SMALL BUSINESS, BIG THREAT: PROTECTING SMALL BUSINESSES FROM CYBER ATTACKS

HEARING

BEFORE THE

COMMITTEE ON SMALL BUSINESS
UNITED STATES
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

HEARING HELD
APRIL 22, 2015

Small Business Committee Document Number 114–009
Available via the GPO Website: www.fdsys.gov

U.S. GOVERNMENT PUBLISHING OFFICE
94–346 WASHINGTON : 2015

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

HOUSE COMMITTEE ON SMALL BUSINESS

STEVE CHABOT, Ohio, *Chairman*
STEVE KING, Iowa
BLAINE LUETKEMEYER, Missouri
RICHARD HANNA, New York
TIM HUELSKAMP, Kansas
TOM RICE, South Carolina
CHRIS GIBSON, New York
DAVE BRAT, Virginia
AUMUA AMATA COLEMAN RADEWAGEN, American Samoa
STEVE KNIGHT, California
CARLOS CURBELO, Florida
MIKE BOST, Illinois
CRESENT HARDY, Nevada
NYDIA VELÁZQUEZ, New York, *Ranking Member*
YVETTE CLARKE, New York
JUDY CHU, California
JANICE HAHN, California
DONALD PAYNE, JR., New Jersey
GRACE MENG, New York
BRENDA LAWRENCE, Michigan
ALMA ADAMS, North Carolina
SETH MOULTON, Massachusetts
MARK TAKAI, Hawaii

Kevin Fitzpatrick, *Staff Director*
Stephen Dennis, *Deputy Staff Director for Policy*
Jan Oliver, *Deputy Staff Director for Operation*
Barry Pineles, *Chief Counsel*
Michael Day, *Minority Staff Director*

CONTENTS

OPENING STATEMENTS

WITNESSES

APPENDIX

SMALL BUSINESS, BIG THREAT: PROTECTING SMALL BUSINESSES FROM CYBER ATTACKS

WEDNESDAY, APRIL 22, 2015

HOUSE OF REPRESENTATIVES,
COMMITTEE ON SMALL BUSINESS,
Washington, DC.

The Committee met, pursuant to call, at 11:00 a.m., in Room 2360, Rayburn House Office Building. Hon. Steve Chabot [chairman of the Committee] presiding.

Present: Representatives Chabot, Hanna, Rice, Gibson, Brat, Hardy, Velázquez, Clarke, Meng, Lawrence, Adams, and Moulton.

Chairman CHABOT. The Committee will come to order.

I want to thank everyone for being here today. A special thanks to our witnesses for coming to share their insights and expertise with this Committee on the very timely and very important subject matter that we will be discussing here this morning.

Cyber security is one of the most pressing but least understood challenges of our time. The American government, American businesses, and Americans themselves are attacked over the Internet on a daily basis. Sometimes they know; sometime they do not. These attacks come from criminal syndicates, activists, and foreign nations. They are after intellectual property, bank accounts, social security numbers, and anything else that they can use for financial gain or for a competitive edge.

The increasing number of attacks come as more people are using the Internet than ever before. In the past five years, global Internet traffic has increased more than fivefold, and in the next five years this number will triple. This is not the Internet of 1995 when most Americans simply got online to check their email. Today, we are using the Internet in increasingly innovative and practical ways. Some pay for coffee with their phones, request ride-sharing service to an exact location, stream live video, and even bank online.

Just two years ago, the average amount stolen from small business bank accounts was around $7,000, and in just two years—last year—that nearly tripled to $20,000.

This technology, and our use of it, is the underpinning of our modern economy and the foundation of our future. That is why we must address cyber security now, so that as a country and as the leader in the global marketplace we can operate without fear of attack. We need the peace of mind that we have adequately prepared, we are protected, and we are constantly learning and adapting and strengthening those systems to protect against cyber attacks.

When hackers affect large corporations, it is a breaking news alert on television and probably on our smartphones. But the majority of cyber attacks happen at small businesses. In fact, 71 percent of cyber attacks occur at businesses with fewer than 100 employees. These are our family businesses and small manufacturers with fewer resources to combat security threats which make them even bigger targets. A cyber attack on a big box store will be reported by the media and probably dent their bottom line; an unreported attack on a small firm may put them out of business, and those Americans who work at that small business lose their jobs.

So today, we are here to examine these issues through the lens of an everyday American. How do we protect ourselves and our businesses? Is it as simple as using a more complicated password, or does it require much more than that? And what is the appropriate level of the federal government's involvement in all of this? Not long ago, an enemy would attack us with bombs, or guns, or ammunition; today they use malware and Trojan horses.

I look forward to hearing from our witnesses here this morning, and I now would like to yield to Nydia Velázquez, the ranking member.

Ms. VELÁZQUEZ. Thank you, Mr. Chairman.

Over the past 15 years, the Internet and associated technologies have changed the way business is conducted. From the mobile banking apps on our phones, to the shopping experience offered by companies like Amazon, activities that once took place in corner stores now take place online. The Internet also affords America's 23 million small businesses a unique opportunity to sell their products not only across the country but around the world. Today, Internet shopping is a $319 billion marketplace, and the Census Bureau estimates 58 percent of all U.S. shoppers will make an online purchase in the next year.

As more consumers and businesses participate in ecommerce, protecting our financial information from cyber attacks is critical. Unfortunately, recent data breaches at Target, T.J. Maxx, and Home Depot compromise financial data of millions of consumers and cost each company tens of millions of dollars in damages and lost sales. It also exposes the weaknesses of the current cyber security landscape.

While these examples highlight some of the largest breaches, the small business community is not immune to the risks of a cyber attack. Over 40 percent of attacks are companies with less than 400 employees and nearly three-quarters of small businesses report being targeted in the past year. Yet, 53 percent of small business owners claim that the high cost in both time and money to secure the business from cyber attacks was not justified by the threat. Unfortunately, the consequences of forgoing investment in proactive cyber security are high. The small business that loses customer information is punished twofold by the direct monetary toll of the breach and by the marketplace when customers leave. A data breach costs upwards of $200,000 per incident and surveys show 20 percent of customers will immediately terminate their relationship with a compromised business. As a result one study found a 60 percent of small businesses closed permanently within six months of a cyber attack.

Clearly, cyber security should be a priority to protect our national security and economy. As we move forward, comprehensive reforms must balance a number of priorities, including being able to adapt to evolving technologies, preventing undue costs and regulations on small businesses, and protecting our sensitive information.

During today's hearing, we will explore the critical issues facing small businesses that operate online. For millions of small firms, the Internet is critical to their success, yet fewer than 15 percent have plans in place to respond to a cyber attack. I look forward to hearing your recommendations to better educate and inform the small business community on cyber issues and how the federal government can facilitate a more robust and efficient cyber security environment.

I would like to take this opportunity to thank all the witnesses for being here today. With that, I yield back.

Chairman CHABOT. Thank you very much. The gentlelady yields back.

If Committee members have opening statements prepared, I would ask that they submit them for the record.

I would now like to inform our panel of the five-minute rule, which basically means you get five minutes to testify, and we will all have five minutes to ask questions. There is a lighting system. The green light will stay on for four minutes. The yellow light will come on to let you know you have a minute to wrap up. When the red light comes on, we ask that you finish up as close to that time as possible. We will give you a little bit of leeway but not a whole lot.

And now we will introduce the panel. Our first witness will be Steve Grobman, who is the chief technology officer with Intel Security Group at Intel Corporation. In this role, Mr. Grobman sets the technical strategy and direction for the company's security business across hardware and software platforms. Mr. Grobman holds 20 U.S. and international patents in the field of cyber security, software, and computer architecture. He earned his bachelor's degree in Computer Science from North Carolina State University. We welcome you here this morning.

Our second witness will be Todd McCracken, who serves as President of the National Small Business Association (NSBA). NSBA is the nation's oldest small business organization, having been founded all the way back in 1937. Mr. McCracken is a graduate of Trinity University with a B.A. in Economics. We welcome you.

And our third witness will be B. Dan Berger, who is President and CEO of the National Association of Federal Credit Unions. Mr. Berger earned a Master's degree in Public Administration from Harvard University and a Bachelor of Science degree in Economics from Florida State University, and we welcome you here as well, Mr. Berger.

I now yield to our ranking member to introduce our fourth witness.

Ms. VELÁZQUEZ. Thank you, Mr. Chairman.

Dr. Jane LeClair is the chief operating officer for the National Cyber Security Institute at Excelsior College here in Washington, D.C., where she focuses on cyber security training, social engineering, and women in cyber. Previously, she served as dean of the School of Business and Technology at Excelsior College, and worked in the nuclear energy sector for over 20 years. She is a vocal advocate for attracting and retaining more women in the technology fields and established the Dr. Jane LeClair Scholarship Fund for Women in Technology at Excelsior College in 2012. Dr. LeClair holds a number of degrees, notably an EdD from Syracuse University and a MBA from City University. Welcome.

Chairman CHABOT. Thank you very much.

Now we will hear from our very distinguished panel here this morning. Mr. Grobman, you are recognized for five minutes.

STATEMENTS OF STEVE GROBMAN, CHIEF TECHNOLOGY OFFICER, INTEL SECURITY GROUP, INTEL CORPORATION; TODD MCCRACKEN, PRESIDENT, NATIONAL SMALL BUSINESS ASSOCIATION; DAN BERGER, PRESIDENT AND CHIEF EXECUTIVE OFFICER, NATIONAL ASSOCIATION OF FEDERAL CREDIT UNIONS; JANE LECLAIR, NATIONAL CYBER SECURITY INSTITUTE

STATEMENT OF STEVE GROBMAN

Mr. GROBMAN. Good morning, Chairman Chabot, Ranking Member Velázquez, and other members of the Committee. Thank you for the opportunity to testify today. I am Steve Grobman, Intel fellow and chief technology officer for Intel Security Group at Intel Corporation.

Intel is a world leader in computing innovation. The company designs and builds the essential technologies that serve as the foundation for the world's computing devices.

Security, along with power-efficient performance and connectivity are key elements of our innovation efforts. As chief technology officer for Intel Security Group, I set the technical strategy and direction for the company's security business across hardware and security platforms.

Intel and I appreciate the Committee's interest in the importance of protecting small business from cyber security threats. My testimony will focus on three main areas—the threat landscape and its implication for small business; how best practices and education can help small business; and how industry can deliver innovative security solutions to help small business.

The threat landscape and specific implications for small business are very unique. Small businesses need to comprehend a wide-range of threats, including attacks from criminals, hacktivists, state actors, and bulk malware that we see targeting consumers. But they also have some very unique challenges. They typically have insufficient cyber defenses, thus becoming an attractive prospective for criminal actors, but yet make up a major portion of the GDP. The other element with small business is small business can act as a conduit or element of a larger breach focused on large enterprise or government.

The latter example is not a hypothetical. Elements of a 2014 major breach compromised a small business as one of the key elements to land on the network of a large enterprise and thus be-came a key factor in that enterprise's overall loss. Understanding how small business impacts supply chain and other elements of large business and government is something that we must comprehend when looking at small business.

Attacks are not only technological; they take advantage of both social engineering and a wide range of attacks on varying platforms from PCs, mobile devices, new cloud architectures, embedded devices, and even hardware.

The challenge with cyber security defense is that the attack has an inherent advantage. It is an asymmetric environment where a target attack against a small business gives the advantage to the attacker. The attacker understands what tools and defensive measures are deployed generally at small business. They also understand that the pragmatic cost complaints of a small business will be such that they cannot afford the same degree of a cyber-operation staff that you would see in some large enterprises or governments. But the most profound reason that we see the asymmetry in the attack advantage being to the attacker is the attacker only needs to be right once, whereas, to defend against cyber attacks, you need to be right always. And this is extremely challenging, especially in a small business environment.

To counteract the cyber security risks of small business, a few key actions need to be taken. Small business, along with all enterprise, need to be thinking about how security evolves. The concept of protection against all cyber threats is not possible today, and we need to shift our thinking to more of a thought process that cyber attacks will occur and be able to not only defend against them but detect them when they occur and correct back to a known good state. This concept of not only comprehending protection but detection and correction is key to the way the industry should develop our next generation of architectures.

It is also important that we understand education for all organizations, regardless of whether you are a small business or a large enterprise. A key educational tool is the cyber security framework, which Intel has been a proponent of and has been a strong advocate in integrating into its own systems.

The final point that I would like to make is new technologies are at the cusp of enabling small businesses to be successful in the emerging threat landscape. Things such as software as a servicing cloud and we will see small businesses shifting to these types of technologies as we move forward.

Thank you again for the opportunity to address the Committee. I will be happy to answer any questions as well.

Chairman CHABOT. Thank you very much.

Mr. McCracken, you are recognized for five minutes.

STATMEENT OF TODD MCCRACKEN

Mr. MCCRACKEN. Thank you, Mr. Chairman. It is good to be here this morning. Thanks for inviting me. Thank you, Chairman Chabot, Ranking Member Velázquez, and the rest of the members of the Committee, to be here to testify on the impact of cyber security and credit card fraud issues on the health and growth potential of millions of small businesses.

I want to focus today a little bit on the overall threat of cyber security on small companies, but then also focus a little bit more specifically on the credit card issue since there is a lot of talk about small companies and the conversion to EMV and the liability shift this year that probably is worthy of a little bit of attention.

In the last few years, cyber security has emerged as a significant problem and concern for the small business community. By the end of 2014, according to our Year-End Economic Report, fully half of small companies reported having been the victim of a cyber attack (up from 44 percent in 2013). And of those, 61 percent say an attack has occurred within the last year.

While a 14 percent increase in the number of small businesses becoming victims is significant, we believe the real story is the increasing impact those attacks are having on small businesses in terms of the interruption of normal business operations and the direct financial cost of the attacks

In 2013, only 12 percent of companies reported that the resolution of the cyber attack required more than one week; by late 2014, more than one in five such attacks were still unresolved in one week, with 13 percent of them requiring more than two weeks. Three in five companies experienced a service interruption, and a third had their websites go down for some period.

A significant problem for small companies, as Mr. Grobman just talked about, is many small companies are not in a position to have a dedicated IT department, and many either outsource IT functions or assign such duties to an employee who has other responsibilities, often the owner him/herself. You can read the results for yourself. We found in our surveys, significant numbers of companies, between 25 and 40 percent in the last four years, report that the owner him/herself is the primary technical support person. They do it themselves, in addition to being the chief marketing officer and chief product development officer and everything else. And so this is an enormous constraint on how they can respond.

