PROTECTING SMALL BUSINESSES FROM CYBER ATTACKS: THE CYBERSECURITY INSURANCE OPTION

HEARING

BEFORE THE

COMMITTEE ON SMALL BUSINESS
UNITED STATES
HOUSE OF REPRESENTATIVES

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

HEARING HELD
JULY 26, 2017

Small Business Committee Document Number 115–032
Available via the GPO Website: www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
26–297 WASHINGTON : 2018

HOUSE COMMITTEE ON SMALL BUSINESS

STEVE CHABOT, Ohio, *Chairman*
STEVE KING, Iowa
BLAINE LUETKEMEYER, Missouri
DAVE BRAT, Virginia
AUMUA AMATA COLEMAN RADEWAGEN, American Samoa
STEVE KNIGHT, California
TRENT KELLY, Mississippi
ROD BLUM, Iowa
JAMES COMER, Kentucky
JENNIFFER GONZÁLEZ-COLÓN, Puerto Rico
DON BACON, Nebraska
BRIAN FITZPATRICK, Pennsylvania
ROGER MARSHALL, Kansas
RALPH NORMAN, South Carolina
NYDIA VELÁZQUEZ, New York, *Ranking Member*
DWIGHT EVANS, Pennsylvania
STEPHANIE MURPHY, Florida
AL LAWSON, JR., Florida
YVETTE CLARK, New York
JUDY CHU, California
ALMA ADAMS, North Carolina
ADRIANO ESPAILLAT, New York
BRAD SCHNEIDER, Illinois
VACANT

KEVIN FITZPATRICK, *Majority Staff Director*
JAN OLIVER, *Majority Deputy Staff Director and Chief Counsel*
ADAM MINEHARDT, *Staff Director*

CONTENTS

OPENING STATEMENTS

WITNESSES

APPENDIX

PROTECTING SMALL BUSINESSES FROM CYBER ATTACKS: THE CYBERSECURITY INSURANCE OPTION

WEDNESDAY, JULY 26, 2017

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, Luetkemeyer, Brat, Radewagen, Kelly, Blum, Bacon, Fitzpatrick, Marshall, Norman, Velázquez, Evans, Murphy, Lawson, Clarke, Chu, Espaillat, and Schneider.

Chairman CHABOT. The Committee will come to order.

Good morning. We appreciate everybody being here.

Cybersecurity has been one of this Committee's top priorities. We have held numerous hearings and worked on meaningful legislation to ensure small businesses have every possible resource to protect themselves against a cyber attack. Weeks ago, I, along with my friend from across the aisle, Representative Dwight Evans of Pennsylvania, introduced legislation to ensure that America's Small Business Development Centers have the best possible cybersecurity training so that they can better assist small businesses with their cyber strategies.

Unfortunately, we have also heard too many firsthand accounts from small business owners who have been victims of cyber attacks. One case in particular that stands out is the story of a small business owner who testified before this Committee last year. He owned an indoor go-karting facility in Maine, and had a number of employees and families that depended on him. He told the Committee that he was struck by a phishing scam. He logged onto his bank account and to his utter disbelief his balance was zero. And that happened on a payday no less, so all his employees were at risk of not being paid that day, so he was really panic stricken. Fortunately, he caught it just in the nick of time and was able to stop the funds from being transferred, but that is usually, unfortunately, not the case.

Cybersecurity experts have told this Committee about the growing number of cyber threats facing America's 28 million small businesses. In 2016 alone, the Justice Department recorded nearly 300,000 cybersecurity complaints. This number increases every year. Sixty percent of small businesses that fall victim to a cyber

attack close up shop within 6 months, and the estimated average cost of a cyber attack on a small business is over $30,000. And that may not be a huge amount to a large corporate entity in the United States, but to a mom-and-pop small business person, $30,000, that can mean why 60 percent of small businesses go out of business within 6 months of being hit by a cyber attack.

In our Committee's efforts to spotlight these serious and growing threats, it has become clear that we need to think outside the box as we work to thwart cyber attacks. Small businesses must also be diligent as they manage their IT systems and educate their staffs about the importance of cybersecurity. They should also be creative as they consider different ways to spread risk and manage their cyber strategies.

One increasingly feasible solution is cybersecurity insurance. Many larger corporations are already exploring this approach to dealing with cyber attacks. It is likely that small businesses will follow.

Of course, the widespread adoption of cybersecurity insurance policies is not without its challenges, both for small businesses and for the insurance providers. Small businesses must determine what policies and coverage options make sense for them and also implement basic cybersecurity best practices. Furthermore, the cybersecurity insurance marketplace is remarkably new and many of the providers still lack the historical data to offer appropriate plans to consumers which drives up the cost to policyholders. Yet, as they look to improve their models and cyber risk scenarios, cybersecurity insurance will become more viable and more accessible.

Today, we will hear from a panel of witnesses that all have some level of experience with cybersecurity insurance and can offer an in-depth perspective on both the benefits of cybersecurity insurance and the challenges that still lie ahead. I look forward to hearing our witnesses' views on how small businesses can more effectively manage their cyber risk and possibly with the help of cybersecurity insurance.

And I would now like to yield to the Ranking Member, Ms. Velázquez, for her opening statement.

Ms. VELAZQUEZ. Thank you, Mr. Chairman.

The internet has undoubtedly transformed the way small business operates. E-commerce empowers America's 28 million small businesses, giving them a unique opportunity to sell their products not only across the country, but around the world. Unfortunately, for small business owners, when it comes to the health of their businesses, cyber hygiene often falls to the back burner. The lack of preventive measures can result in hacks and other cyber incidents that have major and costly implications for small business and their ability to operate.

The topic of this hearing is particularly timely. If Russia was able to use cyber attacks to penetrate our democratic institutions, by comparison a small business seems an easy target. The fact of the matter is there will continue to be cyber threats from those who seek to damage our national security, our economic security, and our political system. And there will continue to be criminals who seek to profit by stealing sensitive data held by the govern-

ment or the private sector. Cyber criminals have realized small entities are more exposed than larger businesses that have dedicated, in-house IT personnel overseeing their systems and networks.

In 2016 alone, more than 1.1 billion identities were stolen. This is worrisome, perhaps lethal, for companies that have a reputation of safeguarding their customers' information and need to maintain their credibility. Small businesses that lose customer information when their security is breached suffer significant costs financially and in the loss of customer trust. And once businesses get compromised, fully recovering from a cyber attack is extremely difficult.

On average, small businesses that get hacked make the discovery more than 200 days after the attack has occurred. For the federal government, cybersecurity should be a priority, but the private sector must also stand up to the challenge and complement existing federal resources.

Given the financial consequences that a cyber attack may have on small businesses, there is a new industry of insurance providers focused on providing policies to protect them; yet, there are a number of factors making this an expensive undertaking. A lack of adequate data underscores the complex nature of creating cyber liability policies for small firms. Also, the type of business that risk management procedures and the continually evolving threats make it difficult for the insurers and the small businesses.

Today's hearing will help us look at this noble idea and learn what role Congress plays in streamlining such an important insurance product. I look forward to hearing the challenges small businesses face in selecting a cybersecurity insurance policy and the hurdles insurers must overcome to offer valuable and comprehensive cybersecurity insurance solutions. It is clear from recent events that these issues are not diminishing. If anything, they are growing more important. Cybersecurity concerns from Russia's attack on our political intuitions to criminal enterprises preying on small businesses merit our attention more than ever before.

I would like to thank you all for being here this morning and I yield back, Mr. Chairman.

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

And if Committee members have opening statements, I would ask that they be submitted for the record.

And I would now like to explain our timing rules and lights here. It is pretty simple. We operate under the 5 minute rule. There is a lighting system to assist you there. The green light will be on for 4 minutes. The yellow light will come on and let you know you have got a minute to wrap up, and then the red light will come on and you are supposed to stop. Most people do. But we will give you a little leeway. But if you could stay within those parameters, we would appreciate it very much.

And I would now like to introduce our distinguished panel. Our first witness is Robert Luft, the Owner and President of SureFire Innovations, a service-disabled, veteran-owned small business and minority business enterprise located in my home district of Cincinnati, Ohio. And Mr. Luft and I actually talked about this a long time ago and he brought this to my attention. And I think that ac-

tually was how this hearing came into being here, so do not screw it up because you are the one who did it.

SureFire Innovations specializes in providing network infrastructure services to companies all across the country. Prior to starting his company, Mr. Luft served our country for 16 years in the Army as a combat engineer. He is testifying on behalf of the National Small Business Association. We thank him for his service to our country and we also welcome him here today.

I would now like to yield to the Ranking Member to introduce our next witness, who I believe is a constituent and whose first name is Erica, which happens to be our daughter's name. You even spell it the same way. So, and I yield.

Ms. VELÁZQUEZ. Thank you, Mr. Chairman.

It is my pleasure to introduce Ms. Erica Davis, senior vice president and head of Specialty Products Errors and Omissions at Zurich. She is also a constituent from my district in Brooklyn, so I am very proud.

Prior to joining Zurich in 2009, she was a senior underwriting officer for technology insurance specialty at the Chubb Group of Insurance Companies. Ms. Davis holds a bachelor of arts degree from the University of Arizona. Welcome.

Chairman CHABOT. Thank you. And our third witness will be Mr. Eric Cernak, Vice President and Cyber Risk Practice Leader at Munich Re in Hartford, Connecticut. In his role, Mr. Cernak provides leadership in all cyber efforts overseas, Munich Re's property and casualty operations, and develops strategies to help the company compete in the cyber marketplace. He is testifying today on behalf of the Reinsurance Association of America, RAA, and the Property Casualty Insurers Association of America, PCI. We thank you for testifying here this morning.

I would now like to once again yield to the Ranking Member for introduction of our fourth witness.

Ms. VELÁZQUEZ. Thank you, Mr. Chairman.

It is my pleasure to introduce Mr. Daimon Geopfert, national leader and principal of security and privacy consulting at Risk Advisory Services. He has over 20 years of experience in a wide array of positions, including time in the U.S. Air Force. Mr. Geopfert has served as the manager and lead technician for security assessments performed on some of the largest corporations and government entities in the world. He holds a bachelor's degree from the United States Air Force Academy and a master's degree in computer science from the University of Michigan. Welcome. Thank you for being here.

Chairman CHABOT. Thank you. And we also thank you for your service, Mr. Geopfert.

And Mr. Luft, you are welcome here and recognized for 5 minutes.

STATEMENTS OF ROBERT LUFT, PRESIDENT, SUREFIRE INNOVATIONS; ERICA DAVIS, SENIOR VICE PRESIDENT, HEAD OF SPECIALTY PRODUCTS ERRORS & OMISSIONS, ZURICH INSURANCE, NORTH AMERICA; ERIC CERNAK, VICE PRESIDENT, CYBER RISK PRACTICE LEADER, MUNICH RE U.S.; DAIMON GEOPFERT, NATIONAL LEADER AND PRINCIPAL, SECURITY AND PRIVACY CONSULTING, RISK ADVISORY SERVICES

STATEMENT OF ROBERT LUFT

Mr. LUFT. Good morning. Thank you, Chairman Chabot, Ranking Member Velázquez.

Chairman CHABOT. You need to turn the mic on there.

Mr. LUFT. I apologize.

Chairman CHABOT. Yeah. You have got to turn it on.

Mr. LUFT. Good morning. Thank you, Chairman Chabot, Ranking Member Velázquez, and members of the House Small Business Committee, for inviting me to testify today on the current state of cybersecurity for small companies and how cyber insurance can help small businesses transfer risk.

My name is Robert Luft, and I am the owner of SureFire Innovations located in Cincinnati, Ohio. I am pleased to be here representing the National Small Business Association where I currently serve on the Leadership Council and the Technology Council.

SureFire Innovations is a certified service-disabled, veteran-owned small business and minority business enterprise, specializing in network infrastructure, design installation of hardwire, wireless, security and smart city networks.

After my military service in the Army, where I had the honor to serve on multiple combat deployments to Iraq during my 16-year career, I decided that entrepreneurship was my path, and hence, the founding of SureFire Innovations.

Cybercrime is growing rapidly with annual cost to the global economy estimated to reach over $2 trillion by 2019. Organizations of all sizes are at risk for cyber attacks.

Small business represents more than 97 percent of business in the U.S. Alarmingly, in 2015, 43 percent of all attacks were directed at small business. Despite the growing awareness of cyber-related crimes, 77 percent of small business owners believe their company is not at risk for cyber attacks.

The risk of being a target for cybercrime is high. Forty-two percent of small businesses surveyed by the National Small Business Association reported being a victim of a cyber attack, with the average cost being $32,000 when business banking accounts were hacked, and $7,000 on average for small business overall.

So what can we do as small businesses to address this issue? We can start with what I learned in the Army. Keep it simple. By utilizing the SBA's top 10 cybersecurity tips, this would provide a framework for all small businesses, even those who are not technologically savvy and currently have zero protections in place; simple measures, like installing antivirus software, the use of complex passwords, and backing up information.

