CISO's) organization is necessary but no longer sufficient on its own. A cyber risk maturity assessment should be broad in nature, considering people, process and technology as well as existing and planned improvement or remediation activities. Foundational elements need to be in place, such as a firm-wide, consistent view of what constitutes cyber risk and the current vulnerabilities and threats. In that context, the effectiveness of existing controls can be evaluated.

2. *Measuring and evaluating cyber risk:* The view on program maturity needs to be combined with a proper assessment of existing threats and vulnerabilities and the evolving threat landscape. Boards should press management to quantify cyber risk as much as possible so that quantitative statements on the degree of cyber risk are

[9] See EY's *GDPR: demanding new privacy rights and obligations* in the Appendix or visit http://www.ey.com/gl/en/services/advisory/ey-general-data-protection-regulation

[10] *The Cost of Malicious Cyber Activity to the U.S. Economy* (page 19); The Council of Economic Advisors, February 2018.

incorporated into the firm's risk appetite statement.[11] The cyber risk appetite statement should link directly to cyber and technology operational thresholds and tolerances.

3. *Developing more robust and transparent management reporting on cyber risk:* Boards should insist on more credible cyber risk reporting, in the context of the approved cyber risk appetite. Boards should also determine how they evaluate the quality, accuracy and timeliness of cyber metrics. Too often, firms use key performance indicators for technology as proxies for real cyber risk reporting. Also, cyber loss estimates are usually too narrow, focusing on cost of recovery and fixing identified problems rather than the broader opportunity costs (e.g., lost business or customers) from technology problems created by cyber attacks. In EY's view, a more expansive view of cyber losses would materially improve decisions made around cyber investments. Cyber metrics should align with the broader firm risk taxonomy and align with metrics for operational, technology and privacy risk. Over time, cyber metrics should become more discrete and evolve to be more forward-looking.

4. *Apportioning oversight duties across the board and committees:* Boards should challenge how they oversee cyber risk across their own governance structure. Certain aspects of cyber risk management could fall to the full board or across various committees; for example:
   - The full board of directors might discuss the integrated, enterprise-wide cybersecurity strategy, supported by regular cybersecurity briefings on the evolving threat environment so every director is informed on the effectiveness of the cyber risk management program.
   - The audit committee often oversees how internal audit and compliance are evolving their reviews and oversight of cyber risk and regulations. The audit committee also oversees the work of the external auditor and may review the privacy dimensions of cybersecurity.
   - The risk management committee may engage the CRO on the evolution of the cyber risk strategy, including the cyber risk appetite and cyber risk metrics and reporting.
   - The operations and technology committee may engage the CISO, chief information officer (CIO), and chief technology officer (CTO) on the overall front-line cyber strategy, security operations, threat intelligence and incident response, as well as approaches to incorporating cybersecurity into innovation, digital and FinTech strategies. (To the extent such a committee does not exist, these dialogues would typically span the audit and risk committees.)
   - Personnel and compensation committees might engage the chief human resource officer on cybersecurity talent acquisition, retention, training and awareness strategies.
   - Nominations, governance and public affairs committee may evaluate cybersecurity and technology expertise among the board of directors, the board's ability to access internal or external cyber expertise, and how to effectively communicate with shareholders.

[11] For an example of an effective cyber risk dashboard, see Appendix F of the "Cyber-Risk Oversight: Director's Handbook Series," National Association of Corporate Directors, 2017.

5. *Overhauling cyber training for directors*: The board should revisit its strategy for keeping directors abreast of cyber threats, trends and the evolving business implications. EY has found that too often, this equates to annual presentations by the CISO but far more is needed. Aspects of cyber risk management should be built into an ongoing training program throughout the year, with overview sessions and deep dives on the most relevant topics and issues.

Ultimately, the board is accountable for ensuring that management adapts quickly enough to manage this enterprise risk more effectively and efficiently, and it is charged with providing a credible challenge to management's approach.

At EY, we believe that boards must be educated about cybersecurity so they are able to make appropriate decisions anchored in sound logic and data. They should embrace the challenge of mastering knowledge in this new, emerging area. By doing so, boards will not only be protecting shareholders but they will be enhancing the company's value. Directors should also set the tone at the top and concretely demonstrate that cybersecurity is an enterprise-wide priority and not just one that sits within IT. Board members possess both formal and informal responsibilities, as well as a duty to instill management accountability to drive outcomes, including with respect to cyber talent strategies, pressing management to identify high value assets, and incorporating cybersecurity into an organization's risk appetite statement.

The board should also elevate the position of an organization's cybersecurity leaders. For example, a leading practice is for the CISO to report directly to the C-suite, most commonly the chief operating officer (COO), chief administrative officer (CAO) or CIO. Consideration should also be given to embedding cybersecurity leaders throughout an organization, and the CISO should be well-versed in business strategy so that she or he can link the cybersecurity threat posture and risk tolerance to business drivers and protect high value assets. To make cyber strategy even more relevant, the board should anchor it to already existing risk frameworks that the organization employs, like those in finance, operations and procurement, in order to safeguard its reputation.

Cyber risk management across the three lines of defense[12]

Many companies seeking to establish an effective enterprise risk management system adopt a governance structure referred to as the three lines of defense (3LoD), which is common among financial services firms. The first line operates the business, owns the risk, and designs and implements operations. The second line defines policy statements and the risk management framework, provides a credible challenge to the first line, and is responsible for evaluating risk exposure for executive management and the board to consider when establishing a risk appetite. The third line of defense, which is also commonly referred to as internal audit, is responsible for the independent evaluation of the first and second lines.

EY has found that establishing a 3LoD approach to cyber risks is not a trivial task for an organization, but it is essential in the cyber-world we have entered. Financial services firms are still grappling with how to best implement the model across their businesses for existing non-

[12] This includes excerpts from *EY Cyber risk management across the three lines of defense*, EYGM Limited, April 2017.

financial risks. Adding cyber risk management as well as strong board oversight during the implementation of the three 3LoD model poses an even greater challenge for organizations.

First line of defense

A strong first line of cybersecurity defense requires a significant effort. Whether in the retail bank, investment bank, corporate bank, private bank or any other area, business heads will have to perform a thorough examination to determine whether the business is doing enough to manage cyber risk. Information security groups can no longer apply one-size-fits-all solutions to the entire enterprise. Instead, each line of business must carefully define the cyber risks and exposures it faces. Cyber risks need be woven into the fabric of the first line's risk and control self-assessment and into fraud, crisis management and resiliency processes.

EY teams advise organizations to achieve a better understanding about the interrelationship between their activities and cyber risks. The lines of business will need to actively monitor existing and future exposures, vulnerabilities, threats and risks associated with their activities. In addition to leveraging technologies, businesses need to determine the impact that cyber risk will have on its clients, operational processes and strategies. These new responsibilities require significant investment in people and tools, including upgraded monitoring and analytic capabilities to provide improved assessments of current levels of cyber risk.

Second line of defense

The independent second-line cyber risk management function manages the enterprise cyber risk appetite and risk management framework within the context of the overall enterprise risk strategy. This group challenges the first line's application of the board-approved cyber framework and appetite. Second-line risk management plays a critical role in managing cyber risks and should not be walled off as a separate risk function. As the keeper of a firm's board-approved risk tolerance, it determines how to appropriately measure cyber risks, embedding quantitative and qualitative (e.g., reputational) thresholds for cyber risks into the statement of risk tolerance for the firm. Moreover, these clearly established appetite and associated thresholds need to cascade down into the operations for each line of business.

Given the relative novelty of applying the 3LoD model to cyber risk, most of the first and second lines focus appropriately on more effective management of these risks rather than the narrower issue of compliance. However, with an increasing volume of regulatory guidance and mandatory requirements stemming from industry, professional and regulatory standards, cyber will increasingly constitute a material compliance risk. Accordingly, it is EY's view that financial institutions should integrate cyber risk compliance into second-line risk management.

Third line of defense

Traditionally, the main role of the third line of defense has been to provide an independent and objective assessment of the firm's process across the first and second lines of defense, with the focus on operational effectiveness and efficiency as part of the firm's overall risk governance approach. Regulators are now focusing on how effective and independent a firm's internal audit team is when it comes to reviewing the firm's approach to cybersecurity. For example, banking regulations focused on cybersecurity often include references to the importance of an "annual independent assessment," such as those included in Federal Financial Institutions Exam Council

(FFIEC) and National Institute of Standards and Technology (NIST) requirements and guidelines.

As a foundation, EY recommends that the internal audit team include within its overall audit plan an evaluation of the design and operating effectiveness of cyber risk management across the first and second lines of defense. Traditionally, industry standards, such as the NIST's Cybersecurity Framework guidelines have been used as the benchmark for evaluating a firm's effectiveness. Going forward, internal audit teams at financial institutions may need to create their own framework or apply multiple industry frameworks. By doing so, internal auditors will maintain greater independence in assessing cyber risk management effectiveness, eliminating the potential blind spots that can result from using a common standard throughout all three lines of defense.

Under the 3LoD model, internal auditors perform procedures such as assessments, validation of applications and technology infrastructure, evaluations of third-party risks, conduct independent penetration testing and vulnerability assessments, incorporate cyber into regular audits, and have a responsibility to stay abreast of cyber threat intelligence.

Getting the cyber 3LoD right

Regulators are encouraging utilization of the 3LoD model to compel banks to improve their risk management in response to failures in recent years. Firms have successfully implemented the 3LoD model in the area of financial risks, such as credit and liquidity. However, there are challenges in areas of non-financial risks, including cyber risk. Getting this right will take time. Given system-wide cyber risks, EY believes the financial services sector needs to move quickly to get the fundamentals in place so that, together, individual firms and the industry as a whole become better protected, more resilient and capable of responding quickly and effectively to the inevitable and increasingly potent attacks the industry will experience over the coming years.

The three lines of defense support cyber resiliency in financial services[13]

Today, the financial services industry is facing tougher questions from external parties as to their cyber resiliency strategy. Increasingly, regulators, investors and major clients are demanding evidence that firms' cyber resiliency strategies are effective. Stakeholders want to know how the organization is reducing the likelihood of a disruption to services; how it will manage prolonged systems outages, including how transactions will be processed; and how it will recover effectively in a timely and well-controlled manner. Financial services firms recognize that cyber resiliency relates to the seamless maintenance and ongoing delivery of operations during a disruption. This includes how firms govern and challenge cyber resiliency with the 3LoD. Additionally, the industry is working on advancing reduction in risk in the financial ecosystem through initiatives led by private sector industry organizations in collaboration with government agencies and the intelligence community. EY recommends that key areas of resiliency include:

1. *Risk-assess cyber resiliency*
   Firms should assess their cyber risk profile and identify major risks, threats and vulnerabilities. This requires:

[13] This includes excerpts from *EY Cyber resiliency: evidencing a well-thought-out strategy*, EYGM, August 2017.

- An effective risk assessment process, which includes taking an end-to-end view so that the entirety of the process and supporting systems, vendors and dependencies can be identified.
- Building effective controls to reduce residual risks to levels within the firm's overall risk appetite for resiliency. This includes understanding how dependency on third parties impacts the control environment.
- An enterprise-wide, prioritized view on critical processes and flows. Given finite resources — management time, budget and people — firms inevitably have to prioritize certain resiliency activities. There will likely be differing views within each firm about what constitutes criticality.

2. *Identify, architect and protect systems, especially those most critical to the firm and the broader financial services ecosystem*
   High value assets that are "sector-critical systems" are generally easier to identify, e.g., the key intraday settlement and clearing systems that help the financial system operate smoothly. Beyond those systems and assets, however, differing views will exist as to what is critical. Once identified, EY advises firms to:
   - Identify those individual systems or assets' ecosystem.
   - Evaluate and, where necessary, improve system architecture and design. Critical systems have to be sufficiently flexible, agile and resilient.
   - Evaluate if systems and tools used to monitor infrastructure present major vulnerabilities themselves. After all, if these tools are breached, attackers could gain access to an even broader swath of important systems.
   - Evaluate system obsolescence. Every firm has adopted its own strategy that may take into consideration the pace at which new versions of software or hardware are installed, the approach to patching, and the degree to which the firm will depend (or not) on systems that are no longer vendor-supported. It is important that firms carefully consider if a differentiated strategy is needed for critical systems. As recent global ransomware attacks have shown, system outages can be traced to dependencies on old versions and bad patching practices.

3. *Manage critical third parties and other key dependencies, especially those that support or connect with critical processes and systems*
   An enterprise-view of critical vendors should be evaluated regularly in the context of recovery and resolution planning. Organizations should evaluate or re-evaluate vendors' resiliency and cybersecurity practices, build contracts that include terms addressing performance and key risk indicators, and establish a process to regularly provide real- or near-time monitoring of critical vendors. Many recent breaches highlight how even vendors outside of the financial ecosystem can create vulnerabilities if systems are not properly segmented.

4. *Detect, respond, recover and communicate*
   Even the most sophisticated organizations will eventually experience a cyber breach. EY advises firms to have fully developed response plans in place before an event occurs. All corporate officers and functions — from the board, executive management, risk functions and general counsel to business units and information technology — need to be considered in

incident remediation. Many incident investigations are far more complicated than simply removing malware. They often involve reviews of the technical facts combined with operational, legal and financial impacts. As a result, victim organizations often call in multiple forensic investigators and counsel to address the variety of external inquiries.

5. *Test systems and recovery plans*
   EY advises financial services firms to regularly test cyber resiliency strategies. The first line has to test the effectiveness of its own controls, in the context of its risk assessment. The second and third lines should review some of these processes to validate the first line:
   - "Tabletop exercises" or role-playing scenarios are an important way to test plans, educate participants and identify areas for improvement. Scenarios should be realistic, include participants from across the 3LoD, and include specific cyber scenarios.
   - Each of the 3LoD should conduct routine tests to assess the degree to which systems can be penetrated. This typically requires external third-party support.
   - In addition to tabletops, when possible, firms should participate in "war games" that involve stakeholders from across the industry. These exercises help firms better appreciate scenarios that could impact the entire financial sector. War games also help organizations better manage expectations about how the market or peers will react.
   - In the end, testing, tabletops and war games are only helpful if identified deficiencies are addressed.

<u>Resiliency extends beyond cyber attacks</u>
At EY, we believe that achieving cyber resiliency requires an integrated approach across technology and the front-line businesses, cybersecurity and information security, the three lines of defense, and across the entire organization, including the board of directors. In practice, resiliency is a broad-based concern that firms can only address effectively and efficiently by integrating a set of disparate activities across the enterprise. That is true for operational resiliency, as much as it is for cyber resiliency.

V. Leveraging cybersecurity advances to fight financial crimes

Financial institutions' customers, whether individual consumers or commercial business partners, expect an experience that is consistent, positive and frictionless. To support digitized banking experiences, financial services providers increasingly rely on cloud-based off-premise solutions in conjunction with their on-premise legacy applications and infrastructure, as well as upon the integration of many third-party technologies, both open and closed source. At EY, we have observed a blurring of the lines between financial services, FinTech, and technology companies. This will only continue to progress as more innovation and efficiency is introduced into digitized and integrated services.