And in the case of another significant share of companies, they outsource the IT function to some other company. Of course, the difficulty there is these small businesses, in the event of a crisis, those smaller clients typically are not the first priority for those IT firms. They have other clients, and some of the bigger clients pay them more money will get a quicker response. So those are unique challenges for small companies.

The big eye opener in our last survey is the increasing cost of these cyber attacks. We look specifically at what money had been stolen from them from bank accounts, and we found in two years the amount that was stolen went from about $7,000 to about $20,000 on average, a 188 percent increase in that amount of time, which is staggering. We think that is largely the result of not only the increase, the total increase in the amount of fishing scams out there, and malware, but also the increasing effectiveness of those. They have become much more real to people. They believe them in a way that they did not two or three years ago for a variety of reasons.

So this is clearly a national problem, and these attacks are coming from outside the country. We have got to find a way to limit those attacks, while increasing the education of small companies on how to avoid them.

The next issue I want to talk about briefly is credit cards and small companies. Various forms of credit card fraud have become more prevalent. We see in the desire to shift to EMV or the chip-based cards. This October 1st we are going to see a shift in liability for credit card fraud, whichever company has the least advanced technology essentially. So if you do not have an EMV reader, then the company could be liable.

So those companies really think about what kind of charges they have actually have, what kind of company they run, what kind of products they well, who their customers are, do they know their customers, to decide if they need to invest now in those more up-to-date readers or whether they will not see a significant increase in fraud if they stay where they are now. But we clearly think that shifting to a more secure credit card environment ultimately has got to be the solution for overall credit card fraud because we do not think to rely on magnetic stripe technology is like to be our future; we have to make the shift and make it fairly quickly because there are too many incentives to shift that data there.

So again, with those highlights, you can read the rest of my statement as it is written, but I appreciate the time to be here today. I stand ready to answer your questions when it is time. Thank you.

Chairman CHABOT. Thank you very much.

Mr. Berger, you are recognized for five minutes.

STATEMENT OF DAN BERGER

Mr. BERGER. Good morning, Chairman Chabot, Ranking Member Velázquez, Members of the Committee. My name is Dan Berger, and I am testifying today on behalf of the NAFCU, where I serve as president and CEO.

NAFCU and our member credit unions, small businesses themselves, appreciate the opportunity to testify before the Committee today on cyber and data security. Cyber and data security needs to be everyone's responsibility. More can and must be done to protect small businesses and consumers on this very important issue.

NAFCU has long supported comprehensive and cyber security measures to protect consumers' sensitive data. Credit unions and other financial institutions already protect data consistent with the provisions of the 1999 Gramm-Leach-Bliley Act. Unfortunately, there is no similar regulatory structure for other entities that may handle sensitive personal and financial data.

Gramm-Leach-Bliley, in its implementing regulations, has successfully limited data breaches among financial institutions. This standard has a proven track record and should be recognized in any future requirements. Gramm-Leach-Bliley requires financial institutions to address the risks presented by the complexity and scope of their business. This allows flexibility, ensures the regulatory framework is workable for the largest and smallest financial institutions. Gramm-Leach-Bliley is an example of how scalability is achievable for varying sized businesses.

A data security breach can have a huge impact on consumers, from waiting for new cards to be issued, to updating all existing accounts connected with a compromised card. Breaches can also result in fraud losses, damaged credit ratings, and even identity theft. Over 23 percent of Americans had their financial identities compromised by a data breach in 2014.

A recent survey of NAFCU-member credit unions found that the respondents were alerted to potential breaches an average of 164 times in 2014, a huge increase from 2013. It is important to remember when credit unions are alerted to breaches, they take action to respond to their members and to protect their members. Our survey also found that in 2014, the average credit union spent $136,000 on new data security measures, in addition to spending $226,000 in costs associated with merchant data breaches. The three main elements of these costs were card reissuance, fraud losses, and account monitoring. Ultimately, this takes away from providing other services and products to their members.

Smaller credit unions, such as Diebold Federal Credit Union in North Canton, Ohio, are especially feeling the impact. Since the beginning of 2014, Diebold has had over $32,000 in losses from data breaches from retailers. While that might not seem like much, for a small business like them, it is a huge burden on that institution.

Unfortunately, credit unions rarely see any reimbursement for these costs. Even when there are recoupment opportunities, such as the recent Target settlement with MasterCard, it is usually only pennies on the dollar in terms of real costs and losses incurred.

Recognizing that a legislate solution is a very complex issue, NAFCU has established a set of guiding principles we would like to see in data security legislation including reimbursement of all costs by the breach entity, national standards for safekeeping of consumer information, breach notification to financial institutions, disclosure of the breached entity to consumers, and of course, enforcement of data retention prohibitions.

Enforcement of the prohibition on data retention cannot be overstated. It is a common sense way to cut down on emerging threats. If there is no financial data to steal, it is not worth the effort of the cyber criminals. In essence, if there is no treasure, there is no private.

NAFCU believes that a possible solution on this issue is a bipartisan legislation introduced by Senators Blunt and Carper. Their bill, the Data Security Act of 2015, sets a strong national data security standard based on Gramm-Leach-Bliley that would be extended to all entities who handle consumer data. We urge the House to take a similar approach.

We would also like to recognize and thank the House leadership, as well as this Committee, for the ongoing focus on cyber and data security issues, including the cyber bills you have on the floor this week. A safer system ultimately benefits all participants, including consumers, financial institutions, and of course, small businesses.

Thank you for the opportunity to appear before you today on behalf of NAFCU. I welcome any questions you may have.

[The statement of Mr. Berger follows:]

Dr. LeClair, you are recognized for five minutes.

STATEMENT OF JANE LECLAIR

Ms. LECLAIR. Mr. Chairman and members of the Committee, on behalf of the National Cyber Security Institute at Excelsior College, I appreciate the opportunity to address you and provide a statement for today's hearing. The National Cyber Security Institute is dedicated to increasing knowledge in the cyber security discipline and assists small businesses to better understand and meet the challenges in today's digital world. My name is Dr. Jane LeClair, and I am the chief operating officer of the National Cyber Security Institute located in Washington, D.C.

Small businesses are challenged both by the ability and the desire to secure themselves against cyber threats, which makes them uniquely vulnerable to cyber attacks. Fifty percent of small businesses have been the victims of cyber attack and over 60 percent of those receiving a significant attack go out of business. Often, small businesses do not even know they have been breached until it is too late. Small businesses are under attack from many avenues, including social engineering, the Internet of things, insider threat, weak passwords, and cyber theft through weak payment systems. Mobile devices and the lack of formal cyber plans and policies spell trouble. Infections brought in through browsers pose a threat, and finally, outdated technology and poor maintenance top the list of problems.

Small businesses are characterized by central management focused around the owner, with lack of a specialized IT or cyber staff, inadequate control systems, and day-to-day, rather than long-term planning for asset protection. Almost 70 percent of small businesses manage their own websites, use the Internet for sales, social media, marketing, and a host of other needs. Small businesses have resource constraints and often ignore cyber security in favor of day-to-day operations or other financial needs.

Yet, small businesses remain a gateway to gain access to clients, business partners, donors, and contractors working with the small business, a backdoor into many large organizations. These organizations frequently lack the knowledge to develop and implement a cyber-policy or the expertise to develop a response strategy. Surprisingly, 96 percent of the attacks on small businesses were fundamentally basic attacks. Small businesses need employees trained in networking, operating systems, and multiple layers of security. Otherwise, who is watching for the signs of an attack and making sure the operating systems are properly patched? Who is responsible for regular backups and reviewing system logs?

There are several ways that the National Cyber Security Institute is offering assistance to the small businesses. An affordable package that provides a targeted cyber security plan, basic training for owners, IT staff and employees, and ensures that the basics of antivirus software and firewall protection are in place is under development. Our media campaign raises awareness through quarterly webinars and weekly blogs. The National Cyber Security Institute is publishing two short books on Cyber security for small business and cyber insurance, and is partnering to offer a small business workshop in medium-sized cities around the country that is affordable and aimed at small business owners and their IT staff.

Cyber security is without a doubt one of the prime concerns of the small business community in America today. The efforts of this Committee in seeking ways to help alleviate those concerns cannot be understated.

Mr. Chairman and members of this Committee, thank you for your interest in this important area, and I thank you for the opportunity to address you today.

Chairman CHABOT. Thank you very much. We want to thank all the witnesses for their very excellent testimony here, and I will recognize myself for five minutes now to begin the questioning.

I will begin with you, Mr. Grobman, if I can. I appreciated your comment particularly about the attackers only have to be right once and we, the business community, has to be right every time or you are going to undergo some serious damage. You heard that a lot after September 11th, too, in dealing with overall terrorism. We have to be very secure all the time and it only takes a terrorist one time to really wreak havoc and I think that is certainly the case here because this is really a form of terrorism in many ways.

Could you kind of walk us through the various stages of a modern cyber attack on, say, a small business, for example?

Mr. GROBMAN. Sure. What would typically happen is if it is a targeted attack, they would focus first on what we call reconnaissance. So understanding what capabilities the small business is actually running so that they can craft an attack that would be able to be successful in that environment. Once they have that information, they can customize a capability that would be able to work through standardized defenses if the small business has them in order to get into the environment and then they focus on perpetrating whatever their actual objective is, typically the theft of information or in the case of either hacktivism or nation state, it might be more of a destructive nature. So it is really a well-formed set of steps that is well understood by the attack community on how to perpetrate such an attack. The thing that is unique here is it can be customized for the target, which makes it very difficult to protect with standard technology.

Chairman CHABOT. Thank you very much.

Mr. Berger, let me turn to you. On behalf of the credit unions, you know, as far as the banking community, are the attacks that you see on the credit unions similar to what you see in say the community banks? Are there similarities? Are there differences? What would you say?

Mr. BERGER. The attacks that we are seeing are very similar across the board. It does not matter what size the entity is. It is the old phrase, “ they attack where the money is.” But because we have Gramm-Leach-Bliley, we have some serious protocols in place that we have to deal with as a financial institution to make sure that the consumer’s information is protected. But the attacks are the same, no matter what size the entity is.

Chairman CHABOT. Thank you.

Mr. McCracken and Dr. LeClair, I will address the next question to the two of you. What steps are being taken to level the playing field to more effectively defend against cyber attacks, and how important is information sharing to those efforts? Either one of you.

Ms. LECLAIR. I would say information sharing is key today. We cannot silo ourselves, and we need to work both jointly with government and private industry to ensure the information is shared and that we are able to protect as we need to.

Chairman CHABOT. Thank you.

Mr. McCracken?

Mr. MCCRACKEN. Yeah. I agree with that. It is very important to get the information out there so that companies can understand what the real threats are and how they can protect themselves. And then share it up within the supply chain. We think there is a significant role that various members of the supply chain need to play in helping each other deal with these attacks because all those companies are interlinked is very clear.

Chairman CHABOT. There are various things that we, as members of Congress, and our staff deal with in trying to keep attacks—cyber attacks on the government. Such things as changing our passwords, and they have improved the passwords so it is a little harder to get them in and you have to remember them with a little more difficulty. It cannot just be your cat's name or your dog's name and that sort of thing. You have got to put question marks after the cat's name now or whatever. So it is a bit more complicated.

And they are also changed periodically, and I do not necessarily want to give out government secrets here as to how often we have to change them, but it was a certain number of months, and now that has been shortened to a fewer number of months. What is the private sector doing along those lines, and what would you recommend to small businesses in that area?

Mr. Grobman?

Mr. GROBMAN. Chairman, I think one of the things that Intel Security is investing in is solving or helping to provide key assets for this problem by making biometrics available to a much broader audience, including small business and consumers. So when you prove that you really are you to another entity, you are doing it not just with a password, which can be transferred to somebody else, but you actually need to use something like facial recognition in order to do that. And I think as these technologies become more consumable, they will be a key part of the strategy to solve the problem you articulate.

Chairman CHABOT. Thank you very much.

Just for the record, we do not have a cat. We have a turtle and I am not going to tell you what his name is.

I will now yield to the ranking member for five minutes.

Ms. VELÁZQUEZ. Thank you, Mr. Chairman.

Dr. LeClair, as we heard today, financial data security is becoming a priority for small businesses, given the fact that more small businesses are offering online mobile buying options. Many of the firms, as Mr. McCracken stated, cannot hire an IT staff. Can you elaborate on the cyber security package that NCI is working on or developing to offer small businesses that opportunity?

Ms. LECLAIR. One of the things that we have under development is a package that would work for small businesses because of the financial constraints they have. That package would allow them to get the basic training for the organization owner, as well as their employees. But special training if they have their own IT person, or if they have another person in the organization who they have selected to do their IT work, to give them the basic training they need to be able to know about to secure their systems. Ensuring that they have basic anti-virus firewall protection as well, and that they are able to develop a policy with us. We have a template, basically a starter template for them that we would work with them to develop their policy, as well as a risk assessment plan for them. So kind of an all-in-one package for them to be able to work with.

Ms. VELÁZQUEZ. Thank you.

How important do you think it is to create national notification standards to replace the existing 49 separate state laws governing breach notification?

Ms. LECLAIR. We feel that is very important. We have spoken about that a couple of places because right now there are 47 states that have different rules and policies. The ability to clarify for organizations the overall requirements would not only simplify but it would allow people to better be able to know what they have to do in that timeframe. In some people's case they feel it will be difficult to meet, but I think overall in a short time people will adjust and it will help us in the long term.

Ms. VELÁZQUEZ. Thank you.

Mr. Grobman, there has been much emphasis recently on cloud computing, and this new model is gaining great traction within the business community and the government. How does cloud computing impact cyber security , particularly for small businesses?

Mr. GROBMAN. So cloud computing is a major asset to helping small business, both as providing the means to execute functions that they are ill-equipped to do as a traditional IT organization would, especially in the area of cyber security defense, cloud computing, and specifically what we call Software as a Service allows a service-based capability to provide security solutions to a small business.

In our submitted testimony, we gave an example where the City of Kenosha with an IT staff of three is able to use a cloud-based solution to provide email protection for all of its government workers, and I think that is a good example of how cloud technology can be a key asset to small business.

Ms. VELÁZQUEZ. Thank you.

Mr. Berger, many small businesses have been quite critical of the high interchange fees charged by credit card issuers. We have seen or we have been told that these fees were needed to cover not only the cost of processing transactions but also to cover the cost of fraud, theft, and data breaches. With the U.S. scheduled to move to the more secure chip and pin technology in October, do you expect interchange fees to come down?