Since total elimination of threats is impossible, protecting against them should be a top management priority. Unfortunately,

many small businesses do not place cyber threat as a top priority. This is evident by the fact that 60 percent of small companies go out of business within 6 months after a cyber attack. Small business need not only think of ways to mitigate cyber attacks, but also how to transfer that risk away from their company.

This can be accomplished with the cyber liability insurance policy, which provides coverage in the event of a cyber attack. A typical cyber liability policy will include the following coverages: theft and fraud, forensic investigation, network business interruption, extortion, and data loss.

What led to my purchase of a cyber liability policy is a subcontractor was performing services on one of my projects, suffered a bank account breach that resulted in the loss of $15,000. This was a catastrophic event. Those funds were required for payroll and put enormous strain on its employees. This event made me realize that our company was just as vulnerable, and despite having a cybersecurity plan, we did not have a cyber liability insurance policy. So in the event we were breached, we would not have any financial protections available.

Unfortunately, we were not the exception, as 75 percent of small businesses do not have cyber liability coverage in place. Most small businesses do not have the appetite to purchase another insurance policy. My annual premium is $3,200. The level of security this provides my company does not completely remove all of my concerns, but it affords me the knowledge that if we were hacked, protective steps had been taken to address any potential damages to the company and my employees.

There are enormous amounts of resources available to help educate small businesses on cybersecurity and the potential ramifications of not having the appropriate plan and policies in place. The issue is awareness. The more we can help inform small businesses on how to mitigate and transfer these risks, the greater the positive impact small business will have on our economy.

Thank you for the opportunity to address this very pressing issue.

Chairman CHABOT. Thank you very much.

Ms. Davis, you are recognized for 5 minutes.

STATEMENT OF ERICA DAVIS

Ms. DAVIS. Mr. Chairman, Ranking Member Velázquez, and members of the Committee, thank you for the opportunity to speak with you today about the private sector's role in providing risk management solutions to protect businesses from cyber risk.

My name is Erica Davis and I lead a team of market-facing underwriters at Zurich North America, one of the five providers currently leading the North American cybersecurity insurance marketplace.

Zurich has invested in identifying risks and delivering solutions for our customers. Zurich is a member of the American Insurance Association, the leading property-casualty insurance trade organization representing approximately 325 major insurers. I appreciate AIA's focus on cybersecurity.

The cyber landscape continues to evolve, making companies increasingly vulnerable to the potential harm of a security or privacy event.

While awareness of the threats is growing across all sizes of organizations, businesses are still struggling how to understand cyber risk. That is, the full scope of their exposures and how best to protect themselves. They must determine whether they should retain the residual risk or transfer it through the purchase of a cyber insurance product.

Our approach to cybersecurity includes understanding attitudes to cyber risk, providing tailored coverage to meet our customers' needs, and working with businesses to adopt a mindset of resilience rather than just protection.

Last fall, Zurich and Advisen released a survey of risk managers and other risk professionals. It found that 87 percent of respondents believe a technology interruption would have a moderate to significant impact on their organization. As with any line of insurance, risk culture is critical to underwriting cyber insurance. Businesses must build a culture of resilience and operational awareness at all levels, rather than simply viewing cyber risk as a technology issue.

Insurance is just one piece of the cyber risk management puzzle, but the role of insurance is increasing as customers seek risk insights and feedback from their insurance advisors. It has really become more of a partnership with businesses now focusing on not just what happens post-event and a loss being paid. They value having qualified, vetted resources available to them, especially in their moment of crisis. And they are focusing more on risk-mitigation tools their insurance providers can provide to them.

The business community's interconnectivity and reliance on technology has increased and that creates additional points of entry and new threat vectors. The cyber insurance and exposure has broadened to include potential property damage for something like critical infrastructure, supply chain ripple effects, bodily injury from autonomous vehicles, or cyberespionage. And the issue is only becoming more complicated.

In an effort to continuously help customers and protect themselves from risk, Zurich began participating as a key industry consult in a public-private partnership by the University of Maryland and the National Institute of Standards and Technology. We are proud to be part of this initiative.

Zurich is also collaborating with Deloitte to help improve a business' cyber resilience. Policyholders can complement Zurich's cyber insurance solution with risk management services through Deloitte to understand their level of cyber exposure and resilience.

Underwriting of the cyber product is evolving, as are the risks. The insurance community is continuously working to understand the full scope of the exposures and what the controls may need to be. Each business needs to be underwritten differently, and as insurers, we must continue to refine our own understanding of those exposures. Finding solutions to the most complicated of cyber risks will require collaboration between the insurance industry, governments, academia, and other think tanks to establish standards, en-

courage information-sharing, build resilience, and create adequate global governance.

As the market evolves, Zurich is committed to staying at the forefront of the cybersecurity issue, and we will continue to develop additional insurance solutions going forward.

Thank you for the opportunity to testify today, and I look forward to answering your questions.

Chairman CHABOT. Thank you very much.

Mr. Cernak, you are recognized for 5 minutes.

STATEMENT OF ERIC CERNAK

Mr. CERNAK. Good morning. I am Eric Cernak, vice president, U.S. cyber and privacy risk practice leader at Munich Re U.S., testifying on behalf of the Reinsurance Association of America and the Property Casualty Insurers Association of America.

Munich Re and HSB provide cyber and privacy-related insurance and reinsurance protection for small and large businesses in the United States and throughout the world. HSB Group has an A++ and Best Financial Strength rating. We were one of the first companies to provide reinsurance for cyber risk to small businesses. In addition to reinsurance, we underwrite cyber risk, develop products, and work with small businesses to help mitigate cyber-related exposures.

Today's hearing is an important discussion to highlight the success of the private sector in developing cyber insurance. It will help raise awareness among the small business community about the importance of purchasing cyber insurance as a preventative risk management tool and critical safety net should a cyber event occur.

A 2017 Risk Management Solutions report concluded that the number of large magnitude data exfiltration events has grown substantially, and companies are increasingly investing in their own cybersecurity systems. However, a June report by broker Aon estimated that only 19 percent of small businesses in the United States had purchased cyber insurance compared to around 75 percent of certain large companies globally. More insurers have offered cyber insurance over time, from less than a dozen in the early 2000s to more than 70 in 2016. As we see more high-profile cyber events, small businesses are increasingly aware of their exposure. This has prompted the insurance industry to add cyber endorsements to existing small business insurance policies.

A significant part of the value proposition of these cyber insurance policies is loss prevention services. Participants in a 2016 Hartford Steam Boiler survey listed vulnerability assessments, next-generation firewalls, IT security audits, and intrusion detection as the most helpful loss prevention services. Participants also listed reasons that they did not purchase cyber insurance: they did not need it, cost of coverage, and an application process that is too complicated and confusing. These results suggest that education is key to increasing the take-up rate of cyber insurance by small companies.

The public and private sectors have a role to play in increasing the cyber insurance take-up rate, helping businesses overcome the "it will not happen to me" mentality, constructively addressing cyber vulnerabilities, and preparing for the aftermath of a cyber

event. Cyberattacks may not be a matter of if, but when. It is essential for businesses, which are increasingly interconnected, to be prepared, protected, and resilient. Insurance can help with all three.

The insurance marketplace needs to continue to refine the process in coverage to reduce complexity associated with the purchasing of cyber insurance. For example, common coverage form terminology could help applicants better understand what different policies cover.

Insurers are also grappling with four factors in offering cyber insurance. As both the chairman and ranking member have stated, there is no significant historical loss data. Second, the cause of loss is generated by an active adversary that changes with new technology. Third, insurers are grappling with the evolving patchwork of State, Federal, international cyber-related requirements. And fourth, cyber is not bound by geography and poses potential aggregation risk for insurers.

As these factors evolve, Munich Re and HSB are continuously talking to our small business customers to better understand their needs. We are also monitoring the technological, regulatory, and society trends that could pose cyber risks.

So what can Congress do to improve cyber protections for small businesses? We specifically encourage Congress and the administration to coordinate cybersecurity policy among Federal agencies and designate lead agencies to coordinate discussions where appropriate. It is critical that this coordination include State insurance regulators and that we all work together to avoid a conflicting patchwork of State, Federal, and international standards. Munich Re and HSB Group stand ready to work with you to protect small businesses from cybersecurity threats. Thank you.

Chairman CHABOT. Thank you very much.

Mr. Geopfert, you are recognized for 5 minutes.

STATEMENT OF DAIMON GEOPFERT

Mr. GEOPFERT. Thank you, Chairman Chabot, Ranking Member Velázquez, and members of the Committee. Thank you for the opportunity to discuss the cybersecurity challenges that have become a constant material threat within the small business community.

My name is Daimon Geopfert, and during my career I have performed hundreds of security assessments and cyber breach intrusion investigations within small businesses. I was asked to speak today regarding how legislation, such as H.R. 3170, and private sector solutions, such as cyber insurance products, can help organizations manage their cyber risk.

In a study performed last year, RSM performed extensive data mining within a set of cyber insurance claims and found that 50 percent of the reported attacks were against organizations with $50 million in revenue or less. Attacks against small businesses are not an anomaly; they are the norm. This is the key demographic that is being targeted by hackers.

What is needed is a venue through which small businesses can find simple, direct guidance on how to protect their environments and mitigate risk, and that also provides access to resources with

the necessary expertise to chaperone them through the implementation of that guidance.

The current legislation addresses part of this requirement by essentially creating cyber mentors within the Small Business Development Centers. These personnel could quickly become the frontline advisors that are so desperately needed to guide small businesses through the deployment of technical security solutions and administrative risk management techniques, such as acquiring cyber insurance.

While this is a critical first step, the SBDCs hold the promise of a myriad of benefits that could be made available in the future. Again, to make material progress on this issue, we need to move to clear, concise, pragmatic solutions. While it might seem like an abnormal suggestion, what is needed is to emulate our peers within the hacking community. The underground markets excel and become exceedingly efficient at turning large masses of unskilled, technically challenged individuals into groups of, while not elite, at least effective cyber attackers. We lack that equivalent process on the defensive side in which we can rapidly take a large number of small businesses and have them become at least efficient and effective at basic cybersecurity.

While it sounds relatively simple, reference environments, as they are known, are not common in the small business community, which often leads to organizations cobbling together their security architecture and governance based on their individual interpretations of best practice.

Similar to the methods of our adversaries, small and middle markets need a dedicated hub where they can find simple, realistic guidance on how to deploy security solutions that are complete and effective at a basic level. This would then need to be paired with programs dedicated to delivering to security training directly to the IT and management members of those small businesses as most of these organizations simply cannot acquire the necessary security talent on the open market.

The SBDCs could play a critical role in the process of working with government entities, private sector consultants, and vendors to create standardized models and security training. It should be mentioned that an additional benefit of deploying such common models is that it would then allow the SBDCs to address the need for actionable cyber threat intelligence that could be easily consumed and put to use by small businesses. If common reference environments are made available to small businesses, many of these entities would be highly interested in deploying these frameworks if they knew they can consume and utilize threat intelligence in a plug-and-play manner. It should be noted that this support was included in the prior H.R. 5064 legislation that passed this Committee last year, but then later expired in the Senate.

At this point, the foundations would be laid for a base-level accreditation program for small businesses in which they can demonstrate that they have achieved basic cyber controls and processes. The SBDCs would be a natural fit to oversee this program and could then coordinate between newly accredited small businesses and insurance carriers to facilitate the acquisition of cyber insurance. These suggestions create a process that naturally flow

from a set of standardized security templates, through the training and the deployment of those templates, through the accreditation that the controls were deployed properly, through the coordination with the cyber insurance market to offset the residual risk. This process in its entirety represents the most requested types of support by small business executives encapsulated in a clear, concise, and pragmatic approach. It would materially improve the current security status of approximately 50 percent of the U.S. economy.

The final point I would suggest would be to use the SBDCs as a coordination point between small businesses and a designated, responsive law enforcement entity. Currently, when a small business is compromised, they can contact their local police departments, which are often willing to help, but technically unable to do so, or they can contact the FBI or Secret Service that are technically able to help, but typically do not have the bandwidth to do so.

This situation has created a mindset within the small business community that when it comes to cyber matters, they have essentially been abandoned to the Wild West where the rule of law does not apply. Legislation that addresses the points I have described above would greatly improve the security and longevity of the U.S. small and middle market businesses.

Mr. Chairman, this concludes my statement, and I look forward to further questions.

Chairman CHABOT. Thank you very much. And I will yield myself 5 minutes.

Mr. Luft, I will go to you first. Could you tell us what process you went through in determining what cyber insurance coverage you ultimately ended up with? And are there any recommendations that you would make to other small businesses who might be considering, first of all, whether or not they should get insurance coverage? And then secondly, you know, who they should get it from? I am not saying what company, but just kind of the process.

Mr. LUFT. Well, it was my first assumption that cyber insurance should just be as simple as any type of insurance, so I reached out to my existing insurance provider. What I quickly found out is that is not the case. He was not familiar with a lot of policies. So once I saw some hesitancy on his end, I sought some additional resources and found an agent that was exclusive to cyber insurance. That would be my first suggestion to any small business.