Each step up the integrated chain of financial services brings risks and challenges for fraud and authentication, as well as the confidentiality and integrity of transactions. Financial services firms have responded to consumer expectations by adding more digital and traditional banking channels and increasing security as channels become more virtual. Complex cross-channel attacks that combine information gathered from social media as well as digital and traditional banking channels are on the rise. Similar to fraud scenarios, anti-money laundering (AML) activities can use similar channels, though in a much less complicated way. As a result, cybersecurity vulnerabilities are increasingly being identified as the "root cause" of fraud events. Advanced technologies and the commoditization of cyber tools, tactics and procedures allow criminals to attempt fraud at unprecedented scales.

There are many challenges, including protecting and monitoring customer touch points across various channels. EY has found that attacks are increasingly targeting data itself as the asset of value. Information sharing between cybersecurity and fraud programs may be missing, insufficient, ineffective or difficult to act upon. A number of corporate cultures do not recognize the link between fraud and cybercrime; although, more firms are drawing links and looking to integrate these capabilities. EY has found that criminals take advantage of organizational issues, and functional silos that exist at many organizations that can make it easier for fraud to be committed in ways that are difficult to detect.

In addition, ransomware attacks, designed to be destructive or to obscure application data, are increasingly common. Ransomware attacks are a very serious concern given that they can result in interruption, disruption or destruction of critical business services. As digitization accelerates, many businesses have lost their ability to protect their enterprise, and they have also lost their capability to understand their infrastructure. As such, there exists a concerning risk intersection between cyber and business resilience.

VI. <u>AICPA's Cybersecurity Risk Management Reporting Framework</u>

Another major challenge in the market is how to communicate effectively with internal and external stakeholders about a company's cybersecurity risk management activities. Limited options have been available to provide relevant, validated information that enable various stakeholders to make informed decisions. Investors trust the board to oversee the management of cybersecurity risk. Boards trust management to effectively manage cyber risk, and often management relies upon various third-party vendors to help support cyber efforts.

However, there has been no independent, validated basis to warrant such trust. To help address this market need, the American Institute of Certified Public Accountants (AICPA) recently undertook an effort that built upon the accounting profession's historical role of promoting trust and confidence in the market. In 2017, the AICPA issued an evaluation framework with an optional reporting model that can provide stakeholders with: (1) transparency into key aspects of an organization's cybersecurity risk management program, (2) confidence in the adequacy of the program and (3) assurance as to the program's effectiveness.

The framework that the AICPA developed is different from existing "implementation frameworks" developed by NIST, International Organization for Standardization (ISO) and others. Implementation frameworks lay out the key building blocks that should be included in a risk management program. The AICPA's evaluation framework, on the other hand, focuses on the outcome of the risk management program and whether a program is properly designed and verified to be operating effectively. The distinction is subtle, but significant. Ernst & Young LLP supports the AICPA guidance, which is voluntary in its application and enables companies to communicate with its stakeholders on three levels:

- At the entity-level, where an organization could report on the effectiveness of its overall cybersecurity risk management program to board members, investors and others.

- At the service provider-level, where an organization could report on the effectiveness of key aspects of its cybersecurity risk management program relative to an outsourced service that they provide to the market.
- At the supply chain-level, where an organization could report on the effectiveness of its processes and key aspects of its cybersecurity risk management program relative to the manufacturing and distribution of supply chain goods provided to the market. This component of evaluation framework is still in development, and final guidance will be available in early 2019.

We at EY note that such attestation engagements cannot ensure a company will be free from material cybersecurity events, but evaluation frameworks enhance the level and quality of communication taking place between companies and their stakeholders to a point where more effective risk management decisions can be made. They can enhance stakeholder confidence in the cyber management security program being employed. The receipt of an unqualified opinion on an attestation engagement is intended to convey that the entity has implemented reasonable controls to complicate attackers' efforts and to detect, respond and recover from a cybersecurity event: (1) when measured against criteria that have been vetted in the marketplace and deemed to be suitable for the intended purpose and (2) based on specific cybersecurity objectives that the company is obligated to achieve. The stakeholder in this case can be the board, or, if the board chooses, it could be reporting to the public in some manner.

In addition to being more comprehensive and business-centric, if a report under one of the AICPA's cyber-related reporting options is issued, adherence to the evaluation framework will be essential, as the criteria and areas of focus will generally serve as the basis of those engagements. Ernst & Young LLP believes the voluntary use of the AICPA guidance can help boards, management, investors or analysts gain a more complete, objective understanding of an organization's cybersecurity risk exposure and controls. It may also be a way for companies to differentiate themselves in the market and reassure customers, investors and other stakeholders.

VII. <u>Role of policymakers</u>

EY is committed to building a better working world and commends the Senate Banking Committee for convening this hearing to engage in meaningful dialogue on this systemic issue. Understanding the nature of cyber risk is the first step in developing more effective solutions. Every organization, public or private, faces this challenge and is exposed to the threat. Engaging your colleagues in Congress on this topic, pursuing and facilitating systems modernization and better cyber risk management in federal, state and local governments, and encouraging the American people to improve their own understanding of cyber challenges and vulnerabilities are important steps this committee can take. Focusing on long-term policy solutions to develop and increase the cyber workforce and working to resolve sector and resource issues known to exist are other opportunities for policymakers to address these challenges.

Unfortunately, there is no silver bullet — no single legislative, regulatory or market solution — that can solve this challenge. And the challenges are great. Not only do threats evolve day-by-day, but those who want to do harm are not constrained by regulatory, liability or jurisdictional issues, let alone ethics. Policymakers and the business community must work together to improve cyber information sharing and develop collaborative, flexible and harmonized policy solutions that help organizations better respond to the dynamic nature of the challenge.

While no one can guarantee that any or all attacks can be prevented, the market is developing best practices and ways to mitigate risk and impact. Companies that exercise good faith efforts, establish cyber risk management frameworks and adopt such best practices as outlined in this testimony should benefit, not only within the company, but in the eyes of stakeholders, regulators and enforcement agencies, especially relative to liability and penalty measures. Given this committee's experience and expertise in the area of corporate governance, and acknowledging the sector and resource constraints that all organizations and this nation face, investigating ways to incentivize responsible and effective corporate governance and risk management strategies by rewarding good behavior could be an area for the committee to pursue.

Given its role in the ecosystem, I would also encourage Congress to consider the modernization and improvement of the cybersecurity posture of all branches of government as well. The same approach to comprehensive enterprise-wide cybersecurity assessments being pursued in the private sector are equally relevant to the public sector. Holistic cybersecurity assessments should be conducted on a regular basis and should span a public sector organization's overall risk management structure. This would help give executive leadership and the American people the confidence that their single most important mission asset — information — is sufficiently protected against current and future threats.

Just as no government agency wants to be hacked, no company wants to be hacked. There are many organizations across the ecosystem that should be commended for their efforts to manage and mitigate cyber risks. The financial services sector may have its challenges, but it is the gold standard in the market today. EY is working with our financial services clients and companies from all sectors to be responsive to the many cybersecurity challenges we all face. While EY does not have the solution to this systemic challenge, we are doing our part to build a better working world by helping our clients develop and implement better risk management controls, educating boards and senior management, and developing a number of market-based solutions to better manage cyber risk and resource shortage challenges. The AICPA's cybersecurity evaluation and reporting framework is an example of a voluntary, market-based solution that can help boards, shareholders and senior management alike.

* * * * * *

I thank the committee for granting me the opportunity to testify today and would be happy to take any questions.

Appendix

In the race to compete in today's digital world, organizations are using social, mobile, big data, analytics and the Internet of Things to gather as much information on their customers as possible, while simultaneously trying to do everything possible to protect their organizations from cyber risks that come from the outside and within. In this environment, privacy protection can become an afterthought, bolted on to information security programs in an ad hoc manner or, in the worst case, organizations have elected to ignore the issue.

For years, regulators and privacy commissions around the world have attempted to regulate privacy protection and develop privacy standards, such as privacy by design (PbD), for organizations to adhere and adopt. However, even as regulators pushed accountability, many organizations saw it as more voluntary than mandatory. They were content to address the letter of the law outlined in the legislation as opposed to its spirit, i.e., to meet minimal compliance obligations without taking responsibility for their role in protecting their customers' or employees' information.

With the forthcoming implementation of the European Union's (EU) General Data Protection Regulation (GDPR), and its implications for organizations across the globe, the days of organizations leaving the responsibility for privacy protection to someone else are about to end. The EU's GDPR puts the onus of specific privacy requirements in the hands of the entities collecting, storing, analyzing and managing personally identifiable information.

Firms subject to the GDPR will have to demonstrate their compliance with the requirements by May 25, 2018. The GDPR is much more demanding, and applies more broadly, than existing EU data protection requirements. Each requirement by itself – such as the right to be forgotten, data portability, 72-hour breach notification, data privacy impact assessments and privacy by design – is demanding, but in aggregate, the GDPR is very onerous.

For more cyber and privacy insights, visit ey.com/fsGDPR **or** ey.com/fscyber

Note: The General Data Protection Regulation is European Union regulation 2016/679, made 27 April 2016, implementation date 25 May 2018.

To date, many non-EU financial services firms have been slow to react to the GDPR. While some firms have taken a proactive and comprehensive approach, many have not. Even firms in the EU are delayed. For example, a recent UK government survey highlighted that only 6% of the Financial Times Stock Exchange (FTSE) 350 companies report being completely prepared to meet the GDPR compliance requirements.[1]

Firms need to focus on the GDPR now. Time is running out!

Immediate next steps

- Educate key stakeholders, including the board of directors
- Risk-assess (including legal applicability) whether the GDPR applies to your organization
- Establish cross-function and cross-business governance structure for assessment of the GDPR's applicability to business operations, evaluation of readiness and management of your overall GDPR remediation efforts
- Conduct a privacy impact assessment, with a strong focus on high-risk data flows of business processes
- Conduct a GDPR gap assessment, with a particular focus on governance, policies, technology, external dependencies (e.g., vendors), existing data flows ("high-risk") and processing operations
- Design and execute a prioritized implementation plan to address gaps based upon risk tolerance, risk priority, resourcing and investment

[1] "FTSE Cyber Governance Health Check Report 2017," HM Government, Crown copyright 2017.

What is the GDPR?

The GDPR is an omnibus data protection law that builds upon, expands and ultimately replaces the EU Data Protection Directive. The GDPR gives individuals new rights over their data, which heightens the accountability on entities collecting, storing, analyzing and managing personally identifiable information. This covers any information relating to an identified or identifiable natural person, such as name, identification number, location data or one of more factors specific to physical, physiological, genetic, mental, economic, cultural or social identity on the nature of the person, as well as online identifiers (e.g., IP addresses). A data subject can be a customer, employee, contractor or third party. Released in 2016, and due to come into effect May 25, 2018, the GDPR applies to any organization, regardless of geographic location, that controls or processes the data of an EU resident in a proscribed way. It dictates to what extent personal data may be collected, the need for explicit consent to gather such data, requirements to disclose breaches of data and stronger powers to substantially fine organizations that fail to protect the data for which they are responsible. And it has real teeth.

The GDPR prescribes certain responsibilities and liabilities to controllers and processors of personal data. It is important to understand these terms as they are defined within the GDPR.

- **Controller:** a body (alone or jointly with others) that determines the purposes and means of the processing of personal data
- **Processor:** a body that processes personal data on behalf of the controller; processing activity can include collecting, organizing, storing, disclosing, using, etc.
- **Personal data:** any information (single or multiple data points) relating to an identified or identifiable natural person such as name, employee identification number or location data

The GDPR imposes new obligations on both controllers and processors of personal data, emphasizing accountability and requiring greater documentation and records.

Firms have until May 25, 2018, to implement changes and comply with the obligations of the GDPR. Penalties for failing to comply with the GDPR's basic processing principles may subject the organization to fines up to €20 million or 4% of the organization's total global revenue, whichever is greater.[2]

Key facts about the GDPR

Applicability: applies to entities – including third parties that are (i) established in the EU, (ii) providing goods or services to EU residents or (iii) are monitoring the behavior of individuals in the EU

Fines: up to €20 million or 4% of the organization's total global revenue, whichever is greater; also provides individuals new rights to bring class actions against data controllers or processors, if represented by not-for-profit organizations, which heightens litigation risk

[2] EU regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

GDPR highlights

Organizations will have only 72 hours to report data breaches.
Privacy-by-design principles must be incorporated into the development of new processes and technologies.
Explicit and affirmative consent will be required before processing personal data.
Most organizations will need to designate a Data Protection Officer.
Organizations will have to maintain records of processing activities.
Organizations will need to scale security measures based on privacy risks.
International transfers are prohibited except through certain mechanisms.
Organizations will report to one supervisory authority.
Organizations will have to facilitate customers' and employees' right to erasure (of data), right to portability, and an increased right of access.

GDPR impacts

Penalties for failing to comply with the basic processing principles of GDPR may subject the organization to fines up to

€20 million or **4%**

of the organization's total global revenue, whichever is greater.

Organizations have only until

25 May 2018

to implement changes and comply with GDPR obligations.

Imposes new

obligations

for both controllers and processors of personal data

Places a greater emphasis on

accountability

requiring greater

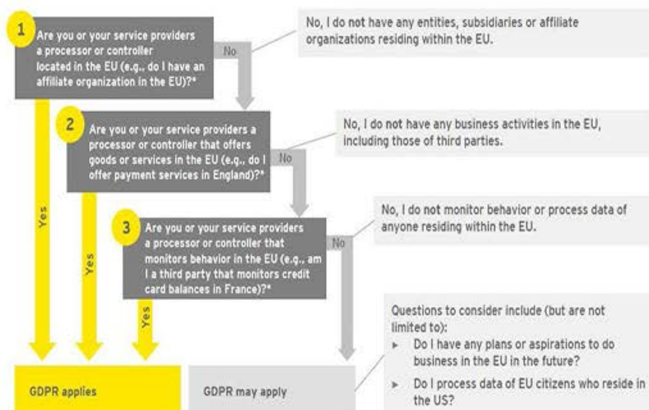
documentation

and records

Is the GDPR applicable to you?

Many non-EU financial services firms have determined that the GDPR doesn't apply to them with limited understanding of how the regulation actually works. Figure 1 outlines three distinct questions that can be used to assess applicability.

Figure 1: Three key questions to assessment applicability



*Note - the responses to these questions should be evaluated based on the facts and circumstances in your organization and discussed with legal counsel.

The question, "Are you or your service providers a processor or controller that monitors behavior in the EU?" captures a broader range of activities than many firms think. Consider centralized functions that conduct surveillance, such as for fraud, anti-money laundering, sanctions or cyber threats. To the extent those functions use data related to EU residents, your organization may be subject to the GDPR requirements. Similarly, many firms' websites continuously monitor traffic and users, and some leverage third-party vendors in the website execution. Those activities – of the firm or the third parties – may subject your organization to GDPR requirements.

Firms are advised to consider these questions and discuss them with their legal counsel. However, firms may be inclined to take too much of a legalistic approach to the GDPR, depending too heavily on outside counsel's advice on whether or how the GDPR applies to their firm. In addition to the legal input, firms should undertake a risk-based assessment to evaluate the relevance and applicability of the GDPR based on a fact-based, documented review of the degree to which their operations or third parties access, store or monitor data related to EU residents. Such an approach takes into the account the firm's strategy, growth plans, risk tolerance, existing controls and capabilities, as well as other contextual factors that may impact the determination of applicability.