Mr. BERGER. Interchange fees were created before it was capped, to create the rails, to invest in the rails and the technology, as well as for fraud recoupment. Now that there is a cap on interchange fees, that is not the case for fraud prevention. And so I do not think the interchange fees will go down because there is no recoupment for financial institutions any longer with the cap.

Ms. VELÁZQUEZ. Okay. Thank you.

Mr. McCracken, it is often hard to persuade small firms to spend money without seeing an immediate return. So what do you think we need to do in order to get more small businesses to understand the importance of investing in cyber security ?

Mr. MCCRACKEN. Well, there are a number of different fronts. One is on the credit card front, I think when they start seeing more chip-based cards, many more of them will begin investing in readers to use them rather than the other way around, which is unfortunately the way it seems to have been pursued so far. And on larger cyber security, I think education is everything. And I think that larger companies who do business with smaller companies have a significant role to play in helping and educating them figure out how to implement some of these services. And also, education on the implications, because it is true that one mistake from a small company can be devastating for them.

Ms. VELÁZQUEZ. Thank you, Mr. Chairman.

Chairman CHABOT. Thank you. The gentlelady's time is expired.

The gentleman from New York, Mr. Hanna, who is the chairman of the Subcommittee on Subcontracting and Workforce is recognized for five minutes.

Mr. HANNA. Thank you all for being here. And thank you, chairman.

I want to ask about not just responsibility to protect one's system but liability as to moves across what the staff calls like a chain. The Internet is comprised of technology links that are dependent upon each other. Is it incumbent upon a bigger organization to help a smaller organization? And what do you see for the future of that? Because clearly, the perception of risk vis-á-vis liability varies across industries, and willingness to provide support to protect oneself varies on the individual and their means. So, so much of this is subjective, yet because of its interconnectedness, it is all critical.

So Mr. Grobman, you talked about the cloud and how that offers. If everybody would like to speak to that, if that is a fair question.

Mr. GROBMAN. Sure. I think it is key for large enterprise to understand the implications that a breach to a small business supply chain or supplier would have, and there are key steps large business can take to help small businesses in this manner. One key example is advocacy and linkage to things like the cyber security framework as a part of supplier guidelines.

Mr. HANNA. You say advocacy. What about demand? I mean, there must be a point at which somebody says if you do not do this, we cannot do business with you.

Mr. GROBMAN. Sure. I think understanding the risk profile of a supplier is a reasonable thing for a large business to do, and having a common language to understand and describe risk is something that the cyber security framework can help facilitate. So I think it is those sorts of communication interactions can help large business assess the risk of using various suppliers.

Mr. HANNA. How do you feel about that, Mr. McCracken, being a representative of small businesses, being demanded to do that?

Mr. MCCRACKEN. Well, on the one hand I think that is a way forward because that, as I discussed before, the supply chain issues are real and we have to have ways of both educating and also helping those smaller companies by giving them incentives beyond—maybe something might happen later, which we are facing now.

Mr. HANNA. Yeah, punitive stuff.

Mr. MCCRACKEN. I think the danger to keep in mind is that what you do when you do that is you begin to restrict some of those possibilities for companies that are trying to grow, because if you do not—if what we are already seeing is larger companies saying, look, if you do not have X capabilities, do not even send us—do not even apply to do business with us. I think that is a mistake, because what you are going to see is larger and larger companies all working together. What I would like to see is for those companies to put in standards that once you are a vendor of ours, here is how we are going to work together to get you to this point. That, I think, would be much more productive and really help smaller companies grow to the point they need to be.

Mr. HANNA. Mr. Berger?

Mr. BERGER. As part of Gramm-Leach-Bliley's implementation rules, we are required to ensure that third-party vendors are up to speed and the NCOA examines for that.

Mr. HANNA. Ms. LeClair?

Ms. LECLAIR. I do not disagree with anything that the other folks have said. What I do see as very difficult for small businesses and any organization to know what to use and coming from a commercial nuclear power background, it was not until the Institute of Nuclear Power Operations came into being that there was an organization that fully structured what was happening in that industry. So in some ways, yes, I agree, and in others I see that you need some definitive, as you said, organization to make that happen.

Mr. HANNA. Thank you.

Mr. Grobman, I have a minute and a few seconds here. I want to ask about mobile devices.

Mr. GROBMAN. Sure.

Mr. HANNA. Given the ubiquitous nature of that, how do you deal with that?

Mr. GROBMAN. I think mobile devices are both a key benefit in cyber security. They have been developed more recently and have had the opportunity to redesign the underlying software architecture to put individual applications into sandboxes. So I think that is a very positive aspect.

The flip side of it though is mobile devices are also generally more closed where the security industry has challenges in looking at the information of what is going on on a mobile device. So when we look at a modern way to do detection of an advanced attack, it is really about understanding the data that is coming out of your environment as far as different events, and the mobile devices do not lend themselves very well to that. So mobile is still a fairly new area relative to other capabilities and is something we are looking at very closely.

Mr. HANNA. Thank you very much.

My time is expired.

Chairman CHABOT. Thank you. The gentleman's time is expired.

The gentlelady from North Carolina, Ms. Adams, is recognized for five minutes.

Ms. ADAMS. Thank you, Mr. Chairman. Thank you, Ranking Member Velázquez. And thank you to the speakers for your insightful remarks.

And, of course, this is a critical issue and I think about collaboration as I think about this. And my question, Dr. LeClair, to you, are credit unions and community banks working hand-in-hand with the small business industry to develop the financial resources that help protect the assets of small businesses as well as the investments of financial firms from the effects of a cyber attack?

Ms. LECLAIR. Are they working, was that your question?

Ms. ADAMS. Yes. Yes. I mean, is there a collaboration in terms of the banks and the businesses?

Ms. LECLAIR. Yes. The collaboration that is out there is what we need to have and continue to have in order to be able to not only be prepared but to recover.

Ms. ADAMS. Is it working, in your opinion?

Ms. LECLAIR. I think that we have a ways to go still.

Ms. ADAMS. Okay. All right

Protecting the businesses, of course, is crucial, but it is also costly, especially when we talk about small businesses. And most of the insurance that small businesses have does not actually cover cyber attacks. What can we do to encourage that?

Ms. LECLAIR. Again, from the standpoint of if you are talking cyber insurance——

Ms. ADAMS. Right. And investing in it.

Ms. LECLAIR. And investing, yes, I do not think that small businesses really have any clear understanding of cyber insurance and what the capabilities are for them. I think it is a new area that is being developed. One of the reasons we are writing a book is to be able to give that to small businesses so they can understand what the options are out there for them and what they can expect from it.

Ms. ADAMS. Thank you.

Mr. McCracken, can you comment on it?

Mr. MCCRACKEN. Well, I do think it is worth noting that many very small companies are run by people who, you know, they are at the nexus of the individual and the business world. They see—these are very small companies I am talking about now—as extensions of themselves. And they are often very surprised to find out that their business bank accounts do not have the same kinds of protections that a consumer or personal account might have. And so when they are the victim of some sort of fishing scheme and their money is just gone, they initially often expect, well, I will go to the bank and we will get this fixed, like I know my neighbor did. And in fact, if it is a business account, that is simply not the case in many cases because they operate under different standards and they have different levels of protection. So I think that is something that we may need to address. And it is certainly something that we need to educate more small companies about in the first place because they do not understand it.

Ms. ADAMS. Okay. I was going to follow up with a question about the technological sophistication that was necessary, and I think you have probably answered that.

But Mr. Grobman, would you like to comment?

Mr. GROBMAN. Sure. I think one of the important things on the education side for small business is we can simplify some of the critical questions to something every small business can understand whether they are running security operations for themselves or relying on others. Even simply asking the questions of how would I be able to detect if a breach has occurred and what would my plan be to get back to a known good state after a breach, those are things that I think, unfortunately, many small businesses do not think about. They understand the threat of cyber security is real but they are maniacally focused on protecting without thinking about the other elements. And I think just the simple education things are key things that we need to do as a partnership.

Ms. ADAMS. Okay. Mr. Berger would you comment, please?

Mr. BERGER. Yes, ma'am. We completely agree. I think education is a very important component because some of the cyber experts, when they are looking at it from a forensic standpoint, they say 80 percent of credit card fraud and data breaches could be prevented by some simple things that the chairman actually talked about—updating the patches, doing the downloads that are necessary, and changing your passwords on a regular basis. Something like 80 percent of those breaches could be stopped. So it is an education component for that as well.

Ms. ADAMS. Proactive?

Mr. BERGER. Yes, ma'am.

Ms. ADAMS. Thank you very much.

Mr. Chairman, I yield back.

Chairman CHABOT. The gentlelady yields back. And I apologize for having to leave. I had to change my password.

The gentleman from Nevada, Mr. Hardy, who is the chairman of the Subcommittee on Investigations Oversight and Regulations is recognized for five minutes.

Mr. HARDY. Thank you, Mr. Chairman.

Mr. Grobman, you mentioned that small and medium businesses are just as vulnerable to the same as the sophisticated cyber security threats as large corporations. Although small businesses are vulnerable as large corporations, do you think that the susceptible threats to emphasize or do you believe that the cyber criminals are only targeting small business because they know that they do not have cyber security ? Or would these cyber security criminals only focus on the large corporations due to their financial benefit?

Mr. GROBMAN. I think what we see is adversaries go after targets that will most effectively meet their objectives. If their objective is to generate money, they will look at is it more valuable to breach a large company and steal a mega database or target many small businesses and breach many of them? And I think we see both happening per the data that we cite. So it is not " one size fits all" and that is one of the reasons why it is critical that all organizations think about cyber security because it is really about the objectives of the adversary.

Mr. HARDY. Thank you.

Mr. McCracken, with that being said, you mentioned that the EMV will be costly to small businesses for replacing that equipment and training for the employees on how to use that. I understand your concern for that small business owner, these costs, but do you not believe that the cost is insignificant in comparison to the loss to the consumer and the potential that it may impact that small business in maybe losing business competition by not implementing those standards?

Mr. MCCRACKEN. Well, what is going to go into place October 1st is a shift in liability. So if they do not have a chip card reader and that kind of card comes in and it is fraudulent, they are on the hook rather than the issuing bank. Our point was there are many small companies that simply do not have the kind of customer base where they are subject to that kind of fraud. If you are a deli and all you are selling are sandwiches and sodas on credit cards, the odds that someone is going to take a stolen credit card number and come in to your shop and buy a whole bunch of sandwiches is probably pretty remote. Also, if you know all your customers personally, then you are probably not at very much risk for that fraud. But if you sell high-dollar electronics or jewelry and you do not know who your customers are, you had better switch to the EMV system as soon as possible because you are going to be on the hook for those. That is really our point. But we want to get to the point really where mag stripe cards do not exist at all anymore. We think that really is the ultimate solution because right now we have these kinds of cards that are very easy to put fraudulent data on and go out and use, and so long as those exist, we think cyber criminals are going to find ways to get that day, if not this way, then that way. And we can patch this and it will pop up over here. We have got to get to a point where we have only chip-based cards.

Mr. HARDY. Thank you.

Mr. Berger, I appreciate your statement when you just stated that cyber security is everybody's responsibility. I believe that is the truth. Also, you state that the United States Government is identifying malicious actions in their networks and preparing to monitor program that strengthen their areas. I guess the question is, the private sector, you see the expansion and the growth of things like Life Lock and other businesses growing out of this challenge that we are having to help the small businesses, or will that be a benefit at all to them?

Mr. BERGER. I think any improvement in technology that prevents cyber fraud is fantastic and it is welcomed. But when you have the entire payment ecosystem, if you have the financial institutions, the payment processors, the payment networks all doing a pretty darn good job in protecting people's personal and financial data, the cyber criminals attack the weakest component of that ecosystem. And so from our standpoint, we still think there needs to be a national standard at a minimum, not on an equal basis but on a flexible basis because I am not talking about the small mom and pops where you get your Yoo-Hoos and your Slim Jims from, but some of the larger retails, it is flexible and it should be scalable, but there needs to be some set standard to hold people accountable for that kind of stuff.

But back to your original question, we do like technology and we welcome any technology that prevents the bad guys from winning.

Mr. HARDY. And I guess my last question maybe to one or all of you is just what are we doing together as a collaborative group here, along with the federal government, to assure this can happen in a quick, safe manner, because expediency is of real importance.

Ms. LECLAIR. I think from going back to the original question, we keep going to the 10 percent. If you think of the 90/10 rule where 90 percent of the issues revolve around people, we focus a lot of our time on the 10 percent, which is the technology. So I think we have to continue to think of the 90 percent and how we are going to educate people because they are in every piece and part of what we talk about.

Chairman CHABOT. The gentleman's time is expired.

Did any other witnesses want to answer that?

Mr. Berger?

Mr. BERGER. Yeah. Just real quickly.

This being Washington, D.C., there are probably 35 coalitions working on this issue right now here, so. There is a collaborative effort amongst merchants, financial institutions, as well as the payment networks.

Chairman CHABOT. That is great to hear. Thank you. Thank you very much.

The gentlelady from New York, Ms. Meng, is recognized for five minutes.

Ms. MENG. Thank you, Mr. Chairman. And thank you to our witnesses for being here and helping us learn more about this newer and important topic.

My question is in relation to the SBA and many of the resource centers and locations that they have throughout the U.S., and particularly in my home county and borough of Queens, New York. What more can the SBA do, whether it is training, increasing awareness? And are there any incentives, financial incentives that might be helpful for small businesses to encourage them to have these plans in place?

Anyone can answer.

Ms. LECLAIR. I can start out. I think one of the things that we could work on is perhaps grants for small businesses in order to upgrade their security and train their staff. Those would be a quick start to get us there.

Mr. GROBMAN. I think one of the other things is the very nature of cyber security is that it changes very rapidly and it is very difficult to use static policies to really resolve the core issues. The SBA has a strong relationship with small business and it is structured well to comprehend the rapid change in the evolving landscape. And looking at it from that perspective may be a key area of focus.

Mr. BERGER. And if I may add, the SBA actually has done a pretty good job in creating recently some workshops and modules in small business that deal specifically with cyber and data security and do some of the components to protect their business.

Ms. MENG. Do you think there are additional measures that the SBA or federal government can take in addition to what they are already doing? Maybe working or collaborating with law enforcement? Is that something we should see more of in relation to small businesses?

