S. Hrg. 114–412

PROTECTING AMERICA FROM CYBER ATTACKS: THE IMPORTANCE OF INFORMATION SHARING

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

JANUARY 28, 2015

Available via the World Wide Web: http://www.fdsys.gov/

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PUBLISHING OFFICE

94–272 PDF WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin *Chairman*

JOHN MCCAIN, Arizona
ROB PORTMAN, Ohio
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MICHAEL B. ENZI, Wyoming
KELLY AYOTTE, New Hampshire
JONI ERNST, Iowa
BEN SASSE, Nebraska

THOMAS R. CARPER, Delaware
CLAIRE MCCASKILL, Missouri
JON TESTER, Montana
TAMMY BALDWIN, Wisconsin
HEIDI HEITKAMP, North Dakota
CORY A. BOOKER, New Jersey
GARY C. PETERS, Michigan

KEITH B. ASHDOWN, *Staff Director*
WILLIAM H.W. MCKENNA, *Investigative Counsel*
SEAN C. CASEY, *Senior Professional Staff Member*
GABRIELLE A. BATKIN. *Minority Staff Director*
JOHN P. KILVINGTON, *Minority Deputy Staff Director*
STEPHEN R. VIÑA, *Minority Chief Counsel for Homeland Security*
MATTHEW R. GROTE, *Senior Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*
LAUREN M. CORCORAN, *Hearing Clerk*

CONTENTS

WITNESSES

WEDNESDAY, JANUARY 28, 2015

ALPHABETICAL LIST OF WITNESSES

APPENDIX

PROTECTING AMERICA FROM CYBER ATTACKS: THE IMPORTANCE OF INFORMATION SHARING

WEDNESDAY, JANUARY 28, 2015

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 1:34 p.m., in room SD–342, Dirksen Senate Office Building, Hon. Ron Johnson, Chairman of the Committee, presiding.

Present: Senators Johnson, McCain, Lankford, Ayotte, Ernst, Sasse, Carper, Baldwin, Booker and Peters.

OPENING STATEMENT OF CHAIRMAN JOHNSON

Chairman JOHNSON. This hearing will come to order. Senator Carper is on his way, but we have just been told we can get going here.

I want to keep my opening remarks very brief because we do have votes and I want to make sure we get to the testimony. But I want to thank the witnesses for their very well thought out, well-prepared testimony, certainly the written testimony. I am looking forward to your oral testimony. I want to thank you for your flexibility. We have obviously moved the hearing up.

We have in this Committee agreed upon a mission, and the mission is pretty simple: to enhance the economic and national security of America. If we focus on that goal, a goal that we all share—whether you are Republican or Democrat, we really share that. And particularly when it comes to this cybersecurity hearing about sharing information to protect our cyber assets, it is also a goal we share. So if we concentrate on that, recognizing there are different viewpoints on this, I think we have a far better chance of actually succeeding. So when Senator Carper gets here, we will give him a chance to have an opening statement.

The tradition of this Committee is to swear in witnesses, so I would ask the witnesses to stand and raise their right hands. Do you swear that the testimony you will give before this Committee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Mr. GORDON. I do.

Mr. CHARNEY. I do.

Mr. BESHAR. I do.

Mr. BEJTLICH. I do.

Mr. NOJEIM. I do.

Chairman JOHNSON. Thank you.

What I would like to do is get right into testimony then, and I will start with Marc Gordon. He is the Executive Vice President and Chief Information Officer (CIO) of American Express. He previously served as CIO of Bank of America and Best Buy. Mr. Gordon, your testimony, please.

TESTIMONY OF MARC D. GORDON,[1] EXECUTIVE VICE PRESIDENT AND CHIEF INFORMATION OFFICER, AMERICAN EXPRESS

Mr. GORDON. Thank you, Chairman Johnson and Members of the Committee. As you heard, my name is Marc Gordon. I am the Executive Vice President and CIO at American Express. I oversee the global technology organization for our company, as well as information security, and I really appreciate the opportunity to testify before this Committee on information sharing. It is a topic that I am very passionate about.

Based on my experiences as CIO across both the retail sector and the financial services sector in Fortune 100 companies, I would strongly urge the Committee to move forward swiftly with information-sharing legislation. I believe that effective information sharing may actually be the single highest-impact, lowest-cost, fastest-to-implement capability we have at hand as a sector and as a Nation to raise the level of capability against the many and varied threats that we face. The way I like to think about it is an attack against a single company can be the entire sector's and Nation's defense, quickly shared.

I realize you are familiar with the threat landscape, and we have included many examples in my written testimony on the nature and the scale of the threats we face. I will not go through those now. What I would emphasize here is that while cyber crime is growing meaningfully for us and across industries, we are increasingly concerned about what appears to be the convergence of players, capabilities, and intentions—namely, nation-state players or those with nation-State capabilities with a particular attention around destructive intent across industries.

In response to these threats, the financial services industry has invested literally billions of dollars to protect our networks. But there are steps that we can take together within and across industries and with the government to make the total ecosystem more secure.

And while there is some sharing of information today, I would characterize it as highly variable within industries, and especially highly variable across industries. And meaningful legislation I believe would expand both the quality and volume of cyber information sharing and raise the security level overall for all of us.

But legal barriers and the threat of lawsuits are obstacles to information sharing today, and that is where legislation that provides targeted protections from liability and disclosure is sorely needed.

---

[1] The prepared statement of Mr. Gordon appears in the Appendix on page 37.

There are a few notable items that I would also emphasize today in terms of attributes of information sharing that we believe are particularly important for effective information sharing and to have the desired results.

First is an emphasis on real-time sharing.

Second is liability and disclosure protection, not just for sharing but also for acting within one's own network on the information that is shared.

Third, that the protections that are afforded in terms of liability and disclosure and so forth are extended not just to government-sanctioned entities but to private entities, businesses sharing among themselves. We feel that is actually very important.

And, finally, that the sharing needs to be bi-directional, that is to say, we believe the government should be directed to share in the right way classified indicators only known and knowable from the government. We think that is a big value add to this proposition for the private sector as we protect our customers' information.

Finally, we are committed to protecting the privacy of our customers' information and believe that concerns around privacy protection should be discussed but can be effectively addressed in the legislation.

Again, I just want to thank you for asking me to be here today. I look forward to working with this Committee and other Members of the Senate and House, and I look forward to helping in any way that we can.

That concludes my prepared remarks, and I would be happy to answer questions.

Chairman JOHNSON. Well, thank you, Mr. Gordon.

Our Ranking Member has arrived, so, Senator Carper, do you have some opening comments?

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. As we say in Delaware, bienvenido. [Laughter.]

Bienvenido. We are happy you are here, looking forward to this hearing. This is a timely, important topic. Let us see what we can learn from all of you.

Thank you.

Chairman JOHNSON. Thank you for that.

Our next witness is Scott Charney. He is the Corporate Vice President of Microsoft's Trustworthy Computing Group where he focuses on the security and privacy of Microsoft's products. Scott has also worked for PricewaterhouseCoopers and as Chief of the Justice Department's Computer Crime and Intellectual Property Section.

Mr. Charney, you have the floor.

TESTIMONY OF SCOTT CHARNEY,[1] CORPORATE VICE PRESIDENT, TRUSTWORTHY COMPUTING, MICROSOFT CORPORATION

Mr. CHARNEY. Chairman Johnson, Ranking Member Carper, and Members of the Committee, thank you for the opportunity to appear today at this important hearing. My name is Scott Charney, and I am the Corporate Vice President for Trustworthy Computing at Microsoft. It is good to see the Committee's first hearing of the 114th Congress focuses on cybersecurity. I commend this Committee and the Members of the Senate for addressing one of America's most complex challenges.

Let me start by describing the cyber threat. The threat comes in two forms:

First, there are opportunistic criminals who, like burglars testing doorknobs, do not care who falls prey as long as someone does.

Second, there are actors described as advance persistent threats because they are intent on compromising a particular victim.

These two different types of threats require somewhat different responses. Basic computer hygiene—such as running the latest version of software, applying updates, and using antivirus products—can thwart many opportunistic threats. Addressing advanced persistent threats, however, requires much more. Computer security professionals must prevent, detect, and respond to sophisticated attacks.

Knowing about threats, vulnerabilities, and incidents can help computer security professionals and others take the right action. So how does such information sharing occur in practice. Simply put, a party collects information, identifies a computer security issue, and then shares it with those who can act on it. The recipient uses that information to prevent, detect, or respond to the event, normally collecting more data and sharing it in return. Often parties are added to the process as the evidence dictates. Throughout this process, all parties will maintain the data responsibly, protecting its confidentiality as appropriate.

Does this work? Absolutely. For example, Microsoft has partnered with other companies and law enforcement agencies to take down two botnets which had infected millions of computers around the world and were each responsible for over $500 million in financial fraud.

So if information sharing is so important and so helpful, why is such sharing limited? The short answer is that those with critical information are often unable or unwilling to share it. They may be unable to share it due to law, regulation, or contract, all of which create binding obligations of secrecy and expose a company to legal risk if information is shared.

There are also other risks. For example, a company that discloses its vulnerabilities may suffer reputational risk, and such a disclosure may even make security matters worse if hackers leverage that information for further attacks against that company or anyone else.

In light of these issues, how can information sharing be encouraged? While my written testimony detailed six core tenets that

[1] The prepared statement of Mr. Charney appears in the Appendix on page 44.

must guide any information-sharing proposal, let me describe the most important tenets here.

First, privacy is a fundamental value and must be protected when sharing information. While users around the world may have different views about privacy, they want assurances that the information they entrust to others is used properly and protected. It is also important that governments adhere to legal processes for law enforcement and national security requests and do not use computer security information-sharing mechanisms to advance law enforcement and national security objectives.

Second, government and industry policies on information sharing should take into account international implications. Many U.S. businesses are multinational companies. If not properly constructed, rules in the United States can discourage foreign markets from using U.S. technology products and services, as well as lead to reciprocal requirements that could undermine U.S. security.

Third, while information sharing has benefits, it also poses business risks that must be mitigated. As noted, sharing information can expose an organization to legal, regulatory, contractual, and reputational risks. Any information-sharing regime must attempt to reduce these risks by providing appropriate liability protections.

Finally, information sharing need not follow a single structure or model, and governments should not be the interface for all sharing. Information sharing already occurs through both formal and informal processes, within industry and between industry and government, and sometimes across national borders. There is no single model because situations and desired outcomes differ. Flexibility is critical.

With current practices and those tenets in mind, how should we think about information-sharing legislation? In a nutshell, Congress should ensure that existing information-sharing arrangements are left undisturbed, ensure the protection of civil liberties, and reduce disincentives to sharing. This can be done in the following three ways:

First, the legislation should be scoped to cover information that reasonably enables defenders to address cyber threats.

Second, the legislation should be designed to protect privacy and civil liberties by requiring data be anonymized, restricting secondary uses, protecting against inappropriate disclosure, and requiring the government to seek a court order when attempting to pierce the veil of anonymity.

Third, the legislation should grant appropriate liability protection for sharing information while recognizing that companies must fulfill their contractual obligations to their customers.

Thank you for the opportunity to testify, and I look forward to working with the Committee on this effort.

Chairman JOHNSON. Thank you, Mr. Charney.

Our next witness is Peter Beshar. He is the Executive Vice President and General Counsel of Marsh & McLennan Companies. Before joining Marsh, Mr. Beshar was a partner in Gibson, Dunn & Crutcher. Mr. Beshar.

TESTIMONY OF PETER J. BESHAR,[1] EXECUTIVE VICE PRESIDENT AND GENERAL COUNSEL, MARSH & MCLENNAN COMPANIES

Mr. BESHAR. Thank you, Chairman Johnson, Ranking Member Carper, and Members of the Committee.

The evolution in the sophistication and intensity of cyber attacks in 2014 was astonishing. And as bad as it was in 2014, it got worse in the last month. In December, the German Government reported that hackers had caused massive damage to an iron plant by disabling the electronic shut-off systems that turned off the furnaces. And this escalation of cyber attacks reflects a troubling threat posed to our critical infrastructure.

I would like to focus my remarks this afternoon on cyber insurance. Some of you may be saying, "What relevance does cyber insurance have to this issue?" And we would say it has a lot, that cyber insurance has the potential to create powerful incentives that drive behavioral change in the marketplace and that fundamentally that is what this Committee, what the Congress, and all of us are trying to accomplish.

The simple act of applying for cyber insurance forces companies to conduct meaningful gap assessments of their own capabilities because insurers will want to know: Do you have an incident response plan? Do you have good protocols for patching software? Are you regularly monitoring your vendor network? And this process in and of itself is an important risk mitigation tool.

Once a cyber policy is purchased, the incentive then shifts to the insurer to try to assist the policy holders to the greatest extent possible to avoid or mitigate attacks. And so you are seeing many insurers now offering an array of services like monitoring and behavioral analytics and rapid response that help policy holders, and the market is really responding. So in 2014, the number of our clients that purchased stand-alone cyber coverage increased by 32 percent over the prior year. And we tracked specifically which sectors of the economy the cyber take-up rates were the highest, and so they are sectors like health care, education, and hospitality and gaming. Each of these industries handles a substantial volume of sensitive data. We also saw meaningful increases in the power and utility sector.

We also tracked pricing trends on the premiums for cyber insurance, and if you read the headlines alone, you would assume that premiums went up meaningfully. And, in fact, year-over-year pricing was really quite stable. Some industries were up, some industries were down. What we did witness in the fourth quarter of 2014 was in the retailing sector in particular, premium prices went up for obvious reasons. And underwriters really began differentiating between those retailers that were implementing the most sophisticated defenses on point-of-sale systems—end-to-end encryption, for example—and those retailers that were not doing so. And, thus, you are seeing insurance market forces really begin to drive incentives and create meaningful reasons to make the type of investments in cyber defense that we would want. And this phenomenon, Chairman, has occurred many times in many industries—workers'

[1] The prepared statement of Mr. Beshar appears in the Appendix on page 54.

compensation, for example. Insurers were part of the bold work to really identify safety protocols that would improve the security of workers in the workplace. And over the last two decades, you have seen the number of fatalities in the workplace drop by over 35 percent. And this is the type of dynamic that we would like to see unleashed in the cyber insurance arena where carriers begin to give companies specific credit for implementing two-factor authentication or other meaningful protections like detonation software. In sum, cyber insurance is one element of many in a holistic risk mitigation strategy.

A second key element, as this Committee has recognized, is information sharing between industry and government. To accelerate the identification and detection of emerging threats, there needs to be greater trust and greater real-time threat information sharing, and it should be, as other witnesses have commented, more reciprocal.

Accordingly, we support the sharing of cyber threat indicators, like malware threat signatures and known malicious Internet Protocol (IP) addresses, provided that reasonable liability protections and privacy considerations are addressed. We believe that the dual considerations of national security and privacy can be fairly and appropriately balanced.

Thank you, Mr. Chairman.

Chairman JOHNSON. Thank you, Mr. Beshar.

Our next witness is Richard Bejtlich. He is the Chief Security Strategist at FireEye. He is also a non-resident senior fellow at Brookings and previously directed General Electric's Computer Incident Response Team. Mr. Bejtlich.

TESTIMONY OF RICHARD BEJTLICH,[1] CHIEF SECURITY STRATEGIST, FIREEYE

Mr. BEJTLICH. Thank you, Chairman Johnson, Ranking Member Carper, Members of the Committee. I appreciate the opportunity to testify today. I am Richard Bejtlich, Chief Security Strategist at FireEye. Our Mandiant consulting service, known for its 2013 report on Chinese PLA Unit 61398, helps companies identify and recover from intrusions.

So who is the threat?

We have discovered and countered nation-state actors from China, Russia, Iran, North Korea, and other countries. The Chinese and Russians tend to hack for commercial and geopolitical gain. The Iranians and North Koreans extend these activities to include disruption via denial of service and sabotage using destructive malware. We have helped companies counter organized crime syndicates in Eastern Europe and elsewhere. Our recent report on a group we call "FIN4" described intrusions to facilitate insider trading. We have also encountered hacker teams for hire and others who develop and sell malicious software, or malware.

How active is this threat?

In March 2014, the Washington Post reported that in 2013, Federal agents, often the Federal Bureau of Investigations (FBI), notified more than 3,000 U.S. companies that their computer systems

[1] The prepared statement of Mr. Bejtlich appears in the Appendix on page 61.

had been hacked. This count represents clearly identified breach victims, and many were likely compromised more than once.

In my 17 years of doing this work, this is the single best statistic I have ever seen as far as just how bad the problem is.

Serious intruders target more than the government, defense, and financial sectors. No sector is immune.

But how do victims learn of a breach? In 70 percent of cases—and this has held up through our own consulting and also through other companies that we work with—someone else, usually the FBI, tells a victim about a serious compromise. Only 30 percent of the time do victims identify intrusions on their own. The median amount of time from when an intruder initially compromises a victim to when the victim learns about the breach—and, remember, most of the time they are being told by someone else. That time, according to our research for 2014, is 205 days. This number is better than last year's count, which was 229 days and the year before, in 2012, which was 243 days. So we are making progress, but intruders still spend about 7 months inside a victim network before anyone notices.

So what is the answer?

Well, as Mr. Chairman mentioned, so-called network hygiene only gets you so far. We need more strategy here, and in my opinion, the best strategy is to prevent as many intrusions as possible, clearly; but we need to quickly detect attackers who evade regular defenses, respond appropriately, before the adversary accomplishes his mission. Strategically significant intrusions do not occur at the speed of light. It takes intruders time, from hours to weeks, to move from their initial foothold to the information that they seek.

So defenders win when they stop intruders from achieving their objectives. I recommend two metrics that we could track to see whether this is the case, to include the Federal Government.

The first metric is tracking simply the number of intrusions or the types of intrusions that occur in a given year. There are many companies I visit, and I ask that simple question. They cannot answer that question.

The second metric is to measure the amount of time that elapses from when the intruder gets into your network and you notice. We want that number to be as small as possible.

Well, how does threat intelligence play into this?

"Threat intelligence" refers to the tactics, tools, and procedures used by intruders to abuse software and networks. It does not depend upon sensitive information about U.S. persons. And I will note that the President's proposal is compatible with this definition of "threat intelligence."

Will that help?

Threat intelligence will help defenders more quickly resist, identify, and respond to intrusions, but only if the organization is postured to succeed. Unless you have a sound strategy, the right technology, people, and processes, no amount of threat intelligence will help you.

There are usually three cases for sharing threat intelligence: from the government to the private sector; within the private sector, and from the private sector to the government. And all three face challenges.

In the government-to-private scenario, I recommend or I encourage the government to grant clearances to private security teams who are not working on government contracts. The government should also augment their narrative style reports—in other words, text and sentences—with appendices that are in machine-readable format so we could facilitate that real-time sharing that was mentioned by my colleagues.

In the private-to-private case, I would second the idea of having more information-sharing organizations in the private sector.

And now we get to the toughest case, and this is the private-to-government case, and it is contentious, for two reasons.

First, companies are reluctant to publicize they have breaches besides what is necessary to comply with laws. So the private sector fears penalties if they disclose. So I would recommend that they not be held liable simply for notifying the government that they have been compromised.

Second, some privacy advocates fear that liability protection will let companies submit customer data to the government. If you properly format threat intelligence, this will not be a problem. In my written testimony, I have an example of a pilot program in the government involving the Department of Energy that we think is doing a decent job working with this sort of information, but I will leave that to your questions.

Again, I thank you for the opportunity to testify.

Chairman JOHNSON. Thank you, Mr. Bejtlich.

Our next witness is Gregory Nojeim. He is the Senior Counsel and Director of the Freedom, Security & Technology Project at the Center for Democracy & Technology. Greg previously served as Associate Director and Chief Legislative Counsel in the ACLU's Washington legislative office.

Mr. Nojeim.

TESTIMONY OF GREGORY T. NOJEIM,[1] SENIOR COUNSEL AND DIRECTOR OF THE FREEDOM, SECURITY & TECHNOLOGY PROJECT, CENTER FOR DEMOCRACY & TECHNOLOGY

Mr. NOJEIM. Thank you, Senator Johnson, Senator Carper, Members of the Committee. I am pleased to testify on behalf of the Center for Democracy and Technology (CDT). We are nonpartisan, nonprofit technology policy organization dedicated to protecting civil liberties and human rights on the Internet. We applaud the Committee for holding the first hearing of the 114th Congress on cybersecurity. It is an important issue. It should be a particularly important issue for this Committee. It can play a key role in addressing the information-sharing problem.

I am going to explain today the role that information sharing can play in countering the threat of cyber attacks. I will identify different approaches to encouraging information sharing as well as the essential civil liberties attributes of a successful information-sharing policy.

Other panelists have already described very well the direct harms of cyber attacks. I will just add one: Major cyber attacks on Target, JPMorgan Chase, Home Depot, and Sony Pictures com-

[1] The prepared statement of Mr. Nojeim appears in the Appendix on page 65.

mand the headlines so much that, in addition to direct harms, these large-scale attacks also threaten to chill use of online services and of the Internet itself.

There is no silver bullet that will wipe away the danger of cyber attacks. As my colleagues have noted, many cyber attacks could be stopped by basic digital hygiene, and Congress should be encouraging that. And a good way for doing that also is the Cybersecurity Insurance Program.

On the other hand, other attacks, the advanced persistent attacks, they will often require the sharing of information about potential threats and how to defend against them.

Cybersecurity information sharing also poses risks to civil liberties. After all, it does involve the sharing of some communications content and of some personally identifiable attributes of communications. As Mr. Bejtlich mentioned, the flow of this information to the government triggers concerns that cybersecurity information sharing could evolve into a surveillance program, and the concern is particularly acute when the permission to share trumps all laws.

We favor a more focused approach: Create specific exceptions to the laws that inhibit information sharing. Start with the Wiretap Act and with the Electronic Communications Privacy Act. They permit communications service providers to share communications information to protect their own networks. But they do not permit them to share information to protect others. That can be fixed with straightforward amendments that we would be happy to work with you on. As other laws that inhibit necessary information sharing are identified, cybersecurity exceptions could be created to them as well.