What are the main GDPR concepts and requirements?

The GDPR enhances the data protection rights of EU data subjects. In general, firms will need to provide easier access to personal data, with clear and understandable information on its processing, use and storage.

Major requirements and concepts include:

- **Data protection impact assessment (DPIA):** DPIAs (also known as a privacy impact assessment or PIA) are required for all process operations of an organization. DPIAs should be viewed as tools that can help organizations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy. There is a debate in the marketplace about the required approach: are data flows required for GDPR or can data narratives be utilized? Generally, firms seem to be completing data flows to properly assess the GDPR, especially to understand data flows in their high-risk processing activities. An effective DPIA will allow organizations to identify and fix problems, reducing the associated costs and damage to reputation that might otherwise occur.
- **Data privacy accountabilities:** the GDPR attempts to define what privacy accountability means in practice through requirements around proactive monitoring and personal data records. The GDPR states that the controller is responsible for confirming that all of the GDPR privacy principles are adhered to and that firms can demonstrate compliance. Each organization has to understand the principles of lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation and integrity and confidentiality. The DPIAs will help in this regard.
- **Condition for processing:** the processing of personal data is only lawful if it is permitted by the GDPR and has proper customer consent. If the controller does not have a legitimate reason for a given data processing activity, then that activity is not allowed – firms must have at least one legitimate reason for processing, which can include the individual's consent, contractual necessity, legal obligation, regulatory requirements or public interests.
- **Data protection officer (DPO):** firms that establish they conduct large-scale systematic monitoring of EU residents' data or process large amounts of sensitive personal information have to appoint a DPO. "Large-scale" could be as small as the processing of data on more than 5,000 subjects in any 12-month period.[3] DPOs have significant accountability for adherence to the GDPR requirements, and they must be appropriately qualified in data protection laws and practices, independent of management,have access to the necessary resources to monitor GDPR compliance and be actively included on all relevant data protection discussions and decisions. The regulation calls for the DPO to report to the "highest management level," which EU guidance suggests could be the board of directors.[4]
- **Privacy by design (PbD):** is the practice of establishing and implementing privacy controls and principles into business processes and systems as they are being developed and built, rather than layering on controls after deployment. Although PbD has been championed for years by privacy commissions around the world as a leading privacy standard, in our 2015 Global Information Security Survey, only 18% of survey respondents indicate that they have applied PbD to their new processes and technologies.[5] Under the GDPR, organizations will now be required to design policies, procedures and systems that follow PbD principles at the outset of every product or process development.
- **Right to erasure:** the right to erasure enables an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. This right creates significant data retention challenges for firms. The broader EU principle this relates to is the right to be forgotten, whereby residents have the right to have personal data on public media deleted (including by third parties).

[3] "Top 5 Priorities to Prepare for EU GDPR," *Gartner website*, www.gartner.com/smarterwithgartner/top-five-priorities-to-prepare-for-eu-gdpr, 20 June 2017.
[4] Article 29 Data Protection Working Party, Guidance on Data Protection Officers (DPOs), April 5, 2017.
[5] *Can privacy really be protected anymore? Privacy trends 2016*, EYGM Limited, 2016.

- **Individuals have the right to have personal data erased and to prevent further processing:** under the following circumstances:
  - Personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
  - Individual withdraws consent.
  - Individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
  - Personal data was unlawfully processed.
  - Personal data has to be erased in order to comply with a legal obligation.
  - Personal data is processed in relation to the offer of services to a child.
- **Consent and notifications:** under the GDPR, consent must be freely given, specific, informed and unambiguous, indicating the data subject's agreement to the processing of personal data relating to him or her. It should be noted that consent is not required if there is another basis for use – in practice, most firms will point to a signed contract as their basis.

  Breach notifications under the GDPR must be done within 72 hours of the organization becoming aware of the breach. If the breach is sufficiently serious to warrant notification to the individual data subject, the organization responsible must do so without undue delay. Failing to notify or noncompliance can result in a significant fine up to €10 million or 2% of global revenue.[6] Many practitioners expect that when the EU issues new guidance later in 2017 on the breach requirements, it will recognize that it will often be impossible to investigate a breach fully within that time period and will allow firms to provide information in phases, so long as the relevant data protection authority, or DPA, is notified.
- **Data portability:** the right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. The provision allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. It is the responsibility of the controller to confirm this capability exists.

---

[6] EU regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

What is the difference between EU GDPR and US GLBA?

The focus of all privacy regulations is on an individual's right to control access to the personal information that is collected, used (processed) and shared. However, while sharing a common goal of protecting an individual's personal information, the GDPR and US-based Gramm-Leach-Bliley Act[7] (GLBA) differ in approach.

- GLBA, enacted in the US in 1999, indicates that privacy requirements are dependent upon the extent of a financial institution's **continuing relationship with the "consumer"** (i.e., a one-time transaction between financial institution and the consumer would not apply as a continuing relationship). Consumers must also be notified if their information will be distributed to a third party, and in certain circumstances, be presented with an opportunity to opt out of information sharing.
- The GDPR expands what constitutes personal data and mandates that **all institutions maintain the EU resident's right to privacy irrespective of the current relationship** (i.e., heightened security standards apply even after the EU resident cancels their accounts).

These fundamental differences in approach, along with the specific technical requirements outlined in the GDPR, mean that organizations cannot rely on GLBA compliance as an indicator of GDPR compliance. Indeed, firms have to appreciate that GLBA relates mainly to the *sharing* of information, whereas the GDPR relates to the *processing* (collection, use, storage, sharing, retention, etc.) of information. As such, a separate and thorough GDPR assessment is necessary.

[7] Gramm-Leach-Bliley Act, An Act to enhance competition in the financial services industry by providing a prudential framework for the affiliation of banks, securities firms, and other financial service providers, and for other purposes, enacted by 106th United States Congress, effective 12 November 1999.

What are some common misconceptions around the GDPR?

There has been a relatively slow response by many non-EU financial services firms to addressing the GDPR. It is difficult to determine what accounts for this general lack of action. It could be that some firms have, incorrectly, viewed the GDPR to be a continuation of existing EU data protection requirements, so no real change is required. Some firms may have seen a May 2018 implementation date and determined there is ample time to act. Some firms – perhaps many – may feel the rule doesn't apply to them, given it's an EU regulation. Some may have assumed their European teams have this in hand – after all, it's an EU regulation

Whatever the reason, more non-EU firms are now starting to realize that the GDPR may apply to them, and when it does, that it is very demanding. As they do, they should be careful about making some common mistakes:

- **Underestimating the level of effort:** often as a result of misunderstanding the breadth, potency and applicability of the GDPR, firms have underestimated the level of effort required to evaluate the applicability of the GDPR, and where it applies, to implement the necessary changes to become compliant. The reality is that the GDPR affects a broad swath of the firm and requires action by a large set of professionals in the businesses and many functional areas (see below). For non-EU firms, it requires a significant degree of cooperation and collaboration between the home office and operations in Europe, as well as with relevant third parties.
- **Underestimating the breadth of impact:** the GDPR may require significant changes to the way firms operate, including their data management strategy, management of customer consents, management and oversight of third parties, the approach to product development, marketing, applications, notifications and other disclosures, potentially firms' business models, the transportation of data across borders, outsourcing contracts and much more. These impacts are likely material and will take time to fully identify, consider and address.
- **Thinking it's easy to identify EU residents:** in practice, it is hard for firms to identify who within their customer base is an EU resident. To the extent that firms have gathered full residentship data, it is easier. Identifying European mailing addresses as primary residences will also help (including non-EU residents living in the EU, as it applies to them, too). Identifying the number of EU residents within the customer base will be a major determinant of the extent to which the GDPR applies and how much of its impact can be quarantined to specific business, geographies and data sets.
- **Viewing the GDPR as only relevant to retail businesses:** given that the requirements center on EU residents' data, some firms may think incorrectly that it only relates to retail businesses. However, some corporate clients – for example, small and medium-sized businesses – often use personally identifiable information, such as personal addresses and tax or national security numbers, as part of their customer data or during the client acceptance process. To the extent they do, that could mean the GDPR applies to businesses serving those clients, as well, depending on whether the firm trips GDPR compliance, as noted above.
- **Viewing it as a one-and-done exercise:** perhaps the most significant challenge is redesigning a firm's privacy and business processes to be able to demonstrate GDPR compliance on an ongoing basis, especially as the business, client base and product portfolio evolve, and to periodically reassess whether GDRP applies to the firm. Getting to a position of GDPR-compliance is the end of the beginning. Compliance is an ongoing responsibility and, if anything, it will be the inability to execute on GDPR commitments (e.g., enabling customer data portability or maintaining customer consents to use the data as required) on an ongoing basis that will put a firm at the most risk of regulatory penalties and/or customer class action suits. Building in sustainable approaches that provide the firm with the necessary flexibility to redesign how it develops and delivers products and services to its customers is most critical.

Which parts of your organization will be most affected?

The GDPR will have a significant impact across a firm's three lines of defense:

First line (business lines and technology)

- **Business lines:** like other risks, the front-line businesses have to own the risks they create, including privacy and data protection. They have to identify, measure, monitor and mitigate the risks associated with the GDPR, implement the privacy principles, and design and maintain necessary and effective controls. They also have to implement enterprise-wide risk management frameworks developed by the second line, including in this context privacy risk, information technology risk, operational risk and overall enterprise risk management.
- **Operations:** those running day-to-day operations have to develop and implement the necessary standards and procedures that secure personal data through the data life cycle and conduct DPIAs to properly understand and manage the inherent risks. They also tend to be the vendor relationship owners, so they have to manage relevant third parties so that they remain in line with the firm's privacy and GDPR requirements and obligations.
- **Technology, security and data:** the technology group will have to consider what changes are required to the technology and data architecture to enable the proper handling, processing and security of relevant customer and employee data. This will include how the data is gathered (and through what channel), processed, stored, transferred (including cross-border and to other firms) and, when necessary, destroyed. Tracking what data is affected will be a significant effort, especially as it relates to customer and account book-of-record, employee or contractor data (e.g., time and reporting systems)[5], personal data used in customer relationship and marketing databases, and so on. The data management strategy that firms may need to adopt to effectively execute against GDPR requirements – in terms of tagging (including geotagging), tracking, anonymizing, encrypting, quarantining and making destroyable (in actuality or in effect) – could be onerous, depending on how the firm determines it will address GDPR compliance. Those driving data analytics activities have consider how they may be affected.
- **Customer relationship management (CRM):** firms will need to re-evaluate their CRM strategy and data management to determine if more client segmentation is required, from a perspective of quarantining EU residents' data and in terms of how customer data is used to target products and services.
- **Innovation and marketing:** product development activities may need to be evaluated to determine how GDPR considerations are built into the new products and services, as well as how customer-facing design activities – such as customer surveys and focus groups – may need to be adapted. Marketing materials will need to be revised to include the necessary disclosures, consents and notifications. Consent is one of the largest areas of challenge, especially around the need to consider whether you can 'grandfather' existing consent or whether you need to run a 'retrospective re-consent' exercise.
- **Procurement and contract management:** procurement and legal teams may need to evaluate existing standard contractual template terms to understand whether amendments are required to meet the GDPR requirements - for example around the 72-hour breach notification and increased obligations on data processors. Organizations will need to identify which vendors are processing personal data and a perform a risk-based prioritization exercise to review existing contracts, identify required legal term changes, and potentially re-negotiate and 're-paper' existing contractual arrangements.
- **Human resources (HR), training and communication:** HR will need to consider if changes are required in regard to how employee or contractor data is segmented and managed, how HR data is reported upon and appropriate

employee rights and consents are managed and adhered to. Working with the relevant functions and businesses, HR will need to re-evaluate the portfolio of awareness-raising, training and education activities and how those activities remain current and effective.

First/second line of defense

- **Third party risk management (TPRM):** given the way in which the GDPR applies to third parties, the second-line TPRM group will need to re-evaluate their third party risk management framework and how the first line is adapting their standards and procedures to align with the GDPR.
- **Surveillance and monitoring:** as noted above, to the extent firms have centralized some of their surveillance activities and in so doing are monitoring activity and behaviors of EU residents, those functions may create GDPR obligations that apply to some or all of the data, depending on how it is processed and stored. The same is true of website traffic and user monitoring activities. Assessing if and how EU resident data is used in these activities will be important to determine applicability, but may also drive firms to segment those activities more than at present to isolate the degree to which those functions are impacted by the GDPR.

  Consideration should be given to the monitoring activities conducted by the second (and sometimes first) line, including anti-money laundering, sanction and fraud surveillance – or broader testing activities – so that those activities are GDPR-compliant, where relevant.

Second line of defense

- **Compliance, privacy and security:** the DPO has a critical role in this regard, working with other functional teams. The compliance function will have to validate that the privacy and data security strategy aligns with legal requirements, annual regulatory reporting requirements and broader compliance reporting and surveillance strategies. Compliance will need to develop a robust monitoring and testing program for GDPR, which can be leveraged by the DPO, among others.

  The privacy groups will need to review and revise data policies, as well as confirm that front-line standards and procedures are in line with those revisions and assess they are implemented effectively (either through reviewing first-line testing or conducting its own). Privacy notices will need updating, along with exemptions, exclusions and disclaimers and personal data definitions. Data breach processes will need evaluating so that the firm can meet its GDPR 72-hour notification requirements, including where breaches occur within third parties. The privacy group will need to confirm that data subject rights and data security standards are adhered to, in light of more demanding GDPR requirements. Privacy and data governance structures and roles and responsibilities will need re-evaluating, including the assignment of data protection officers and their working relationship with chief privacy officers.
- **Risk management:** ultimately, second-line risk, working with the compliance and privacy functions, needs to measure and monitor overall privacy and information-security – working with the DPO, who is directly responsible for monitoring – and set tolerances for such risks within a firm's risk appetite framework. This is particularly important for the GDPR given the potential for material fines and class action legal settlements. Firms will need to re-evaluate privacy-risk reporting in this context.

Third line: internal audit

Internal audit will need to adopt its approach to consider the GDPR within a number of audits, notably:

- Compliance monitoring programs
- Reviews of access processes and procedures
- Overall privacy framework validation

In re-evaluating its coverage model, internal auditors should monitor a distinct set of privacy and compliance key performance indicators, as well as potentially some that are specific to the GDPR. Some firms' internal audit groups may perform pre-implementation advisory audits, given the breadth of the requirements and the potential size of fines and settlements, or build assessments on the implementation of privacy by design principles into other relevant audits they perform.