Mr. MCCRACKEN. One suggestion I have is actually is helping us to sharpen the focus on the problem because, of course, when you talk about it today, when we say small business, we are talking about all different kinds of companies in various stages of development, different supply chains, different industries, different access to data. I really think that one role some centralized agency, perhaps the SBA could play is to try to define the nature of various threats and the kinds of companies that might face them the most and try to figure out how we can focus our efforts. Instead of saying outreach to small business, let us talk about what do we need to do with this type of retailer or someone who has access to health records. And I think we really have to get much more specific about the kinds of approaches that we need to use, and the SBA might be able to help with that.

Ms. MENG. And just lastly, in terms of just curious, can you tell if a lot of these attacks are coming more from international or domestic? Does that have an effect on the kind of attacks?

Mr. GROBMAN. I think we see attacks coming from all facets, and I think the thing that we do see is regardless of whether an attack is coming from an origin that is domestic or international, they are using the same playbook. So the way that we ultimately defend against cyber security issues I think will be less about where they originate than what they are actually trying to achieve.

Mr. BERGER. We are seeing the same thing. They do not discriminate. The cyber criminals will attack from anywhere.

Ms. MENG. Thank you. I yield back.

Chairman CHABOT. The gentlelady yields back. And the gentlelady from Michigan, Ms. Lawrence, is recognized for five minutes.

Ms. LAWRENCE. Thank you, Chairman, and thank you to our ranking member as well.

Over 250 credit unions have their headquarters in my state of Michigan, and more than 4.5 Michiganders have membership in these credit unions. I want to thank the credit union representatives for making sure that my staff and I clearly understand the challenges you face in the event of data security for no fault of your own.

Mr. Berger, what are data breaches costing credit unions, and have these costs been increasing? And what do these cost impacts have on credit unions to provide services to their members?

Mr. BERGER. For just the Home Depot breach alone was $30 million, and you combine Target and all the other breaches in 2014, it is close to $80 million it hit credit unions. And what happens is that we rarely get any reimbursement for those recouped losses. And so what we are calling for is some kind of national standard that holds people accountable for those breaches.

And we talked about shifting to EMV and chip technology and that is a really important component, but it is not a panacea. That will prevent credit card fraud, but going to EMV or chip technology would not have stopped any of the Target or Home Depot breaches whatsoever. And so it is really important to separate credit card fraud from data breaches, and we need to address data breaches and make sure it is a level playing field. Because I had mentioned earlier, when you look at the payment ecosystem, the cyber criminals attack the weakest component of it, and so if everybody is doing their job and everybody is responsible for cyber and data security, everybody has to be on that level playing field and doing their part.

Ms. LAWRENCE. Well, I look forward to working with the chair and the ranking member, as well as my fellow members of Congress. I just left a briefing, the issue of cyber security and I thank you for understanding that we need to look at data breaches as well as a separate entity. And I just look forward to joining with you to address this issue.

I thank all the individuals who are here today to testify. Thank you so much, and I yield back the rest of my time. Thank you, Mr. Chairman.

Chairman CHABOT. Thank you very much. The gentlelady yields back.

And in lieu of a second round, having discussed this with the ranking member, we have just one question I think we both jointly would like to ask the panel and you can respond in any way that you would like to.

Chairman McCaul, who is chair of the Homeland Security Committee has legislation which will be coming to the floor tomorrow, so it was very timely, the Small Business Committee looking at the aspects of how cyber attacks affect small businesses, so it was very timely to have you all here today because we are going to be voting on legislation that is somewhat relevant this week, tomorrow. The legislation seeks to strengthen the National Cyber security and Communications Integration Center's role as the lead civilian interface for the sharing of cyber security risks and incidents. It also aims to preserve existing public-private partnerships to ensure ongoing collaboration on cyber security .

I will just start with you, Mr. Grobman, and we just go down the line, do you want to comment?

Mr. GROBMAN. Yes, I would.

I think one very important aspect to comprehend is that sharing of information is one aspect of what is needed for an effective cyber defense. Getting data from global threat intelligence, sharing between entities, but also very important is the data that is local to the organization, and combining all of those types of data together in an analytical capability to determine when a breach is underway and be able to react quickly is critical. I do become concerned that there is a focus on just one of the elements around data sharing being the thing that will make things go away. It is as much about looking at the data we have more effectively than just collecting more data.

Chairman CHABOT. Thank you very much.

Mr. McCracken, did you want to comment?

Mr. MCCRACKEN. Not at length, but I would generally agree with Mr. Grobman's remarks. And the bill seems, I think, positive, and a step in the right direction. But obviously, it will not be a panacea, but it will certainly help. Information for small companies is useful but we have got to actually give them a lot more direction on how to use that information as well.

Chairman CHABOT. Thank you.

Mr. Berger?

Mr. BERGER. Yes, Mr. Chairman, we do support the legislation, but we think there needs to be really three key components to be successful in all this cyber and data security. One is the sharing of information. Two is notification. And three, we still think there needs to be a national standard for retailers and merchants. We need to make sure there is a level playing field and everybody is doing their part in holding folks accountable.

Chairman CHABOT. Thank you very much.

And Dr. LeClair?

Ms. LECLAIR. I think that goes back to my earlier comment where I talked about the nuclear industry where you have a central entity that looks at lessons learned, what is happening, identifying that; notification to other organizations within that area; and then standards were created there. So those are the three things, very similar to what you were talking about. So a very similar comment.

Chairman CHABOT. Thank you very much.

And I know the ranking member and I would like to thank our witnesses for their participation today.

I ask unanimous consent that members have five legislative days to submit statements and supporting materials for the record. And if there is no further business to come before the Committee, we are adjourned. Thank you very much.

[Whereupon, at 12:08 p.m., the Committee was adjourned.]

APPENDIX

WRITTEN STATEMENT FOR THE RECORD OF

STEVE GROBMAN
INTEL FELLOW AND CHIEF TECHNOLOGY OFFICER – INTEL SECURITY GROUP

INTEL CORPORATION

Before the

UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON SMALL BUSINESS

FULL COMMITTEE HEARING

On

"SMALL BUSINESS, BIG THREAT: PROTECTING SMALL BUSINESSES FROM CYBER ATTACKS"

APRIL 22, 2015

Good morning Chairman Chabot, Ranking Member Velazquez, and other members of the Committee. Thank you for the opportunity to testify today. I am Steve Grobman, Intel Fellow and Chief Technology Officer for Intel Security Group at Intel Corporation, and I am pleased to address the Committee on the important issue of protecting small businesses from cybersecurity threats. We appreciate the Committee's interest and engagement on this subject.

My testimony will focus on the following areas:

- The threat landscape and its implications for small business
- How best practices and education can help small businesses protect themselves
- How the private sector can deliver security solutions to help small business
- Policy recommendations in support of private sector solutions for small business

First, I would like to provide some background on my experience and Intel's commitment to cybersecurity.

As the chief technology officer for Intel Security Group at Intel Corporation, I set the technical strategy and direction for the company's security business across hardware and software platforms. I joined Intel in 1994 as an architect in IT and have served in a variety of senior technical leadership positions during my Intel career. Before assuming my current role in late 2014, I spent a year as chief technology officer for the Intel Security platform division.

Prior to that role, I spent two years as a chief technology officer at Intel's subsidiary McAfee, where I focused on integrating security technology from the two companies. In prior roles, I served as chief security technologist for the Intel Atom processor system-on-chip design group and spent seven years as chief architect for Intel vPro technology platforms. In the latter position, I led work on the solutions architecture that resulted in a business platform with unique hardware-based management and security capabilities.

INTEL'S COMMITMENT TO CYBERSECURITY

Intel is a world leader in computing innovation. The company designs and builds the essential technologies that serve as the foundation for the world's computing devices. As a leader in corporate responsibility and sustainability, Intel also manufactures the world's first commercially available "conflict-free" microprocessors.

Security has long been an Intel priority. Indeed, security, along with power-efficient performance and connectivity, comprise the three computing pillars around which Intel concentrates our innovation efforts. A little over a year ago, Intel formed a new business unit to further the security pillar – the Intel Security Group – combining our subsidiary McAfee with other security resources from across Intel to form a single organization focused on accelerating ubiquitous protection against security risks for people, businesses, and governments worldwide.

Intel has long shared the sentiment with the U.S. and global governments that we cannot delay in collectively addressing the evolving cybersecurity threats facing us all, and indeed our company has been at the forefront of efforts to improve cybersecurity across the compute continuum. As a leading developer and manufacturer of foundational information and communications technology products, we offer a unique understanding of the gravity of our cybersecurity challenges, and the reality that governments, businesses and consumers are facing a cybersecurity threat landscape that has changed fundamentally. Countering these increasingly sophisticated threats to all organizations requires the cooperative efforts of government, industry and non-governmental organization (NGO) stakeholders working together to improve cybersecurity in a way that promotes innovation, protects citizens' privacy and civil liberties, and preserves the promise of the Internet as a driver of global economic development and social interaction.

Intel Security delivers proactive and proven solutions, services, threat intelligence and analytics that help secure systems and networks around the world, allowing users to more securely connect to the Internet and browse and shop the web. Fueled by an award-winning research team, Intel Security creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. Last year, we co-founded the Cyber Threat Alliance with other security vendors to drive a coordinated industry effort against cyber adversaries through deep collaboration on threat intelligence and sharing of actionable indicators of compromise, allowing alliance participants to deliver greater security to customers including small businesses.

PUTTING SOLUTIONS IN CONTEXT:
Understanding the Threat Landscape and its Implications for Small Business

Increasing Sophistication of Attackers Threatens Organizations of Every Size. Over the past decade, the attacker type has evolved from recreational "hackers" with limited capabilities to organized crime and state sponsored actors employing extensive resources and highly skilled personnel. At the same time, the stakes for breaches continue to rise.

The attacker community has matured so far that a vibrant criminal underground economy has emerged. Online web stores now sell hacking tools to any would-be attacker, and online markets make it easy and efficient to sell stolen credit card information.

The increasing sophistication of attackers and, hence, attack types, places tremendous pressure on today's security processes, tools and people. These sophisticated attackers are developing new techniques that are substantially more difficult to detect and stop. The most advanced techniques extend beyond exploiting vulnerabilities in the operating system or applications and are now starting to attack the underlying virtual machines, firmware and hardware.

Small and medium sized businesses (SMBs) are just as vulnerable to these same sophisticated cybersecurity threats as large corporations, in both strength and type. While most stakeholders today generally acknowledge that cybersecurity threats are becoming increasingly sophisticated, evolving and intensifying, many in both government and industry nonetheless believe the threat an organization faces is commensurate with its size, essentially assuming that smaller organizations face smaller threats. As recent events such as Operation Source and Heartbleed have demonstrated, however, today SMBs face many of the same threats as large organizations, and experience similar negative consequences. According to Verizon's just-released 2015 Data Breach Investigations Report, while larger organizations post higher losses per breach, further investigation finds that larger organizations just typically lost more records than smaller organizations, and thus had higher overall cost. Breaches with equivalent record loss had similar total cost, independent of organizational size.

Innovative Technologies Bridge Resource Gaps for SMBs, But Also Magnify Threats. It should come as no surprise that cyber criminals follow the latest technology trends because that's where the targets are the most promising. Technological innovations help enable some of the key building blocks to provide better security to SMBs, but at the same time present some of the key security challenges facing SMBs, including:

- *Mobile Threats*: Small businesses, as others, are relying more on mobile devices for not only communication but for business processes, and there's every reason to believe this trend will continue. Malware written specifically to attack mobile devices is also increasing, creating new challenges as the security industry adapts to counter threats to mobile as well as traditional compute platforms.
- *Migration to the Cloud*: Another information technology (IT) trend that serves small business particularly well is migration to the cloud. Small businesses, in particular, can find real efficiencies in outsourcing their IT and communications systems to the cloud. They can reduce costs, improve offerings, eliminate complexity and have less need for onsite IT staff. These are great objectives – as long as security is not sacrificed.
- *IOT and the Explosion in Number of Devices.* Coupled with the above are trends such as the Internet of Things (IOT), which multiply mobile growth beyond phones and tablets, to a wide array of internet protocol (IP) devices that SMBs and others now need to worry about, such as networked metering devices, sensors, appliances, and point of sale systems. While the promise of IOT innovation brings great potential benefits to more offices and businesses across the country every day, it also carries with it new security risks that must be managed.

- *Clients are Often not Connected to Company Networks*: Given the mobile nature of today's workforce, as well as the increasing use of BYOD (bring your own device) programs, users at companies of all sizes commonly access resources from external networks such as hotspots and home networks. The result is that company-owned network equipment is simply unable to inspect a growing percentage of traffic and protect a large swath of users and devices.
- *Traffic is Encrypted*: Even when accessible, application and web traffic is increasingly encrypted. Network security devices are therefore unable to inspect the traffic's content. The coarse-grained information available to network products can provide baseline protection, but is insufficient to detect advanced threats. The shift to "Apps" (such as Android or iPhone Apps) further heightens this challenge, as many of these applications require encryption.
- *Performance Issues Preempt Security*: Customers are turning off security vendors' next generation firewall features such as deep packet inspection (DPI) to maintain network performance levels – creating a tug of war between security and performance priorities.

Adversaries Enjoy Significant Advantages. Understanding the complexity of today's threat landscape demands an examination of the threat actors carrying out the cyber attacks. Our research and analysis reveals that cyber adversaries benefit from and exploit several key advantages, including:

- The ability to *quickly enhance the tools and capabilities of attacks* through a community of innovators and service providers continuously specializing in threats and infrastructure. This attribute creates additional exposure for SMBs, who may not have the resources to deploy the latest adaptive technologies, or are not deploying risk management-based solutions at all.
- A *working knowledge of how organizations implement defenses badly*, including knowledge of specific product deployment models, industry architectures, and even specific organizations' defenses that provide opportunities for attack. SMBs may also be particularly susceptible here, as they may be more likely to deploy "yesterday's" solutions due to resource constraints or other factors.
- The reality that those waging cyber attacks have *unlimited opportunities to learn which tactics are effective* against specific standards and products – thus they only have to be right once. Again, because SMBs are more likely to deploy retail products, including those likely intended for consumers, rather than enterprise-focused solutions, they may be disproportionately impacted here.

Countering such advantages is difficult for even well-resourced security vendors or large corporations to manage; the edge adversaries hold over SMBs is even more pronounced.