The broader, riskier approach of trumping all laws that might otherwise stand in the way of information sharing requires exacting civil liberties protections to prevent abuse. All of the major cybersecurity proposals take what we think is the riskier approach of trumping all laws. The White House bill does it; the Cyber Intelligence Sharing and Protection Act (CISPA) did it; and so did Cybersecurity Information Sharing Act (CISA), the Senate Intelligence Committee's bill from last year.

What are those civil liberties protections that need to be incorporated?

First, narrowly define the information that can be shared and include only that which is necessary to describe a threat.

Second, prioritize company-to-company sharing because the private sector owns most of the critical infrastructure that must be protected against cyber attack and because private-to-private information sharing does not create some of the fears about the flow of information to the government.

Third, apply privacy protections prior to any level of information sharing, whether by a private entity or a governmental entity.

Fourth, ensure continued civilian control of the government's cybersecurity program for the civilian sector.

Fifth, require that information shared for cybersecurity reasons be used for cybersecurity, with limited exceptions for law enforcement use to counter imminent threats of bodily harm, and to prosecute cyber crime.

Sixth, be careful about authorizing countermeasures. Countermeasures that could amount to hacking back against an individual or entity suspected of hacking into one's own system should not be authorized. They create more problems. They open a Pandora's Box.

And, seventh, create strong privacy procedures governing the sharing of information by governmental entities.

With respect to these seven factors, I think the White House bill does a better job on all of them except for prioritizing the company-to-company sharing. We have specific concerns with the White House bill. It could be a lot better. But it was a significant improvement over the Senate's last look at information sharing, which was CISA.

I close by observing that today is Data Privacy Day. It is a day observed around the world for promoting data privacy. Let us work together to ensure that cybersecurity information respects data privacy, even when it is shared, and helps preserve the Internet as a great engine of communication, innovation, and prosperity. Thank you.

Chairman JOHNSON. Well, thank you, Mr. Nojeim. Again, thank you to all the witnesses for your thoughtful testimony.

To give more Members a chance to ask questions, we are going to limit the time for questions to 5 minutes each. Also, to remind veteran Members and let the new Members know what the tradition of this Committee is in terms of order of questioning—it is the people here in attendance when the gavel drops. It will be in order of seniority, rotating between sides. And then after the gavel falls, just in order of appearance.

So, with that, I am not going to ask questions so that more Members have a chance to ask questions. I will turn it over to our Ranking Member, Senator Carper.

Senator CARPER. I want to thank the Chairman for yielding his time to his Ranking Member.

We do a lot of oversight work here. We do a lot of asking of studies by the Government Accountability Office (GAO) and others. Sometimes we just send letters, and I noted a change of behavior, and sometimes we legislate. Last year, when we were in the 113th Congress, we legislated in three or four different Bills with respect to cybersecurity. We sought really to bolster the capabilities of the Department of Homeland Security (DHS) on that front.

We passed three or four modest bills, but I think together they are very meaningful. One was to make the Cyber Ops Center of DHS real and meaningful, codified it. I think that is a very good thing. We also have enabled them to strengthen their workforce. And a third area that we have worked in is to better enable them to protect the dot.gov domain. And so those three things taken together I think are helpful.

We tried to pass information-sharing legislation, as you know, in the House and the Senate. We got it out of Committee in the Senate but not through the full Senate.

We have shared jurisdiction on that issue, and some would say we actually have maybe more jurisdictional claim on information sharing than other committees. But we are going to be working fairly hard in this vineyard very soon.

We have three places to look—maybe more than three. Your job is going to find more places to look in terms of developing good policy, but, one, the Administration's proposal; two, the Senate Committee's bill, the Intel Committee bill from last year; and then the work that the House has done.

I am going to ask each of you, if you would, using those three as maybe a touchstone for us in cobbling together smart legislative policy on cyber, especially on information sharing, what would be one or two major points that you would have us take into mind to consider as we do our work. Mr. Gordon.

Mr. GORDON. Thank you very much, Senator. I agree there was great progress last year. I would love to see that bill with information sharing.

If I look across the bills—CISA, CISPA, and the President's proposal—the areas that I would highlight as—first, there are many in common, so I am not going to cover those, but the differences or the areas that I would highlight, one, I think there is greater or lesser emphasis on real-time sharing, and I would propose that that is very significant in terms of the speed at which attacks cascade across—within industries and across industries. I believe that real time is very important.

Second—and a number of people have mentioned it here—I think it is important that the construct not just protect in terms of liability entities sanctioned by the government, but also that it encourages and facilitates company-to-company sharing, that is to say that the liability protections would extend to companies sharing among themselves, not just with another entity.

The third and fourth I would highlight very quickly. One is protecting sharing. Liability in terms of sharing is important. But I also believe protecting acting within one's own network is also important. So it is not enough simply to share, but one has to be able to actually act on what is shared, and I would emphasize that.

And then the final one, which a number of folks I think have mentioned as well, that for us is very important is the bi-directional nature of sharing. I believe that as I reflect on it, both the CISA and CISPA bills did have a great deal of focus on basically requiring the government to get more active in sharing, particularly in classified indicators, shared in the right way; whereas, I believe the President's proposal is silent on that. And I believe that bi-directional sharing I feel is very important, and for us there are the threats that we experience that we can share across the private sector. Typically those occur while we are under attack, so what we are sharing is essentially information about an attack that is unfolding. What the government has access to that simply is not known to us are the attacks that could take place and the nature of those attacks. I think that would be a tremendous value-add. So I would include the bi-directional sharing in terms of emphasis.

Senator CARPER. OK. Thanks. Mr. Charney.

Mr. CHARNEY. I agree with the points made. I think certain bills did not go far enough on the civil liberties side. I worry a little with the Administration proposal that we not impact current industry-to-industry sharing that is really working well. Marc's points were spot on. The only other thing I would add is the international flavor of this. As a company that has customers all over the world and

who is constantly combating international threats, it is very important to recognize that whatever the Congress does, others may emulate.

And so, for example, the U.S. Government could say, "Tell us about every vulnerability you know about," and you could say, "Well, that would be really interesting to know." And then every other government in the world will ask for the same thing, and suddenly things can become very difficult. And so thinking about the international implications of what is done here is super important.

Senator CARPER. All right. Thanks. My time has expired.

Chairman JOHNSON. No; go ahead.

Senator CARPER. Mr. Beshar, and maybe I would ask you to just short it up just a little bit, if you will, please.

Mr. BESHAR. Very briefly, Senator Carper, two points.

First, there is a hierarchy of data that would be of interest to the government that sits in these companies' hands. And if you try to focus on the cyber threat indicators and begin this journey there as opposed to trying to go deeper on the data that is part of this exchange, I think that will be a very fruitful step.

Second, the idea that in the President's bill there are obligations that all of our companies have to try to strip out the personally identifiable data, I think that is a very constructive step forward, as Greg has identified.

Senator CARPER. All right. Thanks.

Mr. BEJTLICH. Senator Carper, briefly, I would encourage whatever resources are necessary to help the FBI with its notification mission. Speaking as the spokesperson for the intel community, that third-party notification is just very valuable.

And, second, I would encourage whatever is required to get more prosecutions. I do not think it is necessary to lengthen prison times and that sort of thing. I think we just need to make better use of the laws that are there and to get more of these bad guys.

Senator CARPER. Good. Thank.

Last, but not least?

Mr. NOJEIM. So I think I am going to focus just on three issues:

Stripping out irrelevant personally identifiable information (PII) before you share a cyber threat indicator. The White House bill does a pretty good job of that. CISA did not require that.

Second, on use restrictions, making sure that if a company shares information for cybersecurity reasons, it is used for cybersecurity. There are some national security uses that are cybersecurity uses. Those should be allowed. There are some law enforcement uses that are cybersecurity uses. If you want to prosecute a cyber crime, that serves a cybersecurity purpose. That should be allowed.

Countering an imminent threat to a person, that should be allowed, but not much more. And I think the White House bill did a much better job on that score than did CISA.

And, finally, on hacking back, making sure that if countermeasures are going to be authorized, they can only operate on your own network. You do not want a countermeasure that could, when stolen from your network and placed on somebody else's computer,

including a victim's computer, encrypt or damage data on that computer.

Senator CARPER. Thank you all very much. That was very helpful. Thanks.

Chairman JOHNSON. Thank you. And now we will stay more on time. Senator Lankford.

OPENING STATEMENT OF SENATOR LANKFORD

Senator LANKFORD. Thank you all for being here and being a part of this. Let me ask some cost questions and the gain from this. We are talking about between a hundred—estimates of $100 billion to $450 billion in costs a year somewhere right now on the cyber attacks. Give me a rough ballpark on the breakdown of that between damages that are paid out that are preventable if we have this enhanced information sharing and those that are not preventable because of a zero-day attack and we are stuck, we are at the beginning of it.

So what I am trying to affirm is we get this in motion, we get better information sharing. What difference does it make economically? And anyone can attack that.

Mr. GORDON. That is a great question. I am not sure I can answer it directly in terms of a percentage. But what comes to mind for me is what percentage of those losses are repeat attacks, meaning they happen more than once. And I would say in the right construct of information sharing, bi-directional real time, a very high percentage of repeats—that is back to my comment earlier, which is one company's attack can become the Nation's defense if we do it the right way. It will not prevent that first attack, but it can prevent all the ones that follow potentially.

So I cannot answer specifically the dollar amounts. I do not know how to break that down.

Senator LANKFORD. So the guess here is to try to figure out how many attacks that are out there are repeat attacks.

Mr. GORDON. That might be a way to look at it.

Senator LANKFORD. So any ballpark on that you would see from just what you have seen or anyone has seen on cyber attacks out there that are known threats, or were they just not known to you or to those companies?

Mr. BEJTLICH. Senator, at Mandiant, just even our own customer base, when we do a response, depending on who the actor is, if it is the Chinese or the Russians, they are going to be back. In some cases, their recidivism rate is as high as a third. So that is just against one company is hit, and then they are hit again by the same group after we leave.

Senator LANKFORD. OK. Let me ask a question. What is next on this? Information sharing, I think there is fairly common agreement we need to have some level of information sharing. It is how to protect personally identifiable information and such. What is the next level on this? Where does this go?

Mr. CHARNEY. I can take that. I think to deal with advanced persistent threats, you need a very robust security program that has three elements: you need high-level protections in place; you need great detective capabilities, because the bad guys will keep attacking; and you need very fast response processes. And what we have

found, of course, in many of the hacks that occur today, even if they are called "advanced persistent threats," they are not all that advanced. People attack unpatched systems. People are running old operating systems and old software. And we need to get all boats to rise.

The challenge has been, of course, that for 20 to 30 years people have built networks with tough, hard perimeters, but the middles are really soft. And in these advanced persistent threats, the bad guy comes in and gets a foothold in the network and then moves across the network.

So the information technology (IT) industry and users of IT are all focused on a few core things that are starting to happen.

First, you need multi-factor authentication. You need to get rid of user names and passwords because they are just too easy to guess or calculate and break in.

Second, we need what we call "domain isolation." If someone attacks and gets in somewhere, they should not be able to move everywhere.

And, third, we have to do a much better job, as people say, of detecting things so we can respond quickly. So hopefully with more information sharing you put the detections in place, and then you can act much more quickly and prevent a lot of the damage.

Senator LANKFORD. OK. Let me ask a followup question to that. With a lot of the issues based on the fact that companies are not doing basic patches, they are not doing some of the things that are commonplace, then we have this extra layer that we are adding to this with personally identifiable information that they have got to be able to secure that, sequester that away, and so that does not get out as well. If they are not doing patches, how diligent are they going to be to make sure they are also protecting the information once it gets shared that people truly have their privacy protected as well?

Mr. CHARNEY. Well, so it is absolutely clear that if you do not have a good protection program, you are going to lose valuable data——

Senator LANKFORD. Right.

Mr. CHARNEY [continuing]. Whether it is economic data or personally——

Senator LANKFORD. But that is happening right now.

Mr. CHARNEY. That is happening right now, and you need to—there are two things to think about. One is raising the protections, which is what information sharing is supposed to help do, so that you can prevent that. But the second thing is that the security model is changing across the industry in two respects. One is in some cases you actually do not need that personally identifiable information to engage in a transaction.

So, for example, in the credit card arena, there are companies who are looking at—and PayPal does this already—not giving the credit card to every merchant in the world, but just passing an authentication code to authorize the payment. And if you do things like that, then it is much harder—even if you steal the information, you are not getting anything that is replayable and reusable, and you will see that coming in many new ways because we are going to start attaching identities to particular devices. People have tab-

lets. They have phones. They have portable PCs. And if we can tie your credential to that device, then if someone else tries to use that credential from another device, it will not work.

So there is a lot of preventative things we can do from protecting networks to thinking about information differently and how we protect it.

Senator LANKFORD. Thank you, Mr. Chairman.

Chairman JOHNSON. The remaining order will be Senator Booker, Senator Baldwin, Senator McCain and then Senator Ayotte. Senator Booker.

OPENING STATEMENT OF SENATOR BOOKER

Senator BOOKER. I want to thank the Chairman. This is a fantastic and very important hearing that we are having. I appreciate your leadership, and I want to thank my Ranking Member as well.

Gentlemen, it is the balance, again, between privacy and security, and I think that there is a huge tension in this area. The degree and nature of the attacks are startling and stunning. And I just have really quick questions that should be very brief. But the first is: What role does the government have, being that so many mistakes are being made in what is called the hygiene area? It is remarkable to me how many mistakes we make, and I sat with my staff and realized even for my own passwords I was not using dual authentication methods and the like. But so many businesses out there just are not doing the basic common sense that would prevent a lot of this from going on.

And so I am wondering, in just the idea of the role of government, what could we be doing to either incentivize or mandate levels of hygiene? Or is that, in some of your opinion, not the role of government at all?

Mr. NOJEIM. I am going to start with that. I do not think it is a good idea to mandate levels of hygiene. I think that the mandates will rapidly grow outdated, and they will become the floor instead of the ceiling. Companies are going to innovate. They are going to come up with new ways to protect data, and I think that you want to encourage them to do that. Give them tax credits, give them other assistance, but I do not think you should try to mandate exactly what they do.

Mr. BEJTLICH. I would concur with that, Senator. The insurance example is a great one. If someone keeps breaking into my house, it is going to be tougher for me to get a premium because they can tell I do not lock my doors and that sort of thing.

The government should restrict itself to the things that it will not let the private sector do, which is hack other people, or prosecute or do those sorts of things. So I think the role of the government should be to do those things that are unique to the government, to do the threat mitigation by either deterrence or by prosecution or that sort of thing, and the private sector can work on the things that we are good at.

Senator BOOKER. Yes?

Mr. CHARNEY. I would add one more point. The government can lead by example. The government is a large enterprise, and it has customers, too, but their customers are called "citizens." And citizens file taxes online and file for benefits online and want informa-

tion from the government. So the government could do a better job, I think, of adopting the latest technologies, managing their systems really well, and leading by example.

Senator BOOKER. OK. Let me just shift for a second.

And, by the way, 14 months in the U.S. Senate, we are not leading by example with a lot of the practices I see. But I just want to then to the perverse business incentives and the idea that you provide some kind of full liability or when it comes to information sharing with the government, are we creating an environment where we are going to promote oversharing with government some of the privacy information? And I am really worried about that. In many ways, it is just giving the government access to another level of domestic surveillance by creating perverse business incentives for oversharing. Is that a concern?

Mr. GORDON. The way we look at sharing, if we actually look at both what we share and what is shared with us and what we would like to amplify over time in terms of sharing, what we are essentially talking about are things called "cryptographic hashes" or pieces of software code. There is nothing associated with customers in any shape or form in terms of essentially what is effective for sharing. And so I think even the way the prior legislation speaks to pulling out PII, our view is—and I went back and looked at what we have shared and what we like to share more of—it is indicators of attack, indicators of compromise, and the like that we do not see that there is any real issue at the end of the day as long as we focus on sharing that type of information.

Mr. BESHAR. Senator Booker, we would concur with that, that even in the last year, the extent of the threat has intensive; that if there are going to be attacks on critical infrastructure and it is less graffiti and financial crime and more threatening of power grids and the like, then that balance has to at least be calibrated. And as the other witnesses have said, I think by stripping out the personally identifiable data, you legitimately address the privacy concerns that are there, at least with respect to cyber threat indicators.

Mr. GORDON. I would like to add one more thing and think about it this way: If somebody broke into our data center and started attacking our computers with an axe, we would report the fact that they have done that. If they broke into our data centers and started siphoning off customer information, we would report the same thing. The analog for me here is I am reporting the axe that got used and the fact that siphoning is occurring. I am not even reporting because I do not know in most cases who it is.

So that is the nature of what we are talking about sharing essentially, is the fact that an axe was taken to our data center.

Mr. NOJEIM. Senator, there are three steps here.

First, you narrowly define the information that can be shared. It has to be necessary to describe the threat.

Second, you require companies to look for and strip out any personally identifiable information that is not relevant to the threat.

And, third, you make it so the liability protections only operate when the companies play by those rules. That would do the trick.

Mr. CHARNEY. Can I add one point to that? There are times when we do need to do attribution and find source. So if you only share

anonymous data, you can protect and detect, but you cannot deter. And that is why in our testimony, one of the things we point out is when you need to get identifying information so you can do attribution and take action, we have legal processes, court orders, and other things that are designed to protect civil liberties and strike the right balance.

Senator BOOKER. Thank you.

Thank you, Chairman.

Chairman JOHNSON. Senator Ernst has returned, so we will go to you next, and then Senator Baldwin.

OPENING STATEMENT OF SENATOR ERNST

Senator ERNST. Thank you, Mr. Chairman. Gentlemen, thank you for being here today. We greatly appreciate your expertise in this area.

Iowa just in recent years has really become a tech hub. We have Google located there, Facebook. We have Microsoft coming soon to West Des Moines. We also have many financial institutions, insurance companies, both large and small. We have a lot of small business.

So when we are talking about this, we largely think about those larger entities, but what can we do through a voluntary process to assist and encourage small businesses to voluntarily share information and do it in a way that is not cost prohibitive or time prohibitive for those smaller groups? I would love to hear your thoughts on that. Thank you.

Mr. BEJTLICH. Senator Ernst, this may sound counterintuitive because a lot of people have worries about the cloud. But to tell you the truth, the cloud may be—assuming you use a worthy cloud provider who has their act together, the cloud is of great benefit. I advise many small startups, and they do not build out networks the way we did 10 or even 15 years ago. They do everything on the cloud.

So if the cloud providers—Google, Microsoft, Amazon, and these others—have a robust security program and they protect—or the users protect how they access those services using two-factor and other methods, that is actually a pretty good scenario. It takes the IT duty away from that mom-and-pop shop and puts it in the hands of some professionals.

Mr. BESHAR. Senator Ernst, I am proud to report that we have 1,500 employees in Urbandale, and it is a terrific workforce and a great asset for our company.

Senator ERNST. Yes. Thank you.

Mr. BESHAR. It is similar to Senator Lankford's question, that it is difficult to visit burdens on small and mid-sized enterprises that are perhaps customary and commonplace for the larger companies.

At the same time, one of the real takeaways from 2014 is that the security of the larger organizations is really dependent upon smaller enterprises, that many of the companies that have been in the news have been attacked not through the front door but through the side door of the back door of the vendor network. So things like the Administration's cybersecurity framework, the National Institute for Standards and Technology (NIST) framework, I think is a helpful, relatively straightforward tool to try to assist

small and medium enterprises to go through some of the steps that we are talking about.

Senator ERNST. Any other thoughts?

[No response.]

Thank you, Mr. Chairman.

Chairman JOHNSON. Senator Baldwin.

OPENING STATEMENT OF SENATOR BALDWIN

Senator BALDWIN. Thank you, Mr. Chairman and Ranking Member, for holding this hearing. I really appreciate it.

I have a couple questions I want to get out there, but I wanted to actually start, having heard the response to Senator Booker's first question about the appropriate government role, and I just want to make sure I understand your responses as really coming from the business enterprises that you have the expertise in, because, as I have looked at it, I have seen perhaps areas where we should have a more robust government role when we deal with things like—I know, Mr. Beshar, you mentioned the electrical grid, critical transportation infrastructure, some of our infrastructure. Is that fair that you are really answering for your industries and not—or is this advice throughout no matter what type of attack we are looking at? I just want to clarify that for the record. Do you want to just go down the—Mr. Gordon?

Mr. GORDON. The role of the government question, in the context of hygiene, which I think was a substantial part of it, I would concur. I feel that, first of all, the definition of "hygiene" is very dynamic. I mean, it literally changes day to day. I do not think the government should have much of a role in that. And I would say the market has very quickly taken care of that in terms of boards paying attention to hygiene. I think that is an increasingly smaller problem.

The other dimension, which I think is outside the purview of this discussion, but I do think the question of the role of the government in preventative action and in deterrence, I think that is still unclear probably to some greater or lesser degree, not the role of the private sector.

Mr. CHARNEY. In my written testimony, I talked about the four roles of government relative to IT, because in addition to being a large enterprise with customers, they also do have a traditional public safety and national security responsibility. And, I am a big fan of market forces, and they work great for innovation, but it is hard to make a market case for the cold war. When you have a national security imperative, the government often has a major role to play, and part of that is that, as a large enterprise, they are attacked a lot. As former Chief of the Computer Crime and Intellectual Property Section, I can tell you that, in the early days, the two most attacked agencies were the Department of Defense (DOD) and the National Aeronautics and Space Administration (NASA) because NASA had cool stuff. And the government has this information and often knows of threats and shares it with industry, which makes us more effective in protecting the ecosystem and our customers.

And then there is also the question of how to deter particularly these nation-state attacks. Microsoft has been very vocal that we

need norms for the Internet. We have norms for State behavior in a range of areas, like money laundering and weapon of mass destruction. We actually do not have norms for cyber activity. And so we see nation-state activity that would be very hard for the private sector to fend off. I mean, nation states can put spies in your organization. It is well known that a Russian spy was arrested at Microsoft. How does a private company fend off a well-funded, persistent nation-state attack?