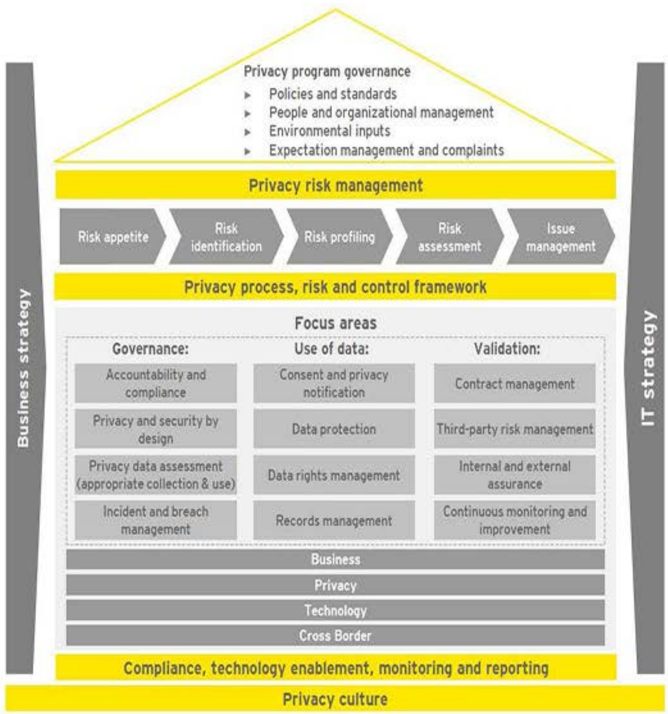
How should you implement the GDPR?

Implementing the GDPR should be viewed as an integrated exercise set within each firm's overall privacy risk management framework. GDPR touches on all aspects of an organization, reaching across people, processes and technology and, as such, establishes a cross-functional team that supports the transformation of the company, which is a critical step for a successful implementation.

EY has developed our own proprietary framework (see figure 2),which links risk management, compliance, privacy and governance with key privacy domains and allows our teams to put privacy in the context of each firm's business and information technology strategy. The framework allows firms to set the privacy strategy within the context of the firm's overall business and IT strategy, and focus on:

- **Program effectiveness:** there has to be an enterprise view of the firm's privacy program, which allows for firm-wide oversight of the program, program-level reporting and escalation, and the application of consistent policy and standards.
- **Privacy risk management:** privacy risk needs to be well managed, in a way that is consistent with the firm's overall risk management strategy, covering the risk life cycle, from risk appetite to risk identification to risk assessment to issues management. The overall privacy framework should link to the firm-wide process and risk and control framework, as well as the third-party risk management program. The various roles and responsibilities across the different lines of defense and functions (compliance, legal, privacy, cyber, etc.) should be clearly defined.
- **Compliance and monitoring:** compliance with relevant rules and regulations should be hardwired into the framework, with robust, ongoing program, compliance and privacy risk reporting to senior management and the board.
- **Data and breach management:** the firm's privacy risk strategy has to be firmly linked to the strategy for managing data, including collecting, processing, storing and destroying data. The data architecture, classification and flows have to enable the firm to conform with its privacy strategy, meet compliance requirements and support customer rights, and meet ever-more challenging incident breach and notification requirements.
- **People and culture:** the talent requirements to properly implement the privacy framework need to be spelled out, and plans need to be in place to confirm the needs are met. This includes the front-line-business talent requirements. After all, those on the front line manage privacy risk on a day-to-day basis. Privacy also needs to be firmly embedded in the firm's culture, with active, ongoing awareness programs and training.

Figure 2: EY's privacy risk management framework



To support business stakeholder understanding of privacy, and the impact of the GDPR on business lines and functions, EY applied its privacy framework to the GDPR and categorized 12 focus areas into 3 themes, as shown in Table 1.

Table 1: GDPR requirements across the EY privacy risk management framework

	Focus area	Desired outcome
Governance	**Accountability and compliance:** privacy operating model, training/awareness, policy development	Creating structures and processes that enable proactive, systematic and ongoing compliance reporting for senior management
	Privacy and security by design: privacy impact assessment, program design based on business model	Achieving risk reduction and management through the application of requirements and tools integrated at various junctures in your process landscape
	Incident and breach management: data incident response plan, 72-hour operational effectiveness process	Enabling rapid management of a data breach, including internal investigations and external reporting
	Privacy data assessment: data use case management/framework, data classification, data flow mapping, data discovery, cloud discovery, high-value asset identification	Establishing and operationalizing governance over personal data usage and analytics as well as understanding the most meaningful attributes of your data that impact compliance risk and optimized use
Use of data	**Consent and privacy notification:** freely given and explicit consent, right to withdraw consent, privacy notices	Increasing transparency through explicit consent to process data and privacy notifications
	Data protection: identify and access management, technology selection, encryption strategy	Approach designed to achieve data protection and enhance your security hygiene
	Data rights management: data subject's right to access, correction, erasure, portability and/ or objection	Empowering your organization to support data rights to access, deletion, portability and rectification
	Records management: attach requirements to physical files, electronic documents and emails	Strategy and program design that balances global privacy regulation with data protection, legal and business needs
Validation	**Contract management:** assessment of service-level agreements, assess internal or third-party contracts to identify gaps or identify opportunities to strengthen language	Discovery and revision of contractual provisions pertaining to privacy and security, including data permissions and restrictions
	Third-party risk management: third-party risk assessment, compliance monitoring and data controls	Understanding, designing and monitoring for the management of your third-party personal data access, protection, responsibilities and liabilities
	Internal and external assurance: internal audit assessment, third-party attestation, certification against industry standard	Providing independent confirmation that governance, risk management and internal controls as they relate to both privacy and security are designed and operating effectively
	Continuous monitoring and improvement: compliance monitoring program design, monitoring of key controls, dashboard reporting for management	Designing for ongoing awareness of privacy and security compliance to facilitate risk management and optimization of the control environment

The clock is ticking: act quickly

In enacting the GDPR, the EU gave companies two years to get ready to comply. When enacted, this was viewed as providing sufficient time.

Now, with limited time remaining, many non-EU financial services firms still have a long way to go to validate if the regulation applies to them and, if so, to make all of the necessary changes to be ready for the May 25, 2018, implementation date. Building an approach that is sustainable beyond that date is even more challenging.

Time is of the essence. Non-EU financial services firms need to act quickly.

The first step is assessing applicability; here, a risk-based (not just legalistic) assessment is strongly suggested.

For firms impacted by the GDPR, it is important that the right governance and program structure is put in place from the outset. A cross-functional, cross-business team is required. To be successful and sustainable, this effort cannot be buried in legal and compliance.

A thorough GDPR gap assessment is needed, one that reaches across the swath of affected businesses and functions. To the extent that the assessment is too narrow, it will make timely implementation much harder. Important factors will be identified too late, causing decisions made to degrade the quality of the approach, leave the firm open to regulatory scrutiny and ultimately cost more as work needs to be redone to make the approach sustainable on an ongoing basis.

And, finally, there is a need to prioritize. After all, the timeline to implementation is getting shorter, so firms need to prioritize those activities that get to baseline compliance. Building more sustainable processes can be completed after May 25, as necessary.

It is time to act.

EY contacts

Americas

Cindy Doe
+1 617 375 4558
cynthia.doe@ey.com

John Doherty
+1 212 773 2734
john.doherty@ey.com

Ed Keck
+1 216 583 1296
ed.keck@ey.com

Angela Saverice-Rohan
+1 213 977 3153
angela.savericerohan@ey.com

Mark Watson
+1 617 305 2217
mark.watson@ey.com

EMEIA

Tony de Bos
+31 88 40 72079
tony.de.bos@nl.ey.com

Steve Holt
+44 20 7951 7874
sholt2@uk.ey.com

Asia-Pacific

Jeremy Pizzala
+852 9666 3428
jeremy.pizzala@hk.ey.com

For more cyber and privacy insights, visit ey.com/fsGDPR **or** ey.com/fscyber

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EY is a leader in serving the global financial services marketplace
Nearly 51,000 EY financial services professionals around the world provide integrated assurance, tax, transaction and advisory services to our asset management, banking, capital markets and insurance clients. In the Americas, EY is the only public accounting organization with a separate business unit dedicated to the financial services marketplace. Created in 2000, the Americas Financial Services Organization today includes more than 11,000 professionals at member firms in over 50 locations throughout the US, the Caribbean and Latin America.

EY professionals in our financial services practices worldwide align with key global industry groups, including EY's Global Wealth & Asset Management Center, Global Banking & Capital Markets Center, Global Insurance Center and Global Private Equity Center, which act as hubs for sharing industry-focused knowledge on current and emerging trends and regulations in order to help our clients address key issues. Our practitioners span many disciplines and provide a well-rounded understanding of business issues and challenges, as well as integrated services to our clients.

With a global presence and industry-focused advice, EY's financial services professionals provide high-quality assurance, tax, transaction and advisory services, including operations, process improvement, risk and technology, to financial services companies worldwide.

EYG no. 05767-171Gbl
1709-2407447 BDFSO
ED None

ey.com

RESPONSES TO WRITTEN QUESTIONS OF THE SENATE BANKING COMMITTEE FROM BILL NELSON

Q.1. Mr. Nelson, in your written testimony you requested greater clarity on legal protections for financial institutions that want to share information in accordance with the Patriot Act. What clarity would you like to see?

A.1. Under section 314(b) of the USA Patriot Act, financial institutions may share information when there is suspicion of money laundering and terrorist activity. This authority provides financial institutions with an opportunity to reduce money laundering and terrorism financing. However, doing so necessarily involves sharing personally identifiable information, such as names and account information.

In the absence of specific legal guidance regarding the manner in which such information may be shared, banking attorneys have limited sharing to those instances in which money laundering or terrorist activity can be confirmed. It would be preferable to share such information earlier in the process, but liability concerns preclude it.

For example, in the case of suspected money mule activity associated with business email compromise, banks have questioned FinCEN if payment information can be shared between approved financial institutions and an approved association of financial institutions under the safe harbor of section 314(b). FinCEN has responded verbally that this information can be shared and encouraged the sharing to provide more complete information in SAR filing. FinCEN has not provided written guidance to this question. Sharing the information in this example by a large network of FinCEN-approved financial institutions would reduce risk to the financial institutions and their customers. Federal law enforcement would benefit from more complete SAR filing information that will lead to more effective investigations and prosecution of cyber criminals.

Q.2.–Q.3. A year and a half ago, William and Margaret Frederick sold their home in Ohio so they could buy a home in Las Vegas, Nevada. The couple expected to make a $216,000 profit on the sale. But, their real estate agent read a hacked email supposedly from William—the fake email had three L's in Bill instead of two—and sent the profit to the hacker. William was 83 and Margaret 77. Someone stole the money they intended to live on in retirement. Real estate transaction fraud is a problem in Nevada and nationwide. Thieves wait for the right time to impersonate a bank or realtor and send you different wire transaction instructions. Estimates are as much as $400 million a year in losses. What more can financial institutions do to prevent thieves from stealing people's down payments, earnest money and even the entire home payment if someone is buying a home for cash? Please identify the best practices for realtors, title agents and mortgage brokers? One way to protect consumer's information is to not collect it. For example, why should merchants of any sort, including doctors, insurance companies and utilities, require social security numbers as part of their information or data-set on their customers? Should we limit Social Security numbers provided to merchants?

A.2.–A.3. In this example, it appears that criminals, using money mules to launder the funds, stole the money. When banks discover this type of potentially criminal activity they are required to file Suspicious Activity Reports (SAR) with FinCEN. While banks want to share this suspicious activity within a network of FinCEN-approved financial institutions under the protections of section 314(b) of the USA Patriot, some banks are reluctant to share this suspicious activity because FinCEN has not provided written guidance. If banks had network intelligence about active money mule accounts in the Nevada case, the money transfer to the criminals may have been delayed and investigated by the bank staff. A bank investigation could then lead to the money transfer being stopped.

Closing attorneys, mortgage brokers and title companies should be encouraged to join an ISAC for their industry. Given that criminals change tactics regularly, it's helpful for communities to share information about these tactics and effective risk mitigation measures. This "strength in sharing" approach goes a long way in protecting the companies and their customers. In addition, collaboration with law enforcement agencies are also effective in educating the community and sharing tips. For example, the FBI's Internet Crime Complaint Center (IC3) has published numerous publications, including this one in May 2017 on tactics for defending against business email compromise (BEC): *https://www.ic3.gov/media/2017/170504.aspx.* The recommendations below come from the IC3 report referenced in the link.

Businesses with an increased awareness and understanding of the Business Email Compromise (BEC) scams are more likely to recognize when they have been targeted by BEC fraudsters. Therefore, they are more likely to avoid falling victim and sending fraudulent payments. Businesses that deploy robust internal prevention techniques at all levels (especially for front line employees who may be the recipients of initial phishing attempts) have proven highly successful in recognizing and deflecting BEC attempts. Some financial institutions reported holding their customer requests for international wire transfers for an additional period of time to verify the legitimacy of the request.

The following list includes self-protection strategies:

- Avoid free web-based email accounts: Establish a company domain name and use it to establish company email accounts in lieu of free, web-based accounts.
- Be careful what you post to social media and company websites, especially job duties and descriptions, hierarchal information, and out-of-office details.
- Be suspicious of requests for secrecy or pressure to take action quickly.

- Consider additional IT and financial security procedures, including the implementation of a two-step verification process. For example:
  - Out-of-Band Communication: Establish other communication channels, such as telephone calls, to verify significant transactions. Arrange this two-factor authentication early in the relationship and outside the email environment to avoid interception by a hacker.
  - Digital Signatures: Entities on each side of a transaction should utilize digital signatures. This will not work with web-based email accounts. Additionally, some countries ban or limit the use of encryption.
- Immediately report and delete unsolicited email (spam) from unknown parties. DO NOT open spam email, click on links in the email, or open attachments. These often contain malware that will give subjects access to your computer system.
- Do not use the "Reply" option to respond to any business emails. Instead, use the "Forward" option and either type in the correct email address or select it from the email address book to ensure the intended recipient's correct email address is used.
- Beware of sudden changes in business practices. For example, if a current business contact suddenly asks to be contacted via their personal email address when all previous official correspondence has been through company email, the request could be fraudulent. Always verify via other channels that you are still communicating with your legitimate business partner.
- Create intrusion detection system rules that flag emails with extensions that are similar to company email. For example, a detection system for legitimate email of abc_*company.com would flag fraudulent email from abc-company.com.*
- Register all company domains that are slightly different than the actual company domain.
- Verify changes in vendor payment location by adding additional two-factor authentication, such as having a secondary sign-off by company personnel.
- Confirm requests for transfers of funds. When using phone verification as part of two-factor authentication, use previously known numbers, not the numbers provided in the email request.
- Know the habits of your customers, including the details of, reasons behind, and amount of payments.
- Carefully scrutinize all email requests for transfers of funds to determine if the requests are out of the ordinary.

Q.4. What other sorts of information should financial institutions or others STOP collecting?

A.4. Financial institutions collect information to identify individuals, assess credit worthiness and maintain security. This detailed collection of personal information is required by law and regulation. This personal information is required to be protected by the Gramm-Leach-Bliley Act of 1999 (GLBA) and the regulations issued by numerous financial regulatory agencies. Financial institutions are examined by bank regulators to determine if the information collected is adequate and appropriate. Regulatory examiners also review the security of this personal information in compliance with GLBA. Bank regulators may be more knowledgeable in answering the question, what information should banks stop collecting?"

Q.5. What are the pros and cons of a Federal data breach law?