The Attractiveness of SMBs as Targets. If we add up the elements of the threat landscape we've covered thus far – the sophisticated threat landscape facing SMBs, the challenges magnified by innovative technology trends, and the advantages enjoyed by potential adversaries – it should come as no surprise that SMBs represent increasingly attractive targets for cyber attacks. Many highly sophisticated and well-resourced attackers perceive that large organizations have deployed greater defense resources and so over time have become harder to breach. In response, they have turned their attention to SMBs as a means to create revenue from a large number of less-protected targets, or as an alternate and easier path to infiltrate large organizations.[1]

This last point is worthy of particular emphasis. Small businesses are not only at risk of high-volume attacks intended to infect as many devices/systems as possible, such as ransomware attacks, but are also at risk of being specifically targeted by adversaries. A primary reason for this is SMBs are attractive as an attack conduit to breach larger business or government targets rich in high-value data or other assets. This concern is not hypothetical. Some of the major breaches in 2014 were originated via SMBs providing facility services to major corporations.

Attacks of this type launched on SMBs can impact numerous industries and vertical markets. While the details of each attack differ, modern attacks share a common pattern with five distinct stages. The full lifecycle of a targeted attack may take months or even years to plan and execute. As an illustrative example, consider the five stages of a recent attack against a retailer that was in part facilitated by an SMB:

- *Reconnaissance*: The goal of reconnaissance is to learn about the organization's employees, IT infrastructure, and other details relevant to launching an attack. A common method for gathering information is through social engineering where an end-user is fooled into surrendering data or undertaking action to compromise his or her environment. In the case of one larger retailer, cyber criminals found vulnerabilities not within the retailer itself, but through a much smaller outside vendor. The attackers used reconnaissance to learn the identity of the retailer's heating, ventilating, and air conditioning (HVAC) vendor and then used email phishing to steal passwords used by employees of that SMB provider.
- *First contact*: Once the attacker finds an entry point, s/he gains initial access to a company's network or endpoints. The retail victim's attackers used the HVAC employee credentials to access the retailer's network. They scanned the network and identified the Point of Sale (POS) terminals.

[1] "Smaller companies are attractive because they tend to have weaker online security. They're also doing more business than ever online via cloud services that don't use strong encryption technology. To a hacker, that translates into reams of sensitive data behind a door with an easy lock to pick." *Why Your Business Might be a Perfect Target for Hackers*, Inc. Magazine, available at: http://www.inc.com/magazine/201312/john-brandon/hackers-target-small-business.html

- *Local execution*: After having infiltrated a network, the next step of an attack is to design and execute code to exploit vulnerabilities on a device. The most dangerous exploits are often sophisticated "zero-day" attacks that uniquely target the victim and have never been seen previously. In the case of this retailer, however, the malware used to infect the point of sale systems were well known.
- *Establish presence*: The next step is to execute code to gain privileges, expand to other systems, and take evasive action to avoid detection. Malware often provides "back door" access to allow full remote control. In this example, the goal was to obtain credit card information. The malware spread to 90% of the company's stores, used a technique to scrape credit card details from the systems' memory, aggregated the information on a staging server, and ultimately transferred it to servers located overseas.
- *Malicious activity*: The final step is to perform the malicious activity, be it destructive or financially motivated. The attacker in this example sold the harvested credit cards on the black market for an estimated $25 to $45 U.S. dollars each.

There were a number of high profile cyberattacks in 2014 impacting hundreds of millions of individuals in the aggregate that followed a similar and a predictable pattern performed by sophisticated adversaries (though not all involved an SMB as an attack vector). Traditional security technologies have proven inadequate in the face of these attacks.

LAYING THE GROUNDWORK FOR SOLUTIONS:
Helping SMBs Help Themselves through Education and Best Practices

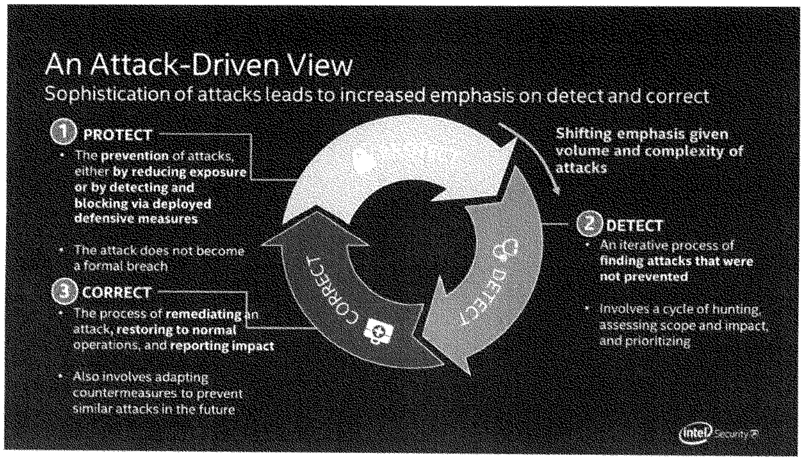
The biggest problems facing SMBs seeking to protect themselves from cyber attacks are often not related to technology. A foundational question is whether they have the resources, know-how and capacity to deploy existing technology solutions efficiently and effectively across their small enterprises. While the reality is today they may not, we offer some suggestions to help lay the groundwork for the more efficient deployment of technologies by SMBs.

Significant education and support of SMBs is needed in order for the promise of technological solutions to be fully realized. This committee has likely heard previously that many SMBs lack the resources to stay current with cybersecurity best practices, and many SMBs may believe that cybersecurity is not an issue or priority for them because of their size. In reality, small businesses store personal information, implement operational requirements and own valuable intellectual property just as large enterprises do, so they too need strong cybersecurity protections. A compelling and focused education system for SMBs is needed to ensure they understand the need for cybersecurity at all organizations, to better and more quickly enable them to determine the best practices to meet their specific risk issues and implement them efficiently. According to the Small Business Administration, SMBs comprise 95% of all U.S. businesses and generate more than half of the nation's gross domestic product. When looked at in the aggregate, budget constraints amongst smaller businesses accentuate the need to drive adoption of connected, ecosystem-based strategies around security planning and investment.

SMB education efforts should be grounded in flexible and nimble risk management based solutions that protect, detect and correct. As discussed above, cybersecurity risk is not only complex but dynamic. Because we face a constantly evolving threat landscape, we must develop best practices to help mitigate those shifting risks. Regardless of their size or resources, SMBs and all organizations must be allowed to prioritize and focus on the most serious risks to the most critical assets, systems, and processes based on their unique business and threat profiles.

The increasing sophistication, volume and complexity of attacks are driving Intel Security and the rest of the security industry to focus more on non-deterministic detection of attacks. This is part of a holistic, risk management based approach that places a proportionate emphasis on protecting systems, detecting the attacks, and a corrective process that involves responding to and remediating attacks so as to restore normal operations.

This three phase construct – protect, detect, correct - encapsulates what I like to refer to as an attack-driven view. (See Figure 1.)



An Attack-Driven View

Sophistication of attacks leads to increased emphasis on detect and correct

① PROTECT

- The **prevention** of attacks, either **by reducing exposure or by detecting and blocking via deployed defensive measures**
- The attack does not become a formal breach

③ CORRECT

- The process of **remediating** an attack, **restoring to normal** operations, and **reporting impact**
- Also involves adapting countermeasures to prevent similar attacks in the future

Shifting emphasis given volume and complexity of attacks

② DETECT

- An iterative process of **finding attacks that were not prevented**
- Involves a cycle of hunting, assessing scope and impact, and prioritizing

Figure 1.

Large enterprises are now comprehending the reality of today's threat environment, and are investing resources not only to protect their IT and network assets, but also in the detect and correct pieces of the puzzle. As SMBs are often vendors to large enterprises, those large enterprises need to analyze the threats posed by connecting SMB systems to their greater and extended company IT infrastructures. While SMBs of course need to continue deploying solutions designed to protect their networks, they also need to invest in all three of these fundamental risk management functions. No organization, large or small, is ever going to eliminate threats entirely and successfully block all attacks from penetrating its systems. Cybersecurity spending at any scale must reflect this reality, and adequately apportion resources across all risk management functions.

A useful reference tool for SMBs in prioritizing and managing risks is the Framework for Improving Critical Infrastructure Cybersecurity (the "Framework"),[2] which Intel has supported from its inception through its early implementation. President Obama issued Executive Order 13636 – Improving Critical Infrastructure Cybersecurity in February 2013 and over the ensuing year Intel collaborated with government and industry stakeholders to help develop the Framework as a flexible risk management tool to improve cybersecurity, grounded in consensus best practices and international standards. The first version of the Framework was delivered on February 12, 2014, and soon thereafter Intel launched a pilot project to test the Framework's use at Intel. Our pilot project assessed cybersecurity risk for our Office and Enterprise infrastructure, and demonstrated that the Framework provided clear benefit to Intel.

We focused on developing a use case that would create a common language and encourage the use of the Framework as a process and risk management tool, rather than as a set of static compliance requirements. Our early experience with the Framework helped us harmonize our risk management technologies and language, improve our visibility into Intel's risk landscape, inform risk tolerance discussions across our company, and enhance our ability to set security priorities, develop budgets, and deploy security solutions. The pilot resulted in a set of reusable tools and best practices for utilizing the Framework to assess infrastructure risk; we plan to use these tools and best practices to expand Intel's use of the Framework. A detailed account of our pilot project and the benefits we derived from using the Framework is contained in the white paper we published in February, *The Cybersecurity Framework in Action: An Intel Use Case*,[3] which we can provide to the Committee upon request.

[2] To read about the Cybersecurity Framework, visit: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf. It is worth noting that the five core functions of the NIST Cybersecurity Framework (identify, protect, detect, respond, and recover), are the rough equivalent of and track closely the upleveled, even more simplified protect-detect-correct construct discussed above.

[3] To read Intel's White Paper, *The Cybersecurity Framework in Action*, visit: http://www.intel.com/content/www/us/en/government/cybersecurity-framework-in-action-use-case-brief.html

Intel encourages other organizations to follow the path we forged by developing their own Framework use cases and driving adoption of the Framework across their ecosystems. Intel recently took the initiative to link the Framework to our Supplier Guidelines,[4] in an effort to make sure our ecosystem of suppliers, including many SMBs, are using sound risk management-based security practices focused on not only protecting, but other important risk management functions such as detecting, response and recovery.

Indeed, the Framework can serve as a foundational educational tool for SMBs, providing a common language for better communicating with security vendors and other business partners, as well as key learnings as to why cybersecurity should be grounded in a risk management approach. Security vendors such as Intel Security can also play a role in helping SMBs help themselves, by developing innovative new solutions and implementing functionality in their products to provide the risk management benefits of the Framework in ways that can be efficiently deployed by smaller enterprises.

DELIVERING SOLUTIONS:
How the Private Sector Can Provide Technology Solutions to Small Businesses

As I testified earlier, often the biggest problems faced by SMBs are not related to the technologies that can help them better protect, detect and correct in the face of cyber attacks. The primary obstacles to realizing better cybersecurity in SMBs are better characterized in terms of resources, know-how and capacity to deploy existing technology solutions and capabilities efficiently and effectively in a holistic manner.

As mentioned previously, the security industry faces significant challenges to staying ahead of attackers. But security innovation is helping us make progress toward overcoming adversary advantages, better mapping technologies to risk management functions, and providing security connected solutions.

Overcoming Adversary Advantages. Viewed through the lens of a security provider, for our industry to effectively defend against targeted attacks, we must overcome the advantages discussed earlier that tilt the playing field in favor of our adversaries. At a conceptual level, doing so calls for: (1) integrated and collaborative solutions; (2) simple and sustainable architectures; and (3) analytical, active and adaptive environments.

- **Integrated & Collaborative Solutions**. We must counter our adversaries' *innovation and infrastructure advantages* with solutions that enable individual solutions to quickly share what they are seeing (detections, indicators of attack,

[4] To review Intel's Supplier Policies and Framework Guidance, visit: https://supplier.intel.com/static/governance/supplierpolicies.htm

indicators of compromise), and update collective threat detection based on shared information.

- **Simple & Sustainable Architectures**. We must counter our adversaries' *organizational/enterprise knowledge advantages* by allowing organizations to easily and efficiently implement new technologies that reflect changing business requirements and the evolving threat landscape over time. Doing so requires the industry change how we design security technologies, and organizations such as SMBs change how they think about buying, implementing, and managing those solutions. We discuss some of these changes below in the context of our "Security Connected" approach.
- **Analytical, Active & Adaptive Environments**. We must counter our adversaries' *tactical advantages* by forcing them to be right more than once, providing a security environment that analyzes data, recognizes targeted attacks in progress, anticipates their tactics, and takes action to contain and mitigate their impact, while also enabling organizations to recover and adapt their security posture to deflect future attacks.

Mapping Security Capabilities to Risk Management Functions. The Security industry also needs to more fully map critical security capabilities to all phases of risk-management-based solutions, including the protect, detect and correct functions discussed in the preceding section.

Technologies used to defend against the attacks of today can be grouped into three, self-reinforcing, categories:

- *Protect*: Protection is a deterministic approach to stop hackers from infiltrating systems. These technologies protect information from unauthorized modification, destruction or disclosure by reducing the attack surface, encrypting confidential data, authenticating users, defining policies and blocking known attacks. Much of the vendor ecosystem has historically focused on this class of technologies. Many products use "signatures" and other deterministic algorithms for detecting malware.
- *Detect*: With the increased threat environment, even the most sophisticated protection technologies are likely to prove insufficient alone. Timely detection and notification of a compromise become critical. Security teams need more non-deterministic tools to inspect events across their environment to identify malicious activity. Early signs suggest detection is becoming a greater area of focus.
- *Correct*: A system must be recovered to a known-good state following a breach. Security teams address alerts, investigate breaches, complete forensic analysis, remediate damage and restore services. Ultimately, teams implement future

protection safeguards to prevent similar attacks from reoccurring. Scalable and comprehensive correction technologies are only just beginning to emerge.

With the increase in attack volume and sophistication, defenders are naturally shifting their emphasis from a protection-centric approach to one more equally balanced with detection and correction.

Putting It All Together: How a "Security Connected" Approach can help SMBs. In order to do security well, you need integrated solutions, as well as a common mechanism for those solutions to exchange information. At Intel, we refer to this concept as "Security Connected," or the ability of multiple security solutions and products to work together to exchange information. A Security Connected architecture is the primary methodology that Intel Security is investing in to more rapidly detect threats, and we urge the rest of the Security Industry to make similar investments.

Executed correctly, a Security Connected architecture can detect behaviors over time and begin to recognize, almost biologically, threats before they can overtake systems or network functionality. A connected, behavior-based approach enables solutions to communicate observed behavior amongst each other. Security can thus be managed in real-time based on policy that adapts to current threats and provides resilience: the ability to run while under attack. These intelligent systems are the result of innovation, and we need to help small businesses make wise – not expensive – choices to create a connected security foundation.