And so the government can help by helping establish those norms and in the right places taking steps to help, regulate the behavior of others, so to speak.

Senator BALDWIN. OK. I am hoping to get to another question, so either real quick, or——

Mr. BESHAR. Please.

Senator BALDWIN. OK. For Mr. Nojeim, you talked—I really appreciate your analysis of the three principal proposals and your recommendations to strengthen them. Just narrowing in on the Obama Administration's cybersecurity proposal, obviously critical details have yet to be finalized in that, including for privacy guidelines. So I am wondering what are your recommendations for, first, defining what constitutes personally identifiable information; and, second, for sharing cyber threat data that includes such personally identifiable data.

Mr. NOJEIM. So we went through an exercise of trying to list all the types of personally identifiable data that we are talking about. I do not think that Congress should try to go down that road. We did not know years ago that IP addresses could become personally identifiable with the additional information. Maybe some people knew it; maybe some people did not. But the fact of the matter is that sometimes the aggregation of information can make it personally identifiable when people thought it was not before.

So rather than going down the road of trying to list the particular categories of personally identifiable information, I think it is better to require that personally identifiable information be stripped out and then task DHS with coming up with the list through a Notice and Comment process, and that list will change over time, and everybody will know it will change over time. So I do not think you want to go down the road of trying to list that in the statute.

And then when it comes to removing it when it is not necessary to describe a threat, I think that is going to happen naturally in the automated process of sharing threat information. Companies are going to develop systems that other companies will buy that they will use to share this threat information. They will have to be able to describe the threat. And those same systems that describe the threat can be used to filter out the irrelevant information.

Chairman JOHNSON. Senator McCain.

OPENING STATMENT OF SENATOR MCCAIN

Senator MCCAIN. Thank you, Mr. Chairman. I thank the witnesses.

A week ago or a couple weeks ago, the Armed Forces Network was hacked into and not only did radical messages show up on the screen, but also names and addresses of individuals. And I do not

think a lot of Americans know that Armed Forces Network is at every base, every ship, every defense installation of any size, not only in the United States but in all our bases all around the world.

So it was a pretty clever action on their part and I think pretty sophisticated, and not only did it give them a propaganda coup, but most people believe that Armed Forces Network is run by the Armed Forces. It is not. It is contracted out to a commercial organization. And it not only was propaganda, but also when names and addresses of people are put out, it obviously poses a direct threat to literally their lives.

What happened? What could we have done to prevent it? And what do we need to prevent something like that in the future? Is that you, Mr. Charney, or Mr. Gordon? Whoever wants to take that.

Mr. CHARNEY. Well, first and foremost, many large organizations outsource IT functions, and it is absolutely crucial that their outsourcing contracts have requirements for security and privacy that meet the needs of the party that is hiring the contractor.

Senator MCCAIN. So the Pentagon should have been smarter.

Mr. CHARNEY. I have a lot of friends in the Pentagon. I think they are great. But certainly their contracts should require that the information be protected at the right level, and now with things like the NIST framework, the International Organization for Standardization (ISO) standards, there are more and more ways to audit and measure the security controls in an environment.

And so, for example, for a lot of our cloud-based customers, they now ask to see our audit reports, which we share, because they want to make sure before they entrust their data to us that we are taking the necessary steps to protect it. And we have to enforce that through contracts with customers.

Senator MCCAIN. So, again, whoever in the Pentagon let that contract did not let the right contract.

Mr. CHARNEY. Either that or the term was in the contract but no one evaluated whether the contractual terms were being followed.

Senator MCCAIN. Mr. Gordon, do you have any comment?

Mr. GORDON. Not a lot to add other than when you look at the most common attack factors, websites is one. One of the most prominent is websites, so companies put a lot of energy into a set of controls around that. I am not familiar with actually what the vulnerabilities were that were breached, but I agree with Scott. I think that the right third parties and businesses put those controls in place to prevent those kinds of breaches.

Mr. BEJTLICH. Senator McCain, I think on paper almost anyone looks good, but the proof is when you can test it and find out if your defenses are strong. I am sure you are familiar with the term "red-teaming." If someone had red-teamed against that user account or a system or a network and found, wow, it is very easy for me to get in here, I am not going to cause any damage, I am going to report back to the owner, it took me 5 minutes to break into this system, and you fix the problem before the bad guy finds out. That is one way to avoid it.

Senator MCCAIN. Anyone else?

[No response.]

Well, it was interesting that General Dempsey, our Chairman of the Joint Chiefs of Staff, recently said that we have a technological advantage in every form of warfare over our potential adversaries except for one, and that is the issue that we are discussing today. I thank you.

OPENING STATEMENT OF SENATOR AYOTTE

Senator CARPER [presiding]. Senator Ayotte.

Senator AYOTTE. Thank you, Chairman.

Senator CARPER You are welcome. [Laughter.]

Senator AYOTTE. I wanted to followup on a comment that Mr. Bejtlich made about law enforcement capacity here, and you had said we do not need more laws, what we need is greater prosecutions and an ability of the FBI and other law enforcement agencies to prosecute these individuals.

I was Attorney General of our State, and in the limited cases that I was involved in on these issues, the prosecutions are very challenging. As you know, often the actor can be from another country, and we are not even talking about nation-state actors there, just the location.

What thoughts do you have as to how we can better help our law enforcement agencies have the right tools to pursue appropriate cases, so that we have some examples that we are not just allowing these things to happen?

Mr. BEJTLICH. Thank you for the question, Senator. I think there are a couple angles to it. One of them is, as you mentioned with overseas actors, international cooperation. If you are a hacker and you are in the United Kingdom and you are attacking the United States, that is a bad situation for that hacker. We are going to work with our partners and are going to get them back. If you are in an Eastern European country or some other location—so international cooperation is first.

Second is training. You need to be trained to do this sort of work. You need to know how to carry off a successful prosecution, what are the defenses that could be there, and how to collect the information properly. It is very similar to what we saw in the intel world in warfare. Guys used to go in, smash the computers, and then they would bring back fragments, and you realize you could not use it. You had to teach them how to collect evidence and that sort of thing.

And the third part is you have to make it a career path. We saw this with the turnaround in the FBI now where it is now a career path to be an intel person; it is a career path to be a cyber person. You need to have that sort of recognition and success for following those.

Senator AYOTTE. Thank you. I was very interested in the discussion we had that Senator Ernst asked about, the challenges for smaller and mid-sized businesses. Having been briefed, for example, on the Sony hack—that obviously was a nation-state actor, but, frankly, SONY is a larger company and even some of our larger companies do not have all the protections in place that need to be there. And so, there are challenges for smaller and mid-sized businesses. You have talked about the use of the cloud-based system in terms of resource efficiency for smaller companies.

As we look at more of our companies moving to that, what are the security challenges we are going to have to be aware of with the cloud-based system that we should be focusing on? Because, as you know, getting into the system from the smaller connection is probably the easier way to do things.

Mr. CHARNEY. So Microsoft, of course, offers large-scale cloud services, and people often ask me, "Is the cloud good or bad for security?" The answer is yes.

It is good for security because, as mentioned earlier, because it is core to our business and we have a lot of security expertise. We probably are more rigorous about security than many companies might be.

At the same time, it is important to understand that in the cloud model you have a multi-tenanted environment. You have a lot of customers using the same cloud service, which makes it a very rich target.

Senator AYOTTE. Right.

Mr. CHARNEY. And so we do things to make sure that our customers' data is segmented from one another and prevent that lateral movement.

But the other important thing is that, even when you use the cloud, security becomes a shared responsibility. What I mean by that is a small business might issue its user names and passwords to its employees, and if an employee loses that password to a bad person, that person can log on as that employee. The cloud will not know.

Senator AYOTTE. Right.

Mr. CHARNEY. It looks like an authorized use.

So we have been committed for quite some time to providing more security technologies that are just secure by default in our newer products—and I talked about this a little earlier—identities that cannot be stolen because they are bound to machines. We have to get to a place—I am all for user education. It is a wonderful thing. But I think we put too much of a burden on end users to manage security when it is actually a complex undertaking.

Senator AYOTTE. You have all talked about what you see as a problem with the Administration's proposal not allowing sharing and liability protection among companies. So in a cloud-based system, is that the way the legislation drafted is particularly acute? Or does that not matter because you are thinking about transmitting the information at a higher level?

Mr. CHARNEY. So for us, we have to be clear. We have two types of information. We have our information about our network that we can share as we see fit, even if we take some risk in sharing. And Microsoft actually does a lot of sharing today. We have programs where we share threat and vulnerability information with customers, with governments, and others. We share our source code with governments as well. So we can accept that risk.

At the same time we have customer information, and they have expectations, usually enforced through contractual terms, that they do not want us using their data in any way without their permission and consent.

And so when we look at some of this information sharing, we want to make sure that the information we share today, which is

substantial, is not disrupted by a new regulation or regime that says, for example, you can only give data to DHS. Well, no, we want to share data with our partners all the time, and we do, so do not disrupt that. It does not solve the problem of sharing customer information. That we will not do without the customer's permission, and we want to make sure that any regulatory regime respects that contractual obligation, because the biggest problem we have, as a global company, I go overseas all the time, and customers in other countries say, "Will you turn over our data to the U.S. Government?" That is what they are worried about. And when the answer is sometimes yes because we could get a court order or other things—we are fighting a case like this right now involving a U.S. order to turn over data from our Irish data center, a customer e-mail. it is not our data. It is the customer's data. And if we do not protect the privacy of that information, then what happens all over the world is people say, "So I should use a local provider, right? Because if I use your cloud service, you are a global company; you are headquartered in the United States. You are just going to give all our data to the U.S. Government." And what will happen over time is American information technology products and services that have been so successful around the world, well, in all those other parts of the world people will say, "Whoa, maybe we are better off with local technology, not being compelled by the U.S. Government." And that in the long term for America would be a terrible thing.

Senator AYOTTE. Thank you very much for clarifying this. I appreciate it.

Senator CARPER. Senator Ayotte, I think we are going to wrap it right there. Would you all just stay in place, and, Senator, we are going to take a real quick recess. Senator Johnson has run to vote. He will be right back, and when he does, he will resume, and I know he has some questions. And I might join you back again, too. Thank you very much.

Senator BOOKER. Mr. Chairman, is the vote imminent, or do we have a chance for one more round?

Senator CARPER. The vote started 11 minutes ago. I think we have 3 or 4 minutes left on the clock.

Senator BOOKER. Being that I cannot come back, may I ask one more?

Senator CARPER. You may go ahead, and when you have finished, just recess unless Senator Johnson is back.

Senator BOOKER. That is a lot of power you are leaving me with, sir. [Laughter.]

Senator CARPER. I have every confidence in you.

Senator BOOKER [presiding]. Thank you very much.

Gentlemen, just real quick. I have seen how perception problems with private business affect those businesses' abilities to operate overseas. And I have seen comments by high-level officials here that then make other countries demand that our American companies have servers located in their country as well.

Do you have any concerns about us sharing information, companies sharing information with the Federal Government agencies, then making foreign countries more concerned about those companies operating in their nations?

Mr. BESHAR. I think it is a legitimate consideration, Senator Booker, so the draft legislation really speaks about exempting company that provide information from U.S. civil and criminal liability. If there is data from Europe or other parts of the world that is embedded in some of the information, a question at least arises of the scope of that liability protection.

Senator BOOKER. OK. Any other thoughts of the child that it could be creating or something we should worry about?

Mr. CHARNEY. Well, we have had to grapple with this problem post the Snowden disclosures where government and customers all over the world have expressed concern about relying on U.S. technology. And we have been very clear that we do defense, not offense. We do not put the back doors in products. We do not turn over encryption keys.

Where you can get stuck at the end of that discussion is if the U.S. Government does compel the production of data and does it with a non-disclosure order, there is some risk to the foreign enterprise that their data will be turned over to the United States without notice.

Senator BOOKER. Right.

Mr. CHARNEY. And that does worry them. What we have tried to do is explain to them, because I think this is true, government access is a business risk. It is really what it is. I was with a group of chief security officers in France, and I knew some of them were running very old technology and were not current on their patching and hygiene. And they started talking to me about U.S. Government access if they put their data in our cloud. And I said, OK, so you have networks that are wide open and hackers can get in and steal all your stuff, but you are worried about putting it in my more secure cloud because the U.S. Government might get it. Who are you more worried about—hackers or the U.S. Government? What business are you in? I mean, if you are in the terrorism business, you should be worried about the U.S. Government. But it still does create friction in the system.

Mr. NOJEIM. After the Snowden disclosures, a number of U.S. companies said, "We are not going to voluntarily turn over customer information to the National Security Agency (NSA)." OK? Now along comes cybersecurity legislation, and some of the iterations of the legislation say it is all voluntary, companies will voluntarily share information; some of the information is going to be from their customers. So if a company is going to play by those rules, how can it promise that it is not going to share information with the NSA if the legislation says anything you share with a government agency for cybersecurity reasons must immediately be shared with all these other agencies, including the NSA?

That was a problem in the CISA bill, the Senate bill that never came to the floor, that I do not think you want to repeat.

Mr. GORDON. I come back to the nature of what we are sharing, which is attack and threat information, and the sharing of that information only enhances our security for our customers in the United States and around the world. That is how we think about it.

Chairman JOHNSON. [presiding]. Thank you for holding down the fort there, Senator Booker.

I do have a number of questions I would like to put forward until the next vote is called, and then we will wrap up the hearing. So, again, I just want to thank all of you for coming here and taking time and really preparing some very thoughtful testimony and, I thought, really good responses to questions.

Mr. Nojeim, let me test my theory in terms of us all sharing the same goal. I think it is just true that if we do not get this under control, if we allow cyber attacks to continue, the threat in terms of loss of privacy really is even greater, correct?

Mr. NOJEIM. I think that if there was a major cyber attack like the scale of what triggered the attack on—it is the cyber equivalent of the attacks on the Twin Towers, that we would end up with a cyber PATRIOT Act.

Chairman JOHNSON. So we share the same goal. Here in government we can pass a law that can help. It is not going to be a panacea. It is not going to solve all the problems. But I think if everybody on all sides of this issue, if we work together, focus on that goal, let us face it, another—I hate to single out instances, but another Target instance. Their privacy is just destroyed. So we do share that same goal of trying to get to a particular result.

Mr. NOJEIM. We do.

Chairman JOHNSON. I want to ask all of you this. When you take a look at the White House proposal, what is coming out of the Senate Intelligence Committee, that is what we are going to be dealing with here in the Senate, either of those two proposals or some kind of combination.

What is going to be the biggest threat in terms of us crossing the goal line with a piece of legislation? I will start with you, Mr. Nojeim.

Mr. NOJEIM. The biggest threat that you are trying to avoid or the biggest problem in the bill?

Chairman JOHNSON. I would say the biggest problem in the bill as well as the outside interests in terms of attacking whatever is presented. In other words, what are the poison pills in some of these bills? What do we need to be worried about? What do we need to work on?

Mr. NOJEIM. Here is what I think you need to work on:

First is ensuring that you properly define the information that can be shared and that you ensure that any irrelevant personally identifiable information is removed prior to the share.

Second, make sure that whatever legislation, whatever rules govern the sharing of information within agencies of the government, that those procedures are clear and that they are strong and that they protect privacy.

Third, I think you should prioritize company-to-company sharing—do more on that score. And I think also that you have to be mindful of the role that the intelligence agencies are going to play in the information-sharing scheme.

I think you want to ensure civilian control, and the best way to do that is to ensure that the shares, the initial information shares, go from the private sector to DHS, and that DHS then applies privacy procedures to the data before any of it is reshared with any other agency.

Chairman JOHNSON. OK. Well, thank you.

Mr. Charney, I will give everybody a chance to answer that question, but we had an interesting conversation in terms of the necessity of sharing personal information in terms of what information we are talking about sharing. And you said there is no need whatsoever in terms of sharing personal information if we are just trying to prevent attacks. In other words, if we are sharing those threat signatures, no personal information is required. But if you want to go solve the crime, if you want to go find the bad actors, that is where you might need personal information. Is that correct?

Mr. CHARNEY. Yes, that is correct, and also just to be clear, sometimes an attack indicator is an IP address, like attacks are coming from this IP address, so we will go look at our network to see if that IP address is reaching out to us. And in some places, IP addresses alone are considered personally identifiable information.

I think in the United States we more try to focus not on the IP address, but does it combine with other information to point to a person. And I think the way to solve this problem generally about using PII is to make sure that when the government wants to get personally identifiable information, it uses the transparent, judicial procedures already in place with which we are all familiar and balance the competing interests between government access to PII and privacy.

Chairman JOHNSON. In other words, you go to the court system, you get a warrant in order to do that. Mr. Nojeim, does that——

Mr. GORDON. There is——

Chairman JOHNSON. I just want to ask Mr. Nojeim, does that comport with what you would be willing to do or agree to?

Mr. NOJEIM. You do not need a warrant for the IP addresses. It is a lesser process.

Scott, I am not sure that it is going to work that way. At the end of the day, IP addresses are often needed to investigate a cyber attack to find out where it is coming from. Companies are going to want to do that. The private sector information-sharing entities that the White House envisions, I think they are going to get IP addresses that are relevant to the cyber attacks.

Mr. CHARNEY. They are going to get the IP address, and you can do an IP lookup and open source. But if we turn over information about an attack and the government says, OK, we now want to see account information and subscriber information, we require a judicial process. It may be a subpoena, it may be a 2703(d) court order, or it may be a search warrant. My point is it reached a point where the government wants more, and we require a legal process to be followed so that our customers know we are protecting their privacy and not just giving away the data voluntarily.

Mr. NOJEIM. I agree.

Chairman JOHNSON. Mr. Gordon.

Mr. GORDON. I think there is an important subtlety with IP addresses because that does tend to be the place that this conversation converges, and an IP address in the context in which we see it is not a customer's IP address. It is not affiliated in any shape or form with a customer. When we see an IP address in the context of sharing, it is a place from which an attack is unfolding, or it is

a place from which stolen data has been sent. That is all we know and, frankly, all in our context we care to know.

And so sharing that would enable someone else to in turn block an attack from that same location without ever knowing who it is on the other end. I think the law enforcement attribution, that is where there are other dimensions to this, but I do not think it is a yes-no. I think there is a context to sharing. We would never share information related to our customers. This is information related to an attack.

Chairman JOHNSON. Mr. Charney, real quick.

Mr. CHARNEY. Yes, that is true for you, and it is true for us. But if one of us was with a phone company or a cable provider that provided the Internet access and the government said here is the IP address, who is the customer, for them IP address is more than just an attack factor. It might be a customer's name and address.

Mr. GORDON. Sure, but they would require a subpoena for that.

Chairman JOHNSON. Now you almost start answering another question I had. Does the White House proposal contain adequate liability protection to induce the private sector to share with the government, to induce the private sector to share within the private sector? I think a number of you have testified that is really one of the primary information-sharing platforms we want.

Mr. GORDON. From what I understand, it does not cover company-to-company sharing at all, so it will not incentivize that.

Likewise, it does not cover, as I understand it, the acting from the sharing, even within your own network. And I think those appear to be two gaps.

Chairman JOHNSON. So how important is the company-to-company? And what level are we at right now? What level do we want to be at?

Mr. GORDON. I think it is very important. I think there is a tremendous amount of company-to-company sharing that happens today, and this essentially would potentially incent us away from that and toward this more structured into the government sharing. And there are numerous instances that I have been involved in where we have information that pertains only to a single company, it is very specific. And so sharing that through some hub-and-spoke context I think would be inappropriate.

Mr. NOJEIM. To be fair to the White House proposal, it does allow for the sharing—you could call this private-to-private, right? You can share to a private hub, and then that hub can share out back to the private sector. It does not allow the company-to-company sharing. It does not incentivize the company-to-company sharing that we all think is necessary. But it does allow the sharing to the hub.

The trick with the company-to-company sharing is to create a mechanism that ensures that the companies are playing by the information-sharing rules. So far, the mechanisms that have been discussed have all been rejected by the companies. They include things like creating a private right of action if the company does not play by the rules, and things like audits. They have all been rejected. So the question is: How do you ensure that the companies play by the rules? I do not think that we have gotten to that point

yet, and I think that is why the White House went with this hub-and-spoke model.

Chairman JOHNSON. Mr. Beshar, I am intrigued by the role that insurance can play and quite honestly, being a manufacturer, having been ISO certified, I can see a role that things like ISO certification can play, just simply private sector, here are the standards that can be created, that can be revised and updated very rapidly. Can you just kind of speak to that?

Mr. BESHAR. Sure. I think that is really the power of insurance, Mr. Chairman, that it can drive behavior change across large swaths of the people that is not driven by the government. It is just because there is a creation of the appropriate set of incentives that each one of these actors—large companies, small, mid-sized companies, even individuals—they take it upon themselves to say here are the steps that I can take to position myself as a better risk or I just think are prudent under the circumstances. So I think it has a tremendous power.

I think the Administration's proposal has actually struck quite a nice compromise that there are clear liability protections from civil and criminal exposure. There is the idea that it will not be used, the information, for extraneous purposes by regulators, and it will not be subject to FOIA requests or similar State laws. But then at the same time, there is an obligation on the companies to try to take out and strip out the personally identifiable information. So I think that is the path to go down.

Chairman JOHNSON. Mr. Bejtlich, can you kind of chime in on this? I was really struck by your testimony in terms of really what percentage of companies do not even know they have been hacked. So can you just speak to me in terms of where you think the hole is there?

Mr. BEJTLICH. Well, Senator, I think part of the problem is that many companies measure the wrong things. The example I like to use is you have a football team, and imagine if the way you determined how you were doing was to measure how tall all your players were, how fast they ran the 40, where they went to college, and then you took a look at them on paper and said, "Oh, that is how good we are," when really you need to find out how they play in a game. And that is where these metrics of how long has it been since someone broke in and to when you discovered it, and what steps can you take—technology diagnostic, process diagnostic, what are the steps you can take to reduce that count?