A.5. I fully support handling data breaches in a manner that safeguards customer data, addresses breaches expeditiously, and properly involves law enforcement so as to bring bad actors to justice. One means of achieving this would be to create a Federal data breach law that would eliminate the possibility of a plethora of regulatory and/or State laws on the subject, some of which would prove inconsistent and contradictory in part. The current development of cybersecurity law is hindered by such problems, leading the financial sector to pursue efforts to harmonize such Federal and State laws.

One concern with a Federal approach is its possible effect on smaller organizations, such as community banks and credit unions. A Federal law should not be tailored to the largest, global institutions, but should be flexible enough to apply to smaller entities without burdening them.

Q.6. How should Federal data breach laws coexist with other international laws?

A.6. Whether regulatory, State, Federal, or foreign, cybersecurity rules generally, and data breach laws specifically, should be reasonable, consistent, and harmonized. Firms will increasingly be subjected to the laws of many nations in the growing global economy. We must do our best in this environment to facilitate the flow of commerce, while also protecting consumer data and responding appropriately and effectively to any breach of that data. In this situation, NIST may be able to play an important role.

Q.7. Firms that fail to secure their data pay substantial penalties. Hundreds of hackers go to prison. The woman [Paytsar Bkhchadzhyan] who hacked into Paris Hilton's accounts and stole her credit card information received a 5-year prison term. Taylor Huddleston (26) of Arkansas was sentenced to serve nearly 3 years for building and selling a remote access Trojan (NanoCore) to hackers. Can you give me some examples of fines, penalties and sentences for firms and individuals that engaged in cyber theft? Are these costs an appropriate deterrent?

A.7. Aleksandr Andreevich Panin and Hamza Bendelladj were sentenced to a combined 24 years and 6 months in prison for their roles in developing and distributing the SpyEye banking trojan, a powerful botnet similar to the ZeuS malware. Both hackers were charged with stealing hundreds of millions of dollars from banking institutions worldwide. The Department of Justice characterized SpyEye as a "preeminent malware banking Trojan," which was used to infect over 50 million computers worldwide from 2010 to 2012, causing nearly $1 billion in financial losses to individuals and financial institutions globally.

I support the sentences handed down in this case, which were justified and tailored to deter other hackers. However, the allure of stealing hundreds of millions of dollars while ensconced in safe havens from which arrest and conviction are unlikely render lengthy sentences, as well as fines, insufficient deterrents. The relative ease and low cost of cyber crime is unlikely to abate without greater cooperation among international law enforcement agencies. Moreover, where nation states are involved, the Federal Government should play a greater role in deterrence and enforcement.

Q.8.–Q.10. Seventy-seven percent of cyber attacks come from the outside. Yet sometimes, figuring out who the hackers were is hard to figure out. Hackers can spoof evidence. They can embed other hackers' tools. How big of a problem is figuring out attribution for hacks? Are there ways we can enhance information sharing between industry and the Federal Government to enable more rapid detection and response to cyber attacks? What tools or resources would make it easier for financial institutions to correctly attribute cyber-attacks?

A.8.–A.10. Obfuscation techniques adopted by threat actors can inhibit timely and accurate attribution. Many cyber defenders can be more interested in learning threat actor tactics, techniques, and procedures which will help to detect anomalous activity than the threat actor origin. Attribution for the private sector can be most helpful, however, in identifying adversary intent. Armed with knowledge of intent, the financial sector can put additional monitors on systems. Furthermore, while the private sector is reliant on many sources of information, Government is uniquely situated to assess intent with the greatest credibility based on its intelligence sources and methods. Perhaps the most valuable way to alert the private sector about threat actor attribution and intent is through timely declassification of intelligence, or to provide requisite clearances and classified exchanges for industry professionals who can make security decisions within their organizations. Likewise, timely information on changes in known adversary methods and tools is also helpful in correctly attributing activity. Many financial institutions do not have the resources to independently attribute cyber activity and are reliant on timely Government releases or attribution provided by vendors.

Q.11. In 2015, French-language TV station, TV5Monde was subjected to a significant cyber-attack which disrupted its broadcast for several hours by Fancy Bear. These are the same Russian government and military hackers that hacked the Democratic National Committee. Multiple television channels went dark. Social media channels run by the broadcasters began to spew ISIS propaganda. The attack was the work of Russian hackers which pretended to be ISIS. Russian government hackers also attacked the World Anti-Doping Agency, the power grid in Ukraine and the French electorate with another document dump. How significant is the threat to private businesses—from hostile foreign governments or terrorist organizations?

A.11. Nation-state-sponsored activity is a top concern of financial firms. While the majority of the financial sector most commonly sees criminal activity, the risk of impact posed by nation-state actors is much greater. Furthermore, cyber criminals typically seek to steal funds, but have a vested interest in keeping the financial infrastructure intact. Nation states could have more nefarious intentions to disrupt the functions of the financial system in an effort to impact the U.S. economy. Businesses are reliant on the integrity of third parties and other critical infrastructure dependencies—such as electricity, communications, water, *etc.*—in order to keep their businesses running. Nation-states have seemingly been the most interested threat actors in disrupting or destroying these functions, evidenced in part by NotPetya, WannaCry, and Shamoon attacks.

Q.12. Some of the lessons from that attack was documenting IT processes, restricting access to IT processes, and keeping communications separate from incident responses. What should businesses do now to prepare for a possible attack in the future?

A.12. Thoughtful and exercised incident response plans are encouraged for all financial institutions. The plans should involve multiple offices within the organization including security, legal, communications, business resilience and executive leadership. Incident response plans can aid in more accurate and prompt information sharing, as well.

Businesses should also focus on the security of their third-party suppliers and remain in an active dialogue about their security practices. The prevalence of third-party risks, such as digital supply chain attacks, has increased as attack surface expands through use of the cloud and online services. Such attacks can affect institutions of all kinds, even those with robust cybersecurity measures in place. As evidence, NotPetya was initially distributed via a compromised accounting software update from the provider's server and, separately, malicious actors leveraged compromised credentials and malware to corrupt another software provider's updates to distribute malicious data-stealing code. Further, a USG Technical Alert released this year shed light on ongoing campaigns affecting critical infrastructure sectors which compromised staging targets, such as third-party suppliers, with less secure networks to reach intended victims.

RESPONSE TO WRITTEN QUESTION OF SENATOR JACK REED FROM MICHAEL DANIEL

Q.1. In your written testimony, you stated that:

> the Government can facilitate disclosure of information that can help customers, clients, shareholders, and other relevant parties take appropriate defensive actions, better assess risk, and advocate for improved security. Examples of such requirements could include data breach reporting, information about material cybersecurity risks on financial statements, and public acknowledgements about how a publicly traded company is assessing and managing its cyber risk, particularly at the board of director's level. Such disclosures do not assist criminals or other bad actors—they already know where the weaknesses are; instead these requirements allow market forces to operate more efficiently.

Could you please go into greater detail about how cybersecurity disclosure would allow market forces to operate more efficiently?

A.1. Right now, consumers often lack information about a product or service's cybersecurity. As a result, they cannot factor that information into a purchasing decision. Just as with disclosing calorie counts in food products, if consumers had more access to information they could use that information to make better choices. And if some consumers began to discriminate among products or services based in part on their cybersecurity, then producers and suppliers would have an incentive to create more secure outputs.

RESPONSE TO WRITTEN QUESTION OF SENATOR MARK WARNER FROM MICHAEL DANIEL

Q.1. Is verifying that financial institutions have an internal cybersecurity audit function or an independent third-party assessment sufficient, or should financial regulators develop their own view of the cybersecurity posture of supervised entities in addition to requiring independent third-party assessment?

Are you and others in the industry seeing an uptick in interest from regulators in cyber risk? What issues do regulators focus on in their examinations?

What do you believe is the appropriate role of the financial regulators in assessing the cybersecurity of institutions they regulate?

A.1. I believe that regulators should largely rely on third-party assessments, rather than trying to develop the capability in-house to conduct reviews at the scale required for our financial sector. That said, financial regulators should have staff capable of interpreting those assessments and determining whether the assessment demonstrates that the institution is meeting its requirements.

I cannot speak to what financial regulators focus on in their examinations but I can suggest the Committee explore the oversight and examination material of the financial regulatory agencies and bodies such as the Federal Financial Institutions Examination Council.

The key issue is whether the institution is appropriately considering systemic risk as well as the immediate risk to the company in managing its cybersecurity. Institutions have an incentive to ensure that they can conduct business, maintain customers, and preserve their reputation. However, the incentives are not strong enough on their own for the institution to invest in cybersecurity that in turn helps drive down risk across the sector (and therefore to the broader economy) as a whole. That's where—systemic risk to the broader sector and economy—the Government regulators should focus.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR CORTEZ MASTO FROM MICHAEL DANIEL

A year and a half ago, William and Margaret Frederick sold their home in Ohio so they could buy a home in Las Vegas, Nevada. The couple expected to make a $216,000 profit on the sale. But, their real estate agent read a hacked email supposedly from William—the fake email had three L's in Bill instead of two—and sent the profit to the hacker. William was 83 and Margaret 77. Someone stole the money they intended to live on in retirement.

Real estate transaction fraud is a problem in Nevada and nationwide. Thieves wait for the right time to impersonate a bank or realtor and send you different wire transaction instructions. Estimates are as much as $400 million a year in losses.

Q.1. What more can financial institutions do to prevent thieves from stealing people's down payments, earnest money and even the entire home payment if someone is buying a home for cash? Please identify the best practices for realtors, title agents and mortgage brokers?

A.1. Although the Internet often makes fraud easier to perpetrate, the best practices to combat cyber-enabled fraud are often the same in other domains. I would point to references like the Federal Trade Commission, the Financial Crimes Enforcement Network, the Federal Bureau of Investigation—Financial Institution Fraud division, the Financial Services Information Sharing and Analysis Center, and similar organizations that lay out best practices to combat fraud.

One way to protect consumer's information is to not collect it. For example, why should merchants of any sort, including doctors, insurance companies and utilities, require social security numbers as part of their information or data-set on their customers? Should we limit Social Security numbers provided to merchants?

- What other sorts of information should financial institutions or others STOP collecting?
- State and International Laws Relating to Cybersecurity
- What are the pros and cons of a Federal data breach law?
- How should Federal data breach laws coexist with other international laws?

A.2. The first step in managing cyber risk more effectively is understanding your information environment: what information does your organization hold and why is it holding it? An organization should only hold and manage information for which there is a legitimate business purpose, and it should only hold that information for as long as needed for the business purpose (or according to law, if the organization has legal obligations for data retention). Thinking through these questions will enable an organization to determine what information it really needs to collect and store, and then how long it needs to retain that information.

In terms of digital identity and how best to conduct identity proofing without relying on social security numbers, I would recommend that the Committee look at research being done related to digital verification processes in cyberspace. Some examples of this work and related suggestions can be found at the National Strategy for Trusted Identities in Cyberspace (NSTIC) and the Better Identity Center here in Washington, DC.

Q.3. Firms that fail to secure their data pay substantial penalties. Hundreds of hackers go to prison. The woman [Paytsar Bkhchadzhyan] who hacked into Paris Hilton's accounts and stole her credit card information received a 5-year prison term. Taylor Huddleston (26) of Arkansas was sentenced to serve nearly 3 years for building and selling a remote access Trojan (NanoCore) to hackers.

Can you give me some examples of fines, penalties and sentences for firms and individuals that engaged in cyber theft? Are these costs an appropriate deterrent?

A.3. This specific question falls outside my area of expertise. However, measuring deterrence is always challenging, whether in the physical world or in cyberspace.

Q.4.a. Seventy-seven percent of cyber attacks come from the outside. Yet sometimes, figuring out who the hackers were is hard to figure out. Hackers can spoof evidence. They can embed other hackers' tools.

How big of a problem is figuring out attribution for hacks? Are there ways we can enhance information sharing between industry and the Federal Government to enable more rapid detection and response to cyber attacks?

A.4.a. Attribution remains a challenging endeavor for multiple reasons. First, attribution involves combining technical capabilities, data from a number of victims, and considerable time. While the U.S. Government and cybersecurity companies have improved their attribution capabilities significantly, even these organizations have to invest considerable resources into this work. Second, even if cybersecurity companies can attribute malicious activity to a particular group or adversary, taking the next step of tying that attribution to an individual in the real world is even harder.

Q.4.b. What tools or resources would make it easier for financial institutions to correctly attribute cyber-attacks?

A.4.b. We can definitely improve information sharing between the Federal Government and the private sector. In particular, we need to build the technical mechanisms, the business processes, and the legal understandings to enable this exchange to occur at both machine speed and at human speed.

Financial institutions may not be able to attribute most malicious activity on their own and it may not be in their best interest to do so. However, they can provide forensic and other data that can help organizations, such as threat researchers and Government agencies that can make the attribution.

Q.5. In 2015, French-language TV station, TV5Monde was subjected to a significant cyber-attack which disrupted its broadcast for several hours by Fancy Bear. These are the same Russian government and military hackers that hacked the Democratic National Committee. Multiple television channels went dark. Social media channels run by the broadcasters began to spew ISIS propaganda. The attack was the work of Russian hackers which pretended to be ISIS. Russian government hackers also attacked the World Anti-Doping Agency, the power grid in Ukraine and the French electorate with another document dump.

How significant is the threat to private businesses—from hostile foreign governments or terrorist organizations?

A.5. Criminal actors conduct the overwhelming majority of malicious activity online and, as a result, are the primary cybersecurity threat to most businesses.

However, the threat from nation-state actors is very real and organizations should take it seriously. Fortunately, the best practices that work against criminal organizations can also impede nation-state actors. Therefore, companies should focus on implementing cybersecurity best practices, regardless of the adversaries they face.

The threat from most terrorist organizations remains fairly nascent. Terrorist groups are effective at using the Internet as a recruiting platform, but their ability to use it to carry out operations remains limited. Some groups attempt to hack into companies to expose private information, but few have the capability to do more than that right now. However, given terrorists' high motivation to cause damage, if a nation-state decided to supply a terrorist organization with malware or other tools, that group's capability to cause harm could grow rapidly.

Q.6. Some of the lessons from that attack was documenting IT processes, restricting access to IT processes, and keeping communications separate from incident responses.

What should businesses do now to prepare for a possible attack in the future?

A.6. All organizations should adopt a holistic risk management approach and that should include managing their cyber risk. Best practices for managing cyber risk have been promulgated in the Cybersecurity Framework published by the National Institute of Standards and Technology and in collaboration with the private sector and other Government agencies. Such an approach can guide an organization to understand its information assets and business processes; invest in more effective protections; have a capability to detect when malicious activity is occurring; develop an incident response plan for when bad events occur; and create a plan for restoring business operations as soon as possible. Adopting a holistic approach is the most effective way a company can prepare for malicious cyber activity.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARNER FROM PHIL VENABLES

Q.1. How do banks—much less regulators—evaluate and manage risk of IT environments that combine not only third-party software and products, but also decades-old legacy IT?

A.1. Third-party software and hardware risk is an ongoing challenge requiring institutions to have clear policies and practices to manage the risk of third-party products in the environment. In more sophisticated organizations a risk assessment, code analysis and operational penetration testing may be conducted to ensure any critical and externally facing applications and platforms are appropriately hardened.