And one of the first things that a company needs to look for when they are looking at that, there are some standard coverages in there: the extortion coverage, data loss. So the company could assume that those things are going to be included in a policy.

But one thing that they need to ask for is retroactivity. When you first initially buy that policy, it is going to become effective that inception date, but anything that may have happened previously, it would behoove that small business to ask for maybe a year of retroactivity, just in case there is something lurking there in their network, to ensure that they are safe.

Chairman CHABOT. Thank you very much.

Ms. Davis, let me go to you next. You mentioned in your testimony that not all causes of loss are covered by a particular insurance policy. Could you provide the Committee with an example of

what would be an uninsured loss and how small businesses can protect themselves from that type of liability?

Ms. DAVIS. Sure. So the exposures that arise from cyber threat continues to evolve and there are certain elements of loss that at this point are not transferable to an insurance policy. There is work being done by the insurance community to try and develop insurance solutions for some of those losses, but my advice to small businesses really echoes some of the comments that we have heard already, and that is just providing additional education to those businesses, so things like this hearing today really bring awareness to the topic. But where assistance is needed is helping them connect the dots.

I think small businesses today have an understanding of what the exposures are and what risks they may bring to the business, but they are struggling with the "how." What sort of action items they can implement to make their operation more resilient and secure. So it really does come down to businesses understanding the risk and protecting themselves from it, which is really done through risk mapping. Smaller businesses need to understand what downtime could mean to their organization.

Also, the sensitive data that they are holding, what sort of costs they may incur if that data is compromised, and I think that qualitative aspect is an area and it is an opportunity where the insurance community can assist with some of that process.

The other point that I will mention is just in terms of connecting the dots and bringing action items to them, it is about understanding if employee training is only being offered by roughly 80 percent of organizations now, that does not translate to the fact that we have seen a growing number of threats really come out of exploitation of that human element, of that big vulnerability. And 50 percent of respondents to that Advisen Zurich survey noted that humans or their employees unintentionally infecting their network was a top concern. So just helping bring together those pieces.

Chairman CHABOT. Thank you. I have got less than a minute to go and I have got two witnesses. I am going to throw this question up and it is kind of maybe an impossible question, so if either one of you want to answer this. If a business has X-amount of insurance where they are covering fire and a whole range of things and now they have got to consider cybersecurity insurance, and let us say they are going to go with the insurance company they have now, how much more typically could they expect to pay for this that they are not paying without it right now? Percentage-wise, are we talking an additional 10 percent, 25 percent? And I know that is a tough question. It would depend on how big the company is. What would your estimate be if you have one?

Mr. CERNAK. That is an excellent question, and as you point out, it is going to depend on the class of business that they are in, the amount of data that they have, what coverages they are actually looking for. And there are two approaches to cyber insurance in the marketplace today. One is a standalone policy, which is probably going to cost you thousands of dollars.

Chairman CHABOT. Yeah. I would guess that would be probably more. So let us say you went with the company that you have now and they did have the expertise, unlike what Mr. Luft had said he

experienced, I mean, ballpark, what range are we probably talking about? Either one of you want to venture this?

Mr. GEOPFERT. Again, that is hard to formulate because every one of the organizations, when we work with them—and I am not on the insurance side; I am on the breach investigation side, so I see the flip side of it—every one of the organizations, the question is going to come down to what does your network look like? How much data do you have? How does the data pass through? Do you pass through credit card payments to a third party? Depending on how they answer that, you can have two organizations that are the same size in the same industry that have put together their networks differently. They are going to pay vastly different amounts for insurance.

Chairman CHABOT. I told you it was an impossible question.

Do either one of the first two witnesses want to take a quick stab at it, ballpark?

Ms. DAVIS. So there are a number of factors that contribute to that. So coverages, but also limits and retention. So it really depends on what an organization's risk tolerance is. Somebody may say to themselves, "I feel as though I can retain this risk. I am not at high risk of this sort of event occurring," and they may be purchasing a $1 million limit with a $250,000 retention purely to satisfy a contractual requirement; somebody else may opt for hundreds of billions in coverage. So those are some of the influencers.

Chairman CHABOT. Mr. Luft, you are from Cincinnati. I expect you to give me an answer.

Mr. LUFT. So, Chairman, I can talk specifically about what is happening with my company. And so for my liability policy, covering our installation, for a million-dollar policy that is about $4,000. When I bought that standalone cyber insurance policy, that was $3,200, so roughly about 80 percent.

Chairman CHABOT. Good. Thank you very much. I appreciate it.

My time is expired. I apologize for going a little bit over.

The Ranking Member is recognized for 5 minutes.

Ms. VELÁZQUEZ. Thank you.

Mr. Cernak, I believe that you stated that it is not if small businesses are at risk, the question is when is it going to happen. So we need to operate under the assumption that aggressors are already inside our networks. With that said, what alternatives do small businesses have once they become aware an aggressor already has access to that information and technology?

Mr. CERNAK. Sure. Yeah, once you have identified that someone may be within your four walls, I think it is incumbent and imperative that you get somebody, like my colleague here to the right, that could come in and identify exactly what is wrong. And not to stop at the first answer. We have seen instances where ransomware is extremely popular now. A lot of businesses are being impacted by ransomware, and it is a very visible attack. But what the criminals are doing on the other side of that is they are loading additional software in the back end so that once you rectify the very visible issue, and you may think your problem is solved and go back to managing your business, there is this other software that is going to start exfiltrating data down the road. So you

really need to get a professional in to do a thorough analysis and your insurance company can help you identify those people.

Ms. VELAZQUEZ. Mr. Geopfert?

Mr. GEOPFERT. The part I am going to hit is this actually delineates quite a difference between the small business market and even the mid-market in that both of those groups are going to struggle preventing the breach. It is very difficult in today's day and age with the types of exploits and malware to keep them out. The more complex the organization, quite often they will notice that they are breached earlier. And even if the attacker did get in, quite often they have stood up security monitoring of the tools that can let us retrace the steps of the attacker so we can reconstruct what did the attacker do in the environment, how long were they there, what did they take, what did they touch?

In the small markets, quite often they are not even that mature. The attackers can get in. By the time the organization finds out that an attacker is in, when we show up there is no evidence or the small business has already destroyed the evidence in their initial response. They have overwritten it.

And so when we are talking about the damages for small businesses, a big part of their problem is they always have to assume the worst-case scenario. Because they either did not have the evidence or they destroyed it, we have to assume the attacker essentially reached everything and legal precedence says they have to do mass notification, whereas in the larger environments it might be the same attacker who did the same thing, we can constrain. We can put bounds around what the breach actually was. So it inordinately impacts the smaller environments simply because they are less able to reconstruct what the issue was even if they could not stop the attack.

Ms. VELAZQUEZ. Thank you.

Ms. Davis, cyber insurance is in its infancy as an insurance product. How has it evolved since its inception to meet the demands of small firms and the needs of neutralizing relentless cyber attackers?

Ms. DAVIS. So the roots of the product were really in the technology, you know. And as some of the first-party costs to an organization, the immediate costs after a breach began to evolve with notification standards and credit monitoring, et cetera, the policy was built out to include those first-party coverages. And what we are finding now is that financial institutions, healthcare organizations, those early adopters in heavily regulated segments are really more driven towards that personal information and healthcare information.

Next, we have a three-tail organization, and what we are finding now is that the coverages have evolved to really address the interdependencies that we are seeing across the supply chain. And so business interruption, loss of income, extra expense that an organization would have to pay in the event of downtime is becoming a key driver in the coverage discussion.

Ms. VELAZQUEZ. And can you explain how the process to create policies is complicated by various state and federal laws and a disjointed federal cybersecurity effort?

Ms. DAVIS. Sure. So we talked about some of the first steps when an organization realizes that they have been compromised, and certainly, forensics is a big piece of that to understand what went wrong and why and how many, you know, the extent of the information that was compromised. I would argue that very early on in that process there also needs to be legal representation, attorney breach coaches who are helping to prioritize those notifications and needs to individuals who were impacted. And the challenges that creates is really each and every State, at this point an attorney general is handling those topics differently. What is considered legal compliance and what timeframe individuals need to be notified? How they need to be notified, does it have to be through USPS? Is email sufficient? And so the costs, the legal costs for small businesses really add up in that process, and so standardization of those requirements would help bring down the costs associated with it,

Ms. VELAZQUEZ. Thank you.

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

Ms. VELÁZQUEZ. I yield back.

Chairman CHABOT. Thank you.

The gentleman from Missouri, Mr. Luetkemeyer, who is the Vice Chairman of this Committee, is recognized for 5 minutes.

Mr. LUETKEMEYER. Thank you, Mr. Chairman. This is a subject that we are talking about today that 10 years ago it would not even be on our radar, and yet today, here we are. And so it is kind of scary from the standpoint of what are we going to be talking about 10 years from now that is not on our radar today? And so that is how fast our society and evolution of all these things is happening. That is just an aside.

Mr. Cernak, you represent a reinsurance company, and we are talking about cyber today and your company provides cyber insurance. Why are you a reinsurance company that reinsures insurance companies here today talking about cyber?

Mr. CERNAK. Thank you for the question. And it is a great question.

I think the role that reinsurers play in this realm is to help make more coverage available to the end consumers, the small businesses, by enabling other property and casualty insurance companies to put products out in the marketplace, and not only provide those carriers with the capacity, but also the technical knowledge to provide a sustainable product that they can feel comfortable bringing to their insured customers. And so beyond the dollars that a reinsurer can provide to these P&C carriers, it is also the claims expertise, the service provider networks, the forms development, and the rate development. You need all of those things to create a compelling product, and by doing that we help other carriers introduce products in the marketplace, thus helping the end insureds.

Mr. LUETKEMEYER. Very good.

Evaluating the risk here is really difficult, and I know Mr. Luft made a comment in his opening statement that 43 percent of the attacks are on small businesses. My staff has got a number here of businesses under $300 million in value, 50 percent of cyber at-

tacks are on those businesses. This tells me we have got a very vulnerable group of folks here that probably do not have the expertise to deal with it. And so how do we protect them? So that is where insurance comes in.

So I guess my concern is not necessarily, I know we have talked a little about the business interruption, basically coverages that you guys are involved in, but to me the biggest risk for a small business is the liability exposure. And liability exposure is such that if I am in the lending business and I am lending to a small business and I see that they are very highly leveraged and I see that they deal with lots of personal information, to me there is an exposure there that could really harm that credit. Therefore, that whole line of credit is in danger. Therefore, it is going to hurt me as a financial institution.

And I can see that at some point the regulators are going to get involved in this and start asking and requiring for cyber insurance for certain lines of business that deal with more information.

So if Mr. Cernak or Ms. Davis would like to take this, it looks to me like small businesses are the low-hanging fruit for the bad guys to go after and I think in some cases, I was talking to some folks a while ago, that it can even be the back door to bigger business, which means you have an even bigger liability risk. So would you like to talk about that just for a second, how you want to approach that particular part of the coverage?

Mr. CERNAK. Sure. And I think you are right on with that assessment that we are starting to see small businesses be that back door into the larger businesses, and we are starting to see the larger businesses require contractually that these smaller businesses carry some level of cyber insurance. The struggle there is oftentimes they may or may not have an arbitrary dollar amount in terms of the limit they want carried, and they also do a fairly poor job of identifying the exact coverages they want those folks to carry.

Your comment relative to the lending industry in particular, I don't think I have seen that as of yet, but I think it is a valid concern.

Mr. LUETKEMEYER. Go ahead, Ms. Davis. Would you like to comment?

Ms. DAVIS. I totally agree. And thank you for the question. Absolutely, we are seeing that back-channeling take place where it does feel as though the larger organizations are locked and loaded when it comes to their information security measures, but that supply chain that we reference has become a huge vulnerability, especially in the manufacturing space and when we think through items like corporate confidential information.

Mr. LUETKEMEYER. I think Mr. Luft made a comment a while ago with regards to a question I think one of our other folks made. And the comment was made with regards to covering things that may have happened prior to the coverage being effective. And so my question is, does your policies, are there policies out there that will take care of things that you put in place that were not accurate or that exposed you not only before, but what happens if you put something in place, you let the policy drop or go to a different carrier, do you have tail coverage or something as well with this?

Can you kind of explain the before and after coverages here if there is such a thing?

Ms. DAVIS. Yeah. So it is an important development in the cyber insurance space, the idea of prior acts. And the reason why it came about is because of the statistic that Congresswoman Velázquez noted of 200 days potentially where a perpetrator has been in the network and we found the nature of the threats has changed as attackers used to enter a network, grab as much information as they can, and then get out, and now they tend to lurk and try to stay under the radar, grabbing small bits of information at a time. So that coverage is available in the marketplace, and typically, we do find that affordable coverage to that effect is available as customers change carriers as needed.

Chairman CHABOT. The gentleman's time has expired.

The gentlelady from New York, Ms. Clarke, is recognized for 5 minutes.