I see this in the Federal Government. With the continuous diagnostic monitoring, all the emphasis is on make sure we are patched, make sure we are configured properly. That is all great, but that is hygiene. That does not tell you what the score is going to be when you get on the field and you encounter the adversary.

Chairman JOHNSON. Let us continue going down the row here just in terms of looking at these proposals that are out there. What are going to be the impediments to putting something together and actually get it passed? I will start with you, again, Mr. Bejtlich.

Mr. BEJTLICH. Senator, one of the biggest issues I see is the deficit of trust in the security community. The security community up to the Snowden revelations, things were getting better. I mean, you had General Alexander appear at a hacker conference, DEF CON.

There was real good will being built there. And then the Snowden revelations came out, and now we have this real trust deficit.

I think one of the ways to perhaps address that would be to take a look at the Computer Fraud and Abuse Act. Some of the changes that have been proposed to that have really scared the security community into thinking that just being a researcher and trying to do the right thing and find vulnerabilities and report them so that they can be fixed could be a prosecutable event in and of itself.

So maybe one of the ways to approach this is to pair reforming the CFAA so that it is friendlier to good hackers with this information sharing and try to address that trust deficit.

Chairman JOHNSON. OK. Mr. Beshar.

Mr. BESHAR. I think the focus, Senator, should really be on information sharing and the rebuilding of trust between industry and government. Personally, I think the intercompany issues should be pushed somewhat to the side.

Chairman JOHNSON. Mr. Charney.

Mr. CHARNEY. I agree that industry and government sharing is important. The other party I would think about is the customers, because the privacy concerns stem from the customers who want to entrust their information to third parties, and I think the discussion we have had today about how could we provide privacy protections for the data that is shared but ensure that the data could be used with less risk of liability is the right formulation.

Chairman JOHNSON. Mr. Gordon.

Mr. GORDON. I agree. I think that is the one issue that looms around this. Otherwise, I think there is, at least for the private sector, tremendous support for this. And I think the conversation about removing PII in the way that we share information is a very reasonable approach that really would solve this.

Chairman JOHNSON. That is a real critical aspect of this. One thing we really have not talked too much about—unless it was asked when I was gone—is really breach notification. Can you just kind of speak to the necessity for that and what problems that creates for any organization that is going to be required to do so? We will start with you, Mr. Gordon.

Mr. GORDON. I think that having a national breach notification standard is appropriate and would actually be helpful, and especially one that supersedes because, as you know, every State has a version of it and it is very complicated to navigate. I think it is appropriate and we should do it.

Chairman JOHNSON. Is that the only level we are at right now, is just State? Have there been smaller jurisdictions that have offered any?

Mr. GORDON. I am only aware of State at this point.

Chairman JOHNSON. OK, Mr. Charney.

Mr. CHARNEY. I agree with that. The only other thing I would pay attention to is when breach notification has to be given. There have been some proposals, for example, that there should be a definitive timeline. But very often when you are investigating these cases, it takes awhile to figure out exactly what has happened and who has been breached, and you do not want to give out partial notifications. You want to understand the scope of the adversary's ac-

tivity and whether he is still in. And once you start giving notification, you have told the adversary that you are on to them.

So there should be some reasonable time to give breach notification, but a time fixed in stone, like 48 hours, is not flexible enough.

Chairman JOHNSON. What would be a reasonable timeframe? And, again, that looks to me like any kind of timeframe is somewhat of a conundrum.

Mr. CHARNEY. It is a little bit of a conundrum, and it certainly should not be open ended. But in all sorts of places, the law requires reasonableness and a reasonable-man standard, so to speak. And the reality is these cases can be very complex, and it can take awhile to figure out exactly what happened and who should be notified. And what you do not want to end up is notifying too soon and actually compromising the investigation, and maybe even a law enforcement investigation.

Chairman JOHNSON. I am assuming you are not going to give me a timeframe.

Mr. CHARNEY. I am not going to give you——

Chairman JOHNSON. And that is actually reasonable. Mr. Beshar——

Mr. GORDON. I would completely support that. I think putting any time against it is nonsensical, because every instance is different, and I think reasonable is the right standard.

Mr. BESHAR. We strongly support a uniform Federal breach notification standard, and our hope, Mr. Chairman, would be that it preempts the State regimes.

Chairman JOHNSON. OK. Mr. Bejtlich.

Mr. BEJTLICH. Mr. Chairman, the one thing—I would concur with my colleagues, but the one caution I would add is that breach has to be properly defined. There are many low-level things that get caught, stopped, and so forth. If you had to somehow report on all of those, it would be a disaster.

Chairman JOHNSON. Can you kind of typify some sort of level? We were talking about data breach. Now you are talking about when personal information is lost and people really need to understand that so they can either cancel your credit card or——

Mr. BEJTLICH. That is right. You would not want to define a breach as someone broke into a computer. You would want to define it as they stole PII, something that the person who is affected would not know otherwise and they need to——

Chairman JOHNSON. Going back to your testimony, where 67 percent of the businesses that you are potentially auditing do not even know they have been breached.

Mr. BEJTLICH. That is right.

Chairman JOHNSON. So how do you account for that? Is it the point where they actually are aware of it? Is that when the data breach notification requirement would hit in? I mean, you also have to account for that as well, right?

Mr. BEJTLICH. Right. There needs to be some time—because you can receive a notification and it may not actually represent a real problem. I have been involved with some of those as well. You do need some time to identify yes, this notification does point to something real and—for example, if someone stole dummy data that was not actually real and the bureau noticed it, there is no problem

there. It was dummy data for testing or whatever. But if you get the notification, you see this is real data, now I have to report.

Chairman JOHNSON. Mr. Nojeim.

Mr. NOJEIM. So the biggest obstacle to passing information-sharing legislation is failure to pass legislation to deal with the NSA's bulk collection program. I think you have to do that before you get to cybersecurity information sharing, because everybody knows that some of this information shared under the cybersecurity program is going to end up at the NSA. Unless you do something to reform NSA, I do not think you can do the cyber first.

The biggest obstacle to the data breach notification legislation is the way, for example, the White House bill preempts State laws that protect data that the White House bill does not protect. So, for example, California protects health information, but the White House bill explicitly carves that protection out. But it would preempt that California protection anyway. I think that is a problem that needs to be fixed.

Chairman JOHNSON. OK. We have the second vote called, so I am going to have to be closing this hearing. But I want to ask one more question because I want to go back to the data breach notification.

When you are not even aware that you have been hacked and some of that information is already flowing, I mean, how do we address that to make sure that companies are not unfairly penalized?

Mr. BESHAR. I would just say, Mr. Chairman, it has to flow from discovery.

Chairman JOHNSON. Discovery, OK. Very good. Well, again, I just want to thank all the witnesses for your, again, thoughtful testimony and answers to our questions.

The hearing record will remain open for 15 days until February 12 at 5 p.m. for the submission of statements and questions for the record.

This hearing is adjourned.

[Whereupon, at 3:07 p.m., the Committee was adjourned.]

APPENDIX

Opening Statement of Chairman Ron Johnson
"Protecting America from Cyber Attacks: The Importance of Information Sharing"
January 28, 2015

As prepared for delivery:

Good morning and welcome.

Today's hearing—the Committee's first hearing in the 114th Congress—is about the cybersecurity threat our nation faces and what we can do to mitigate it.

Two years ago, then Director of the National Security Agency, General Keith Alexander, described cyber thefts from private and public organizations as "the greatest transfer of wealth in human history."[1] Recent attacks on private companies have shown that statement to be true, and the threat continues to grow.

Over the past year alone, we saw cyber-attacks on Sony Pictures Entertainment; retailers like Target, Home Depot, and Neiman Marcus; and U.S. government systems, from social media to systems with sensitive personnel records. A recent study by the Center for Strategic and International Studies estimated the total economic loss of cyber-attacks to be up to $100 billion annually.[2] A study commissioned by HP Enterprise Security figured the mean annualized cost of cybercrimes in the U.S. to be $12.7 million per company.[3]

One of our missions for this Congress is to address the cybersecurity threat. The first step in addressing any problem is defining it. The purpose of this hearing is to take that first step and develop an understanding of the reality of the cybersecurity threat—the frequency and complexity of the cyber-attacks U.S. businesses endure every day, what businesses can do to better defend themselves, and what businesses need from the federal government.

Today we will discuss two important things Congress can do to help businesses mitigate the cybersecurity threat: cybersecurity information sharing with liability protection and a national data breach notification policy. On information sharing, we will consider its value in mitigating cybersecurity threats, what information must be shared for it to be useful, with whom that information must be shared, the importance of liability protection to participation, and privacy considerations. On data breach notification, we will consider the need for federal preemption of the patchwork of state laws that all provide different requirements for when, how, and who businesses must notify upon a data breach.

Thank you. I look forward to your testimony.

---

[1] Keith B. Alexander, *An Introduction by General Alexander*, 19 NEXT WAVE 4 (2012).
[2] CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, MCAFEE, THE ECONOMIC IMPACT OF CYBERCRIME AND CYBER ESPIONAGE (July 2013).
[3] PONEMON INSTITUTE, 2014 COST OF CYBER CRIME STUDY (2014).

Opening Statement of Ranking Member Thomas R. Carper:
"Protecting America from Cyber Attacks: The Importance of Information Sharing"
January 28, 2015

As prepared for delivery:

I would like to thank the Chairman for calling this very important and timely hearing. I believe it is very fitting that our first hearing this Congress will focus on cybersecurity. This is an area where our Committee achieved a number of key legislative successes last year to strengthen our nation's defenses against cyberattacks. We need to make further strengthening those defenses a top priority again this year.

Over the last few years, we have witnessed many troubling cyber attacks. We've seen banks get hit by huge denial-of-service attacks intended to frustrate customers and make it harder to do business. We've seen retailers big and small suffer massive data breaches that have put Americans' finances at risk. And we've seen government agencies fall victim to cyber intrusions time and time again, threatening our national security.

What we saw happen to Sony Pictures at the end of last year, however, was in many respects a turning point. Some have called it 'a game changer' when it comes to spreading awareness of the threats we face. Instead of just having data stolen, Sony Pictures was the victim of a destructive cyber attack at the hands of another nation – North Korea. The attack destroyed thousands of computers and caused data on its systems to simply vanish. We have heard about these types of destructive attacks in other countries, but never one of this magnitude here on U.S. soil. This devastating attack did not stop in cyberspace. It was coupled with threats of violence against American moviegoers and an assault on the values we cherish.

Many experts believe that destructive cyber attacks will grow even more common. In fact, just two months ago, the Director of the National Security Agency, Admiral Mike Rogers, stated that we will likely see a dramatic cyber attack on America in the next decade. He also said that other countries have the capabilities today to disrupt our critical infrastructure.

Last Congress, our Committee took several important steps to better secure our country against this ever-growing threat, sending a number of bipartisan cybersecurity bills to the President's desk for his signature. We passed a bill codifying the basic functions of the National Cybersecurity and Communications Integration Center at the Department of Homeland Security. This is the information sharing hub where the federal government interacts with critical infrastructure companies on cybersecurity. This new law provides our private sector partners in cybersecurity greater certainty that they have someone to work with in combatting the threats they face every day. It also encourages greater sharing of cyber threat information.

We also enacted legislation to modernize how Federal agencies secure their networks, scrapping an extensive and dated paperwork-heavy system with a more nimble one based on the latest and most-effective strategies. The new law also requires agencies to share more cyber threat information with each other. And finally, we passed two laws to help the Department of Homeland Security hire and retain the top-level talent it needs to fulfill its cyber missions.

While we made important progress last year, there are still important pieces of cyber legislation on our 'to do' list. Today, we will be focusing on one of these issues – cyber threat information sharing.

While businesses and the government appear to be getting better at sharing information all the time, more must be done to take the remaining uncertainty and guess work out of the process. This is necessary because the lines of communication between businesses and government are unfortunately not always clear. Often times, legal ambiguities make companies think twice about sharing cyber threat information with the government or their peers. In some cases, companies are uncertain about what they can do to defend their own networks. Legislation can fix these problems.

I have a very strong interest in introducing and moving strong, sensible legislation to better enable the sharing of cyber threat information. And, I expect that this Committee – with its jurisdiction over the Department of Homeland Security – will be very engaged in cyber threat information sharing legislation this Congress. That said, I recognize that we share the responsibility of figuring out the right solution for information sharing with many stakeholders, including the Executive Branch and other Senate committees.

In fact, our friends on the Intelligence Committee, particularly Senators Diane Feinstein and our former colleague Saxby Chambliss, worked tirelessly to move an information sharing bill last Congress. Senator Feinstein also had an information sharing bill in the Congress before that. And of course, this Administration has made cyber threat information sharing a priority.

I was pleased to see the President put forward his own legislative proposal to improve information sharing. While not perfect, I believe it includes constructive proposals that will help us continue the conversation on this issue. I look forward to hearing from our panel today about the President's proposal as Senator Johnson and I and our colleagues consider our options for moving legislation. We must find a legislative solution that will address our information sharing needs while upholding the civil liberties we all cherish. And we must move with a sense of urgency on this important legislation.

I should hasten to add that an information-sharing bill, however, is not a silver bullet. We need to pursue additional ways to help businesses better protect their networks and deter our would-be attackers. A national data security and breach notification standard, then, is also an essential tool that I intend to pursue this Congress.

On Election Day, American voters sent Congress a clear message: they want us to work together in a bipartisan fashion, they want us to achieve real results, and they want us to take actions that help grow our economy. Passing bipartisan information security and data breach measures would do all three of those things.

In closing, I think it's important to note that in approximately one month, the current funding for the Department of Homeland Security will expire. We cannot let this happen. The threats to our country in cyberspace and in any number of areas are just too great, and we will discuss some of those today. DHS has a lot to say grace over, and we do them no favors by playing games with their budget. We need to promptly pass a clean bill to fund DHS for the rest of this fiscal year so

that department and its employees can continue to effectively carry out their critical role of helping to keep Americans safe in an ever more dangerous world.

Prepared Testimony and Statement for the Record of
Marc D. Gordon
Executive Vice President and Chief Information Officer
American Express

Before the
United States Senate
Committee on Homeland Security and Government Affairs

Hearing on "Protecting America from Cyber Attacks: The Importance of Information Sharing"

Wednesday, January 28, 2015

Chairman Johnson, Ranking Member Carper, members of the Committee, my name is Marc Gordon and I am Executive Vice President and Chief Information Officer at American Express. In this role, I oversee the technology organization that is helping to drive the digital transformation of the company through innovative technology solutions that are powering revolutionary products and experiences across the commerce cycle. I also oversee the delivery and operations of technology capabilities and services globally, as well as information security for the Company.

I appreciate the opportunity to testify about the serious threats we face today and my views on information sharing programs. Based on my roles in multiple global fortune 100 firms and the experiences I have had in information sharing within and across sectors, I would strongly urge the Committee to swiftly move forward with information sharing legislation. While effective information security requires a web of inter-related controls, I believe effective information sharing may be the single highest impact/lowest cost/fastest to implement capability we have at hand as a nation to accelerate our overall defense from the many and varied and increasing threats around us.

Threat Landscape

The threat environment today is increasingly complex, increasingly challenging and constantly changing. While defending our networks, protecting sensitive information and making our services available to our customers as part of an increasingly digital economy, we operate in an environment where:

- In 2014, we received over 5000 FS-ISAC cybersecurity alerts providing information of a variety of threats, attacks and other information supplied by members for members (an example of information sharing that goes on today),

and have received approximately 100,000 technical indicators (describing malicious IP addresses, websites, malicious code components or some other aspect of a cyber threat to help maintain our defenses) from a variety of intelligence sources.

- Distributed denial of service (DDoS) attacks, where attackers send so much internet traffic to a company's website as to render the site unavailable to legitimate consumers, have more than tripled in strength in the last 18 months, challenging even the best defended companies to maintain availability of vital web services to their customers. (source – Prolexic Q3 2014 State of the Internet Security report)
- During the last year, there were nearly 60 million records compromised in reported security breaches affecting businesses, including financial institutions and retailers. (source – Privacy Rights Clearinghouse)
- The increasing use of 'ransomware' to encrypt a victim's entire computer and extort them for money to regain access to their files is especially pernicious and threatens consumers and corporations alike. One estimate indicated that over $27 million in ransom payments were made in just the first two months since a common ransomware known as *Cryptolocker* was first discovered in late 2013. (source – FBI.gov, June 2014 Issue 62)

While cyber crime is growing meaningfully across industries, and that is a clear concern, we are also increasingly concerned about the convergence of players, capabilities and intentions: as reported in the press, nation state players with destructive intention and capability that have targeted various industries.

Information Sharing Legislation

In response to the threats above, the financial services industry has invested billions of dollars to protect our networks from cyber attacks. These investments are expected to continue and in most cases accelerate.

In addition to the investments being made across industries, there are steps we can take to make the total ecosystem more secure, beginning with the right private/public partnerships that can help companies better protect themselves. This requires Congressional guidance. Meaningful legislation would greatly expand the quality and volume of cyber information sharing; raise the level of security overall; and reduce the variability of security within and across industries both for critical infrastructure and non-critical infrastructure organizations.

Today, members of the financial services industry have a mechanism for sharing threat data with one another. Through our FS-ISAC, or Financial Services Information Sharing and Analysis Center, we securely share cyber threat information including threat signatures used in certain attacks. The FS-ISAC also allows the industry to exchange threat data regarding tools, techniques and procedures that help alert the broader financial services community of impending threats. Venues like the National Cyber Forensics Training Alliance, or NCFTA, provide an opportunity to collaborate closely with law enforcement to combat the problem of cyber crime and help protect customers, banks and retailers alike.

Despite this, more information could be shared within and between industries. In addition, industry should be able to more freely send and receive threat data from the government. Unfortunately, there are existing legal barriers to us doing so, including the

threat of lawsuits, and that is where Congressional guidance is desperately needed. Legislation that provides targeted protections from liability and disclosure – both for business-to-government sharing but also for business-to-business sharing – is sorely needed. By affording targeted protections from liability and disclosure, entities across sectors will be more willing to share key threat data without fear of unnecessary and wasteful litigation or public disclosures that could further compromise their systems. This could allow, for instance, a member of the Financial Services sector to provide threat data to the retail sector, which could potentially prevent the next major breach, or protect from the potential loss or destruction of customer information, or the theft of intellectual property. Without these targeted protections we lose a real opportunity to improve the security of the overall ecosystem.

Further, statutory protection from Freedom of Information Act (FOIA) requests related to cyber threat information shared with the government would help improve the information sharing frameworks that exist today. The lack of a FOIA exemption undercuts the very intent of more effective voluntary information sharing by allowing public access to the sensitive threat information organizations voluntarily provide. Once the information is public, it could be used by bad actors searching for system weaknesses or other information that may help them accomplish their cyber objectives. As a result, an organization's willingness to share such information diminishes greatly.

Significant progress was made in the last Congress towards enactment of meaningful information sharing legislation. Multiple industries, law enforcement, and cybersecurity experts worked with committees in both the House and Senate to develop bipartisan legislation. Though there were modest differences in the approaches taken by

the House and Senate, these bills can serve as a template for the new Congress. There are a few notable items we would emphasize in terms of attributes of information sharing that we believe are important:

- real time sharing: threats unfold in minutes and hours and cascade company to company and sector to sector rapidly; sharing needs to be real time to be most effective
- liability and disclosure protection needs to include not just the sharing itself, but 'good faith' action taken (within the company's network and systems) based on the information shared; otherwise sharing itself may not result in the necessary action being taken
- companies should be protected from sharing among themselves, not just with the government or government sanctioned entities, to ensure every opportunity to protect systems is available
- sharing needs to be bi-directional; the ecosystem is much stronger when indicators only known/knowable by the government are shared back to the private sector; we would encourage the legislation to include active and clear requirements for this to occur
- effective sharing will require a designated 'hub' within the government for bi-directional sharing but should also not prevent other public/private sharing from occurring

Finally, we recognize that there are important privacy questions that must be answered as part of information sharing legislation; we are committed to protecting the

privacy of our customers' information; and believe that concerns around privacy protection can be effectively addressed.

Conclusion

I want to thank you again for asking me to be here today. We truly appreciate the opportunity to share our views on this important issue, and we look forward to working with this Committee, and other members of the Senate and the House going forward. This concludes my prepared remarks. I would be happy to answer any questions that you may have.

Written Testimony of
Scott Charney
Corporate Vice President, Trustworthy Computing, Microsoft Corporation
Before the
Senate Committee on Homeland Security and Governmental Affairs
Hearing on "Protecting America from Cyber Attacks: the Importance of Information Sharing"

Chairman Johnson, Ranking Member Carper, and members of the Committee, thank you for the opportunity to appear today at this important hearing. My name is Scott Charney, and I am the Corporate Vice President for Trustworthy Computing at Microsoft. I currently serve on the President's National Security Telecommunications Advisory Committee and I previously served as one of the co-chairs for the Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency. Prior to joining Microsoft, I was Chief of the Computer Crime and Intellectual Property Section in the Criminal Division of the United States Department of Justice. During my government service, I oversaw every major hacker prosecution in the United States from 1991 to 1999, worked on major legislative initiatives, Chaired the G8 Subgroup on High-Tech Crime, and was Vice Chair of the Organisation for Economic Co-operation and Development's Group of Experts on Security and Privacy. Finally, I should note that I have had the privilege of testifying before Congress about cybersecurity several times.[1]

It is good to see that the committee's first hearing of the 114th Congress focuses on cybersecurity issues generally, and information sharing in particular. I commend this Committee and the members of the Senate for your continuing commitment to addressing one of America's most complex national and economic security challenges. You and your staff are creating a venue for private sector input into deliberations on cybersecurity, which is essential given that the U.S. private sector not only owns and operates most of this country's critical infrastructure, but also creates and provides information technology products and services used by governments, industries and consumers throughout the world.