Legacy IT infrastructure risk is a challenge facing many medium-to-large organizations. Most financial institutions have been required by Federal regulators to conduct an appropriate risk analysis of their IT environment to identify that infrastructure which is not able to have software patches applied to address current vulnerabilities and threats. Sophisticated organizations prioritize protection and remediation of these legacy environments based on relative risk of the platforms and technology. Externally facing systems are generally the priority for remediation and Federal regulators will generally require evidence of an appropriate ongoing vulnerability management and vulnerability scanning program to ensure that high-risk vulnerabilities are adequately being managed.

Effectively managing third-party and legacy infrastructure risk is predicated on the organization having up-to-date inventories of hardware and software and understanding the associated risks. This can be challenging in large, global organizations and requires significant and ongoing discipline with appropriate policies and practices to ensure consistency.

Q.2. Could the kind of meltdown we're seeing in the United Kingdom with TSB Bank happen in the United States as a result of an IT migration?

A.2. Public reporting on the TSB Bank incident indicates the issue was caused by a variety of failures in the organization's testing, change management, migration, communications and regulatory engagement processes.

The migration of such a large volume of customers (5.2 million) in one activity is a significant risk. There is no public information available as to what testing took place behind the scenes prior to the upgrade and what processes failed in the transition so our ability to assess what went wrong in the migration is extremely limited. Media reporting also indicates TSB, and parent company Banco Sabadell, declined assistance from Lloyd's early in the migration crisis.

Sound change management policies and practices, exercised and comprehensively tested using a phased migration approach are clear recommendations for any complex or significant migration or upgrade. For significant changes and migrations it is recommended to have a prepositioned communications plan supporting clear and transparent customer and regulatory notification should issues be encountered.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR CORTEZ MASTO FROM PHIL VENABLES

Q.1. What more can financial institutions do to prevent thieves from stealing people's down payments, earnest money and even the entire home payment if someone is buying a home for cash? Please identify the best practices for realtors, title agents and mortgage brokers?

A.1. Fannie Mae and Freddie Mac provide comprehensive resources including fraud mitigation best practices to provide guidance for all entities in the mortgage transaction flow.

https://www.fanniemae.com/singlefamily/mortgage-fraud-prevention

http://www.freddiemac.com/singlefamily/fraud.html

http://www.freddiemac.com/singlefamily/pdf/fraudprevention_practices.pdf

Small- to medium-sized organizations supporting mortgage services should review and follow cybersecurity best practices, such as those offered by the "Staysafeonline" website maintained by the National Cybersecurity Alliance, in order to provide appropriate protection for the personal identifying and bank account information they collect. Public reporting indicates some mortgage brokers and smaller organizations may be utilizing public email services for transacting business that if compromised could allow identity theft and fraud. Businesses should conduct a security review of their email accounts based on the provider's recommendations and implement the appropriate enhanced security offerings for these email services.

https://staysafeonline.org/cybersecure-business/

https://landing.google.com/advancedprotection/

https://help.yahoo.com/kb/SLN5013.html

Fannie Mae and Freddie Mac further offer recommendations for consumers around red flags that may be indicative of fraud during mortgage transactions. One significant indicator of attempted wire transfer fraud may be an unexpected email indicating a late change to the payee/beneficiary account information prior to an upcoming funds transfer. The safest course for consumers is to not trust any wire transfer instructions received via email and to validate all financial details via phone call to a confirmed number that was not provided in any email communications.

https://www.fanniemae.com/content/news/mortgage-fraud-news-0116.pdf

https://www.fanniemae.com/content/tool/mortgage-fraud-prevention-consumers.pdf

http://www.freddiemac.com/singlefamily/fraud.html

http://www.freddiemac.com/perspectives/robb_hagberg/20170612_combating_mortgage_fraud.html

Q.2. What other sorts of information should financial institutions or others STOP collecting?

A.2. We support the adoption of the principle of "data minimization" under which a business should collect and process only such personal information as is necessary for it to achieve the task at hand, whether that be servicing the customer, complying with its own legal or regulatory obligations, or pursuing some other legitimate purpose.

Q.3. State and International Laws Relating to Cybersecurity

A.3. To date, most States have avoided the imposition of detailed, prescriptive requirements as to the safeguarding of personal and business related information opting instead for a high level, and more flexible, approach of requiring businesses to implement and maintain "reasonable security procedures and practices" appropriate to the nature of the information processed, the type of activities conducted, the size and complexity of the organization, *etc.* Notable exceptions to this general rule are Massachusetts, Nevada and, more recently and only as to organizations s under its supervision, New York State's Department of Financial Services.

In general, the "data protection" laws outside of the United States are principles based, particularly as it relates to security controls. Although an obligation to maintain the security of personal data is one of these principles, most countries have, like the majority of our states. These laws generally do not impose prescriptive safeguarding obligations and instead taken the approach of imposing an obligation to implement "appropriate technical and organizational measures" to protect personal data. This approach is reflected in the E.U. General Data Protection Regulation which took effect late last month. Laws focusing on the protection of information other than personal data or on cybersecurity measures more generally have been less common. That trend changed, as to Europe at least, in 2016 with the adoption of the Network and Information Security Directive which was required to be implemented by E.U. Member States on or before May 9, 2018. The Directive is the first EU-wide piece of legislation concerning cybersecurity.

Q.4. What are the pros and cons of a Federal data breach law?

A.4. The main and very significant benefits of a Federal data breach notification law are consistency and efficiency. Although the State laws on this point share many similarities, there is enough divergence in the underlying requirements to make responding to an incident having a multi-State impact very challenging. Analysis of these differences across State laws and their application to the specific facts of each incident is time consuming and can result in unnecessary delay in notifying impacted individuals. A single requirement at the Federal level would promote consistency. Assuming a breach notification regime is to be required, there is very little downside in having this imposed at the Federal, rather than at the State, level.

Q.5. How should Federal data breach laws coexist with other international laws?

A.5. Individuals, regardless of where they are located, who are exposed to a significant risk of harm when their personal information is compromised due to a cybersecurity breach, should be apprised of that breach and given sufficient information to take the measures necessary to protect themselves. State breach notification laws have led the way in this regard and, with the inclusion of a breach notification requirement in the new General Data Protection Regulation, the European Union has now formally acknowledged the value of this principle. In light of this new E.U. requirement, it is more important than ever that the United States adopt a single breach notification regime nationwide in order to ensure that incidents having international impact are responded to promptly, consistently and efficiently.

Q.6. Can you give me some examples of fines, penalties and sentences for firms and individuals that engaged in cyber theft? Are these costs an appropriate deterrent?

A.6. Recent examples of sentencing and penalties for criminal groups and individuals are as follows:

- On April 18 2018, Dwayne C. Hans of New York was sentenced to 36 months in prison for attempting to steal more than $3 million from the Pension Benefit Guaranty Corporation, Defense Logistics Agency and General Services Administration. He was ordered to pay restitution of $134,000.00 for activities conducted between July 2015 and October 2016, when he committed fraud by impersonating an authorized representative of a U.S. financial institution and a defense contractor. Hans had previously pleaded guilty to one count of wire fraud and one count of computer intrusion. *https://www.justice.gov/usao-edny/pr/cyber-criminal-sentenced-36-months-prison-attempting-steal-more-3-million-financial.*

- On November 30, 2017, Russian cyber-criminal Roman Valeryevich Seleznev aka Track2, Bulba and Ncux, was sentenced to serve 168 months in prison for one count of participation in a racketeering enterprise and 168 months in prison for one count of conspiracy to commit bank fraud with the sentences to run concurrent to one another. In both cases, Seleznev was ordered to serve 3 years of supervised release to run concurrently and ordered to pay restitution in the amount of $50,893,166.35 in Nevada and $2,178,349 in Georgia. Seleznev pleaded guilty to the charges and admitted affiliation with the *Carder.su* organization, an Internet-based, international criminal enterprise whose members trafficked in compromised credit card account data and counterfeit identifications and committed identity theft, bank fraud, and computer crimes. *https://www.justice.gov/opa/pr/russian-cyber-criminal-sentenced-14-years-prison-role-organized-cybercrime-ring-responsible.*
- On May 25, 2017, three Nigerian cyber actors were sentenced for Federal offenses including mail fraud, wire fraud, identity theft, credit card fraud, theft of Government property, and conspiracies to commit bank fraud and money laundering. The maximum penalty imposed on a defendant was 115 years in prison and the minimum sentence handed down was 25 years. Overall 21 defendants had been charged in the case which was led by Homeland Security Investigations. The stronger penalties were imposed due to the bank fraud and money laundering elements of their activities. *https://www.justice.gov/opa/pr/three-nigerians-sentenced-international-cyber-financial-fraud-scheme.*

Federal Judges may face difficulty in determining sentencing in cyber crime cases due to the broad types and scope of impact, including where there may be difficulty in articulating a direct financial loss. Based on sentencing guidelines from the Department of Justice, fraud cases where there is direct loss to specific victims are generally easier to determine than matters where there is no direct loss, such as theft of information. Further, in general charges asserted in most cyber crime cases are generally a subset of a broader array of activity by the perpetrator, and for some alleged crimes there may be only limited evidence for some crimes. Consequently, many cyber criminals may only ever be charged and sentenced based on a small subset of their overall criminal behavior, which in many cases stretches back over many years.

Many overseas higher order cyber-criminal actors are unlikely to ever face prosecution and sentencing due to their location in countries that will not extradite or work with U.S. law enforcement. Further in some countries, advanced cyber criminals may present a potential asset to Government military and intelligence capabilities so there is even less incentive to proceed with prosecution. The use of cyber criminals to support state-sponsored cyber operations was publicly confirmed with the release of the indictment in the Yahoo email compromise incident. *https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions.*

There is likely some deterrent value in stiff sentencing for cases, but the broad nature of offenses and diversity of sentencing is likely to present little deterrent to those adversaries located overseas, particularly if they have relationships supporting intelligence and military operations.

Q.7. How big of a problem is figuring out attribution for hacks? Are there ways we can enhance information sharing between industry and the Federal Government to enable more rapid detection and response to cyber-attacks?

A.7. The ability to potentially attribute cyber threat activities to a specific actor or series of actors varies greatly based on the type and impact of the incident. Attribution is generally a complex problem and an investigative challenge based on the availability of a set of technical fragments of evidence, which are aggregated, analyzed and compared against other cyber activities where the perpetrators have been identified with some degree of confidence.

At the strategic level, where nation states are the primary threat actors, geopolitical context may suggest from an intelligence perspective that an adversary is responsible for a set of cyber threat activity that was triggered in response to specific event(s).

Ability to attribute consequently varies between national security and purely criminal threats, with national security threat actors much more likely to be proactively monitored by the Intelligence Community. In criminal cases there is generally a requirement for significant forensic reconstruction of events to be able to coherently trace and attribute malicious activity. Further in the majority of cyber-criminal cases involving fraud and theft, following the network and financial transaction trails will generally lead overseas as criminals know that cross international jurisdictions substantially increases the complexity of investigation for U.S. agencies, particularly if some of the traffic is routed through countries which have tense or poor relations with the United States.

Nation state military and intelligence services may also attempt to actively obfuscate and potentially misattribute activity.

The financial sector has a variety of robust information sharing arrangements with U.S. Government agencies through sector associations including the Financial Services Information Sharing and Analysis Center (FS–ISAC) and Financial Systemic Analysis and Resilience Center (FSARC), and at the individual financial institution level. During the 2011–2014 Distributed Denial of Service (DDoS) attacks the FS–ISAC and individual member institutions worked collaboratively and individually with the Government agencies to identify, attribute and mitigate cyber threat activities. That collaboration has continued through the current time.

Q.8. What tools or resources would make it easier for financial institutions to correctly attribute cyber-attacks?

A.8. To further clarify, the term cyber-attack is, at times, misused in the media which unfortunately confuses the issue of determining the actual objective of an adversary, which may be surveillance, theft, disclosure, manipulation/alteration or disruption/destruction, and much of which has distinctly different impacts to a victim organization.

Attribution is generally a confidence weighted activity and the ability of a private institution, or group of institutions, to successfully attribute cyber activity varies greatly on the type of activity and the type of adversary. In nation-state cases, there may be geopolitical indicators which provide a level of inference lacking in other types of cyber activity.

Publicly attributing cyber activity may present risk to any institution making the statements as an adversary may become particularly focused on that institution in response. This was seen during the 2012 DDoS attacks where an institution that publicly attributed the attacks in media to Iran was subjected to ongoing focus as a result.

Q.9. How significant is the threat to private businesses—from hostile foreign governments or terrorist organizations?

A.9. Nation states have conducted cyber-criminal, cyber espionage and cyber-attack actions against private sector firms globally.

Q.10. What should businesses do now to prepare for a possible attack in the future?

A.10. Businesses should understand the domestic and global operational risk environment in which they operate and have a clear view of which assets are at most cyber risk. They must adopt a defense-in-depth approach to cybersecurity that emphasizes a "default deny" approach and assesses organizational controls against most like adversary capabilities.

Determining the identity, capabilities and likelihood of the most significant cyber adversaries an organization faces is an ongoing activity that can then be used to assess the adequacy of the controls against the threat's technical capabilities.

This ability to conduct this risk analysis is predicated on the following organizational capabilities:

- Identifying targeted campaigns against the organization from broader activity targeting the industry and Internet as a whole
- Analyzing and attributing the campaigns that have been previously observed and are currently being observed
- Ascertaining the adversary's objectives in the campaigns
- Utilizing observations and threat intelligence to develop a model of adversaries technical capabilities and then prioritizing them based on the highest technical capabilities
- Modeling adversaries' capabilities against the organization's control capabilities should result in a residual risk assessment of the organization's abilities to defend against their prioritized adversary capabilities and highlight control gaps or deficiencies that need enhancement.

More broadly this type of analysis should be conducted on an ongoing basis against the broader cyber threat environment to ensure the organization always understands its ability to mitigate current and developing cyber threats.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR WARNER FROM BOB SYDOW

Q.1. Do regulators, who have the ability to supervise the banks and their relationships, but not the third-party vendors themselves, have sufficient authority to monitor these risks appropriately?

A.1. Regulators have been addressing the topic of third-party risk and the vendors across a number of dimensions, including but not limited to:

- Issuing guidance and requirements for outsourcing risk and third-party risk management
- Setting expectations that regulated firms have effective programs over their third parties to confirm that they are fulfilling the firms' contractual, compliance, consumer protection, legal and obligations
- Examination of how firms manage third parties—especially critical vendors—within the context of how they assess and manage risks across various domains (*e.g.,* cyber, critical business processes, Recovery and Resolution Planning).

For example, the Office of the Comptroller of the Currency (OCC) has issued the following guidance for managing third-party risk:

> When circumstances warrant, the OCC may use its authority to examine the functions or operations performed by a third party on the bank's behalf. Such examinations may evaluate safety and soundness risks, the financial and operational viability of the third party to fulfill its contractual obligations, compliance with applicable laws and regulations, including consumer protection, fair lending, BSA/AML and OFAC laws, and whether the third party engages in unfair or deceptive acts or practices in violation of Federal or applicable State law. The OCC will pursue appropriate corrective measures, including enforcement actions, to address violations of law and regulations or unsafe or unsound banking practices by the bank or its third party. The OCC has the authority to assess a bank a special examination or investigation fee when the OCC examines or investigates the activities of a third party for the bank. (OCC Bulletin 2013–29.)