Ms. CLARKE. I thank you, Mr. Chairman. And I thank our ranking member. I want to also thank our witnesses for your expert testimony today. This is very important information. I think the average small business is really at a disadvantage in this day and age, not really conscious of the intrusion of those who would want to either extort them or use them as a tool for penetrating even larger enterprises. So I want to thank you once again for your insights.

Ms. Davis, I did want to find out from you how does your company tailor insurance policies? Is it for each client? Is there a "one size fits all" package? Can you give us some insights into that?

Ms. DAVIS. Sure. So it is helpful to understand the underwriting process when answering this question, so let me start with that. Organizations would typically complete one to two underwriting applications and those are submitted to various carriers by an insurance broker. It was noted earlier to really partner with a broker who has expertise in this space since it is such an evolving area. And those applications have questions on them. Some are reflective or inclusive of controls kind of noted through the NIST framework; others are outside of that. So there would be various applications and levels of information that are provided at the time of the application process.

But what the customers request, what an insured requests is really driven again by more of their risk tolerance, why they are purchasing the policy. Are they looking at it as more of a contractual requirement? Or are they looking for a more robust, cutting-edge solution? So, and a lot of that will influence the price as well.

Ms. CLARKE. So it is more of a tailored process based on the questionnaires that the individuals fill out?

Ms. DAVIS. That is correct.

Ms. CLARKE. And how widespread would you say this sort of practice within insurance, how widespread has that become to your knowledge?

Ms. DAVIS. The tailoring of solutions?

Ms. CLARKE. No, I am sorry. This sort of insurance practice for small business getting cybersecurity insurance?

Ms. DAVIS. So just so I understand, you are asking how widespread is it that the small businesses——

Ms. CLARKE. Within the industry of insurance, your company is one that has been identified. Have other insurers begun moving into this space?

Ms. DAVIS. Yes, absolutely. There is a growing recognition that small businesses are looking and actively seeking to raise their risk awareness, and insurance is one piece of that puzzle. It should not be the entire solution, but we are seeing increases in small- to medium-sized organizations actively seeking out insurance policies for cyber.

Ms. CLARKE. Yeah, because sort of most brick-and-mortar type of businesses have insurance, right?

Ms. DAVIS. Right.

Ms. CLARKE. Theft insurance, what have you. But not many of those types of mom-and-pop establishments, which are very prevalent in Brooklyn, New York, where we are from——

Ms. DAVIS. Yes.

Ms. CLARKE.—would be looking to essentially look at their sort of connectivity and determining how they would add that to a current policy.

Ms. DAVIS. And I think that is a great point and it really gets at the way that the product has evolved from just a couple of years ago, where it was really focused on more privacy exposed organizations, and now we are at that new cusp of buyers and coverages that are more driven towards that business interruption, that network interruption, and the downtime and financial impact that it could mean to those mom-and-pop organizations.

Ms. CLARKE. Wonderful. Thank you.

Mr. Luft, in your testimony, you point out that small businesses often do not perceive themselves as being targets for cyber attacks. What can we do to educate the general public on the risks of not being protected? And what can we do to ensure that they have a place to go after a cyber attack takes place? As it stands now, where do they go?

Mr. LUFT. Well, I would say the first step is the small business needs to understand that there is extreme risk out there and they need to look no further than to television. There are plenty reports about what is happening to major corporations, to small businesses on a daily basis. So my first suggestion is that small businesses need to take that initiative.

From an education standpoint from this body, I do know from the Federal resources, from the SBA, especially within Cincinnati, they do a tremendous job of having events informing small businesses about cybersecurity and actions they need to take place. So I would think more what needs to happen is the initiative from the small businesses to take action.

Ms. CLARKE. And probably partnering with some Chambers of Commerce?

Mr. LUFT. Absolutely. Yes.

Ms. CLARKE. And things of that nature?

Thank you very much again for your testimony here today. Mr. Chairman, I yield back.

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

And the gentlelady from American Samoa, Mrs. Radewagen, who is the Chairman of the Subcommittee on Health and Technology is recognized for 5 minutes.

Mrs. RADEWAGEN. Talofa. Good morning. Thank you, Mr. Chairman and Ranking Member, for holding this critical hearing. Thank you all for appearing today.

Ms. Davis, my first question is for you. You mentioned that businesses with personal health and personal financial information consider data security as more of an issue. Are there any industries that you believe are prone to cyber attacks, but currently do not see cybersecurity as a pressing issue?

Ms. DAVIS. I would say the one class of business where we are definitely seeing an increase in awareness is in the manufacturing space. And again, that gets back to more of the corporate confidential information, the supply chain, and what interruption, network interruption could mean to those organizations. Manufacturers, historically, had felt like the product did not necessarily speak to their coverage needs, to their exposures, and we are definitely seeing that maturity start to change in their thought process.

Mrs. RADEWAGEN. Thank you.

My second question is actually for all of you. What do you think are the biggest risks for cybersecurity insurance providers that do not exist in other insurance markets? Mr. Luft?

Mr. LUFT. Your question was specific to the cyber insurance companies?

Mrs. RADEWAGEN. Insurance providers. Yes.

Mr. LUFT. In speaking about the small businesses, the reason why they need to think about that as the statistic has been mentioned several times today, that after a cyber attack, 60 percent of small businesses are out of business within 6 months. I think that is the greatest call for action from a small business perspective.

Mrs. RADEWAGEN. Ms. Davis?

Ms. DAVIS. I think one of the biggest challenges to insurers right now is really not having a solid sense of what their aggregation concerns may be. When we think through property as an example, you are able to model, right, what your windstorm-exposed areas are. When it comes to cyber, there are all of these hidden or sort of silent interdependencies that you may not be able to track or to model in the underwriting process. So that is definitely a concern for us.

I would also say the intersection of the various lines of business is unique to the cyberspace. We are talking today about kind of the standalone cyber policies, but what we are finding is that as the threats evolve, some of these coverages are creeping into different policy lines, and so making sure that we have a way of identifying those gaps and redundancies to make sure we are providing good, holistic, meaningful solutions to our customers.

And lastly, I would just say that this is a product still in its infancy and so we are learning together across the industry to make sure that we provide more consistent underwriting processes, more consistency in our application process, and in the language and vernacular that is being used. And I think all those things are hurdles for us at this time.

Mrs. RADEWAGEN. Mr. Cernak?

Mr. CERNAK. Thank you for the question.

I see two major challenges right now, in addition to the ones that Ms. Davis pointed out. First is the patchwork of regulations that we are faced with in terms of trying to address and create products. We have to not only worry about the State, but the Federal, and now international regulations and security standards. So that is one item.

The other, as Congressman Luetkemeyer mentioned in his remarks, is the smartphone is turning 10 years old this year, right? Never have we tried to insure an exposure that is evolving this quickly. It is moving with the speed of technology, and that in and of itself poses challenges.

Mrs. RADEWAGEN. Thank you.

Mr. Geopfert?

Mr. GEOPFERT. I will speak as the neutral third party in the room. Quite often when things go bad, what we see working as responders with the insurers and the small businesses, it is more of a syntax issue. There is no common language to talk about security and risk within these organizations. So what we see is the insurance companies reaching out to the small businesses trying to put together their policies and packages and understand the risk of the organization they are going to insure. And the small business, not being malicious, they simply do not understand security.

When they are filling out the package and trying to communicate how much data do they have? How do they control it, their business partners, their systems? They do not know how to fill out the packages and applications in the right way. So quite often the insurance companies will pick up that policy and not really understand what is underneath the hood until there is a breach, until we come in on the technical side and start touching the environment. Quite often, the insurance companies really do not understand how bad bad can get.

And so until we can get to the point where there is sort of a standardized language where the insurance companies know how to rate the risk of a small organization and the small organization knows how to rate themselves, there simply could be missed expectations on both sides.

Mrs. RADEWAGEN. Thank you. Thank you, Mr. Chairman. I yield back.

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

The gentleman from Pennsylvania, Mr. Evans, who is the Ranking Member of the Subcommittee on Economic Growth, Tax, and Capital Access, is recognized. And I would like to thank him for his leadership on this issue and introducing legislation to ensure that the SBDCs accredit the people that will help to train small business folk to better protect themselves against cyber attacks. So we appreciate his leadership on this. And he is recognized for 5 minutes.

Mr. EVANS. Thank you, Mr. Chairman. I appreciate you and the ranking member's leadership collectively on the fact that this is really a bipartisan approach and we have all got to work together.

So what I want to piggyback a little bit and expand a little deeper on what Ms. Davis said and the term that she used, "risk map-

ping." And used that term, and kind of if you have a crystal ball, if you say "risk mapping," what particular industries, much more subject to the risk aspect in terms of where we are today? You said risk mapping. Give me a sense on categories of small businesses.

Ms. DAVIS. So when I speak through risk mapping, I am thinking through, you know, it varies by industry, but it is also about identifying what is at risk from a pure data network security view, but also the broader implications that that may have on your organization. So the lost revenue or the downtime, it could mean the reputational risk. It could mean bodily injury or property damage, and bringing together a multi-stakeholder approach when evaluating cyber risk so that you are thinking of it as an organization, as an enterprise level.

And in terms of the cyber or the IT risk mapping component of that, it could mean from a retail organization how many records you are holding. How long are you retaining them? For what reason are you retaining them? So that you are always keeping a proper calibration between your data risk and your data value.

Mr. EVANS. Okay. I am starting my business. I mean, where would you go to kind of get that little sense of the mapping and understanding? To your knowledge, does anybody keep track of what takes place in terms of the community? Because listening, you just said the smartphone is 10 years old. Is there anywhere you can go to get a little sense of that?

Ms. DAVIS. So there are businesses that you can turn to to help you do that, but I would say the very first step is doing it internally. And again, engaging your stakeholders within an organization to make sure that you have got either a risk manager or somebody who is acting in a risk manager role. You know, talking with HR or if you have somebody handling the IT business in-house. But really just beginning to have that dialogue internally so that you can start to gain and act on the information that you learn through something like an incident response plan to help you engage and limit your damages if and when an event does occur.

Mr. EVANS. To the rest of the panel, hearing what Ms. Davis said, we just had this discussion about risk mapping. And as you look at it, what would you say in your particular case to your clients, understanding the aspect of risk mapping?

Mr. GEOPFERT. The first point I am going to make is this is, again, dealing with small businesses. If you tried to explain this concept to them, to your point, they do not know where to start.

Mr. EVANS. Right.

Mr. GEOPFERT. This would be a perfect role for the Small Business Development Centers.

Mr. EVANS. Right.

Mr. GEOPFERT. Because they touch so many different entities, in a lot of cases they become the de facto knowledge-sharing centers. And in a lot of cases, they would be able to start you on that process and lay that out.

The other point that I want to make out, when we deal with risk mapping, in a lot of cases that operates off the mindset that, like what you see in the news, that there are hacking crews that are out targeting your specific organization and going after you. A lot of small businesses, when they are trying to consider their risk,

they do not feel that they are at risk because we are too small, we are too new. No one is shooting at us. It misses the point that the vast majority of breaches are not targeted and you cannot plan for that risk. If you are plugged into the internet, there is sort of the background radiation of the internet that is constantly grinding through looking for anybody that happens to be vulnerable and it might happen to be you.

And so a lot of organizations, when we first sit down to do risk mapping with them, they are shocked with that realization that they are not targeted; they simply were a target of opportunity on the network. And so I think the Small Business Development Centers would be great at communicating that message of in your specific industry, this is what a risk map would look like. But do not forget there is a permanent residual risk that you simply cannot excuse yourself because you are too small or you are not in that industry.

Mr. CERNAK. I think there is also an opportunity for insurance agents and brokers to begin that process as well. Because as they are sitting down discussing with their clients what their exposures are, they can start to ask the leading questions, if you will, as to what data do they have, where is it stored, and how do you use it, a lot of the points that Ms. Davis suggested. So I think insurance agents and brokers need to raise their level of education to help the clients.

Mr. EVANS. I yield back the balance of my time. Thank you, Mr. Chairman.

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

The gentleman from Iowa, Mr. Blum, who is the Chairman of the Subcommittee on Agriculture, Energy, and Trade, is recognized for 5 minutes.

Mr. BLUM. Thank you, Mr. Chairman. Thank you to the panelists for being here today to talk about a very important issue to small businesses.

I am and was a small business person, and a few years back my high-tech company was compromised via a cyber attack. I was absolutely shocked at how untrained law enforcement was on how to handle this situation because we lost value. We lost value.

Two questions concerning that for the entire panel: A, has that changed? Is law enforcement, in general, across the country better trained now to handle the theft of a company's information via cyber attack?

And B, what can Congress do or what can government do, assuming we are not where law enforcement needs to be? What can we do to—any ideas or suggestions on how we can change that?

Mr. LUFT. To your first question, I hope. And the second question, as far as what Congress can do, whatever can be done to help inform small businesses about the number of threats that are there and helping small businesses understand what steps they can do to protect themselves is the greatest thing that could be done right now.