The below diagram provides a high-level depiction of how the products and systems comprising a Security Connected infrastructure might fit together and communicate in a non-deterministic way.

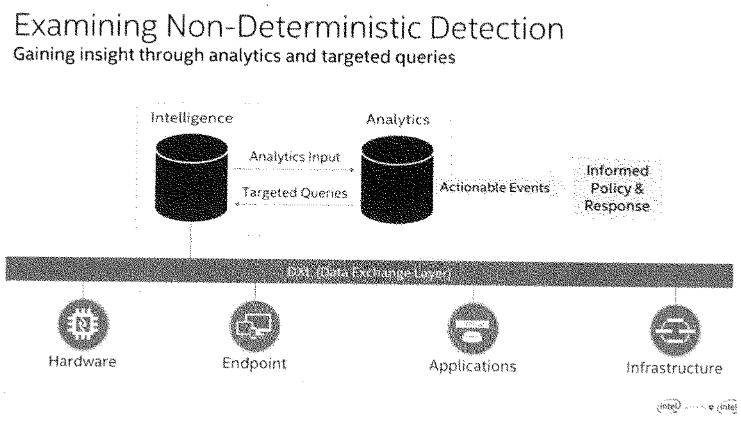

Examining Non-Deterministic Detection
Gaining insight through analytics and targeted queries
Intelligence
Analytics
Analytics Input
Targeted Queries
Actionable Events
Informed Policy & Response
DXL (Data Exchange Layer)
Hardware
Endpoint
Applications
Infrastructure

Figure 2.

Together, Intel's fully-integrated Security Connected platform embraces a number of security capabilities, though certainly not all organizations are likely to require deployment of all capabilities. Key capabilities represented in the above diagram include:

- **Analytics**, or optimized performance for actionable decision-making
- **Threat Intelligence**, or adaptive intelligence that provides stronger protection
- **Security Management**, or a simplified management experience that reduces effort and cost
- **Context & Orchestration**, or an integrated data exchange that helps deliver cohesive defense

Intel Security is particularly focused on three sustainable advantages that, when delivered together, improve overall security by amplifying the collective capabilities of the many individual solutions referenced above:

- **Messaging layer – Data Exchange Layer (DXL)** provides a standard for classifying and communicating details on attacks between individual product components
- **Centralized inspection – Threat Intelligence Exchange (TIE)** provides a framework for security products to collectively pinpoint threats and act as a unified threat defense system, providing adaptive security resilience and immunity to infections
- **End to end intelligence – Global Threat Intelligence (GTI) and local threat intelligence** provide a wealth of information and actionable insights on attacks across all the key attack vectors: file, messaging, network, and mobile.

Consistent with the above concepts, companies like Intel Security can develop world class security capabilities that larger companies with well-funded IT security departments can run as on premise solutions. However, we shouldn't think of SMBs as needing to necessarily acquire and deploy these capabilities directly. In certain SMB scenarios, deploying such solutions on premise may of course make sense. However, it is viable for even the smallest of companies to have access to these very same solutions, even if they do not have the resources to hire an army of IT security professionals, thanks to innovations such as the cloud and the Software as a Service (SaaS) offerings it helps enable. The security industry is able to leverage cloud and SaaS innovations to provide integrated security solutions that deploy increasingly complex technology and are comprised of multiple software and other products, but at the same time essentially mask the underlying complexity from the leanly staffed IT departments at SMBs who deploy them.

The way in which SaaS can help take the complexity out of the equation for small businesses by leveraging the Cloud is perhaps best illustrated by an example. Kenosha is a city in Wisconsin with a limited budget and relatively small IT staff of three protecting a network of approximately 300 work stations distributed across thirteen locations. To meet its security requirements, the city of Kenosha utilizes a cloud-based SaaS integrated solution for Kenosha's email security and encryption, web security, desktops and file servers, as well as intelligent routing technology. The fact that this type of SaaS security system is utilized across 13 different locations, yet managed by a team of only three IT professionals, demonstrates how cloud based-solutions can be leveraged in lieu of on premise solutions larger organizations have the luxury to deploy.[5]

Security Connected and the Cybersecurity Framework. The Security Industry has begun the process of mapping products and services to the Cybersecurity Framework as part of an effort to help SMBs and other customers bring order to the chaos of seemingly too many products and a lack of knowledge regarding how to use them. Because the Framework was informed by industry inputs and existing best practices, we believe current and future security solutions will map easily and intuitively into the Framework. Doing so should help SMBs better understand what solutions they need – and which to deploy.

Even absent a fully mature mapping to the Cybersecurity Framework, Intel Security's Security Connected platform unifies and simplifies the management of network and other defenses, while enabling real-time exchange of threat intelligence, analysis, and response that reduces time to detection and mitigation of attacks, and lessens the damage inflicted by them.

The Role of Continued Innovation and Integration. In addition to providing integrated security solutions, the security and IT industries must keep their focus on innovation in order to help small business and other organizations. At Intel, we feel strongly that the path forward is for security to be integrated into products at the beginning, for disparate islands of security to be connected, and for security vendors to offer real-time situational awareness of threats.

We also believe that as a security industry we must unify, simplify, and strengthen the way we provide security. We need to provide frameworks and open standards for integrating potentially disparate technologies – building bridges between security islands to close coverage and technology gaps. This is the rationale for our Security Connected approach. With cybersecurity integration, security companies and their small business customers will be able to more quickly and comprehensively detect and deter threats.

FURTHERING SOLUTIONS:
Recommendations for Policymakers to Further SMB Cybersecurity Efforts

Government can play a vital education and awareness role. As discussed earlier, government can help SMBs by promoting the value of risk management approaches

[5] http://www.mcafee.com/us/case-studies/cs-city-of-kenosha.aspx

such as the Cybersecurity Framework, and all cybersecurity efforts regarding SMBs (educational and otherwise) should acknowledge the high level of threat faced by even the smallest of organizations. The government can additionally help reinforce the value of affordable cyber security solutions to SMBs, filling a vital role in enabling industry to meet the cybersecurity needs of SMBs by raising awareness among vendors and solutions providers of the role SMBs actually play in protecting the nation's critical infrastructure. Doing so will inform and educate industry providers to understand the nature of the threat and foster innovative SMB solutions accordingly.

Don't Forget about the Framework ... and be patient. Implementation of the Cybersecurity Framework is still in its infancy, and policymakers should resist the urge to prejudge it. For instance, we understand why government stakeholders are anxious to gain a better understanding of whether the Framework is "working," and that some of those stakeholders will perhaps be less patient than others as we collectively seek to make sense of the extent to which the Framework is gaining traction across industry. It will take some time to see the impact from efforts such as Intel's inclusion of the Framework in our Supplier Guidelines, and in the meantime the government should encourage similar Framework advocacy.

Cybersecurity is a shared responsibility, but industry should lead. Private industry is already conducting a significant amount of work around best practices via consortia and other arrangements, as well as developing and deploying security products, services and other solutions. We do not believe government agencies should play a role in establishing guidelines for security providers, as that is not consistent with the voluntary nature of the Framework, and we note that any policy that may inhibit the market or innovation, or restrict the flow of necessary threat and risk information, could inhibit the marketplace from providing such solutions, impacting the availability of such solutions to SMBs and others.

Leverage lessons learned from small government organizations. State, local, and tribal governments (SLTG) are very similar to SMBs. The very largest SLTG economies draw the most attention and are often the model used when considering all of SLTG. However, the large majority of SLTGs are actually much closer to private SMBs in size and maturity, as suggested by the Kenosha example cited earlier. There are some obvious differences, but consideration of SLTGs should be included in efforts to improve SMB cybersecurity as the risks and solutions will often apply to both.

There is no need to reinvent the wheel—many existing interfaces and solutions within the Small Business Administration (SBA) can be leveraged to help SMBs. Many SMBs already have established relationships with the SBA, and are familiar with the services they provide as well as the procedures used to access them. We urge policymakers and other interested agencies such as DHS to fully partner with and support SBA and its programs when working with the SMB community.

Security mandates on SMBs won't work. Private industry provides a range of products and services at various price points, designed to address the needs of organizations of varying sizes and sophistication. We recognize some SMBs may struggle with limited resources to implement their security plans. However, we believe that it is ultimately up to the organizations themselves, not government, to ensure they have met their own cybersecurity goals, just as it is up to industry to find ways to enable SMBs to more effectively manage their own cybersecurity risks in the marketplace. That is why we advocate for education and support efforts intended to better equip SMBs with the tools to assess and implement their own cybersecurity goals and plans, and for security vendors to develop cost-effective solutions to aid in this effort.

Policymakers should explore whether economies of scale could be used to make a market for SMB cyber security solutions more attractive and financially viable for both buyers and sellers. There are likely multiple mechanisms possible to address the issue, such as consortia and combined purchasing agreements. Intel recommends policymakers work with the Small Business Administration and other SMB advocates to understand the market drivers and any existing programs.

CONCLUSION

Thank you again for the opportunity to address the Committee. I will be happy to answer any questions.

Testimony of Todd McCracken
President and CEO

NSBA
National Small Business Association

House Committee on Small Business Hearing:

"Small Business, Big Threat: Protecting Small Businesses from Cyber Attacks"

April 22, 2015

Good afternoon. My thanks to Chairman Chabot, Ranking Member Velazquez and the members of the Small Business Committee for inviting me to testify today on the impact of cybersecurity and credit card fraud issues on the health and growth potential of millions of small businesses.

My name is Todd McCracken, and I am President and CEO of the National Small Business Association (NSBA)—the nation's first small-business advocacy organization. NSBA is a uniquely member-driven and staunchly nonpartisan organization. NSBA has members in all sectors and industries of the U.S. economy from retail to trade to technology—our members are as diverse as the economy that they fuel. Small employers comprise 99.7 percent of all employer firms in the U.S. One in two workers in the private workforce run or work for a small business, and one in four individuals in the total U.S. population is part of the small-business community. Those are certainly impressive figures.

In the last few years, cybersecurity has emerged as a significant problem and concern for the small-business community. By the end of 2014, according to NSBA's Year-End Economic Report, fully half of small businesses reported having been the victim of a cyber-attack (up from 44 percent in 2013). Of those, 61 percent say an attack had occurred within the last year.

Cyber-Attacks on Small Businesses are Becoming More Prevalent

While a 14 percent increase in the number of small-business victims of a cyber-attack is significant, we believe the real story is the increasing impact those attacks are having on small businesses, in terms of both the interruption of normal business operations and the direct financial cost of the attack.

In 2013, only 12 percent of businesses reported that resolution of the cyber-attack required more than one week; by late 2014, more than one in five such attacks were still unresolved after one week, with 13 percent of them requiring more than two weeks. Three in five businesses experienced a service interruption, and a third had their websites go down for some period.

Small Companies Have Fewer Resources to Deal with Cyber-Attacks

Many small companies are not in a position to have a dedicated IT department, and many either outsource IT functions or assign such duties to an employee with other responsibilities—often the owner him/herself. In fact, the number of business owners who personally handle IT support appears to be on the rise. When we asked in 2010, 25 percent of business owners indicated that they were primarily responsible for IT support in their companies, while a larger number (36 percent) said they contracted with an outside vendor. By 2013, those numbers had essentially reversed, with 40 percent of business owners handling IT personally and only 24 percent indicating that they outsourced the function.

In the case of an outsourced IT function, a very small business might not be high on the IT firm's priority list of clients, even though such a firm is more likely to have the experience and technical expertise to resolve the issue quickly. In the case of in-house functionality, new issues might require research and training, making mistakes and delays more likely. In either scenario, dealing with the technical side of a cyber-attack presents unique challenges to our smallest companies.

Cyber-Attacks are Becoming Much more Costly

Perhaps the most startling finding of our most recent cybersecurity data was the sharp increase in the direct financial cost of cyber-crime on small companies. Of those companies reporting some kind of cyber-attack, the *average* amount of money stolen from a bank account rose from $6,927 in 2013 to $19,948 by late 2014, a 188 percent increase in a short amount of time.

This dramatic increase in stolen funds appears to be related to a sharp rise in the incidence and sophistication of so-called phishing scams. These scams send emails closely mimicking those of banks or other trusted institutions and citing an urgent need to login to an account or provide some other vital information. Small businesses are particularly vulnerable to these attacks, since multiple employees could have access to vital information. Further, business accounts do not enjoy the same level of protections and guarantees against loss and theft as those provided to consumers—a reality that many small-business owners do not discover until it is too late. Consumers are protected by Regulation E, which dramatically limits their liability in a cyber-heist. Commercial accounts, however, are covered by the Uniform Commercial Code (UCC). The UCC does not hold banks liable for unauthorized payments so long as "the security procedure is a commercially reasonable method of providing security..." Few small businesses that are the victims of theft from their bank accounts ever recover those funds.

According to Verizon's 2015 Data Breach Investigations Report, phishing has increased dramatically in just the last four years, having gone from about 2 percent of cyber-attacks in 2010 to over 20 percent in 2014. Moreover, these phishing attacks have become much more sophisticated, with a high degree of verisimilitude. Small companies need to engage in ongoing employee training to recognize and avoid these dangerous traps.

Credit Card Fraud and Small Businesses

Various forms of credit card fraud have been part of our financial landscape for some time. However, the increased technical prowess of cyber-thieves—and the continued prevalence of magnetic stripe cards—has taken credit card fraud to heightened levels. The U.S. finally appears to be taking significant steps toward the introduction chip (EMV) enabled cards, or so-called chip and PIN cards.

Liability Shift

As EMV cards begin to enter the U.S. market, the credit card issuers will begin to shift liability for card fraud to the entity with the lowest level of security. The practical effect of this rule—effective Oct. 1, 2015—is that merchants will, for the first time, become liable for fraudulent card use if they have not upgraded to the latest EMV card reader technology and software.

This move to EMV means that millions of countertop card readers will need to be replaced. The change is also likely to mean new software and a need for employee training. Therefore, since the transition will both be expensive and time-consuming, smaller merchants should carefully consider whether the shift to EMV card readers makes sense for their businesses, at least for now.

Merchants who sell low-priced goods and consumables, for instance, are unlikely to be targets for credit card fraud, so they are unlikely to see their potential liabilities significantly rise as a result of the shift. However, merchants that sell more expensive goods with strong re-sale value (e.g., electronics, jewelry), and who do not know their customers well, have a higher incentive to move to EMV card readers. Small businesses should carefully examine their own "charge-back" history to determine whether the investment in the new technology and processes makes sense for them at this time.