Another example is:

> Guidance for Managing Third-Party Risk," FIL–44–2008, published by the Federal Deposit Insurance Corporation. It states in part: "Review of third-party relationships contributes to the FDIC's overall evaluation of management and its ability to effectively control risk. Additionally, the use of third parties could have a significant effect on other key aspects of performance, such as earnings, asset quality, liquidity, rate sensitivity, and the institution's ability to comply with laws and regulations. Findings resulting from the review of an institution's third-party relationships will be addressed as needed in the Report of Examination. Appropriate corrective actions, including enforcement actions, may be pursued for deficiencies related to a third-party relationship that pose a safety and soundness or compliance management concern or result in violations of applicable Federal or State laws or regulations. Financial institutions are reminded that indemnity or other contractual provisions with third parties cannot insulate the financial institution from such corrective actions.

Q.2. Are regulators focusing on third-party vendor management in their examinations? Are you seeing increased enforcement or other critical action from regulators against banks due to insufficient compliance programs for third-party vendor management?

A.2. EY sees banking regulators conducting exams that include a specific focus on third-party vendor management. The focus of these exams is across topics ranging from governance, due diligence, risk assessment, ongoing monitoring, cyber, resiliency, contracting and the cataloging and inventory of third-party vendors.

Q.3. In its semiannual report in 2017, the Office of the Comptroller of the Currency noted that concentration in third-party service providers, such as providers of enterprise software or security products and services, has increased cybersecurity supply chain risk. Do you agree with this assessment? Do you believe that there is a potential systemic risk issue with dependencies on key third-party vendors or the wide use of certain software? Should regulators require a software bill of materials to understand what's inside third-party IT products?

A.3. A number of factors are contributing to an increase of cybersecurity supply chain risk including: emerging interconnected technologies that drive fundamental transformations and create complex third-party ecosystems; the volume, velocity and precision of attacks; and the shortage of cybersecurity resources and skilled professionals. Additionally, many entities face not only third-party risk, but may also need to consider fourth and fifth parties in their evaluation of risk.

While vendors can help provide solutions to address some of the resource constraints, third parties inherently create additional risk. Any single entity can be a potential threat entry point, which may cause a ripple effect across the enterprise or industry. Heightened regulatory and market focus have increased pressure on financial institutions to account for how third-party suppliers and vendors use and protect their data and manage sustainable operations, especially for critical services.

Additionally, many financial services companies work with Fin Tech and RegTech companies or are looking for efficiency and innovation through use of the cloud. These also put further focus on third-party vendor cybersecurity risks.

The private sector is also focused on components of the supply chain that could create systemic risk and is working with the regulatory community to identify, evaluate, plan and exercise cyber response plans. This includes but is not limited to the power and utilities sector, payment processors, servicers, financial market utilities and infrastructure providers. Continued collaboration and focus on these efforts will be critical for preparedness.

Leading practices for companies to enhance their cyber capabilities, including consideration for third parties, include:

- Identify their most important assets consisting of critical business processes, systems, infrastructure, data and dependent third parties that are most critical to the financial institutions, including their role in the broader financial services ecosystem.
- Protect their high-value assets and underlying system architecture for enhanced security.
- Detect threats and vulnerabilities to proactively identify threats with better threat intelligence, detection and management capabilities.
- Respond to cyber incidents to rapidly contain the damage, and mobilize the diverse resources needed to minimize impact—in-

cluding direct costs and business disruption, as well as reputation and brand damage.

- Recover from cyber disruptions to resume normal business operations as quickly as possible.

Q.4. Is verifying that financial institutions have an internal cybersecurity audit function or an independent third-party assessment sufficient, or should financial regulators develop their own view of the cybersecurity posture of supervised entities in addition to requiring independent third-party assessment?

A.4. Traditionally, the main role of internal audit, which is often referred to as the third line of defense in the three lines of defense (3LoD)[1] risk management model described below, has been to provide an independent and objective assessment of the firm's processes across the first and second lines of defense, with the focus on operational effectiveness and efficiency as part of the firm's overall risk governance approach. As qualified technical resources are limited, internal audit groups often turn to co-sourcing arrangements with a qualified third party to augment their teams to provide technical resources to assess risk and execute audit programs to validate controls over applications and technology infrastructure, cyber risk governance and risk managements, conduct independent penetration testing and vulnerability assessments, *etc.*

In cases where a firm has taken the appropriate actions so that qualified technical resources are available to support their internal audit team, the need for an independent third-party assessment and/or independent regulatory review would not appear to be necessary. Conversely, in cases where a firm does not have sufficiently qualified technical resources inhouse and has elected not to utilize the services of a qualified third party, some form of annual—independent assessment may be necessary.

Q.5. Are you and others in the industry seeing an uptick in interest from regulators in cyber risk? What issues do regulators focus on in their examinations?

A.5. In light of the heightened threat presented by cyber risks, regulators globally have stepped up their focus on cybersecurity. Each regulator reviews cybersecurity in its own way, and takes into consideration its own view of the cyber risks in the industry and specific institutions, when conducting its reviews.

Across the course of their ongoing supervisory reviews, supervisors increasingly assess a bank's ability to manage cyber risk across the 3LoD. The first line operates the business, owns the risk and designs and implements operations. The second line defines policy statements and the risk management framework, provides a credible challenge to the first line and is responsible for evaluating risk exposure for executive management and the board to consider when establishing a risk appetite. The third line of defense, which is also commonly referred to as "internal audit," is responsible for the independent evaluation of the first and second lines.

EY has found that establishing a 3LoD approach to cyber risks is not a trivial task for an organization, but it is becoming essential

[1] This Includes excerpts from EY's *Cyber risk management across the lines of defense,* EYGM Limited, April 2017.

in the cyber world we have entered. Financial services firms are still grappling with how to best implement the model across their businesses for existing nonfinancial risks. Adding cyber risk management as well as strong board oversight during the implementation of the 3LoD model poses an even greater challenge for organizations.

First line of defense

A strong first line of cybersecurity defense requires a significant effort. Whether in the retail bank, investment bank, corporate bank, private bank or any other area, business heads will have to perform a thorough examination to determine whether the business is doing enough to manage cyber risk. Information security groups can no longer apply one-size-fits-all solutions to the entire enterprise. Instead, each line of business must carefully define the cyber risks and exposures it faces. Cyber risks need be woven into the fabric of the first line's risk and control self-assessment and into fraud, crisis management, and resiliency processes.

The lines of business will need to actively monitor existing and future exposures, vulnerabilities, threats and risks associated with their activities. In addition to leveraging technologies, businesses need to determine the impact that cyber risk will have on its clients, operational processes and strategies. These new responsibilities require significant investment in people and tools, including upgraded monitoring and analytic capabilities to provide improved assessments of current levels of cyber risk.

Second line of defense

The independent second-line cyber risk management function manages the enterprise cyber risk appetite and risk management framework within the context of the overall enterprise risk strategy. This group challenges the first line's application of the board-approved cyber framework and appetite. Second-line risk management plays a critical role in managing cyber risks and should not be walled off as a separate risk function. As the keeper of a firm's board-approved risk tolerance, it determines how to appropriately measure cyber risks, embedding quantitative and qualitative (*e.g.,* reputational) thresholds for cyber risks into the statement of risk tolerance for the firm. Moreover, these clearly established appetite and associated thresholds need to cascade down into the operations for each line of business.

Given the relative novelty of applying the 3LoD model to cyber risk, most of the first and second lines focus appropriately on more effective management of these risks rather than the narrower issue of compliance. However, with an increasing volume of regulatory guidance and mandatory requirements stemming from industry, professional and regulatory standards, cyber will increasingly constitute a material compliance risk. Accordingly, supervisors should assess whether financial institutions integrate cyber risk compliance into second-line risk management.

Third line of defense

Traditionally, the main role of the third line of defense has been to provide an independent and objective assessment of the firm's process across the first and second lines of defense, with the focus on operational effectiveness and efficiency as part of the firm's overall risk governance approach. Regulators are now focusing on how effective and independent a firm's internal audit team is when it comes to reviewing the firm's approach to cybersecurity. For example, banking regulations focused on cybersecurity often include references to the importance of an "annual independent assessment," such as those included in Federal Financial Institutions Examination Council (FFIEC) and NIST requirements and guidelines.

As a foundation, EY recommends that the internal audit team include within its overall audit plan an evaluation of the design and operating effectiveness of cyber risk management across the first and second lines of defense. Traditionally, industry standards, such as the NIST's Cybersecurity Framework guidelines have been used as the benchmark for evaluating a firm's effectiveness. Going forward, internal audit teams at financial institutions may need to create their own framework or apply multiple industry frameworks. By doing so, internal auditors will maintain greater objectivity in assessing cyber risk management effectiveness, eliminating the potential blind spots that can result from using a common standard throughout all three lines of defense.

Under the 3LoD model, internal auditors perform procedures such as assessments, validation of applications and technology infrastructure, evaluations of third-party risks, conduct some level of intrusive-based testing, either by themselves or using third parties, incorporate cyber into regular audits and have a responsibility to stay abreast of cyber threat intelligence.

Board oversight of cyber risk management

Supervisors should also assess the degree to which boards of directors provide effective challenge and oversight of the bank's cyber risk management. Boards need to understand the maturity of their organizations' approach relative to evolving industry and regulatory trends. A cyber risk maturity assessment should be broad in nature, considering people, process and technology as well as existing and planned improvement or remediation activities.

The view on program maturity needs to be combined with a proper assessment of existing threats and vulnerabilities, and the evolving threat landscape. Boards should press management to quantify cyber risk as much as possible so that quantitative statements on the degree of cyber risk are incorporated into the firm's risk appetite statement. The cyber risk appetite statement should link directly to cyber and technology operational thresholds and tolerances. Boards should insist on more credible cyber risk reporting, in the context of the approved cyber risk appetite. Boards should also determine how they evaluate the quality, accuracy and timeliness of cyber metrics. Boards should challenge how they oversee cyber risk across their own governance structure.

The board should revisit its strategy for keeping directors abreast of cyber threats, trends and the evolving business implications. Boards should press management to quantify cyber risk as much as possible so that quantitative statements on the degree of cyber risk are incorporated into the firm's risk appetite statement. The cyber risk appetite statement should link directly to cyber and technology operational thresholds and tolerances. Aspects of cyber risk management should be built into an ongoing training program throughout the year, with overview sessions and deep dives on the most relevant topics and issues.[2]

Ultimately, the board is accountable for requiring that management adapts quickly enough to manage this enterprise risk more effectively and efficiently, and it is charged with providing a credible challenge to management's approach.

Q.6. What do you believe is the appropriate role of the financial regulators in assessing the cybersecurity of institutions they regulate?

A.6. We see several regulatory roles related to cybersecurity including:

- Engaging in public/private sector dialogues and efforts to support sharing intelligence and leading practices
- Considering how effectively cyber resiliency has been built into an organization's three lines of defense as referenced in my testimony
- Considering the level of board engagement in cyber risk management
- Advancing opportunities to seek sources of new talent for both public and private sector needs, as observed during my testimony

Companies that exercise good faith efforts, establish cyber risk management frameworks and adopt such leading practices as outlined in the previously submitted testimony should benefit, not only within the company, but in the eyes of stakeholders, regulators and enforcement agencies, especially relative to liability and penalty measures.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR CORTEZ MASTO FROM BOB SYDOW

Q.1. A year and a half ago, William and Margaret Frederick sold their home in Ohio so they could buy a home in Las Vegas, Nevada. The couple expected to make a $216,000 profit on the sale. But, their real estate agent read a hacked email supposedly from William—the fake email had three L's in Bill instead of two—and sent the profit to the hacker. William was 83 and Margaret 77. Someone stole the money they intended to live on in retirement.

Real estate transaction fraud is a problem in Nevada and nationwide. Thieves wait for the right time to impersonate a bank or realtor and send you different wire transaction instructions. Estimates are as much as $400 million a year in losses.

What more can financial institutions do to prevent thieves from stealing people's down payments, earnest money and even the entire home payment if someone is buying a home for cash? Please identify the best practices for realtors, title agents and mortgage brokers?

[2] For an example of an effective cyber risk dashboard, see Appendix F of the "Cyber-Risk Oversight: Director's Handbook Series," National Association of Corporate Directors, 2017.

A.1. Consumer education about common financial fraud methods and how to securely communicate their sensitive data should be driven as a combined effort by the private sector and public entities to foster an ongoing culture of greater awareness. Financial institutions can work to implement two-way verification of identities on the web, mobile and other virtual spaces to gain greater confidence that they are interacting with their intended customer and for the customer to have confidence they are communicating with their intended institution. Additional monitoring controls for higher-risk consumers and transactions should be considered, but this should be balanced with the need to maintain fluidity and velocity of transactions without adding risk to the banks themselves for delays or rejected payments. Underpinning all of these controls, however, is the growing need for an improved form of digital identification for all entities, consumer and institutional, that can support enhanced authentication and be easily used and verified for online transactions.

Educating individual business owners about cybersecurity and cyber posture is a topic on which the public and private sector should work together. EY recognizes the importance of better cyber hygiene throughout the ecosystem, and would encourage policymakers to consider what levers it has available to reach individual business owners.

Q.2. One way to protect consumer's information is to not collect it. For example, why should merchants of any sort, including doctors, insurance companies and utilities, require Social Security Numbers as part of their information or data-set on their customers? Should we limit Social Security Numbers provided to merchants?

A.2. The value of the Social Security Numbers (SSN) as a private and unique identifier must be viewed relative to the risk that currently exists based upon years of propagating this same identifier across multiple systems. In my view, continued usage of this same identifier, coupled with the aggregation of cybersecurity breaches that have gained access to this identifier, diminish its value and instead heightens the risk associated with using it. Unique identifiers must be evaluated from multiple perspectives before deciding upon their value. For example, the use and collection of an identifier that is unique to a particular industry segment may be reasonable, if its usage across various entities encourages innovation, benefits society, limits other risks or provides convenience to consumers and furthermore, if the risks associated with using the identifier do not outweigh those values or may be mitigated. It is the data that is associated with the unique identifier that creates the risk and hence there may be ways to still achieve value while minimizing risk by limiting those data elements about an individual that are associated with any identifier.

In other contexts, there may be better ways than using a unique identifier to manage risk. One example is when the identifier is being used solely for the purpose of authenticating someone's identity. There are other ways to achieve this, including through encrypted identifiers and multifactor authentication.

Q.3. What other sorts of information should financial institutions or others STOP collecting?

A.3. Many companies across industries are required to collect SSNs to comply with legal and regulatory requirements. For example, financial institutions are required to collect and retain SSNs when customers open an account or apply for a mortgage. Health insurance companies are also mandated by Government to collect SSNs for individuals they insure. In such cases, companies cannot voluntarily choose whether or not they collect SSNs from their customers.