Mr. CERNAK. Again, I think, you know, the patchwork of regulations also can hinder a little bit of that because there is this attitude of, you know, well, who is ultimately responsible for that por-

tion of the law enforcement if you have got different regulatory bodies that are involved in cyber events? So I think, again, streamlining that may help as well.

Mr. BLUM. In your opinion, is law enforcement better trained than they were 5 or 10 years ago on cyber attacks? And how to prosecute and how to find out what the value is of what was taken, et cetera, et cetera?

Mr. CERNAK. Yeah. No, and that is an excellent question. Unfortunately, my focus is more on helping the small businesses recover relative to the issue and that is where my expertise stops.

Mr. GEOPFERT. Sir, it pains me to say, as I am a former special agent, so that is where I came from, are they better than they were 5 or 10 years ago? Yes. Has it materially improved the situation? No.

Per my comments earlier, in a lot of cases, what happens with a small business especially is they do not register on the Richter scale enough to draw the attention of the law enforcement entities that could actually do something to resolve the situation. And so the FBI and Secret Service have a lot of very skilled people that do exceptional work, but there is only so much availability, so much bandwidth. And they are naturally going to gravitate to the larger events. And so while they would be interested to hear of the issues within the small businesses, the idea that they are going to send an agent down to start working on those cases is just not reasonable.

And so what you are left with is local law enforcement, who usually are very excited to help, but they technically cannot do anything. They are very effective, and they have put a lot of people through training where if you have internal theft, if you have an employee that is committing fraud or something, they can assist with those types of issues, but at the end of the day, the goal of law enforcement typically is to affect an arrest against somebody. And with the vast majority of the attackers overseas, it is quite often hard to get them interested. And what they seem to miss is they do play a key role in this.

Take a typical small business that might not have great security monitoring themselves, so they do not produce the evidence internally for us to reconstruct what the events were. But let us say we can see an offending IP address that touched them where the attacker came from on the last hub. That IP address is in somewhere else, another business, another citizen of the U.S. We cannot go acquire that system. But if I worked with a law enforcement entity, I could very rapidly get some type of search authority. They can go acquire that system. We might be able to recover the evidence we need to see how bad the event was off of that system. And when we try to do that now, quite often that is weeks or months to go through that process. By that time, all the evidence we could have used to limit the damage is gone.

And so there is a role, but because they normally are not going to end up in arrest, it is hard to get them engaged.

Mr. BLUM. Thank you very much.

Last question, assuming the value of the compromised data is covered by insurance, how do you quantify? How do you put a number on compromised data? How does that work? That has got to be,

I mean, that has got to be a tough thing. Give me some insight into that, please.

Ms. DAVIS. So it is a tough thing. In talking about the patchwork of laws, it largely depends when you talk about how those records are compromised, you know, where they were compromised, the extent of them, the number of people who are going to require notification. There is a general sentiment that there is desensitization happening across the population, so fewer and fewer people are taking carriers up on offers for things like credit monitoring. It depends largely on the forensics, how long they were in your network, how much information was compromised, and really driving up those forensics costs; any fines and penalties that could be resulting from that and if there were data restoration costs involved. So the sums, they range wildly.

To get to your earlier question, I just want to point out that they say the prosecution rate for these kind of nefarious actors only ranges around 10 percent, and so that means that criminals who were sort of lurking in the dark web are currently coming out because there is no reason to be in the dark and that means they are talking to each other. And so the sophistication and nature of the attacks really continues to increase.

Chairman CHABOT. The gentleman's time is expired.

Mr. BLUM. I yield back the time I do not have, Mr. Chairman.

Chairman CHABOT. Thank you very much.

The gentleman from Florida, Mr. Lawson, who is the Ranking Member of the Subcommittee on Health and Technology, is recognized for 5 minutes.

Mr. LAWSON. Thank you, Mr. Chairman. And welcome to the Committee.

Ms. Davis, as you are well aware, many small businesses may be unaware of the lack of capital to purchase cyber insurance. What can small business organizations, SBAs, as well as local entities, do to better educate the small businesses about the risk of cyber attacks and the importance of purchasing cyber insurance?

And I say that because I was in small business and I have been trying to wind some things down. And a young person came in. I heard Mr. Cernak talk about the birthday of this here is 10 years old and I had a typewriter in the office, an IBM Selectric typewriter. And one of the young persons said, what is that? You know, and I said this is one of IBM's best. They said, they still make those?

So my question is, I just wanted to say that because when you talked about the birth of this, what can we do to educate small businesses about it?

Ms. DAVIS. So I think when it comes to small businesses, you know, we really have to think through the culture of an organization. When it comes to controls, the expectations across industry class are really going to vary wildly, so you cannot say this one control will make you a better risk. There is no silver bullet answer, but it is about building a culture of resilience. It is about understanding what your risks may be. It is about ongoing employee training. And these are items that do not have a significant price tag associated with them. That is just an ongoing effort to make sure that you are bringing the right people into the conversation

and that you have that multi-stakeholder incident response plan in place if and when an event occurs. Because what we do find is organizations who are lacking that sort of preparation are the ones who have a longer amount of downtime, more financial impact to their organizations because they were not prepared.

I would say from an insurance perspective, do keep in mind that although the costs will vary based on some of the subjectivities we have talked about, you know, they cannot afford to be out of business for a prolonged period of time. And so when you think of the safety net that an insurance policy can bring to the equation, it will likely be a fairly small financial cost compared to that longer hardship if the downtime is significant.

Mr. LAWSON. Okay. And I have read the staff report on cyber insurance can be customized to the specific needs of the company. Mr. Cernak, what are some of the more innovative ways that you see cyber insurance can be crafted to the specific needs of small businesses?

Mr. CERNAK. One of the trends we have seen lately is tailoring it to small businesses by making it even more comprehensive. So a lot of the policies that may be out there currently offer higher limits, but you have to choose which exact coverages you feel you need as a small business owner. And the concern is maybe I select the wrong coverages for what I need.

So we are seeing a trend of packaging multiple coverages under a common limit, making it a very streamlined approach so that they do not have to answer 12 pages of underwriting questions where you are going to get the wrong information, not by any malicious intent, but simply by the fact that they do not understand the application. Perhaps provide cyber insurance as an endorsement to a policy they might already be buying. So perhaps they are already buying a business owner policy that is providing them with property and liability insurance. Can we add on a very nice and tidy package of cyber coverages as an endorsement to that?

Mr. LAWSON. And a real quick question, anyone can answer. Will small businesses in the small business be able to do group coverages, hopefully, to stabilize their premiums?

Mr. CERNAK. So along the lines of almost a captive or some sort of that, there has been, I know, some conversations around that idea. It is a little bit of a challenging idea because as we stated earlier, you know, cyber does provide some level of aggregation exposure. And so by doing a group approach, you may be doubling down on that aggregation exposure as well. But there may be some cost savings, especially as these policies tend to bring services into play. Those services may be had at a more competitive price.

Mr. LAWSON. Okay. My time has expired, but I hope you all remember the IBM Selectric typewriter.

Mr. Chairman, I yield back.

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

And we want to very much thank the panel here for helping the Committee to better understand an issue that more and more small businesses all across the country are facing, and that is the cyber risk that is out there, the attacks that they could be facing. We are committed as a Committee to doing everything we can to assist the

small business community to better protect themselves, whether it is best practices, whether it is potentially cybersecurity insurance, and you all have assisted us in doing that, so we thank you very much for that.

I would ask unanimous consent that members have 5 legislative days to submit statements and supporting materials for the record.

Without objection, so ordered.

And if there is no business to come before the Committee, we are adjourned. Thank you very much.

[Whereupon, at 12:22 p.m., the Committee was adjourned.]

APPENDIX

Testimony of Robert Luft

Owner

SureFire Innovations

On behalf of the National Small Business Association

House Small Business Committee

"Protecting Small Businesses from Cyber Attacks: the Cybersecurity Insurance Option"

July 26, 2017

1156 15th Street, N.W., Suite 502
Washington, DC 20005
202-293-8830
www.nsba.biz

Good morning. Thank you, Chairman Chabot, Ranking Member Velazquez and members of the House Small Business Committee, for inviting me to testify today on the current state of cybersecurity for small companies and how cyber insurance can help small businesses mitigate risks.

My name is Robert Luft and I am the owner of SureFire Innovations located in Cincinnati, Ohio. The company is a certified Service Disabled Veteran Owned Small Business (SDVOSB) and Minority Business Enterprise (MBE). SureFire Innovations is a network design, security, and installation company that specializes in developing robust network management systems. Our clientele base is largely comprised of medium-and-large-size companies on a national scale.

SureFire Innovations originated shortly after my return from the Army, where I served 16 years as a Combat Engineer. I had the privilege to serve the nation on multiple combat deployments to Iraq. It was during my time in service where I developed the necessary leadership skills to transfer over to the civilian sector as a successful entrepreneur.

I am pleased to be here representing the National Small Business Association (NSBA), where I currently serve on the Leadership Council and the Small Business Technology Council. NSBA is the nation's oldest small-business advocacy organization, with over 65,000 members representing every sector and industry of the U.S. economy. NSBA is a staunchly nonpartisan organization devoted to representing the interest of the small business which provide almost half of private sector jobs to the economy.

State of Cybersecurity

Cybercrime is growing rapidly with annual costs to the global economy estimated to reach over $2 trillion by 2019. Organizations of all sizes are at risk for cyber-attacks. Small businesses represent more than 97 percent of total businesses in the U.S. and make up an essential part of the supply chain to some of the largest companies, many of which are in critical infrastructure sectors, from financial and transportation organizations to power, water and healthcare suppliers.[1]

Cyber criminals are becoming increasingly sophisticated in their attacks on networks and their attempts to steal personal information that can ultimately lead to severe financial distress. These attacks happen every day and are often completely undetected until well after the damage is done. Due to this current landscape that our networks are operating within, we all must accept that cybersecurity attacks are now an inherent risk for businesses of all sizes—including small entities. In 2015, 43 percent of all attacks were directed at small businesses.[2] Despite the growing awareness of cyber-related crimes, and the increase of small businesses being a target for these attacks, 77 percent of small-business owners believe their company is not at risk for cyber-threats such as viruses, malware, hackers or a cybersecurity breach. This figure is quite alarming.

[1] Fanelli, B. The State Of Cybersecurity among Small Businesses in North America. https://www.bbb.org/globalassets/shared/media/state-of-cybersecurity/cybersecurity-research-report.pdf.
[2] https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf
[3] https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize- businesses.html

Small Business – Understanding Cyber Risk

Every successful small business owes their success to their ability to understand the risks inherent in their perspective industries. Cybersecurity starts with understanding and managing potential dangers. The unfortunate reality is that many small businesses do not identify these threats until they experience some level of disruption.

The level of risk for being a target of cyber-crime is high, 42 percent of small businesses surveyed by the National Small Business Association (NSBA) reported being a victim of a cyber- attack, with cyber-attacks cost an average $32,021 for companies whose business banking accounts were hacked, and $7,115 on average for small businesses overall.[4] NSBA members who were victims of credit card theft, 13 percent of the attacks the company's entire network was compromised and in 10 percent there banking accounts were breached. Small businesses often operate on very tight profit margins and seldom carry a lot of excess cash. These losses can be devastating to businesses in those circumstances.

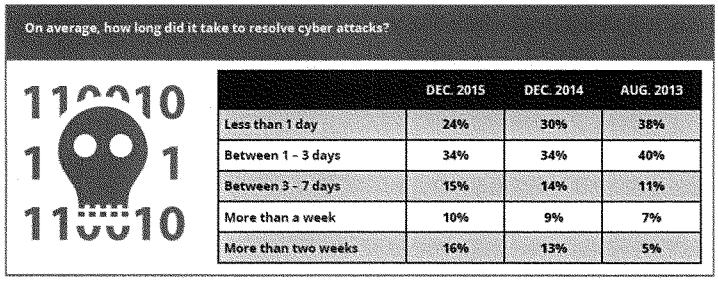
Since total elimination of threats is impossible, protecting against them without disrupting business innovation and growth should be a top management priority. Unfortunately, many small businesses are still not placing cyber-threats within their top priorities for business survival. Growing revenue, increasing profit, managing cash flow and attracting and retaining qualified employees are the top challenges identified by the respondents overall. The Better Business Bureau conducted a survey where only 20 percent of respondents identified cyber-threats, including lack of data security, as a top challenge for growth and survival.[5]

What was the nature of the cyber-attack? (check all that apply)	
My computers were hacked	34%
My credit card information was stolen	31%
My website was hacked	17%
Our entire network was hacked	13%
My bank account was hacked	10%
My company information was hacked from a third-party (i.e.: insurance company, accounting company, etc...)	7%
Our cloud data was hacked	2%
Other	16%

Small Business Operational Perspective

The NSBA 2015 Year-End Economic Report demonstrates that in a technologically advanced economy, network vulnerabilities and the lack of a comprehensive cybersecurity policy can completely disrupt business. Due to the cyber-attacks, almost half of the affected businesses experienced an interruption of service.