The invitation to testify noted that the Committee has three primary objectives:

1. Develop an understanding of the scope and size of cybersecurity threats against U.S. businesses;
2. Discuss the role of various cybersecurity legislative and non-legislative proposals, such as improving information sharing and data-breach notification, in mitigating threats and filling gaps in current practices; and
3. Examine what such proposals must include in order to be effective.

---

[1] Scott Charney Corporate Vice President, Microsoft Corporation's Trustworthy Computing, Testimony before the Senate Committee on Homeland Security and Governmental Affairs Hearing on *Securing America's Future: The Cyber-Security Act of 2012* (February 16, 2012); Scott Charney Corporate Vice President, Microsoft Corporation's Trustworthy Computing "Implementing New Models for Information Age Security," Testimony before the House Committee on Science and Technology Subcommittee on Technology and Innovation Hearing on *Assessing Cybersecurity Activities at NIST and DHS* (June 25, 2009); Scott Charney Corporate Vice President, Microsoft Corporation's Trustworthy Computing "Securing America's Cyber Future: Simplify, Organize and Act," Testimony before the House Committee on Homeland Security Sub-Committee on Emerging Threats, Cybersecurity, and Science and Technology Hearing on *Reviewing the Federal Cybersecurity Mission* (March 10, 2009).

I will address each of these issues in turn.

The Size and Scope of the Cybersecurity Threats Against U.S. Businesses

There is no doubt that cybersecurity is an important issue for America, other nations, the private sector, and individuals. In an effort to better understand and help address the challenges we face, I regularly engage with government leaders from around the world, security-focused colleagues in the IT and Communications Sectors, companies that manage critical infrastructures, and customers of all sizes. From those interactions, I have concluded that cyber-attacks have joined terrorism and weapons of mass destruction as one of the new, asymmetric threats that puts the U.S., its allies, its corporations, and its citizens at risk.

These threats come in two forms. First, there are opportunistic cybercriminals who have discovered that the Internet's attributes – such as global connectivity, anonymous and untraceable communications, and rich targets (e.g., financial information) – make it an ideal place to commit crime. These cybercriminals engage in broad-based attacks, such as sending email spam to millions of users in the hope that some will click on a dangerous link, install malware and/or provide personal information. These cybercriminals do not care who in particular falls prey, as long as some do. It is also worth noting that these attackers do not need to be technically sophisticated; there are many hacker tools that automate the attack process.

The second form of attack is called an "advanced persistent threat" or "APT" although, in many cases, the attack is not advanced, merely persistent. These attackers are willing to work over time, firmly resolved to compromise a particular victim. Often times, the attacker has had access to the victim's system for a long period of time, moving through the organization and placing malware and backdoors throughout. In a very disturbing trend, these attacks – which previously focused on data exfiltration (the theft of data) – have become more destructive. In some cases, data has been erased from thousands of machines and normal operations were particularly hard to restore.

These two different types of threats warrant somewhat different responses. Basic computer hygiene – running the latest version of software, applying updates, running anti-virus, and exercising common sense (e.g., not opening attachments from strangers) – can thwart many opportunistic attacks. To address advanced persistent threats, however, requires much more. In such cases, those responsible for computer security must focus on the entire "prevent, detect, and respond" lifecycle. Even when they do, it is generally recognized that breaches are inevitable because the old adage that "offense beats defense on the Internet" is true. This is because defenders have to secure everything, while attackers have to find only one entry point. That entry point can be through supply chain taint, exploitation of a vulnerability, exploitation of a system misconfiguration, or through social engineering (tricking a user into providing access).

Complicating matters further is that some advanced persistent threats may come from governments, and it is important to appreciate that governments have developed a very complex relationship with the Internet. First, they are large users of information and communications technologies ("ICT"), but their "customers" are "citizens" who may want to find information, file for benefits, pay their taxes, etc. Second, governments are responsible for protecting the Internet as well as the security and privacy of Internet users, and to fulfill that mission, may use its regulatory powers. Third, even though it wants to protect computer security, a government may exploit networks for a number of reasons, including

economic espionage, military espionage, and military operations.[2] Finally, governments often want access to data, in large part to fulfill law enforcement and intelligence missions.

Consistent with these various roles, an increasing numbers of nation states are currently developing both defensive and offensive cyberspace capabilities. Based on internal Microsoft research, we have determined that:

- In the last 6 months, 95 countries have discussed legislative initiatives focused on cybersecurity;
- 42 countries have developed defensive capabilities against cyber-attacks on their networks;
- 18 have developed defensive capabilities, and possibly also have offensive capabilities;
- 13 likely have offensive capabilities that have not been acknowledged, but can be inferred from operational activity; and
- 16 have specifically declared offensive and defensive capabilities.

Attacks by governments pose a particular problem for the private sector, since a government can utilize a range of tactics and capabilities that non-government cybercriminals normally will not. For example, governments are more likely to taint the supply chain, intercept communications, engage in surreptitious physical searches, and/or affirmatively embed spies into private sector organizations of interest. Additionally, deterrents to cyber-attacks, such as arrest and prosecution, are less applicable to government agents pursuing government missions. This is one reason why Microsoft has been promoting cyber norms, as it has become critical that governments (collectively) exercise self-restraint based upon an agreed set of norms.

Finally, it is clear but worth repeating why this threat environment is so problematic: many parts of the world are completely dependent on ICT for every aspect of digital life and work, with new advances in technology creating incredible civic, social, educational, and economic opportunities. Additionally, while all have not yet benefitted from these advances in technology, it is estimated that over the next decade the number of Internet users will more than double to 4.75 billion, connecting more than 91 percent of people in developed countries and nearly 69 percent of those in emerging countries. This will not just be through traditional computing devices and smartphones, but wearables and other devices not yet imagined. As the "Internet of Things" and cloud services are broadly adopted, connectivity and insights from data will yield overwhelmingly positive and beneficial outcomes. The downside of that ubiquitous connectedness is that attacks will have increasingly disruptive effects. In sum, we have a lot to gain from the continued advancement and deployment of ICT, but we must take concrete actions to limit the threats that may undermine these positive outcomes and cause real harm to computer users worldwide. This is of particular concern to Microsoft, as we have hundreds of millions of consumer and commercial customers using over 200 cloud services (such as Office 365, Azure, Outlook, Skype, and Xbox Live) and 1.4 billion people who use Windows in 76 markets worldwide. Our customers demand – and our business depends – on robust computer security and appropriate risk management.

Why Information Sharing Is Important

With global threats, global actors, and global networks, no one organization – public or private – can have full awareness of all the threats, vulnerabilities, and incidents that shed light on what must be managed. There is no doubt that sharing such information can and has protected computer users and increased the effectiveness of the security community's response to an attack. For example, in 2009, the Conficker Working Group came together to share information and develop a coordinated response to the Conficker

[2] *See* Scott Charney, "Governments and APTs: The Need for Norms," *available at* http://aka.ms/rethink2.

worm, which had infected millions of computers around the world. After the working group developed a mitigation strategy, Information Sharing and Analysis Centers ("ISACs") were mobilized, company incident response teams were activated, government responders were engaged, and the media reported as milestones were reached and services were restored. The challenge was addressed, and quickly.

Another example of information sharing that was designed to solve a specific problem can be seen in Microsoft's partnerships with other companies to takedown botnets through civil action, coordinated industry efforts, and with the support of law enforcement in the U.S. and internationally. Working with the Financial Services ISAC, financial services institutions, pharmaceutical companies, and law enforcement, Microsoft has disrupted cyber threats to our customers and increased the risks for criminals. Two particular operations, the Zeus and Citadel botnets, were each responsible for over $500 million in financial fraud. The collective efforts of industry and government freed millions of infected computers from the control of the cybercriminals.

Why is it, then, that after 20 years of discussion and proof of effectiveness, information sharing efforts are viewed as insufficient? The short answer is that while there are success stories, it is often true that those with critical information are unable or unwilling to share it. They may be unable to share it due to law, regulation, or contract, all of which can create binding obligations of secrecy and expose a company to legal risk if information is shared. Even when those restrictions permit sharing pursuant to authorized exceptions, legal risks remain, as parties may disagree on the scope of the exception. There are also non-legal, non-contractual risks; for example, a company that discloses its vulnerabilities may suffer reputational risk, causing both customers and investors to become concerned. It may even suggest to hackers that security is inadequate, encouraging other attacks.

Additionally, even though information sharing may be designed to protect computer users, the misuse of shared information can have the opposite effect. Let me provide a concrete example. For some time, the second Tuesday of each month has been known as "Patch Tuesday:" the day Microsoft releases updates to fix vulnerabilities in products. When these patches are released, others can reverse-engineer the patch, see what was changed, and craft malware. Thus, the Wednesday after Patch Tuesday became known as "Exploit Wednesday." The problem is that large enterprise customers, including governments, cannot deploy patches the moment they are released; these customers must test patches for compatibility with their own network configurations and programs. Thus, these temporarily unpatched customers were vulnerable to new malware created the day after a patch was released.

To address this problem and better protect customers, Microsoft created the Microsoft Active Protections Program ("MAPP"). Under MAPP, we share information on upcoming patches with anti-virus and intrusion detection companies the week before the patch is released. They then write signatures and deploy them to their customers. Thanks to the MAPP program, here is the new sequence of events:

1. Microsoft releases vulnerability information to MAPP partners;
2. MAPP partners write malware signatures and deploy them to their customers;
3. Microsoft releases updates on Patch Tuesday; and
4. Malware is released on Exploit Wednesday, *but customers are already protected even if the update is not yet deployed.*

This is a powerful example of the benefits of information sharing, as MAPP currently has 80 participants worldwide and helps secure 1 billion customers.

Yet that is not the end of the story. Occasionally, we would see vulnerability information released *before* Patch Tuesday; it turns out that a very small number of MAPP partners were inappropriately disclosing our information early, thus allowing malware to be crafted prior to Patch Tuesday. Needless to say, those violating our confidentiality requirements were removed from the program, but this series of events reveals another reason why organizations may be reluctant to share information; it may be disclosed without authorization or otherwise misused.

In addition to the substantive concerns described above, there are at least four operational challenges posed by today's information sharing arrangements. First, most information sharing programs involve organizations in the same industry: banks share information, electric utilities share information, etc. But ICT is horizontal and underpins all of these sectors, thus rendering these sectoral approaches insufficient. Simply put, ICT threats, vulnerabilities, or incidents may affect disparate companies across multiple sectors.

Second, sharing may occur among industry players, from industry to government, and/or from government to industry, and each of these models pose different issues. Companies in the same sector sharing information may worry about antitrust concerns (partially addressed by letters from the Justice Department and the Federal Trade Commission); private organizations sharing with the government may worry about the use of such information for regulatory enforcement or that customers will view such sharing as inappropriate; and the government itself may worry about disclosing sensitive information to non-government personnel.

Third, while sharing may involve indicators of compromise ("IOCs," such as malware signatures) and anonymized data, it may also include personally identifiable information ("PII"), thus raising privacy concerns. While it may be tempting to permit only the sharing of anonymized data, it is impractical for at least two reasons. First, some IOCs may in fact be PII in some parts of the world. For example, when malware steals data and sends it to a particular IP address in a foreign country, looking for other systems sending content to that same IP address is strong evidence of a security breach. Yet, IP addresses are PII in some countries. Additionally, if we hope to deter cyber-attacks through stronger attribution, it is important to identify the attacker, which, in turn, requires analyzing data that often includes PII (e.g., IP addresses, names of account holders).

Fourth, with so many people dependent on ICT and concerned about cybersecurity, it is challenging to define the scope of any disclosures. Many today would say they need threat, vulnerability, and incident information to manage risk but, as we have seen, sharing information poses its own risks.
With all these challenges in mind, we believe there are six core tenets that must guide information sharing arrangements.

Six Tenets to Guide Effective Information Sharing

1. **Information sharing is a tool, not an objective.**

   Information sharing succeeds when it is targeted at solving specific problems and challenges. Put another way, clarity is needed about what should be shared, with whom, and for what purpose. We also need to know how sensitive information will be protected to avoid causing harm or other unintended consequences. Approaches that call for the disclosure of all threat, vulnerability and incident information, regardless of its utility to the recipient or the risks such disclosure creates for the ecosystem, are ill-advised.

2. **Information sharing has clear benefits, but poses risks that must be mitigated.**

   As we have seen, information sharing can help prevent and respond to attacks, but such sharing poses legal, regulatory, contractual, reputational, security, and privacy risks. Any information sharing regime must attempt to reduce these risks wherever possible.

3. **Privacy is a fundamental value, and must be protected when sharing information to maintain the trust of users – individual consumers, enterprises, and governments – globally.**

   Users and governments around the world may have different views about privacy, but they all want assurances that the information they entrust to others is protected properly. As such, government and industry organizations need to be transparent about the policies and processes in place to protect privacy, particularly when information will be shared with and used by others.

4. **Information sharing forums and processes need not follow a single structure or model, and governments should not be the interface for all sharing.**

   Information forums and processes typically reflect several factors, such as the purpose for their establishment, the players involved, the nature of information shared, and the desired outcomes. Because these factors can differ greatly, there is no single model or template for information sharing efforts. Indeed, significant information sharing occurs within the private sector without any involvement of the government, ensuring that millions of customers are protected quickly.

   In the United States, while the Department of Homeland Security and other U.S. government entities play an important role in cybersecurity, they should not be the sole interface or repository for threat, vulnerability and incident data. This approach would limit the flexibility needed to adapt to a rapidly shifting threat environment, particularly when new entities need to be added to information sharing circles quickly.

5. **Government and industry policies on information sharing should take into account international implications.**

   Cyber threats are often international in scope and an attack may have worldwide implications. The U.S. Government must be mindful that many successful U.S.-based ICT businesses are multi-national companies with foreign customers. Domestic rules can discourage foreign markets from embracing U.S. products and lead to reciprocal requirements that could undermine U.S. security. For example, if the U.S. Government required the mandatory disclosure of all threat, vulnerability, and incident information held by a global company, it is likely that other governments would demand the same information. Broad disclosures in so many parts of the world would not improve computer security; to the contrary, it would increase security risks. Similarly, government policies that unnecessarily constrain the private sector's ability to share cybersecurity information across borders will have a negative impact on cybersecurity outcomes, as cyber defenders will be less equipped to address emerging international threats.

6. **Governments should adhere to legal processes for law enforcement and national security requests, and governments should not subvert information sharing to enable or advance law enforcement and national security objectives.**

   In instances where law enforcement and national security agencies require assistance from the private sector, governments should adhere to appropriate legal processes rather than attempting to leverage information sharing forums and processes. Law enforcement and national security requests

are distinct from information sharing, which centers on the *voluntary* sharing of information that enable stronger cyber defense.

Operationalizing Information Sharing to Solve Problems

These tenets can help address operational considerations, which pose their own challenges. An important starting point is to leverage consistent and repeatable processes for sharing information, processes that maximize the benefits and reduce the risks of information sharing. These processes must not only accommodate today's challenges, but scale to address the increasing connectivity across industries and across the globe.

To understand how this can be achieved – and how legislation might help – it is helpful to understand the basics of information sharing. The process generally has five parts: collection, identification, sharing, use, and data handling.

Collection: Organizations collect data from many sources, in part to detect attacks. For example, they may monitor inbound and outbound traffic, attempts to log onto their networks, and logs generated by security products. If a compromise is found – or if a company is alerted to an attack from an outside source – additional collection may then occur. Of course, there are cost implications to broad collection as a company deploys sensors, stores data, and analyzes it. That said, as sensors and storage becomes cheaper – and machine learning permits more data to be analyzed – more attacks may be detected. This may be controversial, however, since collecting haystacks in the hope of finding needles raises privacy concerns.

Identification: Once an anomaly is detected, further analysis must be done to determine that nature of the event and the scope of any compromise. In some cases, the work can be automated; for example, applications can help identify anomalous behavior on networks or identify traffic being sent to a botnet controller. But even with these tools, determining the scope of an intrusion and the damage caused may remain a complex challenge that relies heavily on the expertise of security professionals. This is because tools cannot detect all malicious activity, and not all anomalous behavior is necessary malicious. When security professionals see something, they have to look closely to determine whether it actually indicates that a cyber-attack has taken place or may be underway. This analysis may require outside help if an organization lacks the right security resources.

The products of this phase are typically IOCs, evidence that reveals an intrusion has occurred (e.g., a piece of malware, a log showing that data has been sent to an unexpected IP address). Ultimately, IOCs are the most common type of information that is shared amongst security professionals.

Sharing: In addition to IOCs, parties may also share information on threats, product vulnerabilities, defensive mitigations, best practices, and strategic analysis. In many cases, this sharing begins as an ad hoc collaboration between affected or knowledgeable parties. This may cause individuals to work together even if they have otherwise competitive relationships or little else in common (e.g., they are in different sectors). These collaborative undertakings build trust and, over time, each party expects that the other will work in a consistent and repeatable way that maximizes protection and minimizes harm. Sustaining these ad hoc efforts in a more structured way requires careful consideration of the what, when, how, and why of information sharing. Understanding these building blocks can help develop structures that not only build trust, but also actively support collaboration in reducing cybersecurity risks.

Use: Each type of information has a different use. Some information helps government and private sector entities assess the risk to cybersecurity at a national or an organizational level, including the risk to critical infrastructure. Some information contributes to analyzing cybersecurity in the long term and to creating incentives for better security. Other types of information can be used to detect attacks, identify incidents, and observe those incidents to determine the objectives of the attackers. Some information, such as best practice information, is more directly actionable for improving hardware, software, and services or for making immediate improvements to network defense. Additionally, security information concerning fraud and abuse can be used to protect the identities, defend account compromises, and for general ecosystem hygiene.

Increasingly, vulnerability and mitigation information is seen as useful in helping actors across the different sectors decide how best to assess and manage risk. This trend reflects a growing understanding of the need to develop better analytical capabilities to understand strategic threats and to better anticipate new risks to ICT and the capabilities ICT enables. High-quality strategic information can help to project where the next classes of cyber-threats may come from, identify the motivations of future attackers, and suggest what technologies they may target. Additionally, strategic analysis can help put incidents into a broader context and can drive internal changes, enhancing the ability of any public or private organization to update risk management practices that reduce its exposure to risk.

At the same time, however, those sharing information often remained concerned about unintended or secondary uses of such information. For example, a party sharing vulnerability information with others would not want to see that security weakness serve as the basis of a future marketing campaign. Similarly, if information shared with the government in the name of computer security was then used for regulatory enforcement purposes, the risk associated with sharing increases, which is a disincentive to do so.

Data Handling: Once cybersecurity information is obtained, organizations have to properly manage its classification, handling, and destruction, among other concerns. Data handling is an important consideration for cyber defenders. For many private sector companies, data management may be informed by rules drawn from multiple jurisdictions, which are often not harmonized.

Defining Approaches That Will Work Today and Tomorrow

While the basic steps of information sharing are the same, how the process is and should be used to manage risks naturally varies. Different players have different capabilities to understand and act on cyber threats. The scale and scope of impacts based on those actions also differs. These differences are important because they affect what information industry players want or need from their peers and governments, and how they can use information to protect themselves and others.

Approximately 18 years ago in the U.S., Presidential Decision Directive 63: Protecting America's Critical Infrastructure[3] encouraged the formation of sector-based ISACs with U.S.-based members to improve information security. Microsoft was a founding member of the Information Technology ISAC in 1999. In 2002, the Homeland Security Act created a new category of information protection called Protected

[3] The White House, Fact Sheet: Protecting America's Critical Infrastructures: PDD 63 (May 22, 1998), *available at* http://fas.org/irp/offdocs/pdd-63.htm

Critical Infrastructure Information,[4] or PCII, in an attempt to address industry concerns about sharing with the government and information disclosure (e.g., Freedom of Information Act requests). While both policies sought to encourage voluntary sharing, results have been mixed for a variety of reasons that have been previously discussed, including the fact that not all members of the same community have an equal ability to act on cyber threat information.

There are times, of course, where reporting is mandatory, and Microsoft has long supported a federal breach notification law to eliminate the hodge-podge of state reporting laws that currently exist. But in the dynamic field of computer security, etching in stone what must be reported to whom regardless of whether the information is actionable is the wrong approach. At the same time, however, we need to ensure that those with important information share it with the right party, at the right time, for the right purpose, and with appropriate protections. This can be done both by creating incentives for, and removing disincentives to, such sharing.

As noted above, information sharing has and does work. But it works because the parties see that the benefits (better protection, detection and response) outweigh the risks. History also teaches, however, that information sharing tends to work best when those involved trust each other to respect informal and sometimes formal agreements (e.g., non-disclosure agreements) on information use and disclosure. Occasionally this sharing is ad hoc and unstructured, driven by events that bring participants together in a time of common need. But once that happens, the resulting relationships may form the basis for further, sustained collaboration, collaboration that continues long after the crisis has passed.

In other cases, information sharing arrangements are more formal and based on non-disclosure agreements, legal contracts, or membership agreements. These arrangements establish a clear set of expectations between the participants, including the type of information to be shared, how it can be used, and how the information will be protected – with consequences for those that do not adhere to the agreed upon conditions. As a result, formalized sharing tends to be the most visible form of sharing – including vendor-user relationships one would expect with cybersecurity service providers. Other examples include ISAC and the MAPP program discussed earlier. In a subset of these cases, extremely sensitive information is shared, such as the Department of Homeland Security's Enhanced Cybersecurity Services ("ECS") Program.[5]

Significantly, some of these sharing arrangements are now supported by automated tools with standardized formats, thus allowing machine-to-machine interactions that speed up response times dramatically. For example, malware signatures need not be manually transmitted and entered into detection tools; the entire process can be automated. Microsoft's Interflow is one such tool that allows cybersecurity professionals to exchange threat information using Threat Information eXpression ("STIX") and Trusted Automated eXchange of Indicator Information ("TAXII") to create automated, machine-readable threat and security information that can be shared across industries and groups in near real-time. This approach should help reduce costs and increase the speed of defense by automating processes that are currently performed manually.