When considering policies to change the collection and use of SSNs, it is important to understand whether the proposal would impact the use of the SSN as an identifier or authenticator. SSNs were created to be a unique identifier, and organizations continue to use them in this way to connect disparate pieces of information about a person. Today, SSNs are also widely used as authenticators to verify the identity of a person. This is problematic because authenticators are only valuable if they remain a secret—which is not the case with SSNs after years of massive data breaches have made them widely available to criminals on the dark web.

State and International Laws Relating to Cybersecurity

Q.4. What are the pros and cons of a Federal data breach law?

A.4. Because pros and cons can vary for differing stakeholders, policymakers in Congress are in the best position to determine the path forward that balances the needs of constituents and other key stakeholders. EY believes key considerations include the potential benefit of harmonization and the need for interoperability across jurisdictions, which we address elsewhere in this document.

Q.5. How should Federal data breach laws coexist with other international laws?

A.5. In EY's view, it is important for U.S. policymakers to consider the potential for conflict that could arise across jurisdictional differences in laws. EY routinely hears from clients how regulatory harmonization at the State, Federal, and international levels has the potential to reduce compliance costs and free up capital to invest limited financial resources available to improve their security posture. Conversely, it would add to costs and complexity to have disparate approaches that are not interoperable.

Q.6. Firms that fail to secure their data pay substantial penalties. Hundreds of hackers go to prison. The woman [Paytsar Bkhchadzhyan] who hacked into Paris Hilton's accounts and stole her credit card information received a 57-month prison term. Taylor Huddleston (26) of Arkansas was sentenced to serve nearly 3 years for building and selling a remote access Trojan (NanoCore) to hackers.

Can you give me some examples of fines, penalties and sentences for firms and individuals that engaged in cyber theft? Are these costs an appropriate deterrent?

A.6. There are various Federal and State Government authorities that bring enforcement actions relating to cybercrime. A non-exhaustive list includes the following. The Federal Trade Commission brings actions alleging that companies have engaged in unfair or deceptive practices that failed to adequately protect consumers' personal data; information on such cases is available at *www.ftc.gov/datasecurity*.

The U.S. Securities and Exchange Commission (SEC) also brings actions alleging account intrusion and failure to safeguard customer data, for example, information on such cases is available at *www.sec.gov/spotliqht/cybersecurity-enforcement-actions*. Because various States have their own data protection and breach notification laws, some States have State authorities with enforcement authority relating to cybercrime.

Additionally, there can be criminal sanctions for cyber theft. To take one recent example, the U.S. Department of Justice (DOJ) announced charges against 36 people from the United States and six foreign countries earlier this year alleging that they were responsible for hundreds of millions of dollars of losses from the acquisition and sale of stolen identities and other information. See "Thirty-six Defendants Indicted for Alleged Roles in Transnational Criminal Organization Responsible for More than $530 Million in Losses from Cybercrimes," DOJ Press Release No. 18–145 (Feb. 7, 2018), available at *www.justice.gov/opa/pr/thirty-six-defendants-indicted-alleged-roles-transnational-organization-responsible*. Notably, although DOJ announced the arrests of 13 of the people charged, it was uncertain whether the 23 remaining defendants would ever face trial in the United States.

There are a variety of criminal statutes available to Federal prosecutors. See, *e.g.,* "Prosecuting Computer Crimes," DOJ OLE Litigation Series, Appendix A, "Unlawful Online Conduct and Applicable Federal Laws," available at *www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf*. For example, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, provides for maximum sentences of 10 years for a first offense and 20 years for a second offense. While cybersecurity experts generally feel that there is an important role for law enforcement to play in apprehending cyber criminals, many express the sentiment that these efforts are unduly hampered by the length of criminal sentences that are imposed. More often, cybersecurity experts tend to realize that bad actors in this space are able to operate across the globe, including in places that make it difficult for U.S. law enforcement authorities to reach them.

This is not to say that there is no place for criminal and regulatory enforcement in the cyber realm. Clearly, there is. However, especially given the rapidly changing nature of the threat, and the extent to which the threat can originate overseas, enforcement will never be sufficient on its own. Institutions need to protect themselves and their stakeholders because many actors in cybercrime are unlikely to be deterred, no matter how robust the penalties. As a result, EY encourages the Committee to focus not only on enforcement but also on ways to incentivize responsible and effective corporate governance and risk management strategies by rewarding good behavior and adoption of leading practices.

As stated in the written testimony EY submitted to the Committee, not only do threats evolve day-by-day, but those who want to do harm are not constrained by regulatory, liability or jurisdictional issues, let alone ethics. While no one can guarantee that any or all attacks can be prevented, the market is developing best practices and ways to mitigate risk and impact. Companies that exercise good faith efforts, establish cyber risk management frameworks and adopt such best practices as outlined in this testimony should benefit, not only within the company, but in the eyes of stakeholders, regulators and enforcement agencies, especially relative to liability and penalty measures.

Q.7. Seventy-seven percent of cyber attacks come from the outside. Yet sometimes, figuring out who the hackers were is hard to figure out. Hackers can spoof evidence. They can embed other hackers' tools.

How big of a problem is figuring out attribution for hacks? Are there ways we can enhance information sharing between industry and the Federal Government to enable more rapid detection and response to cyber attacks?

A.7. Attribution can be incredibly difficult depending on the sophistication of the adversary and as a result of the transient nature of digital evidence. An adept adversary understands forensics and cyber investigative methodology and will take steps to minimize their digital fingerprints if they choose to obscure attribution. Additionally, attribution often requires correlation between different investigations or sources of information. Therefore, many organizations that do not routinely respond to breaches lack the data to make correlations and assessments regarding attribution. Finally, some key data points that are helpful in providing attribution are maintained by private or foreign entities that may be unwilling to provide this critical information.

There are a number of initiatives currently underway to promote the sharing of information between the private and public sector including:

- The Department of Homeland Security's Cyber Information Sharing and Collaboration Program (CISCP)
- The Cybersecurity Information Sharing Act (CISA) program, and related Automated Indicator Sharing Initiative
- The Federal Bureau of Investigation's InfraGard program
- The U.S. Department of Energy's Cybersecurity Risk Information Sharing Program for the electric utility sector
- Sector-specific as well as regional Information Sharing and Analysis Centers (ISACs)

These initiatives are each having a positive effect on marketplace efforts to combat cyber attacks, but there is always more that can be done, including: (1) providing enhanced liability protection for private sector companies when good-faith efforts are made when sharing information, (2) increasing the speed with which information is disseminated, and (3) increasing the speed of security clearance investigations (needed before access can be provided to certain protected information).

Q.8. What tools or resources would make it easier for financial institutions to correctly attribute cyber-attacks?

A.8. Attribution can be incredibly difficult depending on the sophistication of the adversary and the transient nature of digital evidence. The rapidly escalating volume, velocity and sophistication of cybersecurity attacks on the financial services ecosystem continues to present a significant challenge to financial institutions in safeguarding their sensitive data. Financial institutions should continue to enhance their cyber capabilities—people, process and technology by identifying their high-value assets; securing their high-value assets and underlying architecture; proactively detecting threats and vulnerabilities; rapidly responding to cyber incidents to contain the damage; and recovering from cyber disruptions to resume normal business operations as quickly as possible.

Additionally, financial institutions should explore the possibility of sharing cyber threat information in a confidential, timely manner with their peers and appropriate external stakeholders and also collaborating with them to protect the financial system ecosystem.

Q.9. In 2015, French-language TV station, TV5Monde was subjected to a significant cyber-attack which disrupted its broadcast for several hours by Fancy Bear. These are the same Russian government and military hackers that hacked the Democratic National Committee. Multiple television channels went dark. Social media channels run by the broadcasters began to spew ISIS propaganda. The attack was the work of Russian hackers which pretended to be ISIS. Russian government hackers also attacked the World Anti-Doping Agency, the power grid in Ukraine and the French electorate with another document dump.

How significant is the threat to private businesses—from hostile foreign governments or terrorist organizations?

A.9. The threat to the private sector from attacks waged by hostile foreign actors is extremely significant. There have been a number of public reports of instances where these actors have demonstrated the ability and intent to maliciously attack private companies with the goal of stealing intellectual property, disrupting operations (*e.g.,* via ransomware attacks), conducting industrial espionage and other nefarious purposes. These attacks directly affect specific companies and have a ripple effect on the U.S. economy as a whole, potentially undermining the public's trust and the backbone of our economy.

Q.10. Some of the lessons from that attack was documenting IT processes, restricting access to IT processes, and keeping communications separate from incident responses.

What should businesses do now to prepare for a possible attack in the future?

A.10. A growing number of companies experience cyber events as part of the routine course of business and are well versed in responding. Incident management, continuity and crisis management programs can support how a company responds to an event. For significant cyber events, many of EY's clients are focused on the following areas:

1. Communications and disclosures: timely and accurate reporting, notification and disclosure is an increasingly critical concern following a cyber breach as it must be factual and meet requirements under Federal and State law as well as other regulatory requirements and guidelines, including the most

recent SEC guidance updates and, where applicable, various foreign requirements such as the new European Union (EU) General Data Protection Regulation (GDPR).

2. Simulation exercises: firms have been practicing technical "war games" and conducting trainings to prepare technical resources for an event. EY is seeing a trend where firms are extending these exercises further to include executive management and in some cases members of the board to practice and refine response mechanisms.
3. Industry efforts: financial services firms are engaging in various industry exercises, collaboration efforts and information sharing programs to help address the potential client impacts as well as possible systemic impacts that could occur.

However, it should be noted that there is no silver bullet. No organization, large or small—public or private—is immune to the cyber threat. As noted in the prepared remarks delivered to the Senate Banking Committee, EY's clients face three significant challenges:

1. Emerging interconnected technologies drive fundamental transformations and create complex third-party ecosystems
2. The volume, velocity and precision of attacks
3. A shortage of cybersecurity resources and skilled professionals

EY works with clients across all sectors, and many should be commended for their efforts. Financial services firms, especially the largest banks, are considered best-in-class not only in terms of organization and investment, but also for leading engagement with stakeholders across the ecosystem. The industry is not without challenges, and there is variation among firms. For example, while the largest banks have considerable resources dedicated to cybersecurity risk management, smaller entities often struggle with costs and access to a competitive talent pool. That is not to say these organizations are not committed to cyber risk management or do not take the issue seriously. Cyber breaches and associated losses are not good for business, and when a company's business model depends on customer trust, a cyber event can cause long-term damage to brand and reputation.

Large banks are accustomed to higher levels of regulatory scrutiny, and their third-party risk management programs tend to be more mature and robust—but challenges remain. Today, financial institutions deal with third-, fourth- and fifth-party risk. In addition to vendor risk, most institutions struggle to secure resources and talent. Experienced cyber professionals are in high demand. Often, small financial services institutions rely on third-party providers to meet those needs. There is no one-size-fits-all solution, but there are three areas where EY believes risk can be mitigated: corporate governance and risk management, the American Institute of Certified Public Accountants' (AICPA) Cybersecurity Risk Management Reporting Framework and policy solutions.

Ultimately, the board is responsible for governing a company's risk appetite and providing a credible challenge to management. By doing so, boards help protect investors and enhance the company's value and performance. Banks use a "three-lines-of-defense" risk management model (described later in this document). The larger ones are adopting this model for cyber. EY considers this a leading practice. Increasingly, regulators, investors and others want financial institutions to build cyber resiliency strategies into the three lines of defense.

Another challenge is understanding and communicating about a cyber program's efficacy. While the National Institute of Standards and Technology (NIST) and others have developed implementation guidance, there had been no means to evaluate and report on program effectiveness. The distinction is subtle, but significant. In response, the AICPA recently developed the Cybersecurity Risk Management Evaluation and Reporting Framework. This is voluntary and can provide stakeholders with reasonable assurance that the identification, mitigation and response controls are in place and operating effectively.

No framework can guarantee against a breach, but the AICPA Framework can offer an independent validated understanding of a company's cybersecurity systems, processes and controls. While the AICPA's model is relatively new, voluntary market adoption appears to be gaining momentum. Unfortunately, there is no single legislative, regulatory or market solution that can guarantee against a cyber event. Bad actors are not constrained by regulatory, liability or jurisdictional issues, let alone ethics.

Policymakers and the business community should work together to foster collaboration and improve intelligence sharing. The private sector needs flexible and harmonized policy solutions that recognize the dynamic challenge of cybersecurity and clarify conflicting directives. There needs to be a balance between the need for compliance with the need to manage cyber risk and protect consumers.

EY believes companies that engage in good faith efforts, establish enterprise-wide cyber risk management frameworks and adopt leading practices should be recognized, especially relative to liability and penalty measures.

Finally, EY encourages Congress to support modernization of the Government's cyber posture, to focus on developing solutions to to address cyber workforce shortages, and to educate the public and help the country as a whole improve its cyber hygiene.

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

Credit Union National Association CUNA

Jim Nussle
President & CEO

Phone: 202-508-6745
jnussle@cuna.coop

601 Pennsylvania Avenue NW
South Building, Suite 600
Washington, D.C. 20004-2601

May 23, 2018

The Honorable Mike Crapo
Chairman
Committee on Banking Housing
And Urban Affairs
United States Senate
Washington, DC 20510

The Honorable Sherrod Brown
Ranking Member
Committee on Banking Housing
and Urban Affairs
United States Senate
Washington, DC 20510

Dear Chairman Crapo and Ranking Member Brown:

On behalf of America's credit unions, I am writing regarding the hearing "Cybersecurity: Risks to the Financial Services Industry and Its Preparedness." The Credit Union National Association (CUNA) represents America's credit unions and their 110 million members.

Credit unions and the financial services industry at large are dedicated to protecting member and customer information along with working to ensure that systems used to provide financial services to Americans are robust, secure and resilient. We understand the importance of securing data from bad actors and thus support the Committee's efforts to monitor industry preparedness. As credit unions and banks continue suffer losses from merchant data breaches, we want to remind the Committee that we are often financially responsible for other industries' lack of cyber preparedness and efforts to protect important data.

CUNA members continue to highlight cybersecurity as a top concern as protecting systems from outside threats becomes ever more complicated. Credit unions of all sizes invest significant resources to protect critical systems from attack. The National Credit Unions Administration (NCUA) and the Federal Financial Institutions Examination Council (FFIEC) have been good partners in assessing cyber risks and providing resources for credit unions. These efforts along with several industry led initiatives to share information and bolster resilience for all types of financial organizations demonstrate that the financial services industry along with the credit union and bank regulators expend great efforts to ensure that system remains robust.

Although credit unions do their part in securing information and operations, we do continue to see an important role for the federal government in requiring cyber preparedness for other industries and working to protect financial institutions and from cyber attack. Furthermore, we fear that bad actors continue to attack less regulated industries as a means to generate revenue for continued cyber attacks and other criminal activities.

Credit unions along with other members of the financial services system make cybersecurity a top priority. Credit unions look forward to working with the Senate and federal agencies on continued cyber best practices.

On behalf of America's credit unions and their 110 million members, thank you for holding this important hearing.

Sincerely,

Jim Nussle

Jim Nussle
President & CEO