[4] National Small Business Association, 2015 Year-End Economic Report 12 available at, http://www.nsba.biz/wp-content/uploads/2016/02/Year-End-Economic-Report-2015.pdf.
[5] Id. The State of Cybersecurity at 17



	DEC. 2015	DEC. 2014	AUG. 2013
Less than 1 day	24%	30%	38%
Between 1 - 3 days	34%	34%	40%
Between 3 - 7 days	15%	14%	11%
More than a week	10%	9%	7%
More than two weeks	16%	13%	5%

The above graph shows the difficulty that small business confronts when resolving a cyber-attack, 34 percent of attacks persisted for up to three days, with 41 percent taking three days are more to resolve. This is an incredible burden on an organization of any size, but when factoring in that these our small businesses with limited financial and technological resources, the problem becomes compounded. Only 14 percent of small business rate their ability to mitigate cyber risk and vulnerabilities as effective. That is an unfortunate reality when factoring that 60 percent of small companies go out of business within six months of a cyber-attack.[6]

This is in stark contrast to larger companies where an attack may not even slow down operations while sophisticated IT departments repair the damages. But many small businesses are not able to have dedicated IT departments and still others must outsource IT functions or assign these duties to an employee as a secondary function. In fact, in 2013, 40 percent of business owners were handling IT personally and only 24 percent were outsourcing the function.

For those owners handling it themselves, it is certainly expected that resolving incidents will require research, training, trial and error, and a great deal of time away from the core functions of the business—acting as accountant, benefits coordinator, attorney, and personnel administrator. Simply outsourcing the function is not necessarily a silver bullet either. It can be cost prohibitive for some businesses and there are also issues with expected service delays. Simply put, a small business might not be high on the IT service provider's list of priorities if there is a systemic problem, even though such a firm is more likely to have the experience and technical expertise to resolve the issue quickly.

As a result, small businesses must become more efficient in their utilization of cybersecurity methods that are designed to help mitigate the potential risk of cyberattacks. The statistics show that there is a sufficient amount of work to be done on part of small companies and their operational strategies. Sixty-five percent of small businesses reported that they do not strictly enforce their password policy, this is the largest gateway for potential breaches. It is imperative that we, as small-business owners, fully enforce the most intrusive method of sabotaging our networks, and therefore our business.

[6] Cyber Security Statistics – Numbers Small Businesses Need to Know
Matt Mansfield - https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html

One of the most popular responses on why small businesses do not allocate financial resources to threat mitigation is that they feel they do not store any valuable data. This is a misconception on what constitutes valuable data – email, phone numbers, billing addresses may be viewed as not valuable information to the small business, but to a cyber-criminal, these are very valuable and effective data points that can be used for malicious purposes. Although, small-business owners are becoming increasingly tech savvy, limited resources and knowledge still leave many vulnerable to cyber-threats.

Transfer of Risk - Cyber Insurance

There are several reasons why small businesses should consider cyber insurance. First, insurance provides the small business to place a value on their current level of cyber risk. This allows business owners who may not be technically versed in cyber-attacks and the threats they pose, to quantify the potential cyber incidents.

Before purchasing SureFire Innovations cyber-liability insurance policy, I was like the vast majority of small-business owners, I felt as though, my company was too small to be targeted, the cost of another insurance policy was not within my operating budget, and did not know the actual value of having a policy. This was my thought process before a fellow business owner was the victim of a cyber-attack.

As with most cyber-attacks, his company was a victim of a phishing email attack, in which the hacker targeted an employee with a seemingly innocent password reset email. This allowed the hacker to gain access to their Amazon Web Services account and steal all the data and then delete everything from their account. This had a severe impact on their company, as within one year's time, they were out of business.

In 2016, I made the decision to evaluate my entire network and cybersecurity methods and make an honest assessment of what our vulnerabilities were and how to effectively mitigate them. The first step was to see what the daily cost and earnings that would be lost if my company was to be a target and shut down for several days. This was a simple formula: daily payroll, daily sales, and the cost to notify any individuals whose sensitive information is stored on my network. The formula I used was an annual sales divided by the amount of business days, which gave me $3,200 in effective lost daily earnings due to a potential cyber-attack. Taking this initial step allowed me to start building dollar amounts associated with any potential cyber-related incident and help me understand the need for a cyber insurance policy.

Second, the process of applying for a cyber liability policy forces you to acknowledge and address the potential vulnerabilities on your company, this is an assessment most small businesses have never taken. The application process made me account for several items that were not in existence for my company's operations. For example, we did not have a cybersecurity policy, this was a sober awakening, as the sheer amount of resources to assist small businesses in building this critical document could not be more plentiful. My company utilized the Federal Communication Commission's (FCC) Cyberplanner to help with the initial building of our cybersecurity policy. I came across the FCC resource, by conducting a simple web search seeking assistance in drafting a cybersecurity policy. This helped me to understand where there were weaknesses and areas that needed to be reinforced in my daily operations. Simple

measures, such as encrypting data, complex passwords, and having a firewall was explained in detail on their necessity. The Cyberplanner serves merely as a guide for companies—such as mine—that currently do not have a policy in place and may be uncertain as to what action steps to implement. This document helped provide a path for me to begin addressing sound cybersecurity protocols needed for my company.

Third, if the small business does experience a cyber-attack, certain policies include incident response assistance. This can be of great value for companies that are uncertain on how to appropriately respond in these dire circumstances. Smaller companies may not have the experience or the manpower to respond to the type of issues that may arise out of a security breach: reputational damage or any type of regulatory concerns. This adds immense value to the policy overall, as it allows the small-business owner to have guidance through an immensely complex and difficult situation.

Policy Selection

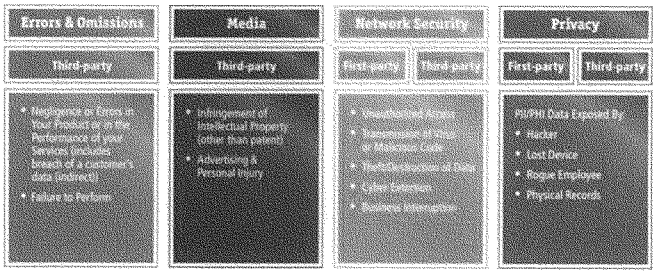
When I reached the decision to purchase a cyber liability policy to help transfer risk, it was an incredibly challenging situation. I was uncertain as to what constituted a good policy and the levels of protection that were needed. It was my assumption that my current insurance agent would have the intimate details of potential polices thoroughly digested, this was not the case. In fact, from the time he introduced the policy to me, it was clear that he was unfamiliar with the underwriting process of cyber policies. As I was completely unfamiliar with the process, my solution was to work with the current agent and wait for him to gather the information and address my questions and concerns. In the end, this process took more than a month, when an experienced agent could have better advised me on the nuances of the plans, in a shorter amount of time.

There were two policies proposals offered: one with an annual premium of $1,800 and another with an annual premium of $3,200. After reviewing the two different policies, it was my interpretation that there was one main feature difference: the $3,200 policy included Technology Errors and Omissions. This was justification enough for me to move forward, as this provides coverage for claims that arise from the failure to perform your business activities for a client to the required standard. Being in the technology industry, standards can change rapidly and having this line of coverage felt necessary and appropriate for SureFire Innovations.

When I look back at my decision-making process, there are several areas that I would have reconsidered had I been more informed and knowledgeable, at the time. Starting with finding a well-informed agent that had experience and expertise in the field of cyber liability policies. I made the mistake assuming that my agent, who issues my other insurance coverages, would also understand cyber liability. This was not an accurate judgement, and it would have been a smoother process if I would identified an experienced cyber insurance agent to help address my coverage needs.

In my opinion and from my experience, it is highly important that a small-business owner, when selecting an agent for their cybersecurity policies, stay within the sphere of knowledgeable cybersecurity agents, as they will be able to better assist with identifying the appropriate policy for the level of coverage required per the business.

Garnering my cyber liability policy was not the smoothest process, but at the end of the day, I did acquire a policy that does suit my company's requirements. There is a variance of policies to choose, but small businesses can expect their cyber coverage in some combination of four components: Errors and omissions, media liability, network security and privacy.[7]



An important coverage element that should always be considered, which was not considered during my initial purchase, is retroactivity coverage. Many cyber policies limit coverage to breaches that occur after a specified "retroactive date." In some, this date is the same as the policy's inception date. This means there may be no coverage provided for claims made due to breaches that occurred before the policy period, even if the insured did not know about the breach when it bought the policy. Because breaches may go undiscovered for some time before claims are made, insured should always ask for a retroactive date that is earlier than the inception date. This will ensure that the coverage includes unknown breaches that first occur prior to the policy's inception, but do not manifest themselves until after that date. Insurers do not always offer retroactive coverage unless asked, but it is commonly available for periods of one, two, five or ten years. Some offer unlimited retroactive coverage.[8] Before finalizing my policy, I attended a small business cybersecurity symposium where it was suggested that before purchasing a cyber policy, request that retroactivity be included. That simple request allowed my policy to include one year retroactivity at no additional premium increase.

Conclusion

When I started my company, I was unsure of many of the challenges that would happen to a small-business owner and the need for sound, quick, and effective decision making. SureFire Innovations has had the opportunity to build a strong reputation in the technological space and work with large commercial enterprises as our customer base.

[7] Cyber Insurance 101: The Basics of Cyber Coverage I Wooodruff-Sawyer
https://wsandco.com/cyber-liability/cyber-basics/
[8] Top 10 Recommendations for Negotiating Your Cyber Insurance Policy
https://www.pillsburylaw.com/en/news-and-insights/don-t-wait-until-it-s-too-late-top-10-recommendations-for.html

Our customers have afforded us the opportunity to provide network services across the country and provides us a platform for growth. This has been incredibly difficult, but the rewards of building and managing a young company that is growing far outweigh the challenges. Which is why the area of cybersecurity and small business effectively mitigating and transferring risk is so important to me.

As small businesses become increasingly dependent on services and applications that connect to the internet, they also become a larger target for cybercriminals looking to exploit vulnerabilities to steal money and credit card credentials, intellectual property, personally identifiable information as well possibly destroy data and disrupt operations. These threats are very real and immediate. I have personally witnessed a company taken out of business at no fault of their business operations, employees, or completion, but rather an individual lurking on the internet with the intent to destroy an entire company and the opportunities it provides to its employees.

In fact, according to NSBA data, ninety-four percent of small-business owners are concerned about being targeted by cyber-attacks. The potential for loss from a singular cyber incident to a small business can completely neutralize its ability to compete in the marketplace. Additionally, for many small firms, a cybersecurity incident could lead to an entire network being down for many days until the full extent of the problem is known and then fixed. Not to mention that a highly public breach could also damage the business's brand and lead to long-term loss of income. The ripple effect that this issue can have on the overall economy is staggering.

This is the ongoing threat of the internet age, as more and more small businesses rely on web-based products and services, and it will only persist and evolve as long as the internet continues to facilitate commerce in the global economy. It is unlikely that there will be one solution to stop all the attacks. In fact, slowing and preventing these attacks will most likely require an ongoing process to identify new threats, vulnerabilities and ultimately solutions. NSBA urges Congress and this committee to always bear in mind the unique challenges that small businesses face and continue to include the small-business community in that process.

Thank you for allowing me to testify before the committee today. I would be happy to answer any questions you might have for me.

Robert Luft
SureFire Innovations
President

Robert Luft is the Owner, President of SureFire Innovations, a Service Disabled Veteran Owned Small Business (SDVOSB) and Minority Business Enterprise (MBE) based in Cincinnati, Ohio that designs and installs wired and wireless, security, and smart city networks.

Robert started SureFire Innovations after serving in the Army for sixteen years, which included multiple combat deployments to Iraq as a combat engineer conducting route clearance operations to defeat the Improvised Explosive Device (IED) threats. Robert has a Bachelors in Marketing with a minor in Public Relations. These experiences provide the requisite leadership skills that would transfer over to the civilian sector as an entrepreneur.

After his military service, Robert devoted himself to entrepreneurship and founded SureFire Innovations. The company's focus is in the technology sector, specifically network infrastructure. SureFire Innovations has been able to service large-scale enterprises on their infrastructure requirements through an emphasis on employee development, training, and immersion in the latest technological advancements in the industry.

Robert serves on the National Small Business Association (NSBA) Leadership, Economic, and Technology councils. He also serves on the Board of TechDefenders, an organization whose mission is to offer technology training to underprivileged students in the Cincinnati area.

As a proud veteran, Robert's passion for the veteran community is evident by his involvement with the Disabled Americans Veterans (DAV) and United Service Organization (USO).

Testimony of Erica Davis

Senior Vice President and Head of Specialty Products Errors and Omissions

Zurich North America

before the

House Committee on Small Business

"Protecting Small Businesses from Cyber Attacks: the Cybersecurity Insurance Option"

July 26, 2017

Chairman Chabot, Ranking Member Velazquez, and Members of the Committee, thank you for the opportunity to speak with you today about the important issue of cybersecurity and the role of the private sector in providing risk management solutions to businesses to protect against cyber risk.