---

[4] 6 U.S.C. § 133 (Section 214 of the Homeland Security Act of 2002).

[5] Department of Homeland Security, Enhanced Security Services, *available at* http://www.dhs.gov/enhanced-cybersecurity-services

How Congress Can Help

The two most important things Congress can do are (1) ensure that the information sharing arrangements that are working effectively are left undisturbed; and (2) encourage additional information sharing by providing protections for shared information and addressing risks posed by information sharing, including privacy risks. As you consider legislating in this area, I would suggest the below key principles to guide you.

1) New legislation should make clear that it is not meant to impact existing information sharing efforts.

2) New legislation should be scoped to cover information that reasonably enables defenders to protect against, detect, or respond to cyber threats (that is, attacks against the confidentiality, integrity and availability of data and systems).

3) New legislation should not impose additional burdens on industry, but rather incentivize sharing by providing greater protections for shared information. More specifically, the legislation should:

   - Not require the mandatory reporting of threat, vulnerability and incident information, except as necessary to provide breach notifications to consumers;
   - Protect threat, vulnerability, and incident information from inappropriate disclosure;
   - Restrict the use of voluntarily shared data, and prohibit secondary uses;
   - Require the data to be anonymized, except in clearly defined cases where such anonymization would undermine the use of that data (e.g., removing the IP addresses of a botnet server would render the data useless);
   - Require the government to seek a court order when seeking to pierce the veil of anonymity;
   - Require the government to share threat, vulnerability, and incident information with a company if that company (1) participates in information sharing and (2) can action the information. To the extent the information is sensitive and/or classified, Congress should direct the government to evaluate whether the information can be declassified or shared in a way that otherwise protects government interests;
   - Grant liability protection for sharing that occurs consistent with the legislation, without undermining contractual obligations between a company sharing information and its customers; and
   - Provide additional liability protections during well-defined government declared emergencies.

Thank you for the opportunity to testify and I look forward to working with the Committee on this effort.

Marsh & McLennan Companies, Inc.
1166 Avenue of the Americas
New York, NY 10036
+1 212 345 5000
Fax +1 212 345 4808

Testimony of

PETER J. BESHAR

Executive Vice President and General Counsel

Marsh & McLennan Companies

Before the United States Senate
Committee on Homeland Security & Governmental Affairs

"Protecting America from Cyber-Attacks:
The Importance of Information Sharing"

January 28, 2015
Washington, DC

Introduction

Good afternoon Chairman Johnson, Ranking Member Carper, and members of the Committee. I am Peter Beshar, the Executive Vice President and General Counsel of Marsh & McLennan Companies. I am grateful for the opportunity to participate in this important hearing about enhancing cyber resilience.

Marsh & McLennan operates through four market-leading brands — Marsh, Guy Carpenter, Mercer, and Oliver Wyman. Our 56,000 employees provide advice to clients across an array of industries in the areas of risk, strategy, and human capital. As the leading insurance broker in the world, Marsh has a unique perspective on the cyber insurance market.

The evolution in the sophistication and intensity of cyber threats has been astonishing. Just a few years ago, the principal form of cyber threat was a denial of service, or DDoS, attack that might disable or deface an organization's website for a brief period.

In 2013 and 2014, hackers turned their focus to the theft, particularly in the retail sector, of credit card and other personal data.

Last month, however, we saw an attack whose ramifications are far reaching. On December 17, Germany's Federal Office for Information Security reported that hackers had caused "massive damage" to an iron plant by disabling the electronic shut off systems on the plant's furnaces. Armed with "detailed knowledge of the industrial control systems," hackers utilized an elaborate spear phishing campaign to damage the entire plant.

This escalation of cyber-attacks to physical assets reflects the growing threat posed to our critical infrastructure.

Senior government officials who previously warned of the threat of a "Cyber Pearl Harbor" appear increasingly prescient. Indeed, the government has been out in front of most of the business community in identifying the significance of the threat posed by cyber-attacks. The adoption of the NIST Cybersecurity Framework in early 2014 has helped organizations — large and small — conduct gap assessments regarding their cyber preparedness. Though under no obligation to do so, the FBI, the Secret Service, and other government agencies have repeatedly alerted companies and non-profit organizations that their systems had been breached. And just last month, this Committee and the entire Congress took an important step

in advancing cyber threat information sharing by formally authorizing the National Cybersecurity and Communications Integration Center (NCCIC) at the Department of Homeland Security.

I would like to focus my remarks today on the importance of incentives, with a particular focus on cyber insurance, to drive behaviors in the marketplace.

What is cyber insurance?

Broadly stated, there are three core types of cyber insurance.

The most basic provides protection for out-of-pocket expenses that a company incurs in the wake of a data breach. These expenses include notifying individuals, setting up call centers and providing credit monitoring.

The second form of coverage protects a company if its computer network is effectively shut down for days or longer. With this broader business interruption coverage, a company can recover the actual harm it suffers in the form of lost profits or extra expenses.

The third type of coverage is for harm caused to an insured's customers or consumers as a result of a significant breach. This is called third-party coverage.

Why does cyber insurance matter?

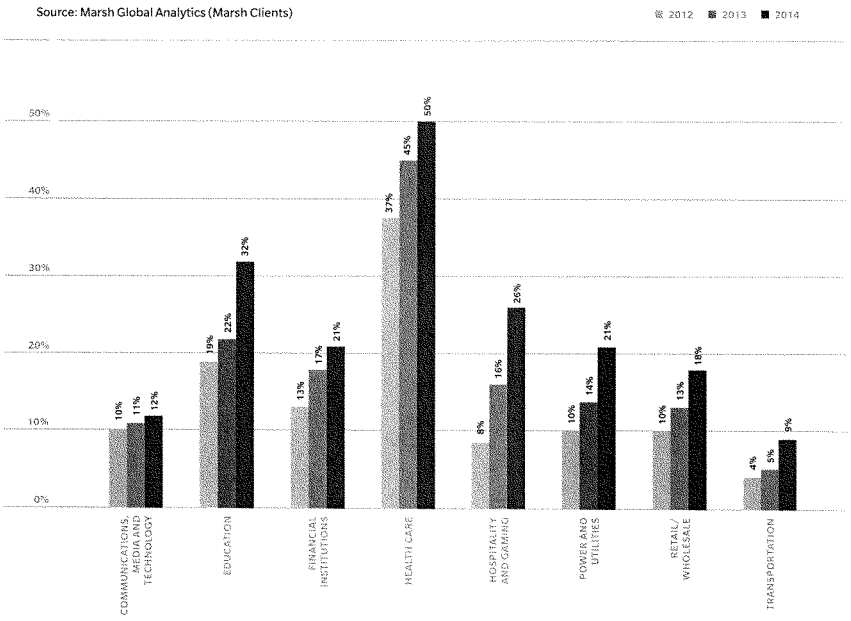
Cyber insurance creates important incentives that drive behavioral change in the marketplace. As a threshold matter, the simple act of applying for insurance forces insureds to assess the strength of their cyber defenses. Whether prodded by a board of directors or by a desire to get coverage as cheaply as possible, companies conduct gap analyses against industry benchmarks, including the NIST Framework and ISO 27001. Underwriters want to know whether the company has an incident response plan, disciplined procedures for patching software and robust protocols for monitoring its vendor network. Thus, this process, in and of itself, is an important risk mitigation tool.

Once a cyber policy is purchased, the insurer then has the incentive to help its policyholders avoid and mitigate cyber-attacks. As a result, many insurers now offer monitoring and rapid response services to policyholders.

Not surprisingly, the market is responding. In 2014, the number of Marsh clients purchasing standalone cyber coverage increased by 32% over 2013. And these numbers do not capture those clients that purchase cyber protection as part of a blended policy covering other lines.

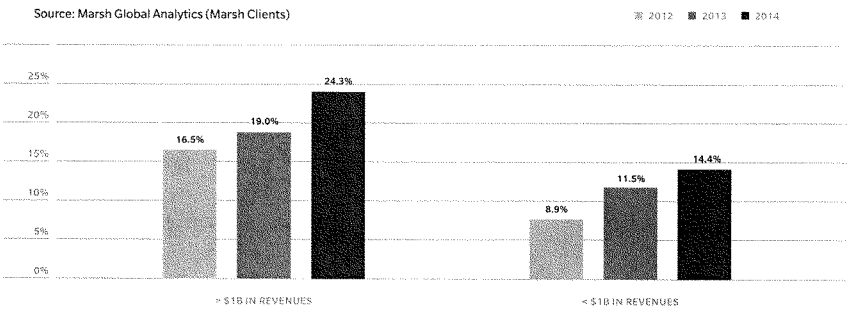
Marsh also tracked cyber insurance take-up rates by industry sector. As reflected in the chart below, the highest take-up rates for cyber insurance in 2014 were in: (1) health care; (2) education; and (3) hospitality and gaming. These industries handle a large volume of sensitive personal information, including health care data, Social Security numbers, and credit card information. In fact, as a result of statutes like HIPAA, the take-up rates in health care are higher than any other sector of the economy. There were also marked increases in the power and utilities sector.

Cyber Insurance Take-up Rates by Industry



A key takeaway from the cyber-attacks of 2014 has been the importance of securing a company's vendor network. Hackers gained access to Fortune 500 companies by stealing passwords and log-in credentials of smaller vendors, including air conditioning and food delivery companies. Thus, a large company's defense is only as good as the weakest link amongst its vendors. Accordingly, Marsh analyzed segment data to assess how the size of a company's business impacts its decision whether to purchase cyber insurance. While take-up rates increased noticeably in both large and small companies, there is a substantial, and indeed growing, gap between the two segments.

Cyber Insurance Take-up Rates by Revenue

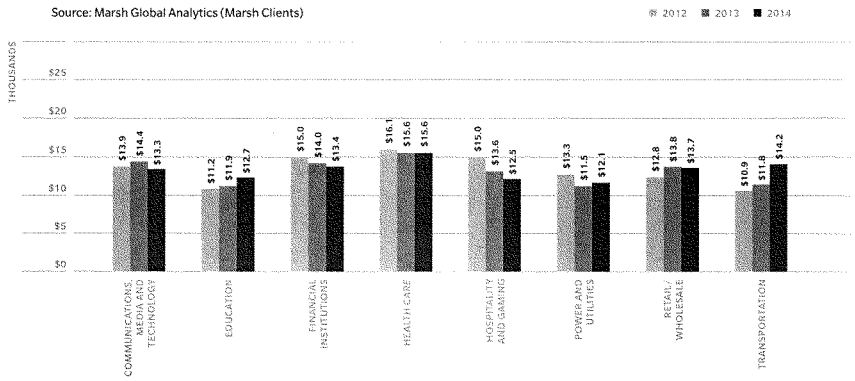


Finally, Marsh tracked cyber insurance pricing trends. Contrary to expectations, pricing trends year-over-year were relatively stable. While certain sectors including transportation and education saw increases, many other sectors saw price decreases.

A deeper analysis of the retail sector is informative. In the fourth quarter of 2014, two trends became evident. First, renewal rates increased by 5% on average and as much as 10% for certain clients. Underwriters have begun differentiating sharply between those retailers that have implemented robust point of sale controls, such as end-to-end encryption, and those that have yet to do so.

Thus, insurance market forces, particularly in the retail sector, are creating important incentives for companies to invest in more robust cyber defenses. In numerous industries, insurers have played a crucial role in developing sound risk mitigation practices. For example, in the area of workers' compensation, insurers identified a set of best practices and provided incentives for employers to reduce injuries and deaths in the workplace. Over the past twenty years, the number of workplace fatalities has fallen by over 35%. This same dynamic can occur in the cyber arena with insurers providing incentives for those companies that implement risk mitigation strategies like two-factor authentication and detonation software.

Cyber Insurance Coverage Price Per $1 Million Across Industry Sectors



Overall, the cyber insurance market remains modest in scale. Marsh estimates that the total written premiums for cyber insurance in 2014 were approximately $2 billion. While up significantly, these numbers are a small fraction of total written premiums in the US insurance market of more than $1 trillion.

As Deputy Treasury Secretary Raskin recently stated in a speech to the Texas Bankers Association, cyber insurance is one element, among many, of a comprehensive risk mitigation strategy. [i]

i Deputy Secretary Raskin: "Cyber insurance cannot protect your institutions from a cyber incident any more than flood insurance can save your house from a storm surge or D&O insurance can prevent a lawsuit. But what cyber risk insurance can do is provide some measure of financial support in case of a data breach or cyber incident. And, significantly, cyber risk insurance and the associated underwriting processes can also help bolster your other cybersecurity controls. Qualifying for cyber risk insurance can provide useful information for assessing your bank's risk level and identifying cybersecurity tools and best practices that you may be lacking."
http://www.treasury.gov/press-center/press-releases/Pages/jl9711.aspx

Information Sharing

As this Committee has recognized, enhanced information sharing between industry and government is another important component of a comprehensive risk mitigation strategy.

Working in isolation, neither the private sector nor the public sector has the tools to protect our nation's critical assets. This is particularly so given that 85% of our country's critical infrastructure is owned and operated by the private sector. To accelerate the identification and detection of emerging threats, there needs to be greater trust and real-time threat information sharing between the private and public sectors. And it should be reciprocal to the greatest extent possible.

Accordingly, we support the sharing of cyber threat indicators, including malware threat signatures and known malicious IP addresses, with the NCCIC provided that reasonable liability protections and privacy considerations are addressed. We believe that the dual considerations of national security and individual privacy can be fairly and appropriately balanced.

I commend you for convening this hearing and look forward to addressing any questions that you might have.

Chairman Johnson, ranking member Carper, members of the Committee, thank you for the opportunity to testify. I am Richard Bejtlich, Chief Security Strategist at FireEye. I am also a nonresident senior fellow at the Brookings Institution, and I am pursuing a PhD in war studies from King's College London. I began my security career as a military intelligence officer in 1997 at the Air Force Information Warfare Center.

My employer, FireEye, provides software to stop digital intruders, with 2,200 customers in 60 countries, including 130 of the Fortune 500. Our Mandiant consulting service, known for its 2013 report on Chinese PLA Unit 61398, helps companies identify and recover from intrusions.

Who is the threat?

We have discovered and countered nation-state actors from China, Russia, Iran, North Korea, and other countries. The Chinese and Russians tend to hack for commercial and geopolitical gain. The Iranians and North Koreans extend these activities to include disruption via denial of service and sabotage using destructive malware. We have helped companies counter organized crime syndicates in Eastern Europe and elsewhere. Our report on FIN4 described intrusions to facilitate insider trading. We have also encountered hacker teams for hire, and others who develop and sell malware.

How active is the threat?

In March 2014, the Washington Post reported that in 2013, federal agents, often the FBI, notified more than 3,000 U.S. companies that their computer systems had been hacked. This count represents clearly identified breach victims. Many were likely compromised more than once.

Who is being breached?

Serious intruders target more than government, defense, and financial victims. No sector is immune. FireEye recently published two reports, showing that 96% of organizations we could observe had suffered compromise during two six-month periods. The best performing sector was aerospace and defense, with "only" 76% of sampled organizations suffering a breach.

In 2014, the top sectors assisted by our Mandiant consultants included business and professional services, retail, finance, media and entertainment, and construction and engineering.

How do victims learn of a breach?

In 70% of cases, someone else, likely the FBI, tells a victim about a serious compromise. Only 30% of the time do victims identify intrusions on their own. The median amount of time from an intruder's initial compromise, to the time when a victim learns of a breach, is currently 205 days. This number is better than our 229 day count for 2013, and the 243 day count for 2012. Unfortunately, it means that, for nearly 7 months after gaining initial entry, intruders are free to roam within victim networks.

What is the answer?

So-called "network hygiene" only takes you so far. I recommend a "best value approach" over "low-cost, technically acceptable" technologies, but there is no purely technical solution to information security. The best strategy is to prevent as many intrusions as possible, quickly detect attackers who evade defenses, and respond appropriately, before the adversary accomplishes his mission. Strategically significant intrusions do not happen at "the speed of light." It takes intruders time, from hours to weeks, to move from an initial foothold to the information they seek.

Defenders win when they stop intruders from achieving their objectives. To that end, organizations, including the federal government, should track the number of intrusions that occur per year, and the amount of time that elapses from the initial entry point to the time of discovery, and from the time of discovery to the removal of the threat. These metrics are "the score of the game" that mark a successful security program.

What is threat intelligence?

"Threat intelligence" refers to technical information about the tactics, tools, and procedures used by intruders to abuse software and networks. It does not depend upon sensitive information about U.S. persons. The President's proposal is compatible with this understanding. It offers privacy protections to

"reasonably limit the acquisition, interception, retention, use and disclosure of cyberthreat indicators that are reasonably likely to identify specific persons."

Not all threat intelligence is created equal. Intelligence in the virtual world is similar to intelligence in the physical world. Acting on intelligence means placing it in proper context, assessing the trustworthiness of the source, and leveraging the capabilities of the recipient.

Will sharing threat intelligence help?

Threat intelligence can help defenders more quickly resist, identify, and respond to intrusions, but only if the organization is postured to succeed. Until one invests in sound strategy, processes, people and technology, no amount of information sharing or threat intelligence will be sufficient.

Who shares threat intelligence, and what are the challenges?

Sharing threat intelligence refers to three cases: 1) from the government to the private sector; 2) within the private sector; and 3) from the private sector to the government. All three face challenges.

In the government-to-private scenario, I encourage officials to grant clearances to private security teams not working on government contracts. The government should also augment its narrative style intelligence reports with digital appendices that list threat data in machine-readable form, similar to that offered by www.openioc.org.

In the private-to-private case, I recommend creating information sharing groups. Adversaries often target whole sectors at once, so it helps to have peer companies compare notes.

The private-to-government case is the most contentious, for two reasons. First, companies are reluctant to publicize security breaches, beyond what is necessary to comply with laws and standards. The private sector fears penalties if they disclose incidents to the government. Companies should not be held liable for voluntarily reporting incidents. Accordingly, the White House proposal prohibits the use of so-called "cyberthreat indicators" in any regulatory enforcement action.

Second, some privacy advocates believe that liability protection will let companies submit customer personal information to the government. This position does not reflect the reality of threat intelligence as defined earlier. Proper threat intelligence contains tactics, tools, and procedures used by intruders to abuse software and networks. It does not contain personal data from or about customers, if properly formatted.

Finally, I'd like to mention an intelligence sharing pilot program organized by the Department of Energy (DoE), the North American Electric Reliability Corporation (NERC), and the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). Along with power companies, they operate the Cybersecurity Risk Information Sharing Program, or CRISP. Participants use commercial security technology at their network borders, and voluntarily share their findings with the Pacific Northwest National Laboratory (PNNL). PNNL extracts threat intelligence from the raw data, and shares it with other CRISP members, including DoE. DoE also shares what it discovers on DoE networks with CRISP participants. This program could provide a model for other sectors, and for the government as a whole.

I look forward to your questions.

KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

STATEMENT OF GREGORY T. NOJEIM

SENIOR COUNSEL AND DIRECTOR OF THE FREEDOM, SECURITY AND TECHNOLOGY PROJECT

THE CENTER FOR DEMOCRACY AND TECHNOLOGY

HEARING BEFORE THE SENATE HOMELAND SECURITY AND GOVERNMENT AFFAIRS COMMITTEE ON PROTECTING AMERICA FROM CYBER ATTACKS: THE IMPORTANCE OF INFORMATION SHARING

January 28, 2015

Chairman Johnson, Ranking Member Carper, and members of the Committee:

Thank you for the opportunity to testify today on behalf of the Center for Democracy and Technology. CDT is a nonpartisan, non-profit technology policy advocacy organization dedicated to protecting civil liberties and human rights on the Internet, including privacy, free speech, and access to information. I direct the Freedom, Security and Technology Project at CDT. It works to develop and promote policies that safeguard individuals from overbroad government surveillance while preserving the government's ability to protect national security against evolving threats. We applaud the Committee for holding the first hearing of the 114th Congress on cybersecurity, an important issue that the Homeland Security and Government Affairs Committee has a key role in addressing.

Today I will explain how Congress can embrace cybersecurity information sharing policies with appropriate authorities and safeguards that enhance both privacy and security. I will first describe the cybersecurity threat and explain the role that information sharing can play in countering that threat. I will then identify different approaches to encouraging information sharing as well as the essential civil liberties attributes of a successful information sharing policy. I will also measure pending legislative proposals against those attributes.

Cyber attacks represent a significant and growing threat. Earlier this year, a study by the Center for Strategic and International Studies estimated that the global cost of cyber crime has reached over $445 billion annually.[1] According to an HP study released in October 2014, the average cost of cyber crime to each of 50 U.S. companies surveyed had increased to $12.7 million per company, up

[1] Center for Strategic and International Studies, *Net Losses: Estimating the Global Costs of Cybercrime* (June 2014), *available at* http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

from $6.5 million per company just four years ago.[2] Frequency and intricacy of attacks has increased as well. The same study concluded that the number of successful attacks per company per year has risen by 144 percent since 2010, while the average time to resolve attacks has risen by 221 percent.[3]

Major cyber attacks represent an ongoing hazard to our financial and commercial sectors, with potential to harm both important institutions and individual online users. 2014 saw major attacks affecting large numbers of people against companies such as Target, J.P. Morgan Chase, Home Depot, and most recently, Sony Pictures.[4] In addition to direct harms – which are substantial – these large scale and highly publicized attacks threaten to chill use of online services.

Unfortunately, there is no "silver bullet" that will wipe away the danger of cyber attacks. Cyber attacks are constantly evolving, and defending against them requires a range of actions from both governmental and private entities. Most successful attacks could be stopped by basic security measures, such as frequently changing passwords, patching servers, detecting insider attacks, and educating employees about risks. Thus, while information sharing is an important tool for enhancing cybersecurity, it is also important to maintain a broad perspective and encourage other measures that would also increase digital hygiene.

I. Information sharing is an important component of an effective cybersecurity policy and must be accompanied by appropriate privacy protections at all levels.