Hastening the Transition to a More Secure EMV Environment

Besides a general lack of awareness of the liability shift issue, there are two other major reasons that smaller merchants have not generally made the switch to EMV card readers:

1. Card issuers are not offering reduced interchange fees for merchants using EMV care readers, despite promised reduction of fraud resulting in their use. Given that card issuers have long blamed fraud as a prime cause for high interchange fees, merchants will naturally expect that EMV implementation will drive down those fees.

2. Card issuers have not yet made their own transition to EMV cards. Until smaller merchants see a market demand (in the form of their customers using chip-enabled cards), they are unlikely to move quickly to accommodate a non-existing demand.

Stepped-up issuance of EMV-enabled cards, combined with the eventual elimination of magnetic-stripe cards altogether is the only logical path toward a significant and lasting reduction in card-based fraud, at least for "card-present" transactions.

Recommendations

Cybersecurity is a large and growing threat to the small-business community. NSBA urges Congress to move forward on establishing streamlined guidelines and protocols to ensure the protection and security of online data and financials, but cautious against a knee-jerk reaction that would unfairly place a disproportionate burden on America's smallest firms:

- Legislation to enhance America's cybersecurity should provide clear, simple steps for companies to follow when their data is breached and must balance the need for greater information sharing with privacy rights.
- Any federal discussion on cybersecurity or development of a private-public partnership or advisory board must include representatives of small business.
- Extend consumer banking protections to the banking accounts held by America's smallest firms.
- Congress should maintain oversight on the credit card technology transition and ensure small firms are protected against any unfair or seriously burdensome costs or liabilities associated with transitioning to the new technology.

Conclusion

Thank you for the opportunity to speak with you today. I hope that we can work with each of you as we advance to solutions to the significant cybersecurity issues before us.

NAFCU

Testimony of

B. Dan Berger

President and CEO

National Association of Federal Credit Unions

"Small Business, Big Threat: Protecting Small Businesses from Cyber Attacks"

Before the

House Small Business Committee

April 22, 2015

Introduction

Good Morning, Chairman Chabot, Ranking Member Velázquez and Members of the Committee. My name is Dan Berger and I am testifying today on behalf of the National Association of Federal Credit Unions (NAFCU) where I serve as President and CEO.

Credit unions and their 100 million members have been heavily impacted by ongoing data security breaches by no fault of their own and I greatly appreciate the opportunity to testify before the committee today on cyber and data security. More can and must be done to better protect consumers. As NAFCU's chief advocate on Capitol Hill, at the White House, and before the regulatory agencies, I know firsthand how important yet complicated this issue is for policy makers to navigate.

Over the past 25 years I have worked in public policy and in a variety of business management positions. I earned a Master's degree in public administration from Harvard University and a bachelor's degree in economics from Florida State. Before joining NAFCU's executive team in 2006, I served as a chief-of-staff in the United State House of Representatives. I was named NAFCU's President and CEO in August, 2013.

As you are aware, NAFCU is the only national organization exclusively representing the interests of the nation's federally-chartered credit unions. NAFCU-member credit unions collectively account for approximately 70 percent of the assets of all federally chartered credit unions.

Background on Credit Unions

Historically, credit unions have served a unique function in the delivery of essential financial services to American consumers. Established by an Act of Congress in 1934, the federal credit union system was created, and has been recognized, as a way to promote thrift and to make financial services available to all Americans, many of whom may otherwise have limited access to financial services. Congress established credit unions as an alternative to banks and to meet a precise public need—a niche that credit unions still fill today.

Every credit union, regardless of size, is a cooperative institution organized "for the purpose of promoting thrift among its members and creating a source of credit for provident or productive purposes." (12 USC 1752(1)). While over 80 years have passed since the Federal Credit Union Act (FCUA) was signed into law, two fundamental principles regarding the operation of credit unions remain every bit as important today as in 1934:

- credit unions remains wholly committed to providing their members with efficient, low-cost, personal financial services; and,

- credit unions continue to emphasize traditional cooperative values such as democracy and volunteerism.

Credit unions are small businesses themselves, especially when compared to our nation's mega banks and largest retailers, facing challenges of meeting the products and service needs of their community, while dealing with various laws and regulations.

Credit Unions and Data Security

My testimony today will cover what credit unions currently do to have a successful track record of protecting information. NAFCU's work on the cyber security and data security front, how recent data breaches hae impacted credit unions and consumers, including the financial burdens they have faced, and NAFCU's principles for data security reform and thoughts on some of the ways forward on this issue.

As members of the committee are well aware, cyber and data crime has reached epic proportions in nearly all sectors of the economy. Symantec's *2015 Internet Security Threat Report* characterized 2014 as a year with "far-reaching vulnerabilities, faster attacks, files held for ransom and far more malicious code than in previous years." According to the report, more than 317 million new pieces of malware were created in 2014 and breaches were up 23 percent from 2013. While large companies across all sectors are still a prime target, 60 percent of all targeted attacks struck small and medium-sized companies last year.

The U.S. government is also constantly working to identify malicious actions within their networks. Earlier this year the Department of Homeland Security's Office of Cybersecurity and Communication announced that a network monitoring program will fully cover the government by the end of fiscal year 2016 through the Einstein program used to strengthen perimeter defenses and the Continuous Diagnostics and Mitigation program designed to better detect hacker's once systems have already been penetrated.

NAFCU supports comprehensive data and cyber security measures to protect consumers' personal data. Credit unions and other financial institutions already protect data consistent with the provisions of the 1999 *Gramm-Leach-Bliley Act* (GLBA). Unfortunately, there is no comprehensive regulatory structure similar to what was put in place for financial institutions under GLBA for other entities that may handle sensitive personal and financial data.

In today's digital economy, cybersecurity poses a threat to businesses of all sizes, individual consumers, and even national security through our government's critical infrastructure. From the financial services perspective, cyber security and data security are inextricably linked—both require the entire payments ecosystem to take an active role in addressing emerging threats, and both require all players to be proactive in protecting consumers personally identifiable and financial information from the onset.

As will be discussed in my testimony, credit unions have been able to successfully minimize emerging threats and data breaches. Still, consumers unwittingly put themselves at risk every time they swipe their debit or credit card. Given the magnitude of the many recent data breaches and the sheer number of consumers impacted, policy makers have a clear bipartisan opening to ensure all players in the payments system have a meaningful federal data safekeeping standard to help prevent breaches from occurring.

This hearing is an important one as we are at a critical juncture in the cyber and data security discussion on Capitol Hill. On behalf of NAFCU and our member credit unions, I appreciate the opportunity to be here today.

Financial Institutions and the *Gramm-Leach-Bliley Act*

GLBA and its implementing regulations have successfully limited data breaches among financial institutions and this standard has a proven track record of success since its enactment in 1999. This record of success is why we believe any future requirements must recognize this existing national standard for financial institutions such as credit unions.

Consistent with Section 501 of the GLBA, the National Credit Union Administration (NCUA) established administrative, technical and physical safeguards to ensure the (1) security, (2) confidentiality, (3) integrity, (4) and proper disposal of consumer information and other records. Under the rules promulgated by the NCUA, every credit union must develop and maintain an information security program to protect customer data. Additionally, the rules require third party service providers that have access to credit union data take appropriate steps to protect the security and confidentiality of the information.

GLBA and its implementing regulations have successfully limited data breaches among credit unions. The best way to move forward and address data breaches is to create a comprehensive regulatory scheme for those industries that are not already subject to oversight. At the same time, the oversight of credit unions, banks and other financial institutions is best left to the functional financial institution regulators that have experience in this field. It would be redundant at best and possibly counter-productive to authorize any agency—other than the functional financial institution regulators—to promulgate new, and possibly duplicative or contradictory, data security regulations for financial institutions already in compliance with GLBA.

Below, I outline the key elements, requirements and definitions of the GLBA. Specifically, the GLBA:

- Requires financial institutions to establish privacy policies and disclose them annually to their customers, setting forth how the institution shares nonpublic personal financial information with affiliates and third parties.
- Directs regulators to establish regulatory standards that ensure the security and confidentiality of customer information.

- Permits customers to prohibit financial institutions from disclosing personal financial information to non-affiliated third parties.
- Prohibits the transfer of credit card or other account numbers to third-party marketers.
- Prohibits pretext calling, which generally is the use of false pretenses to obtain nonpublic personal information about an institution's customers.
- Protects stronger state privacy laws and those not inconsistent with these federal rules.
- Requires the U.S. Department of Treasury and other federal regulators to study the appropriateness of sharing information with affiliates, including considering both negative and positive aspects of such sharing for consumers.

Sensitive Consumer Information

Sensitive consumer information is defined as a member's name, address, or telephone number in conjunction with the member's social security number, driver's license number, account number, credit or debit card number, or personal identification number or password that would permit access to the member's account. Sensitive consumer information also includes any combination of components of consumer information that would allow someone to log into or access the member's account, such as user name and password or password and account number. Under the guidelines, an institution must protect against unauthorized access to or use of consumer information that could result in substantial harm or inconvenience to any consumer.

Unauthorized Access to Consumer Information

The agencies published guidance to interpret privacy provisions of GLBA and interagency guidelines establishing information security standards. The guidance describes response programs, including member notification procedures, that a financial institution should develop and implement to address unauthorized access to or use of consumer information that could result in substantial harm or inconvenience to a member.

The security guidelines require every financial institution to have an information security program designed to:

- Ensure the security and confidentiality of consumer information;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and,
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to a member.

Risk Assessment and Controls

The security guidelines direct every financial institution to assess the following risks, among others, when developing its information security program:

- Reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of consumer information or consumer information systems;
- The likelihood and potential damage of threats, taking into consideration the sensitivity of consumer information; and,
- The sufficiency of policies, procedures, consumer information systems, and other arrangements to control for the risks to sensitive data.

Following the assessment of these risks, the security guidelines require a financial institution to design a program to address the identified risks. The particular security measures an institution should adopt depend upon the risks presented by the complexity and scope of its business. This is a critical aspect of GLBA that allows flexibility and ensures the regulatory framework is workable for the largest and smallest in the financial service arena. As the committee considers cyber and data security measures, it should be noted that scalability is achievable and that it is a misnomer when other industries claim they cannot have a federal data safekeeping standard that could work across a sector of varying size businesses.

At a minimum, the financial institution is required to consider the specific security measures enumerated in the Security Guidelines, and adopt those that are appropriate for the institution, including:

- Access controls on consumer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing consumer information to unauthorized individuals who may seek to obtain this information through fraudulent means;
- Background checks for employees with responsibilities for access to consumer information;
- Response programs that specify actions to be taken when the financial institution suspects or detects that unauthorized individuals have gained access to consumer information systems, including appropriate reports to regulatory and law enforcement agencies;
- Train staff to implement the credit union's information security program; and,
- Regularly test the key controls, systems and procedures of the information security program. The frequency and nature of such tests should be determined by the credit union's risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs."

Service Providers

The security guidelines direct every financial institution to require its service providers through contract to implement appropriate measures designed to protect against unauthorized access to, or use of, consumer information that could result in substantial harm or inconvenience to any consumer.

Third-party providers are very popular for many reasons, most frequently associated with cost-savings/overhead reduction. However, where costs may be saved for overhead purposes, they may be added for audit purposes. Because audits typically are annual or semi-annual events, cost savings may still be realized but the risk associated with outsourcing must be managed regardless of cost. In order to manage risks, they must first be identified.

An institution that chooses to use a third-party provider for the purposes of information systems-related functions must recognize that it must ensure adequate levels of controls so the institution does not suffer the negative impact of such weaknesses.

Response Program

Every financial institution must develop and implement a risk-based response program to address incidents of unauthorized access to consumer information. A response program should be a key part of an institution's information security program. The program should be appropriate to the size and complexity of the institution and the nature and scope of its activities.

In addition, each institution should be able to address incidents of unauthorized access to consumer information in consumer information systems maintained by its service providers. Where an incident of unauthorized access to consumer information involves consumer information systems maintained by an institution's service providers, it is the responsibility of the financial institution to notify the institution's consumers and regulator. However, an institution may authorize or contract with its service provider to notify the institution's consumers or regulator on its behalf.

Consumer Notice

Timely notification to members after a security incident involving the unauthorized access or use of their information is important to manage an institution's reputation risk. Effective notice may also mitigate an institution's legal risk, assist in maintaining good consumer relations, and enable the institution's members to take steps to protect themselves against the consequences of identity theft.

Content of Consumer Notice

Consumer notice should be given in a clear and conspicuous manner. The notice should describe the incident in general terms and the type of consumer information that was the subject of unauthorize4d access or use. It should also generally describe what the institution has done to protect consumers' information from further unauthorized access. In addition it should include a telephone number that members can call for further information assistance. The notice should also remind members of the need to remain vigilant over the next 12 to 24 months, and to promptly report incidents of suspected fraud or identity theft to the institution.

Delivery of Consumer Notice

Notice should be delivered in any manner designed to ensure that a consumer can reasonably be expected to receive it.

NAFCU's Work in Various Cyber and Data Security Initiatives

NAFCU has been an active participant in various industry and government cyber and data security initiatives, doubling down these efforts as data breaches continue to rise and innovations in payments technology make the entire ecosystem more complex for financial institutions and consumers.

Specific to payments, NAFCU is a member of the *Payments Security Task Force*, a diverse group of participants in the payments industry that is driving a discussion relative to systems security. NAFCU also supports many of the ongoing efforts at 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 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 through the process of reducing cyber risks to critical infrastructure. The recommendations are designed to evolve and will be updated to keep pace with changes in technology and threats.

Earlier this year, I also had the opportunity to attend President Barack Obama's *White House Summit on Cybersecurity and Consumer Protection* at Stanford University which featured leaders from across the country—industry, tech companies, law enforcement, consumer and privacy advocates, law professors who specialize in this field, and students—to collaborate and explore partnerships that will help develop the best ways to bolster cybersecurity. Credit unions continue to pursue greater data security through innovation.

During the Summit, NAFCU-member First Tech Federal Credit Union's recent partnership with MasterCard in the area of card security was announced. First Tech is innovative in this area and will implement a new pilot program later this year that will allow consumers to authenticate and verify their transactions using a combination of unique biometrics such as facial and voice recognition. This type of innovation is not unusual at member-owned and member-driven credit unions as they take data security seriously.