As a leader of a team of market-facing underwriters at Zurich North America, I work with brokers and customers on the placement of cyber insurance. While there is increased awareness of the threats across all sizes of organizations, businesses are still struggling to understand cyber risk: the full scope of their exposures and how best to protect themselves and their customers.

Zurich

Zurich is a leading multi-line insurance group with more than 140 years' experience serving businesses worldwide. Zurich employs approximately 54,000 people and serves customers in more than 210 countries and territories.

Zurich entered the United States in 1912, and for more than 100 years has served businesses of all sizes in America, including Fortune 500 companies, small and medium size businesses, as well as farmers and ranchers. We are proud to help them manage risk and give them the confidence to contribute to the U.S. economy. Zurich's North American headquarters is in Schaumburg, Illinois, and supports the jobs of over 9,000 employees across the United States. We are proud to have a market and employment presence in each of your states. We are also pleased to offer risk management solutions to customers in Puerto Rico and will explore the marketplace of American Samoa.

As one of the five insurance providers currently leading the North American cybersecurity insurance market, Zurich is invested in identifying risks and delivering solutions for its customers. Zurich is committed to staying at the forefront of the cybersecurity issues, as both the likelihood of a security breach and costs continue to escalate.

Zurich's Approach to Cyber Risk

Understanding Attitudes to Cyber Risk. As the cyber threat landscape continues to evolve, companies across all industries find themselves increasingly vulnerable to potential harm from a security or privacy event.

Most loss dollars arise from first-party privacy breach costs, such as forensics, breach coaches, consumer notification and credit monitoring. We are also seeing:

- Business interruption loss
- Liability lawsuits
- Regulatory fines
- Reputational damage
- Shareholder suits

Businesses today face difficult decisions about cybersecurity and how best to manage their risks: deciding whether they should retain the residual risk or transfer it through the purchase of a cyber insurance product.

The role of insurance is continuously increasing as customers are now seeking industry feedback and risk insights. It has become more of a partnership, with businesses focusing on not just what happens post-breach and a loss being paid. They value having a stable of pre-vetted vendors available to them if they are impacted by a data or security event. They are also focusing more on pre-breach services to guide them through risk mitigation tools like technology assessments.

In October 2016, Zurich and Advisen (a leading provider of data, media and technology solutions for the commercial property and casualty insurance market) released a sixth annual survey of risk managers, insurance buyers, and other risk professionals on the current state of trends in information security and cyber risk management. Key findings included:

- Eight-seven percent of respondents believe a technology interruption would have a moderate-to-significant impact on their business.
- Over the last six years, the proportion of companies buying security and privacy cyber insurance has increased by 85%, from 35% in 2011 to 65% in 2016.
- For the firsts time in the six years of this study, general counsel has surpassed information technology as the department most frequently responsible for assuring compliance with all applicable federal, state, or local privacy laws, including state breach notification laws.
- Most companies surveyed (97 percent) clearly recognize the importance of collaboration between their risk management and information technology departments on issues related to cyber security.
- Industries with substantial personally identifiable information, personal health information and/or personal financial information, in general, consider data security and privacy to be a more significant risk. As a result, they also are more like-

ly to purchase security and privacy insurance and engage in risk management activities.

- Costs related to a breach of customer/personal information are the leading reason for purchasing cyber insurance.

Coverage. Zurich provides coverage for cyber risk to businesses of all sizes, and cyber coverage is tailored based on customer need. While the historical reason for purchasing cyber insurance is liability concerns and costs related to breach of customer or personal information, coverages recently have focused on business interruption and supply chain downtime as the result of a cyber event.

Risk culture is also critical to underwriting any line of business. Cyber insurance is no exception. It is critical for businesses to build a culture of awareness at all levels. Events in recent years have raised awareness of cyber risk across all industry segments. Businesses must adopt a mindset of resilience rather than just protection.

More businesses are beginning to view information security as an organizational challenge rather than just a technology issue. The business community's interconnectivity and reliance on technology has increased, which creates more points of entry and new threat vectors. The exposure has broadened to include potential property damage for something like critical infrastructure, bodily injury caused by autonomous vehicles or cyber espionage.

Therefore, the underwriting of the cyber product is evolving as the risks are morphing. The insurance community is continuously working to understand the full scope of the exposures and what the controls might need to be. Each business needs to be underwritten differently.

Resilience. Organizations of all sizes now realize they are at risk of a security or privacy event. Finding solutions to the most complicated of cyber risks will require collaboration between the insurance industry, governments, academia and other think tanks to establish standards, encourage information sharing, build resilience and create adequate global governance.

In an effort to continuously help customers understand and protect themselves from risk, Zurich began participating as a key industry consultant in a "first of its kind" public-private partnership by the University of Maryland and the National Institute of Standards and Technology (NIST). The partnership embarked on a research project to assist companies ascertain the effectiveness of their information security and cyber supply chain best practices, with an end goal of helping organizations increase their cyber risk assessment and management capability. The project built on an existing Cyber Risk Portal, which collects data by allowing participating businesses to anonymously upload information to compare their cybersecurity capabilities to the existing NIST Framework, as well as to their peers and competitors.

To further assist businesses with their security and privacy risk management, Zurich is also collaborating with Deloitte to help improve a company's cyber resilience. Policyholders can complement Zurich's cyber coverage with pre-breach cyber risk assessment and

management services through Deloitte to understand their level of cyber exposure and resilience. These services include standards-based risk assessment of an organization's threat detection and incident response capabilities, as well as risk mitigation recommendations. This is just one area where Zurich is focusing on cyber risk mitigation rather than solely risk transfer.

Insurance Issues

Data Breach Uniformity. Because there is a myriad of state laws governing data breach, we are interested in a national, uniform standard on data security and breach notification. While this is not directly in the jurisdiction of this committee, it is certainly relevant for you as Small Business Committee Members to recognize the complexity of cybersecurity governance from a business perspective. We appreciate the efforts of Congressman Luetkemeyer in this regard.

Cyber Accumulation. A challenging issue for all insurers is cyber accumulation. Given the cyber interconnectedness of potential data loss, business functions, and supply chains, the ability to quantify exposures, accurately price risks, and manage accumulations and capital requirements will remain a difficult issue for the insurance community for the foreseeable future.

Cyber as a Peril. Zurich is contributing to the public dialogue around interconnectivity and the full range of exposures from cyber as a peril. The extent of exposures presented by a cybersecurity event is beyond the current scope of coverage. For example, physical damage is rarely offered on a cyber insurance policy, but can result from a cyber attack. The full range of the exposure is too broad to be covered by the private sector; not all causes of loss can be transferred to an insurance policy. Cybersecurity breaches can cause losses including property damage, bodily injury and reputation risk, and we are investigating the best way to consider these impacts.

Conclusion

Zurich continues to refine its understanding of cyber exposures so we can help our customers understand the risk, make thoughtful decisions on our current product, and develop additional insurance solutions going forward.

With data breach, ransomware and other attacks on small businesses occurring daily, we appreciate your focus on risk management solutions provided by the private sector.

Thank you again for the opportunity to testify today. I look forward to answering your questions.

RAA
REINSURANCE
ASSOCIATION
OF AMERICA

STATEMENT

1445 New York Avenue, NW
7th Floor
Washington, D.C. 20005
202/638-3690
www.reinsurance.org

TESTIMONY
OF

ERIC CERNAK
VICE PRESIDENT, U.S. CYBER AND PRIVACY
RISK PRACTICE LEADER
MUNICH RE AMERICA

FOR

THE REINSURANCE ASSOCIATION
OF
AMERICA

AND

PROPERTY CASUALTY INSURERS
ASSOCIATION
OF
AMERICA

HOUSE SMALL BUSINESS COMMITTEE

HEARING ON

PROTECTING SMALL BUSINESSES FROM CYBER ATTACKS: THE CYBERSECURITY INSURANCE OPTION

July 26, 2017

Chairman Chabot, Ranking Member Velázquez, and members of the Committee, thank you for inviting me to testify. My name is Eric Cernak, and I am Vice President U.S. Cyber and Privacy Risk Practice Leader at Munich Re, US. Munich Re provides a range of reinsurance and insurance solutions through various companies that are part of the Group. In the U.S., Munich Re provides cyber- and privacy-related insurance for small businesses through Hartford Steam Boiler Group (HSB) headquartered in Hartford Connecticut. HSB has an A++ (Superior) financial strength rating from A.M. Best Company and has underwritten cyber reinsurance and insurance for over 12 years. Small business cyber insurance clients are served by over 1,500 HSB employees in our Hartford office and regional offices throughout the U.S.

I am testifying today on behalf of the Reinsurance Association of America (RAA) and the Property Casualty Insurers Association of America (PCI).

The RAA is the leading trade association of property and casualty reinsurers doing business in the United States. RAA membership is diverse, including reinsurance underwriters and intermediaries licensed in the U.S. and those that conduct business on a cross border basis. The RAA represents its members before state, federal and international bodies.

PCI is composed of nearly 1,000 member companies, representing the broadest cross section of insurers of any national trade association. PCI members write $202 billion in annual premium, 35 percent of the nation's property casualty insurance. Member companies write 42 percent of the U.S. automobile insurance market, 27 percent of the homeowners' market, 33 percent of the commercial property and liability market and 34 percent of the private workers' compensation market.

Today's hearing is an important discussion to highlight the success of the private sector in developing cyber insurance and to help raise awareness among the small business community about the option of securing cyber insurance, which can offer both preventative, risk-management tools and act as a critical safety net should a cyber event occur. My perspective today is from that of a reinsurer and insurer. Munich Re's Hartford Steam Boiler Group, as a reinsurer (insurance for insurers) for primary insurers, provides reinsurance to share in the risk of loss, helps primary insurers underwrite cyber risk and develop products, and provides other services to primary insurers that are writing, for example, cyber insurance specifically for small businesses. HSB, as a primary insurer, also offers cyber insurance and services directly to customers (via brokers and agents).

ORIGIN AND DEVELOPMENT OF CYBER INSURANCE

Cyber is a rapidly evolving risk and reinsurers and insurers continue to develop products to meet the increasing demand and needs of the insureds, including small businesses. The magnitude of known attacks, development of new technologies and security measures to protect against such attacks are growing dynamically. As reported by Risk Management Solutions in its 2017 Cyber Risk

Landscape Report, the number of large magnitude data exfiltration events has grown substantially in the years prior to 2016 (with 2016 showing some recent flattening of incident rates). To protect against these threats, companies are increasingly investing in their own cybersecurity systems. And, per the RMS report, global expenditure on cybersecurity is estimated to have grown 14 percent year-on-year, from $75B in 2015 to $86B in 2016.

According to a report published last month by Aon titled, "Global Cyber Market Overview, Uncovering the Hidden Opportunities," the global stand-alone cyber insurance market in 2016 was around $2.3 billion in premium, up from $1.7 in 2015, and the U.S. accounted for 90% of the 2015 market. The report noted that "the market is still believed to be in its infancy and penetration levels are still relatively low." It estimated that globally "over 75%" of certain large businesses but "less than 5%" of small and medium-sized businesses secured some cyber insurance. In the U.S., around 19% of small businesses secured some cyber insurance. Aon's report projected that the U.S. stand-alone cyber insurance market gross written premium will continue to grow at 30% per year and could more than triple from 2015 to 2020, from $1.5 billion to $5.6 billion.

More insurers have become interested in offering cyber insurance over time. Less than a dozen insurers offered some cyber insurance in the early 2000s compared to more than 70 in 2016. Reinsurance risk transfer options for insurers with regard to cyber may also become increasingly available. Aon's report mentioned another study by Aon Benfield that "estimates the 2015 global reinsurance market to be worth c. $525m in annual premium." Further, "more than 15 reinsurers actively write standalone cyber treaties and the number is increasing."

Most cyber insurance policies have their roots in liability coverage. Initially, these policies were considered "stand-alone," meaning the business needed to purchase the coverage separately from any other insurance, such as general liability, they might be purchasing, as these policies did not provide explicit coverage for cyber-related losses. The first cyber policies were often expensive, difficult to obtain, and required a relatively cumbersome and confusing application process. For these reasons, the initial success related to cyber policies came from the larger end of the market—Fortune 1000 companies—and provided limits generally ranging from $10M to $25M+.

Early on, many insurers required the applicant to submit to an external data system penetration test. The results of the test were then submitted as part of the insurance application. As cyber insurance became more prevalent, most insurers dropped the penetration test requirement and focused on the application. As the market has evolved, it is now possible for an insured to obtain up to $5M in coverage by answering as few as 4-20 questions.