There is widespread agreement that the sharing of information about cyber attacks, threats and vulnerabilities is a valuable component of an effective cybersecurity policy. As detailed by the National Institute of Standards and Technology's draft "Guide to Cyber Threat and Information Sharing," benefits of information sharing include: 1) Greater awareness of specific cyber threats, and of defenses against them, 2) development of more robust threat indicators, 3) enhanced defensive agility, 4) rapid notification to victims of cyber attacks, and 5) improved ability to efficiently process and preserve criminal evidence.[5]

While cyber attacks sometimes employ malware that exploits "zero-day" vulnerabilities – previously undiscovered vulnerabilities – many cyber attacks are repetitive. Cyber criminals often recycle previously used vulnerabilities, deploying old exploits on systems and software that were not previously attacked. Information sharing can limit the effectiveness of these "recycled" threats: the victim of the first attack can share information that can be used by other potential victims to defend against future iterations of the same attack. Further, by making cyber criminals take additional steps to modify their attacks rather than simply replicating attacks on previously used vulnerabilities, the cost of engaging in cyber attacks increases, thereby decreasing the incentive to engage in them.

---

[2] HP, *Ponemon Institute 2014 Cost of Cyber Crime Study* (September 2014), *available at* http://h17009.www1.hp.com/pub/msc/29FD917C-64F3-46A7-955C-EF9D2F8D9E3C.pdf.

[3] *Id.*

[4] Sharone Tobias, *2014: The Year in Cyberattacks*, Newsweek (December 31, 2014), *available at* http://www.newsweek.com/2014-year-cyber-attacks-295876.

[5] Chris Johnson et al, *Guide to Cyber Threat Information Sharing*, National Institute of Standards and Technology (October 2014), 7, *available at* http://csrc.nist.gov/publications/drafts/800-150/sp800_150_draft.pdf.

Many information sharing mechanisms are already in place, are providing benefits, and should be supported, improved, and built upon. They include sector-specific Information Sharing and Analysis Centers (ISACs) and the DHS Enhanced Cybersecurity Services Program.[6]

The cybersecurity proposal the Administration announced earlier this month[7] includes an important requirement for cybersecurity information sharing: Privacy protections should be applied prior to *any level* of information sharing. Privacy safeguards apply to 1) company sharing with the government, 2) company sharing with the private information sharing hubs the proposal would authorize, and 3) inter-agency sharing. The Administration proposal requires front-end protections prior to a company's sharing of cyber threat indicators – reasonable steps to remove personally identifiable information believed to be unrelated to the threat – as well as privacy guidelines to govern information sharing among government agencies.[8] This contrasts with the Cyber Intelligence Sharing and Protection Act (CISPA),[9] which does not require reasonable efforts to remove such PII prior to sharing, and requires instantaneous, real-time transfer of information, including communications content, from the Department of Homeland Security (DHS) to other government agencies – including the National Security Agency (NSA). While the Administration proposal has ambiguities and omissions that might render it less effective than it could be in protecting privacy,[10] it demonstrates that a viable information sharing policy can empower all players in the cybersecurity ecosystem to rapidly transmit cyber threat information with civil liberties protections built in.

Quite simply, the American public should not – and need not – be forced to choose between being hacked by cyber criminals and being snooped on by the government.

II. Information sharing among private entities avoids significant civil liberties concerns and should be encouraged.

In this section and the next, I describe two approaches to information sharing that we favor because they minimize civil liberties risks – 1) private-to-private information sharing and 2) information sharing facilitated by limited amendments to the surveillance statutes that do not necessitate creation of complex, new programs.

---

[6] US Dept. of Homeland Security, Enhanced Cybersecurity Services (September 8, 2014) http://www.dhs.gov/enhanced-cybersecurity-services

[7] The White House, Updated Department of Homeland Security Cybersecurity Authority and Information Sharing, Section by Section, Analysis (January 13, 2015), http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/information-sharing-legislation-section-by-section.pdf.

[8] Some in industry contend that an obligation to endeavor to remove personally identifiable information before cyber threat indicators are shared would prove too burdensome, particularly for small companies. We believe that the same automated systems that would identify the threat information that could be shared because it meets the definition of cyber threat indicator would be configured to omit irrelevant PII, thus mitigating the burden. Under questioning by Rep. Adam Schiff (D-CA) at a 2013 House Intelligence Committee hearing, certain industry representatives confirmed that a requirement to remove PII irrelevant to a cyber threat prior to information sharing is reasonable and would not dissuade them from participating in a cybersecurity program. *See*, https://www.eff.org/deeplinks/2013/02/industry-experts-congress-we-can-remove-personally-identifiable-information.

[9] H.R. 234, 2015.

[10] See infra, Section VII.

The most important type of information sharing to incentivize is that between private entities. This is because entities in the private sector own and operate most of the critical infrastructure in the country that must be protected against cyber attacks. Information sharing can occur directly between private entities, without any government involvement. Threat analysis would occur more often at the private company level as opposed to within the government.

This not only makes the process more efficient, it does not raise many of the privacy and civil liberties concerns attendant to private-to-government information sharing. For example, private-to-private sharing of information does not convey communications content to the NSA, and does not raise concerns that this sharing of information could result in a new surveillance program through a backdoor, which Congress did not intend to authorize.

The White House proposal does little to encourage company-to-company information sharing – it extends no liability protection for this sharing – and this is a significant shortcoming. Instead, the Administration proposal encourages private-to-private sharing only through information-sharing hubs that the government has designated as such. This approach may have been taken because the Administration and industry have had difficulty in agreeing on a mechanism to ensure that companies play by the rules when they share information company-to-company. We believe such a mechanism is a pre-requisite to expanding such sharing.

One barrier to company-to-company information sharing – antitrust concerns – was largely put to rest by a Department of Justice/Federal Trade Commission policy guidance issued last year.[11] The U.S. Chamber of Commerce correctly read the guidance as a positive step and as a statement, "...that antitrust concerns are not raised when companies share cyber threat information with each other...."[12]

In addition to sharing between private entities, sharing from governmental to private entities represents an area for opportunity. To the extent that the government has information that would be useful for private entities to defend themselves, it should declassify it as necessary and share it. It can do this under current law. As with private-to-private sharing, government-to-private sharing can augment cybersecurity without the same risks to privacy that private-to-government sharing creates.

III. Current law permits sharing to protect oneself, but not to protect others. This can and should be addressed with a narrow amendment.

The other approach to information sharing that we commend to you involves only limited amendments to surveillance statutes. Current law does allow some degree of cybersecurity information sharing, but it does not meet present cybersecurity needs. Communication service providers are permitted to monitor their own systems and to disclose to governmental entities,

---

[11] *Department of Justice and Federal Trade Commission: Antitrust Policy Statement on Sharing of Cybersecurity Information*, April 14, 2014, http://www.justice.gov/opa/pr/justice-department-federal-trade-commission-issue-antitrust-policy-statement-sharing.

[12] *See*, Ann M. Beauchense, *Agencies' Statement on Antitrust and Cyber Information Sharing is Encouraging*, The US Chamber of Commerce (April 11, 2014), *available at* https://www.uschamber.com/blog/agencies-statement-antitrust-and-cyber-information-sharing-encouraging.

and other service providers, information about cyber attacks for the purpose of protecting their own networks. In particular, the Wiretap Act provides that it is lawful for any provider of electronic communications service to intercept, disclose or use communications passing over its network while engaged in any activity that is a necessary incident to the protection of the rights and property of the provider.[13] This includes the authority to disclose communications to the government or to another private entity when doing so is necessary to protect the service provider's network. Likewise, the Electronic Communications Privacy Act (ECPA) permits providers to disclose stored communications[14] and customer records[15] to any governmental or private entity in order to protect its own systems. Furthermore, the Wiretap Act provides that it is lawful for a service provider to invite in the government to intercept the communications of a "computer trespasser" if the owner or operator of the computer authorizes the interception and there are reasonable grounds to believe that the communication will be relevant to an investigation of the trespass.[16]

While current law authorizes providers to monitor their own systems and to voluntarily disclose communications necessary to protect *their own* systems, the law does not authorize service providers to make disclosures to other service providers or to the government to help protect the systems of *other* service providers. Thus, there may be a need for an exception to the Wiretap Act and ECPA to permit disclosures to others about specific attacks.

Any such exception should be narrow so that routine disclosure of Internet traffic to the government or other service providers remains clearly prohibited. It should bar unrestricted disclosure to the government of vast streams of communications data, and permit only the disclosure of carefully defined cyber attack signatures, cyber attack attribution information, and the method or the process of a cyber attack. It should also include privacy protections such as those described below. Rather than taking the dangerous step of overriding the surveillance statutes, such a narrow exception could operate within them, limiting the impact of cybersecurity information sharing on personal privacy. Companies that share information under such a narrow exception will enjoy the liability protections already built into theses statutes. As other statutes that limit information sharing for cyber security purposes are identified, Congress may consider additional exceptions.

We encourage you to embrace this focused approach to enhancing cybersecurity information sharing. If it proves inadequate to promote information sharing, broader, riskier approaches that operate "notwithstanding any law" can be considered. However, because all of the major cybersecurity information sharing proposals take what we believe to be the overbroad, risky approach of trumping all other laws, they are addressed in some detail below. The civil liberties protections we describe are an important part of any cybersecurity information sharing program, but are particularly important for the broader, riskier approaches.

---

[13] 18 U.S.C. § 2511(2)(a)(i).

[14] 18 U.S.C. § 2702(b)(3)).

[15] 18 U.S.C. § 2702(c)(5)).

[16] 18 U.S.C. § 2511(2)(i).

IV. Civilian control of cybersecurity activity involving the civilian private sector should be maintained.

For numerous reasons, it is critical that if private, civilian entities are authorized to share users' communications information with governmental entities for cybersecurity reasons, that information should flow to and be controlled by a civilian agency – DHS – rather than a military agency, such as the NSA or Cyber Command.

First, civilian agencies are more transparent; for understandable reasons, intelligence agencies are more opaque. Details about the scope and nature of civilian agency activities, privacy protections – such as minimization rules – and interpretation of relevant law are all more available from civilian agencies. The Snowden disclosures demonstrate the contrasting approach of military intelligence agencies. Until June 2013, the public was unaware that the PATRIOT Act had been interpreted to authorize bulk collection of metadata, and that domestic phone call and Internet activity records were being collected, used, and retained for years.

Second, DHS has a well-established, statutory, and well-staffed privacy office. The NSA's privacy office was established just last year, with a huge mandate and relatively tiny staff.

Third, the NSA has multiple missions that can create conflicts about how to treat the cyber threat and cyber vulnerability information that it receives. In addition to its mission of defending information security, the NSA is also tasked with gathering signals intelligence, including through use of vulnerabilities. If the NSA receives information regarding a cyber threat or cyber vulnerability, its intelligence-gathering mission may be prioritized, leading the agency to hide, preserve and exploit the vulnerability, rather than disclose it to the entity that could patch the vulnerability.[17] It is for this precise reason that the President's independent Review Group on Intelligence and Communications Technologies recommended moving NSA's information assurance mission into a separate agency in the Department of Defense.[18] Further, while information may be shared to respond to cyber threats, NSA may re-purpose it to support its intelligence-gathering mission, creating a new surveillance program operating under a cybersecurity umbrella.

Finally, public trust in military intelligence agencies was severely compromised in both the U.S. and abroad by the NSA activities that Edward Snowden disclosed. Mass collection of sensitive communications and communications information pertaining to individuals not suspected of

---

[17] Exploitation of vulnerabilities is regularly used by the NSA for signals intelligence purposes. *See e.g.*, Ryan Gallager and Glenn Greenwald, *How the NSA Plans to Infect Millions of Computers With Malware*, The Intercept (March 12, 2014), available at https://firstlook.org/theintercept/2014/03/12/nsa-plans-infect-millions-computers-malware/; *see also*, Barton Gellman and Ashkan Soltani, *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say*, The Washington Post (October 30, 2013), *available at* http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

[18] *See, The President's Review Group on Intelligence and Communications Technologies, Liberty and Security in a Changing World*, (Dec. 12, 2013), 185, *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf ("Those charged with offensive responsibilities still seek to collect SIGINT or carry out cyber attacks. By contrast, those charged with information assurance have no effective way to protect the multitude of exposed systems from the attacks. The SIGINT function and the information assurance function conflict more fundamentally than before. This conclusion supports our recommendation to split the Information Assurance Directorate of NSA into a separate organization.")

wrongdoing has led to strong demands for greater protections. If NSA or Cyber Command were to serve as the government entity receiving cyber threat information from communications service providers, it would almost certainly mean less trust, and therefore less corporate participation. Indeed, in the wake of revelations regarding the PRISM program, many major tech companies stated that they would not voluntarily share users' information or private communications with the NSA.[19] Thus, preserving civilian control by putting a civilian agency in charge of cyber threat indicators shared by the civilian sector with the government will not only enhance civil liberties, it would increase the effectiveness of this effort to promote security.

Main cybersecurity proposals have inadequately addressed this issue. While the Administration proposal requires application of privacy guidelines before information shared with DHS is sent to military agencies including the NSA, it is not clear that the guidelines will offer sufficient protections.[20] CISPA is even more problematic. It requires real-time sharing from DHS to NSA,[21] effectively creating the same concerns as company information sharing directly to the military. The Senate Intelligence Committee's Cybersecurity Information Sharing Act (CISA), reported out in 2014 takes the same problematic approach as does CISPA.[22]

V. Use restrictions should ensure that information shared for cybersecurity purposes is only used for cybersecurity, with narrow exceptions.

Cybersecurity legislation should not be warped into a backdoor wiretap, whereby communications shared to respond to cyber threats are provided to law enforcement agencies that use them for investigation of unrelated offenses, or to intelligence agencies that use them for national security purposes other than cybersecurity. Doing so undermines the privacy protections built into the Wiretap Act, ECPA, and the Foreign Intelligence Surveillance Act, and the critical role of an independent judiciary in authorizing surveillance for criminal and foreign intelligence investigations. For example, the user communications information that a company shares with the government could be stored, then mined for information relevant to crime or national security using identifiers of U.S. persons. Instead of applying for the court order that would permit access to such information under a surveillance statute when the information pertains to a US person or a person in the U.S., the government could simply pull the information from "the corporate store" as the NSA does for the telephone call records it collects in bulk under Section 215 of the PATRIOT Act.[23] Overbroad use permissions also create a perverse incentive for government to retain communications content, and even pressure companies into providing it more frequently than is necessary for cybersecurity.

---

[19] *See*, Gregory Ferenstein, *Report: NSA Collects Data Directly From Servers of Google, Apple, Microsoft, Facebook and More*, Tech Crunch (June 6, 2013), *available at* http://techcrunch.com/2013/06/06/report-nsa-collects-data-directly-from-servers-of-google-apple-microsoft-facebook-and-more/; *see also*, Chenda Ngak, *Apple, Google, Facebook, Yahoo, Microsoft, Paltalk, AOL issue statements of denial in NSA data mining*, CBS News (June 7, 2013), *available at* http://www.cbsnews.com/news/apple-google-facebook-yahoo-microsoft-paltalk-aol-issue-statements-of-denial-in-nsa-data-mining/.

[20] See infra, Section VII.

[21] H.R. 234, Sec. 2(b)(4), 2015.

[22] S. 2588, Sec. 5(c)(1)(C), 2014.

[23] See Patrick Toomey, ACLU, "Let's Lock Down the NSA's Shadow Database," https://www.aclu.org/blog/national-security/lets-lock-down-nsas-shadow-database.

Some law enforcement use of cyber threat information is appropriate. For example, the goal of improving cybersecurity is promoted by prosecuting those who propagate attacks. Permitting information shared with government for cybersecurity reasons to be used for investigation and prosecution of cybersecurity crimes is logical, if those crimes are carefully described. Allowing information to be used by law enforcement to prevent imminent risk of death or serious bodily harm is also a sensible limitation.

Thus, cybersecurity legislation should make it clear that information shared under the bill can be used for cybersecurity purposes (to protect computers against cyber attacks and to mitigate such attacks), to investigate and prosecute people for engaging in such attacks, and to prevent imminent risk of serious bodily harm or death.

VI. Congress should not authorize countermeasures that amount to "hacking back" and should not extend liability protection to "hacking back."

In considering new cybersecurity policies, Congress should be careful to provide no authority to engage in countermeasures against cyber attacks that amount to "hacking back" against entities believed to have perpetrated the original cyber attack. Allowing such countermeasures – or providing liability protection for them – risks opening a Pandora's Box of unintended results that could do far more harm than good for Internet infrastructure and security.

The recent cyber attack against Sony Pictures highlights two of the greatest problems that authorization for such countermeasures would raise: attribution and escalation. It can be extremely difficult to reliably ascertain the source of a cyber attack and to finger the responsible party.[24] Hackers can not only obscure the source of their attack, but also leave a "false trail" that will lead to misattribution.[25] Authorizing companies to use countermeasures that compromise data that is not on their own networks risks harm innocent third parties. Limiting liability for causing such harm would only encourage it.

Private "hacking back" also risks escalation with national security implications that go far beyond the interests of the company engaging in the hack back. As computer security expert Bruce Schneier notes, "The blurring of lines between individual actors and national governments has been happening more and more in cyberspace."[26] Authorizing hacking back risks companies engaging in hostile acts against foreign nations and their agents, potentially leading to a series of increasingly damaging cyber attacks, or even kinetic attacks. The possibility of misattribution

---

[24] *See*, Bruce Schneier, *Attributing the Sony Attack*, Scneier on Security (Janary 7, 2015), *available at* https://www.schneier.com/blog/archives/2015/01/attributing_the.html ("When it's possible to identify the origins of cyberattacks -- like forensic experts were able to do with many of the Chinese attacks against US networks -- it's as a result of months of detailed analysis and investigation").

[25] *See*, Jack Goldsmith, *How Cyber Changes the Laws of War*, EJIL (2013), Vol. 24 No. 1, 129–138, 132, *available at* http://ejil.oxfordjournals.org/content/24/1/129.full.pdf ("A thoughtful adversary can hide its tracks by routing attacks or exploitations through anonymizing computers around the globe. In 2009, a denial-of-service attack – a massive spam-like attack that clogs channels of communication – brought down some American and South Korean websites. Early reports said that the attack came from North Korea, but a few weeks later it was learned that the attack originated in Miami (and possibly, before Miami, elsewhere) and was routed through North Korea. It is still not known for sure who launched the attack, or from where.")

[26] Bruce Schneier, *Attributing the Sony Attack*, Schneier on Security (January 7, 2015), *available at* https://www.schneier.com/blog/archives/2015/01/attributing_the.html.

significantly heightens the escalation problem. A foreign country could engage in a cyber attack against a U.S. company and leave a false trail leading to another nation – something that has been discussed as a viable possibility for the Sony attack[27] – with the goal of provoking an international incident between that nation and the United States. An activity with this level of risk is not something a private company should be authorized to engage in.

Despite the serious concerns about countermeasures that could affect data not on one's own network, authorization of countermeasures and liability protection for using them has received increased attention in recent years. CISA and the 2012 SECURE IT Act would have explicitly authorized countermeasures without adequate limitations,[28] while CISPA strongly risks authorizing problematic countermeasures.[29] The Administration's proposal does not include new authority for engaging in problematic countermeasures.

VII. The privacy provisions of the Administration cybersecurity proposal offer a path forward on some issues, but not on others.

The Administration's cybersecurity proposal wisely requires application of privacy protections prior to all levels of sharing. On the front-end, companies are required to make reasonable efforts to strip out information that can be used to identify specific persons prior to sharing with the government. Within government, inter-agency sharing is to be regulated by privacy guidelines, which must establish rules for 1) destruction of irrelevant information, 2) anonymizing information retained, 3) law enforcement use, and 4) the possibility of disciplinary measures against government employees and agents for privacy violations.

However, the privacy protections have ambiguities and omissions that could severely undercut their effectiveness. While companies would be required to make reasonable efforts to remove personal information prior to sharing, this only includes information that is " reasonably believed to be unrelated to [a] cyber threat." Personally identifiable information about a *victim* of a cyber attack will often include information "related to a cyber threat." Depending on the circumstances, such information may, or need not, be shared to describe or counter the threat. Thus, reasonable efforts to remove personally identifiable information that is "not necessary to describe or counter the cyber threat" should instead be required.

It is difficult to evaluate how effective the privacy guidelines called for in the Administration's proposal will be as they are, of course, not yet written. The bill should provide more guidance about what should be included in the privacy guidelines. In addition to the four specific requirements set forth in the draft, Congress should require that the privacy guidelines comport

---

[27] *See*, Jack Goldsmith, *The Sony Attack: Attribution Problems, and the Connection to Domestic Security*, Lawfare (December 19, 2014), *available at* http://www.lawfareblog.com/2014/12/the-sony-hack-attribution-problems-and-the-connection-to-domestic-surveillance/ ("much more importantly, it is at least possible that some other nation is spoofing a North Korean attack. For if the United States knows the characteristics or signatures of prior North Korean attacks, then so too might some third country that could use these characteristics or signatures – "specific lines of code, encryption algorithms, data deletion methods, and compromised networks," and similarities in the "infrastructure" and "tools" of prior attacks – to spoof the North Koreans in the Sony hack").

[28] S. 2588, Sec. 4(b), 2014; S. 3342 Sec. 102(a), 2012.

[29] H.R. 234, Sec. 3(a), 2015.

with the Fair Information Practice Principles that the DHS promulgated in 2008,[30] during the George W. Bush Administration. Subjecting any privacy guidelines to a public notice and comment process would also be wise. Legislation should also require a timeline for implementation of the privacy guidelines that ensures that newly authorized information sharing occurs only after the guidelines are in place. There is no timeline in the Administration's proposal, and as a result, information sharing could be conducted for a time without privacy guidelines.