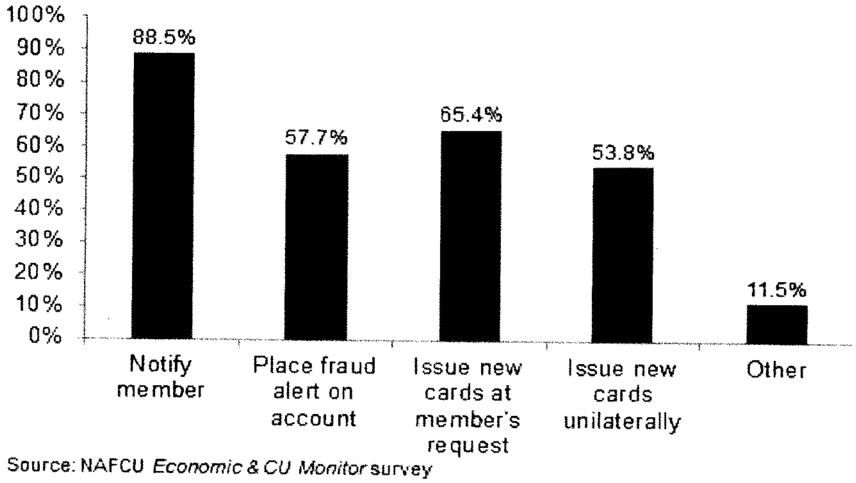
Credit Unions and Consumers Continue to Suffer

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.

Data security breaches are more than just an inconvenience to consumers as they wait for their plastic cards to be reissued. Breaches often result in compromised card information leading to fraud losses, unnecessarily damaged credit ratings, and even identity theft. Symantec's *Internet Security Threat Report* issued earlier this month found that 36% (roughly 74 million consumers) of the 205,446,276 individuals compromised in retail breaches in 2014 had their financial information exposed. That percentage doubled from 18% in 2013. More than 23% of the US population had their financial identities compromised by a retailer data breach in 2014.

While the headline grabbing breaches are certainly noteworthy, the simple fact is that data security breaches at our nation's retailers are happening almost every day. A February of 2015 survey of NAFCU member credit unions, found that respondents were alerted to potential breaches an average of 164 times in 2014. Two-thirds of the respondents said that they saw an increase in these alerts from 2013. When credit unions are alerted to breaches, they take action to respond to protect their members. The chart below outlines the actions that credit unions took in 2014 in response to merchant data breaches.

In response to 2014 merchant data breaches, what actions did you take?



Source: NAFCU *Economic & CU Monitor* survey

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.

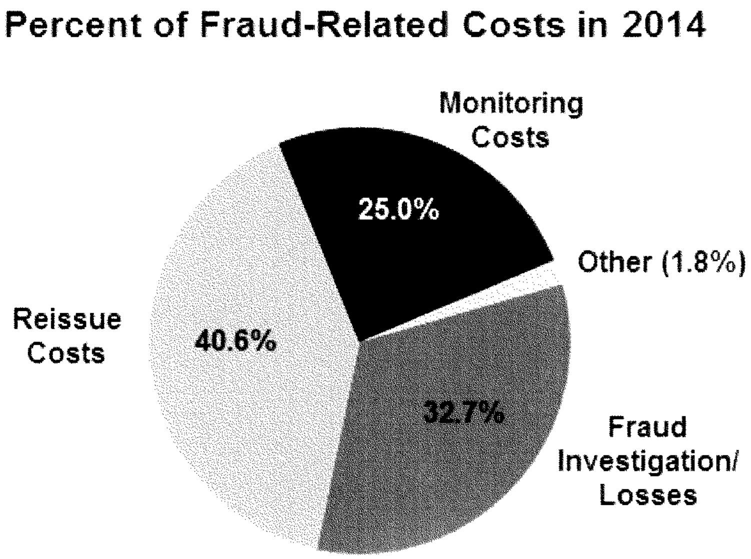
Merchants and credit unions are both targets of cyberattacks. The difference, however, is that credit unions have developed and maintain robust internal protections to combat these attacks and are required by federal law and regulation to protect this information and notify consumers when a breach occurs that will put them at risk. Every credit union must comply with significant data security regulations, and undergo regular examinations to ensure that these rules are followed. A credit union faces potential fines of up to $1 million per day for compliance violations. These extensive requirements and safeguards discussed earlier in my testimony have evolved along with cyber threats and technological advances and have been enhanced through regulation since they were first required in 1999. In contrast, retailers are not covered by ***any*** federal laws or regulations that require them to protect the data and notify consumers when it is breached.

A credit union data security program to protect its own system can have many security components, such as:

1. Firewall
2. Intrusion Prevention
3. Botnet Filtering
4. Anti-Virus protection
5. Malware protection
6. Management and Monitoring Services
7. Anti-Phishing and Phishing site takedown services
8. Third party vulnerability assessments and testing
9. Web Filter
10. Spam Filter
11. Secure Email
12. Encryption
13. End point security

These elements can have a significant cost to the institution. A February, 2015, survey of NAFCU members found that the average respondent credit union spent $136,000 on data security measures in 2014, and that doesn't even factor in the additional costs that the credit union faced due to data breaches at other entities.

The ramifications of recent data breaches for credit unions and their members have been monumental. The aforementioned survey of NAFCU members found that the estimated costs associated with merchant data breaches in 2014 were $226,000 on average per credit union. Almost all respondents noted that merchant data breaches lead to increased member-service costs and needs that are not reflected in these direct costs. The three main elements of these costs were card reissuing costs, fraud investigations/losses and account monitoring. The chart on the next page outlines how these various costs from merchant data breaches are broken down.



Percent of Fraud-Related Costs in 2014

Charlotte Metro Federal Credit Union is a prime example. Their estimated cost for reissuing, additional staffing, member notification, account monitoring, increase in call volume and branch visits among other things is over $200,000. However, a cost cannot be placed on the vulnerability their cardholders are left with as well as the lack of trust and confidence that is created. They have indicated that the impact from the losses and increased expenses affect the fees and rates they are able to offer their members.

Additionally, one of the residual effects that goes largely unnoticed is the impact that the reissuance of a card has on the neural network of a credit union. This is a credit union's own fraud detection system. Some of the components of the system are payment patterns and history of card usage, as is the case with most neural networks. Every time a credit union has to reissue a card, the pattern and history for that member is erased and it starts over. This increases the chance that the member will make a purchase that is perfectly acceptable, but get denied because the network doesn't recognize that what they are doing is perfectly normal. This is especially true for credit union members who travel.

Smaller credit unions such as Diebold Federal Credit Union, a small credit union with only 3,300 members and $17 million in assets in North Carolina, Ohio, are especially feeling the impact. Since the beginning of 2014, Diebold has had over $32,000 in losses from data breaches at retailers. While that may not seem like much, it is nearly $10 in loss for every one of their members and a real burden on the institution. They are not alone. Over that same time period, Chicago Patrolmen's Federal Credit Union has had over $143,000 in losses, which is over a $5 loss for each of their 28,000 members.

Unfortunately, credit unions often never see any reimbursement for their costs associated with the majority of data breaches. Even when there are recoupment opportunities, such as the recent Target settlement with MasterCard, it is usually only pennies on the dollar in terms of the real costs and losses incurred. Meanwhile, big box retailers that were negligent in recent data security breaches are posting record profits. A 2015 Columbia University review of financial statements of merchants such as Target and Home Depot reveals that retailers barely notice a financial hit from massive data breaches, and breach costs were less than one-tenth of one percent of these giant retailers 2014 annual sales.

Payment networks are critical partners to credit unions in ensuring credit union members have the credit and debit card programs they need and demand. Collectively, the networks have worked together to standardize the Payment Card Industry (PCI) Data Security Standard designed to provide merchants and retailers with a framework of specifications, tools, measurements and support resources to ensure the safe handling of cardholder information. While NAFCU appreciates the positive progress in this regard, credit unions and other issuers are still seeing steep losses in the wake of retailer and merchant data breaches and would like to see the networks do everything they can to make reimbursement in the wake of fraud stemming from a data breach more equitable. As discussed, NAFCU believes the negligible entity should be wholly responsible for such damages.

NAFCU's Key Data Security Principles

NAFCU has long been active on the data security front, and was the first financial services trade association to call for Congressional action in the wake of the 2013 data breach at Target. Recognizing that a legislative solution is a complex issue, NAFCU's Board of Directors has also established a set of guiding principles to help define key issues credit unions would like to see addressed in any comprehensive cyber and data security effort that may advance. These principles include:

- **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 the GLBA, credit union and other financial institutions are required to meet certain criteria for safekeeping consumers' personal information. Unfortunately, there is no comprehensive regulatory structure akin to the GLBA 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 *GLBA*.

- **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.

Preventing Future Breaches

NAFCU has long argued that protecting consumers and financial institutions by preventing future data breaches hinges on establishment of strong federal data safekeeping standards for retailers and merchant akin to what credit unions already comply with under the GLBA.

The time has come for Congress to enact a national standard on data protection for consumers' personal financial information. Such a standard must recognize the existing protection standards that financial institutions have under the GLBA and ensure the costs associated with a data breach are borne by those who incur the breach.

While some have said that voluntary industry standards should be the solution, the recently released *Verizon 2015 Payment Card Industry Compliance Report* found that 4 out of every 5 global companies fail to meet the widely accepted Payment Card Industry (PCI) data security standards for their payment card processing systems. In fact, Verizon found that out of every data breach they studied over the past 10 years, not one single company was in compliance with the PCI standards at the time of the breach. This should cause serious pause among lawmakers as failing to meet these standards, exacerbated by the lack of a strong federal data safekeeping standard, leaves merchants, and therefore consumers, more vulnerable to breaches.

In addition, the report finds that the use of EMV cards ("chip cards") in other countries has not been a silver bullet solution to preventing fraudulent activity, but merely displaces it. The report shows that once EMV use increases, criminals shift their focus to card not present transactions, such as online shopping. While some have argued for a "chip card" solution, the reality is that it is not a panacea and does not replace a sound data security standard.

One basic but important concept to point out with regard to almost all cyber and data threats is that a breach may never come to fruition if an entity handling sensitive information limits the amount of data collected on the front end and is diligent in not storing sensitive personal and financial data in their systems. Enforcement of prohibition on data retention cannot be over emphasized and it is a cost effective and commonsense way to cut down on emerging threats. If there is no financial data to steal, it is not worth the effort of cyber criminals.

Legislative Solutions

NAFCU believes that the best legislative solution on the issue of data security that has been introduced in this Congress is bipartisan legislation in the Senate by Senators Roy Blunt and Tom Carper. Their bill, S. 961, the *Data Security Act of 2015*, sets a national data security standard that recognizes those who already have one under the GLBA. We support this legislation and would urge introduction of a House companion measure.

As the committee is aware, the cyber and data security discussions cross the jurisdiction of several Congressional committees. Given the daunting task of making meaningful reform in these areas, early this Congress NAFCU called on Congressional leadership to create a bipartisan and bicameral working group to find a legislative path forward to help better protect consumers from ongoing data breaches.

Conclusion

Cyber and data security, ensuring member safety, and how to incentivize and emphasize data safekeeping in every link of the payments chain is a top challenge facing the credit union industry today. Given the breadth and scope of many recent retailer data breaches, we have reached a tipping point in the public dialogue about how to tackle these issues. NAFCU member credit unions and the 100 million credit union members across the country are looking to Congress to continue work on cyber and data security issues and move forward with legislation that will make a meaningful difference to consumers. It is time to level the playing field and require equal data security treatment to all those who collect and store personally identifiable and financial data.

Consumers will only be protected when every sector of industry is subject to robust federal data safekeeping standards that are enforced by corresponding regulatory agencies. It is with this in mind that NAFCU urges Congress to modernize data security laws to reflect the complexity of the current environment and insist that retailers and merchants adhere to a strong federal standard in this regard.

Thank you for the opportunity to appear before you today on behalf of NAFCU. I welcome any questions you may have.

Statement for the Record

Dr. Jane LeClair, Chief Operating Officer

National Cybersecurity Institute of Excelsior College

Before the

United States House of Representatives

Committee on Small Business

Small Business, Big Threat:

Protecting Small Businesses from Cyber Attacks

April 22, 2015

Mr. Chairman and members of the Committee, on behalf of the National Cybersecurity Institute at Excelsior College. I appreciate the opportunity to address you and provide a statement for today's hearing. The National Cybersecurity Institute is dedicated to increasing knowledge in the cybersecurity discipline and assists small businesses (SMB's) to better understand and meet the challenges in today's digital world. My name is Dr. Jane LeClair, and I am the Chief Operating Officer of the National Cybersecurity Institute located in Washington, D.C.

SMB's are challenged both by the ability and the desire to secure themselves against cyber threats which makes them uniquely vulnerable to cyber attacks. Fifty percent of SMB's have been the victims of cyber attack and over 60 percent of those attacked go out of business. Often SMB's do not even know they have been attacked until it is too late.

SMB's are under attack from many avenues including social engineering, the internet of things, insider threat, weak passwords and cyber theft through weak payment systems. Mobile devices and the lack of formal cyber plans and policies spell trouble. Infections brought in through browsers pose a threat, and finally, outdated technology and poor maintenance top the list of problems. SMB's are characterized by central management focused around the owner, with lack of a specialized IT or cyber staff, inadequate control systems, and day-to-day rather long term planning for asset protection. Almost 70% of SMB's manage their own websites, use the Internet for sales, social media, marketing, and a host of other needs. SMB's have resource contraints and often ignore cyber-security in favor of day-to-day operations or other financial needs. Yet SMB's remain a gateway to gain access to clients, business partners, donors, and contractors working with the SMB ... a backdoor into many large organizations. These organizations frequently lack the knowledge needed to develop and implement a cyber policy or the expertise to develop a response strategy. Surprisingly, 96% of the attacks on SMB's were fundamentally basic attacks. SMB's need employees trained in networking, operating systems and multiple layers of security.

Otherwise, who's watching for signs of an attack and making sure the operating systems are properly patched? Who's responsible for regular backups and reviewing system logs?

There are several ways that the National Cybersecurity Institute is offering assistance to SMB's. An affordable package that provides a targeted cybersecurity plan, basic training for owners, IT staff and employees, and ensures that the basics of antivirus software and firewall protection are in place, is under development. Our media campaign raises awareness through quarterly webinars and weekly blogs. The National Cybersecurity Institute is publishing two short books on Cyber for Small Business and Cyber Insurance, and is partnering to offer a SMB workshop in medium-sized cities around the country that is affordable and aimed at SMB owners and their IT staff. Cybersecurity is without a doubt one of the prime concerns of the SMB community in America today. The efforts of this Committee in seeking ways to help alleviate those concerns cannot be understated. Mr. Chairman and members of this Committee, thank you for your interest in this important area, and I thank you for the opportunity to address you today.