Senate Committee on Banking, Housing, and Urban Affairs

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

Written Testimony of:

Michael Daniel

President & CEO, 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?

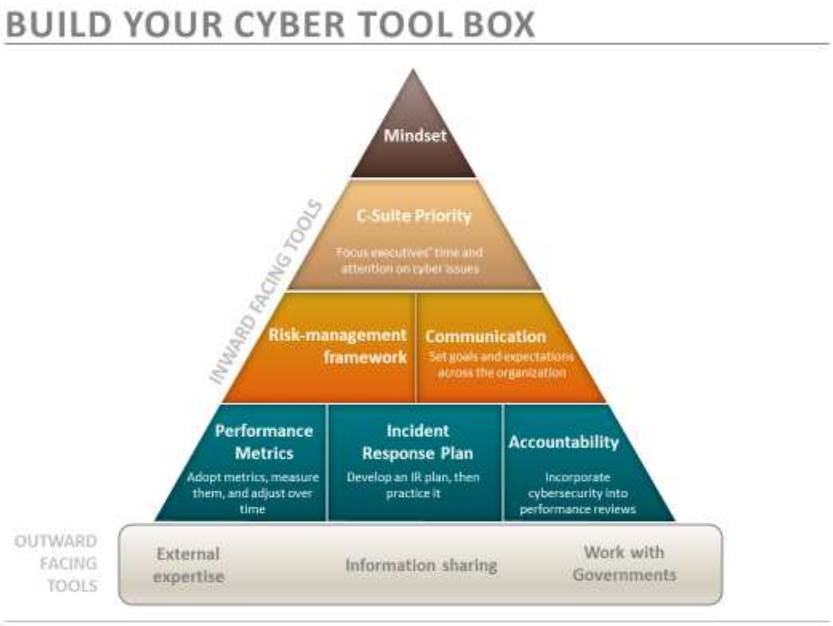
Given the trends, growing complexities, and inherent challenges of the cyber threat, is it possible to design an effective strategy to combat it? The short answer is yes – but implementing such a strategy, whether at the organizational or national level, requires a lot of work, sustained engagement, 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 technical 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.