There are also significant concerns regarding the law enforcement use restrictions in the Administration's proposal. They permit use to investigate, prosecute, disrupt, or otherwise respond to "computer crimes," a threat of death or serous bodily harm, a serious threat to a minor, and an attempt or conspiracy to commit such offense. The term "computer crimes" is undefined, inviting an overbroad interpretation, such as any crime perpetrated in part through use of a computer, which would sweep in many crimes having nothing to do with cybersecurity. Instead, use of cyber threat indicators to investigate and prosecute violations of the Computer Fraud and Abuse Act, 18 USC 1030, and state law counterparts, should be permitted. Because the CFAA is so broad, an even better approach would permit use of cyber threat indicators only to investigate crimes an element of which is cyber threat conduct defined in the proposal if engaged in intentionally.[31] The Administration's proposal also permits law enforcement use in responding to threats of serious bodily harm, but does not require the threat be imminent. This could allow law enforcement to retain and use electronic communications based on suspicion of a vague or unsubstantiated threat.

Finally, the proposal counts on the government to enforce, against the government, the privacy guidelines the government itself authored. This is a weak enforcement mechanism. Instead, cybersecurity legislation should authorize a private right of action, with liquidated damages and attorney's fees, for those who suffer harm if a governmental entity does not abide by the privacy guidelines. CISPA authorizes such a private right of action;[32] the Administration proposal does not.

VIII. Federal data breach notification legislation should properly account for corresponding state laws.

Data breach notification is an area of cybersecurity where significant progress has been made at the state level. Currently, forty-seven states have laws requiring companies to notify consumers or regulatory agencies when breaches occur and personally identifiable information is disclosed. Because many businesses holding sensitive consumer data operate nationwide, they tend to follow the highest breach notification standard for simplicity's sake, and as a result, consumers across the country tend to benefit from the most robust state laws. Thus, while a

---

[30] Hugo Teufel III, Chief Privacy Officer, Department of Homeland Security, *Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security, December 29, 2008*, http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[31] Under this approach, cyber threat indicators shared "notwithstanding any law" could be use to investigate and prosecute a crime an element of which involves intentionally "damaging or impairing the integrity, confidentiality, or availability of an information system or unauthorized exfiltration, deletion, or manipulation of information that is stored on, processed by, or transiting an information system," with certain exceptions.

[32] H.R. 234, adding Section 1104(d) to the National Security Act of 1947.

preemptive federal law might add only *some* simplicity for business, it could actually *weaken* protection for consumers by superseding stronger state laws.[33]

In fact, the preemption clause of the Administration's data breach notification proposal is particularly troubling. This provision is overly broad, pre-empting all state laws that are related to data breach notification— even notification laws that cover data sets not covered by the Administration's proposal. At the very least, federal data breach legislation should only preempt state laws that address the same areas that as a federal law — any exemptions to federal regulation should also apply to preemption. The Administration proposal also fails to include a private right of action, which would preempt the 17 state laws that offer this enforcement mechanism, removing an important incentive to companies to ensure that personally identifiable data is protected.

If federal legislation on the issue is to be considered, it should introduce new protections not present in state law, such as requiring access to information maintained by data brokers, which would allow consumers to more effectively monitor potential risks and the effects of a breach.

IX. Recent events and disclosures should prompt Congress to encourage cybersecurity measures beyond information sharing.

The Snowden disclosures and major cyber attacks conducted in the last year demonstrate that although new information sharing authority has value, other cybersecurity measures should be a high priority for Congress as well. While information sharing would not have averted the Sony or Target attacks as well as other prominent attacks, improved employee education and application of best practice internal security measures might have.[34] Government's best means of preventing attacks like these may be to develop incentives that encourage companies to practice better digital hygiene.

Last year, a number of companies, security experts, and civil society groups with expertise in tech policy – including CDT – issued a letter outlining several of these measures.[35] First, the government should offer incentives to companies that adopt strong security practices, including resolving known vulnerabilities in a timely fashion, making systems more resilient against attacks, and improving security architecture by design. Second, Congress should empower a civilian federal agency to perform the government's information assurance function for the civilian sector, thereby ensuring that conflicting offensive missions would not override information assurance objectives. Third, all administrative agencies that collect or handle personal information should be required to have a Chief Information Officer, Chief Privacy Officer, and Chief Technology Officer, tasked with establishing and publishing responsible disclosure policies and processes for vulnerability reporting. Fourth, government should offer resources to educate users, companies, and other actors on best practices for avoiding and

---

[33] Gautam Hans, Center for Democracy & Technology, "White House Data Breach Legislation Must be Augmented to Improve Consumer Protection," https://cdt.org/blog/white-house-data-breach-legislation-must-be-augmented-to-improve-consumer-protection/.

[34] Mark Jaycox, *Congress Should Say No to "Cybersecurity" Information Sharing Bills*, The Electronic Frontier Foundation (January 8, 2015), *available at* https://www.eff.org/deeplinks/2015/01/congress-should-say-no-cybersecurity-information-sharing-bills.

[35] Available at https://www.accessnow.org/page/-/Veto-CISA-Coalition-Ltr.pdf.

mitigating cybersecurity threats.[36] Fifth, the United States should foster greater international dialogue on cyber conflict standards to discourage foreign attacks. Sixth, government should establish strong transparency obligations that provide access to both oversight bodies and the public.

Congress should also consider the impact on Americans' cybersecurity of NSA stockpiling of vulnerabilities to support offensive cybersecurity operations. Any vulnerability that is left undisclosed and unpatched could also be discovered and used by a bad actor, as shown by recent reports that the Sony hack employed a zero-day vulnerability.[37] In order to promote better cybersecurity and reduce attacks against the United States, the Review Group on Intelligence and Communication Technologies recommended that the government avoid stockpiling zero-days, and instead disclose vulnerabilities to the parties that can patch them."[38] Congress should embrace this recommendation.

X. Conclusion.

The year ahead offers a promising opportunity to move forward in development of new measures that will improve cybersecurity, including information sharing. Despite the scope of the threat, cybersecurity information sharing should be incentivized with care due to the significant risk of harm the privacy of average Internet users. We look forward to working with the Committee and the Congress in pursuit of both security and privacy, and ensuring that the Internet continues to be a vibrant force for innovation, individual empowerment, and prosperity.

---

[36] *See*, Joseph Lorenzo Hall, *Improve Digital Hygiene*, The New York Times (February 23, 2013), *available at* http://www.nytimes.com/roomfordebate/2013/02/21/should-companies-tell-us-when-they-get-hacked/improve-digital-hygiene.

[37] Arik Hesseldahl, Here's What Helped Sony's Hackers Break In: Zero-Day Vulnerability, Re/Code (January 20, 2015), available at http://recode.net/2015/01/20/heres-what-helped-sonys-hackers-break-in-zero-day-vulnerability/.

[38] *The President's Review Group on Intelligence and Communications Technologies, Liberty and Security in a Changing World*, (Dec. 12, 2013), 219, *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.


Agricultural Retailers Association
Airlines for America
American Bankers Association
Building Success. Together.
American Chemistry Council
AFPM
American Fuel & Petrochemical Manufacturers
AGA
American Gas Association
AIA
American Insurance Association
API
American Petroleum Institute
APPA
American Public Power Association
American Water Works Association
ASIS International
Advancing Security Worldwide
Association of American Railroads
The Council
The Council of Insurance Agents & Brokers
CTIA
The Wireless Association
EEI
Edison Electric Institute
Power by Association
Federation of American Hospitals
BITS
GridWise Alliance
HIMSS
transforming health through IT
Internet Commerce Coalition
LPPC
Large Public Power Council
nacd
National Association of Chemical Distributors
NACD
National Association of Corporate Directors
Manufacturers

January 27, 2015

TO THE MEMBERS OF THE UNITED STATES SENATE:

Our organizations, which represent nearly every sector of the American economy, strongly urge the Senate to quickly pass a cybersecurity information-sharing bill. Cybersecurity is a top priority of our associations and members.

The Select Committee on Intelligence passed a smart and workable bill in July 2014, which earned broad bipartisan support. Recent cyber incidents underscore the need for legislation to help businesses improve their awareness of cyber threats and to enhance their protection and response capabilities.

Above all, we need Congress to send a bill to the president that gives businesses legal certainty that they have safe harbor against frivolous lawsuits when voluntarily sharing and receiving threat indicators and countermeasures in real time and taking actions to mitigate cyberattacks.

The legislation also needs to offer protections related to public disclosure, regulatory, and antitrust matters in order to increase the timely exchange of information among public and private entities.

Our organizations also believe that legislation needs to safeguard privacy and civil liberties and establish appropriate roles for civilian and intelligence agencies. The cybersecurity measure approved last year by the Select Committee on Intelligence reflected practical compromises among many stakeholders on these issues.

Cyberattacks aimed at U.S. businesses and government entities are being launched from various sources, including sophisticated hackers, organized crime, and state-sponsored groups. These attacks are advancing in scope and complexity.

We are committed to working with lawmakers and their staff members to get cybersecurity information-sharing legislation swiftly enacted to strengthen our national security and the protection and resilience of U.S. industry. Congressional action cannot come soon enough.

Sincerely,

Agricultural Retailers Association
Airlines for America
American Bankers Association
American Chemistry Council
American Fuel & Petrochemical Manufacturers
American Gas Association
American Insurance Association
American Petroleum Institute
American Public Power Association
American Water Works Association
ASIS International
Association of American Railroads
Council of Insurance Agents & Brokers
CTIA–The Wireless Association
Edison Electric Institute
Federation of American Hospitals
Financial Services Roundtable–BITS
GridWise Alliance
HIMSS–Healthcare Information and Management Systems Society
Internet Commerce Coalition
Large Public Power Council
National Association of Chemical Distributors
National Association of Corporate Directors
National Association of Manufacturers
National Business Coalition on e-Commerce & Privacy
National Cable & Telecommunications Association
National Rural Electric Cooperative Association
NTCA–The Rural Broadband Association
Property Casualty Insurers Association of America
Securities Industry and Financial Markets Association
Society of Chemical Manufacturers & Affiliates
Telecommunications Industry Association
U.S. Chamber of Commerce
United States Telecom Association
Utilities Telecom Council

INDEPENDENT COMMUNITY
BANKERS *of* AMERICA®

January 28, 2015

Cybersecurity: The Community Bank Perspective

On behalf of the more than 6,500 community banks represented by ICBA, thank you for convening today's hearing on "Protecting America from Cyber Attacks: The Importance of Information Sharing." The financial services industry and community banks are typically on the front lines of defending against cybersecurity threats and take their role in securing data and personal information very seriously. ICBA is pleased to take this opportunity to submit the following statement for the record which sets forth the community bank perspective on information sharing and other aspects of cybersecurity:

Threat Information Sharing is Critical. ICBA supports the sharing of advanced threat and attack data between federal agencies and the appropriate financial sector participants, including community banks. Community banks rely on this critical information to help them manage their cyber threats and protect their systems. ICBA supports community banks' involvement with services such as the Financial Services Information Sharing and Analysis Center (FS-ISAC). The FS-ISAC is a non-profit, information-sharing forum established by financial services industry participants to facilitate the public and private sectors' sharing of physical and cybersecurity threat and vulnerability information. ICBA also supports FS-ISAC efforts to take complex threat information across communities, people and devices and analyze, prioritize, and route it to users in real-time as long as those efforts incorporate community banks and such advancements are cost effective to community banks.

Policymakers Must Recognize Existing Data Security Mandates. Any new legislation, frameworks, or standards policymakers develop should first recognize the existing standards and practices community banks observe to protect the confidentiality and integrity of customer personal data as well as to mitigate cyber threats. The Gramm-Leach-Bliley Act, for example, sets forth rigorous and effective data security protocols for the financial sector. It is important to extend comparable standards to all critical infrastructure sectors, including the commercial facilities sector which incorporates the retail industry and other potentially vulnerable entities. The National Institute for Standards and Technology (NIST) framework, and the 2013 Executive Order implementing it, were developed to create a baseline to reduce cyber risk to all critical infrastructure sectors.

Regulators Should Recognize Third Party Risk. Community banks significantly rely on third parties to support their systems and business activities. While community banks are diligent in their management of third parties, mitigating sophisticated cyber threats to these third parties, especially when they have connections to other institutions and servicers, can be challenging. Regulators must be aware of the significant interconnectivity of these third parties and must collaborate with them to mitigate this risk. This can be done by agencies evaluating the concentration risks of service providers to financial institutions, and broadening supervision of technology service providers to include more core, IT service providers by expanding the Multi-Regional Data Processing Servicer Program (MDPS) to include such providers.

Properly Aligned Incentives Will Enhance Data Security and Cybersecurity. When an entity's systems are breached, it is critical that the party that incurs the breach, whether it be a retailer, financial institution, data processor or other entity, bear responsibility for the related fraud losses and costs of mitigation. Allocating financial responsibility with the party that is best positioned to secure consumer data will provide a strong

incentive for it to do so effectively. Additionally, aligning incentives to maximize data security and cybersecurity by all parties that process and/or store consumer data will make the payments system stronger over time.

Thank you again for convening today's hearing. ICBA looks forward to working with the Senate Committee on Homeland Security and Governmental Affairs to improve cybersecurity.

NAFCU
3138 10th Street North
Arlington, VA 22201-2149
P: 703.842.2234
F: 703.522.0594
chunt@nafcu.org

Carrie R. Hunt
Senior Vice President of Government Affairs
and General Counsel

National Association of Federal Credit Unions | www.nafcu.org

January 27, 2015

The Honorable Ron Johnson
Chairman
Committee on Homeland Security
and Government Affairs
United States Senate
Washington, D.C. 20510

The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security
and Government Affairs
United States Senate
Washington, D.C. 20510

Re: Congress Must Tackle Cybersecurity and Data Security Together

Dear Chairman Johnson and Ranking Member Carper:

On behalf of the National Association of Federal Credit Unions (NAFCU), the only trade association exclusively representing our nation's federally chartered credit unions, I write today regarding tomorrow's hearing, "*Protecting America from Cyber Attacks: The Importance of Information Sharing*." Credit unions serve over 100 million members across the country and we appreciate your attention to this important matter.

NAFCU supports the strengthening of existing mechanisms in place to address cybersecurity issues such as the Financial Services Sector Coordinating Council (FSSCC) and the Financial Services Information Sharing and Analysis Center (FS-ISAC). These organizations work closely with partners throughout the government creating unique information sharing relationships that allow threat information to be distributed in a timely manner. NAFCU also has worked with the National Institute of Standards and Technology (NIST) on the voluntary cybersecurity framework released in 2013 designed to help guide financial institutions of varying size and complexity relative to reducing cyber risks to critical infrastructure.

In addition to addressing cybersecurity needs, NAFCU is hopeful that Congress will soon take legislative action to address ongoing data security breaches at our nation's retailers. Data security is an important part of the cybersecurity discussion and every time a consumer uses a plastic card for payment at a register or makes online payments from their accounts, they unwittingly put themselves at risk. Traditionally consumers have trusted that entities collecting this type of information will, at the very least, make a minimal effort to protect them from such risks. Unfortunately, in the wake of several headline grabbing retailer breaches in recent months, this does not seem to be the case today.

With the increase of massive data security breaches at retailers, from the Target breach at the height of holiday shopping in 2013 impacting over 110 million consumer records to the recent Home Depot breach impacting 56 million payment cards, Americans are becoming more aware

and more concerned about data security and its impact. A Gallup poll from October 12-October 15, 2014, found that 69 percent of U.S. adults said they frequently or occasionally are concerned about having their credit card information stolen by hackers, while 27 percent of Americans say they or another household member had information from a credit card used at a store stolen in the last year. These staggering survey results speak for themselves and should cause serious pause among lawmakers on Capitol Hill.

Financial institutions, including credit unions, have been subject to standards on data security since the passage of the *Gramm-Leach-Bliley Act* and it is critical that any data security legislation include language to ensure they are not subject to any new onerous or duplicative regulations. However, retailers and many other entities that handle sensitive personal financial data are not subject to these same standards, and they become victims of data breaches and data theft all too often. While these entities still get paid, financial institutions bear a significant burden as the issuers of payment cards used by millions of consumers. Credit unions suffer steep losses in re-establishing member safety after a data breach occurs. They are often forced to charge off fraud-related losses, many of which stem from a negligent entity's failure to protect sensitive financial and personal information or the illegal maintenance of such information in their systems. Moreover, as many cases of identity theft have been attributed to data breaches, and as identity theft continues to rise, any entity that stores financial or personally identifiable information should be held to minimum federal standards for protecting such data.

NAFCU believes data security is an important part of the cybersecurity debate. Accordingly, we urge Congress to come together in a bipartisan way and put forward legislative recommendations to hold retailers to the same strict standards of data security and breach notification that financial institutions must already adhere to. NAFCU member credit unions and their members have suffered greatly at the hands of negligent entities and have long sought legislation that would ensure retailers abide by a federal data security standard to better protect consumers. As your committee looks at legislative solutions to address cyber and data security, we believe the following areas must be addressed:

- **Payment of Breach Costs by Breached Entities:** NAFCU asks that credit union expenditures for breaches resulting from card use be reduced. A reasonable and equitable way of addressing this concern would be to require entities to be accountable for costs of data breaches that result on their end, especially when their own negligence is to blame.

- **National Standards for Safekeeping Information:** It is critical that sensitive personal information be safeguarded at all stages of transmission. Under Gramm-Leach-Bliley, credit unions and other financial institutions are required to meet certain criteria for safekeeping consumers' personal information. Unfortunately, there is no comprehensive regulatory structure akin to Gramm-Leach-Bliley that covers retailers, merchants and others who collect and hold sensitive information. NAFCU strongly supports the passage of legislation requiring any entity responsible for the storage of consumer data to meet standards similar to those imposed on financial institutions under the *Gramm-Leach-Bliley Act.*

- **Data Security Policy Disclosure:** Many consumers are unaware of the risks they are exposed to when they provide their personal information. NAFCU believes this problem can be alleviated by simply requiring merchants to post their data security policies at the point of sale if they take sensitive financial data. Such a disclosure requirement would come at little or no cost to the merchant but would provide an important benefit to the public at large.

- **Notification of the Account Servicer:** The account servicer or owner is in the unique position of being able to monitor for suspicious activity and prevent fraudulent transactions before they occur. NAFCU believes that it would make sense to include entities such as financial institutions on the list of those to be informed of any compromised personally identifiable information when associated accounts are involved.

- **Disclosure of Breached Entity:** NAFCU believes that consumers should have the right to know which business entities have been breached. We urge Congress to mandate the disclosure of identities of companies and merchants whose data systems have been violated so consumers are aware of the ones that place their personal information at risk.

- **Enforcement of Prohibition on Data Retention:** NAFCU believes it is imperative to address the violation of existing agreements and law by merchants and retailers who retain payment card information electronically. Many entities do not respect this prohibition and store sensitive personal data in their systems, which can be breached easily in many cases.

- **Burden of Proof in Data Breach Cases:** In line with the responsibility for making consumers whole after they are harmed by a data breach, NAFCU believes that the evidentiary burden of proving a lack of fault should rest with the merchant or retailer who incurred the breach. These parties should have the duty to demonstrate that they took all necessary precautions to guard consumers' personal information but sustained a violation nonetheless. The law is currently vague on this issue, and NAFCU asks that this burden of proof be clarified in statute.

On behalf of our nation's credit unions and their nearly 100 million members, we thank you for holding this important hearing. If my staff or I can be of assistance to you, or if you have any questions regarding this issue, please feel free to contact myself, or NAFCU's Vice President of Legislative Affairs, Brad Thaler, at (703) 842-2204.

Sincerely,

Carrie R. Hunt
Senior Vice President of Government Affairs & General Counsel

cc: Members of the Senate Committee on Homeland Security and Government Affairs

TELECOMMUNICATIONS INDUSTRY ASSOCIATION
1320 N. Courthouse Rd., Suite 200
Arlington, VA 22201 USA
www.tiaonline.org
Tel: +1.703.907.7700
Fax: +1.703.907.7727

January 27, 2015

The Honorable Ron Johnson
Chairman
Senate Homeland Security & Governmental Affairs Committee
340 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Tom Carper
Ranking Member
Senate Homeland Security & Governmental Affairs Committee
340 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Johnson and Ranking Member Carper:

The Telecommunications Industry Association (TIA), the leading trade association for global manufacturers, vendors, and suppliers of information and communications technology (ICT), wishes to thank you for holding a hearing this week to examine the importance of successful information sharing in the protection of the United States from cybersecurity attacks, through your January 28, 2015 hearing titled "Protecting America from Cyber Attacks: The Importance of Information Sharing." TIA and our member companies are committed to enhancing the national security through an improved ability for stakeholders to share timely cybersecurity information to improve detection, prevention, and mitigation of threats.

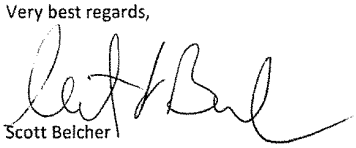
As the number and diversity of cyber-based threats to both businesses and the government continue to increase, it is more important than ever for Congress to act to enable the voluntary sharing of real-time bi-directional cybersecurity information amongst and between key government and industry partners (and their suppliers) by providing adequate liability protections while ensuring that an information sharing regime appropriately addresses privacy and civil liberties concerns. For example, TIA supported the Cybersecurity Information Sharing Act of 2014 (S. 2588) in the previous Congress.

TIA also notes its support for existing public-private partnerships (many of which TIA and its members participate in heavily), as well as efforts of Federal agencies under existing laws and authorities, to facilitate information sharing and to improve cooperation in defense against cyber attacks. The actions of Congress in this space should augment and build upon the successes of these efforts.

Finally, TIA believes that information sharing should not be viewed as the end game. Rather, information sharing is a tool to achieve timely, reliable, and actionable situational awareness through information sharing, analysis, and collaboration. That is why it is important for Congress to, in addition to addressing information sharing, act in other important areas, such as to improve cybersecurity R&D, workforce training and education, and public awareness.

Thank you for your continuing hard work on this important national and economic security issue, and TIA looks forward to working with you moving forward. For more information, please contact Danielle Coffey at (703)-907-7734 or by email at dcoffey@tiaonline.org.

Very best regards,



Scott Belcher
Chief Executive Officer
Telecommunications Industry Association