As more attacks on larger businesses occurred and media coverage increased, smaller business began to take notice of the exposure. The insurance market responded by creating cyber insurance endorsements, which is simply an insurance product that is added

to policies the small businesses were already purchasing, such as their business owners' policy or commercial property policy. Business owners' policies typically cover small business property and liability exposures in one simple insurance package, and commercial property policies typically cover the property exposures of larger businesses. A cyber insurance endorsement can cover various exposures not addressed by Businessowners' or Commercial Property policies by providing coverage for costs resulting from a breach of personal information, cyber extortion, transmission of a virus to another entity, breaching another entity's propriety information, etc. These endorsements afforded the insured a streamlined product and application process (generally an application is not needed for base limits), and lower premium for a commensurate limit (e.g. $100,000). Often these cyber endorsements could be automatically quoted without the insured ever completing an application—greatly simplifying the process.

With either the stand-alone cyber insurance policy or the endorsement approach, a significant part of the value proposition is the value-added loss prevention services that can be "bundled" into the policy to reduce the insureds' exposure. For example, a cyber insurance policy could include risk-management services such as vulnerability assessments, next generation firewalls, IT security audits, and intrusion detection/penetration testing. These were ranked as a the top five most helpful services related to cyber insurance in a 2016 survey of small businesses conducted by Hartford Steam Boiler.

In that same survey, 36% of participants gave three reasons why they did not purchase cyber insurance. The number one reason given was that they claimed they did not need it. The second was the expense of coverage, and the third was that the process was too complicated and confusing. These results suggest that education is key to increasing the take-up rate of cyber insurance by small businesses, particularly given that 86% of the respondents stated that they store Personally Identifying or Personal Health Information.

HOW TO INCREASE THE TAKE-UP RATE OF CYBER INSURANCE BY SMALL BUSINESS

The small business objections to cyber insurance noted above, two of the three speak to the misunderstanding of the value proposition of cyber insurance relative to the exposure. Small businesses would benefit greatly from better understanding the risks presented to their operations by cyber-related exposures and the cyber insurance option to address those risks. Almost every business now relies upon at least one computer to conduct business, whether it is for accepting payments, designing parts, or servicing customers. It is important for small businesses to better understand their reliance upon technology and the impact to their operations should it not perform as expected due to a cyber event.

The public and private sectors have a role to play in helping businesses, small and large alike, to overcome the "it won't happen to me" mentality and constructively address cyber vulnerabilities while preparing for the aftermath of a cyber event. Cyber attacks

may not be a matter of "if" but "when." It is essential for businesses, which are increasingly interconnected, to be prepared, protected, and resilient, and insurance can help with all three. Businesses are no longer being attacked solely for the data they have but increasingly for the access to larger businesses with which they conduct business. This exposure is now being recognized by larger companies as they frequently require smaller business partners to carry cyber insurance as part of their contractual relationship.

In addition to education efforts, the insurance marketplace needs to continue to refine the process and coverage to reduce the complexity associated with purchasing cyber insurance. One significant challenge is that the terminology in a coverage form can vary greatly from insurer to insurer, thus making it harder for an applicant to understand what is covered in different policies. Last year, Munich Re's Hartford Steam Boiler Group participated in a Treasury-led project to develop a glossary of cyber insurance terms to help simplify and standardize cyber insurance terminology.

LIABILITY THAT MAY STILL BE PRESENT EVEN IF AN INSURED PURCHASES CYBER COVERAGE

As previously discussed, the terminology used in coverage forms can vary greatly from insurer to insurer, which makes understanding coverage difficult when a business is evaluating its needs.

Typical cyber-related coverages can include:

- Data Breach Response
- Data Breach Liability
- Computer attack
- Network Security Liability
- Media Liability
- Cyber Extortion
- Misdirected Payment Fraud (e.g. Business Email Compromise)
- Fines and penalties (may not be insurable in all jurisdictions)

Some cyber policies also are beginning to examine and/or address the exposure related to:

- Property and bodily injury resulting from a cyber event
- Failure of the Internet and the potential impact to business operations

However, the insured may still need to examine other policies for potential coverage for cyber-related exposures. These other policies may include:

- Crime
- Directors & Officers (which covers legal actions against top company executives)
- Contractual Liability (which protects a policyholder from liabilities assumed under a contract)
- Technology Errors & Omissions for exposures resulting from IT products the insured creates

MINIMUM SECURITY EXPECTATIONS FOR OBTAINING COVERAGE

Where an application is required for a cyber product, insurers may want to understand if the applicant complies with various security requirements (when applicable for the industry in question) such as the Payment Card Industry Data Security Standard (PCI-DSS), Health Information Technology for Economic and Clinical Health Act (HITECH), Gramm-Leach-Bliley Act (GLBA), Red Flag Rule, and Sarbanes-Oxley.

Additionally, from a technical perspective, many applications will inquire about encryption being deployed, systems patching cadence, back-up procedures, password management, firewalls installed, anti-malware software, intrusion detection/protection devices deployed, etc.

However, there is growing recognition that strengthening companies' security culture, embodied by various policies (privacy/security and document retention/destruction), criminal and credit checks conducted on employees, and robust training programs, deserves strong consideration as part of the underwriting process. This also is supported by the above-referenced Hartford Steam Boiler survey finding that nearly half (47%) of all data breaches were attributed to a vendor/contractor, followed by employee negligence or malfeasance (21%), and lost or stolen mobile device (20%). Hacking or other cyber-attack only represented 11% of data breaches.

By contrast, when no application is needed for an endorsement-based cyber product, often the form may contain language stating that the insured needs to comply with reasonable and industry-accepted protocols. These protocols may include:

- Providing and maintaining appropriate physical premises, computer, and Internet security
- Maintaining and updating at appropriate intervals backups of computer data
- Protecting transactions, such as processing credit card, debit card and check payments
- Appropriate disposal/destruction of files containing sensitive personal or corporate information/data

HOW INSURERS DETERMINE COVERAGE AND PRICE

Cyber insurance is unlike most other insurance coverages in four fundamental areas. Insurers are grappling with the following factors in offering cyber coverage and at what premium/limit.

There is no significant historical loss data.

The exposure is relatively nascent as the Internet has only been commercially viable since the late 1990's. Further, the loss data generated even 10 years ago does not fully represent the exposure today. For example, virtual currencies and smartphones did not exist 10 years ago.

Due to the lack of loss data, insurers have adapted pricing, terms, and conditions from other lines of business, such as tech-

nology errors and omissions, crime, media liability, etc. Some insurers also have looked to conduct primary research and have interviewed experts in various fields, including IT forensics, attorneys, breach response service providers, public relation firms, and others. Through this process insurers can better understand the frequency of events, how long events may take to address, and the associated costs for the various services. These figures are then converted into insurance premiums. As experience develops, these initial figures can be blended with the actual insurance claims results to refine the premiums being charged.

Another tool insurers have deployed to improve cyber insurance products and pricing is the survey of potential customers (e.g., business owners) to understand specific kinds of concerns, the frequency of issues they face, and the costs to address them. This helps insurers prioritize which coverages to develop and include in a cyber insurance product and determine associated terms and pricing.

The cause of loss is generated by an active adversary, which is capable of changing tactics and targets to suit their needs based on advances of technology.

As new technologies are introduced, exposures that previously did not exist become commonplace. For example, cyber extortion was typically limited in scope to targeted attacks where the attacker threatened to release data that had been stolen or to continue with a Denial of Service attack unless a ransom was paid. These attacks took significant time to conduct and often posed a significant risk to the perpetrator as they needed to interact with the company to receive payment. With the advent of virtual currency, ransomware exploded and is now a leading cause of loss.

Legislative and regulatory requirements continuously evolve.

Insurance companies need to monitor the evolving state, federal, and international privacy and data protection laws. While these laws are designed to protect consumers, they may create an exposure to small business owners. For example, there are 48 different state breach notification/data protection laws with which a small (or large) business must comply. Many of the first cyber insurance policies focused solely on liability exposures of third parties (as opposed to those faced by the entity purchasing the coverage) and only provided a small sublimit (the maximum amount for which the insurance policy would pay for in the event of this type of loss, which is less than the overall limit of the policy) for costs the insured might incur complying with various breach notification laws. As more states followed California in the mid-200's with their own breach notification laws, insurers responded by expanding their breach response coverages.

Cyber poses potential aggregation or accumulation risk for insurers.

Cyber risk is not bound by geography, which greatly increases the aggregation risk from an insurer's perspective.

Many insurers will identify potential causes of aggregation (e.g. particular industry, service providers, failure of the Internet, etc.) and either decide to exclude that cause of aggregation or to monitor the amount of insurance being provided very closely. For example, an insurer may monitor the number of insureds using a particular cloud service provider.

CONCLUSION

As the private cyber insurance market continues to rapidly expand, reinsurers and insurers will continue to monitor and analyze cyber risks, survey and work to better understand the needs of existing and potential customers, develop insurance products and services accordingly, and help insureds following a cyber event. It is equally, if not more important, to U.S. businesses for federal and state governments' lawmakers, regulators, and other entities focusing on cybersecurity and evaluating potential regulatory changes, to develop clear, consistent requirements and to avoid a patchwork of different requirements and standards. Such a patchwork would impede companies' ability to effectively implement cyber security protocols and respond quickly and appropriately to a cyber security event. Although the nature of reinsurance means that reinsurers do not directly interact with consumers, and therefore reinsurers' obligations in the event of cyber security events differs somewhat from the primary insurance industry, the entire insurance and reinsurance industry (as well as consumers) benefit from uniform, consistent standards that are both proportional and flexible enough to work in an ever-changing cyber environment.

We also encourage the Administration to coordinate cybersecurity policy among federal agencies and designate lead agencies to coordinate discussions where appropriate. This should include discussions with state insurance regulators to encourage healthy cyber standards while eliminating conflicts and duplicative regulation.

Thank you for your time and your interest in this very important issues.

Testimony before the Committee on Small Business: House of Representatives

Protecting Small Businesses from Cyber Attacks: the Cybersecurity Insurance Option
H.R.3170 - Small Business Development Center Cyber Training Act of 2017

Statement of:
Daimon Geopfert, Principal and National Leader of Security, Privacy, and Risk at RSM US LLP

Background

Chairman Chabot, Ranking Member Velázquez, and members of the Committee, thank you for the opportunity to discuss the cyber security challenges that have become a constant, material threat within the small business community. My name is Daimon Geopfert, and I was asked to speak today regarding how legislation such as H.R 3170, and private sector solutions such as cyber insurance products, can help small organizations manage cyber risk. I spent almost 14 years within the Department of Defense (DoD) including 12 years as active duty Air Force, officer and enlisted, and two years as a defense contractor building Security Operations Centers (SOCs) for various government agencies. While on active duty, I was a secure communications specialist, a Computer Crimes Investigator (CCI) with the Air Force Office of Special Investigations (AFOSI), and a cyber specialist within the Air Intelligence Agency. Since leaving the DoD, I have spent the last ten years as a security consultant, initially with a "Big 4" firm and now as a principal with RSM US LLP ("RSM"), where we specialize in cyber security consulting within small and middle-market businesses. My specializations include ethical hacking, security monitoring, digital forensics, incident response, and malware analysis.

During my career, I have participated in hundreds of security assessments and cyber intrusion investigations for small businesses. Because of my role, I am often in a position to witness every stage of an attack within these organizations, including the devastating economic and emotional impacts that often linger after the technical aspects of the issue are resolved. On more than one occasion, I have had to sit with a client, who is often uninsured, explain to them the extent of a breach, and listen to their anguish as the realization sets in that their business might not survive the costs related to an incident. In my profession, there are few things more painful than listening to a client debate how they are going to inform their employees that they will soon be unemployed, or to listen to

a family-owned business lament that their legacy, which might span generations, will simply cease to exist.

Purpose

I am here today in the hope that my experiences can play some small part in addressing this issue, which appears destined to be a continuous, ever increasing threat to the U.S. economy. My role has allowed me to observe the many weaknesses that, if corrected, would have an exceedingly positive impact on a small business ability to prevent, or at least survive, future incidents. These organizations want to do the right thing, even if out of simple self-preservation, but they often lack the means to acquire the necessary resources to actually understand and execute what must be done. What is needed is a venue through which small businesses can find simple, direct guidance on how to protect their environments and mitigate risk, and that also provides access to resources with the necessary expertise to chaperon them through implementation of that guidance.

Legislation such as H.R 5064 and H.R. 3002 were both early attempts by this body to modify the Small Business Act to allow the Small Business Development Centers (SBDCs) to begin serving such a role. The current H.R. 3170 legislation addresses part of this requirement by essentially creating "cyber mentors" within the SBDCs. These personnel could quickly become the front-line advisors that are desperately needed to guide small businesses through the deployment of technical security solutions as well as administrative risk management techniques such as acquiring cyber insurance. It should be noted that this is very close to the how the Cyber Essentials program works within the United Kingdom. This approach has proven to be quite successful at mentoring small businesses through a basic cyber hygiene program including acquisition of cyber insurance.[i] Not providing access to resources of this nature is no longer a viable option, as it is essentially conceding that approximately half of the U.S. economy should be left to defend themselves against highly skilled attackers in search of money, intellectual property, and nation-state political advantage.

Current State

While serving within the Department of Defense, I had unfortunate opportunities to witness how aggressive, persistent, unpredictable, and innovative cyber attackers can be. After leaving the DoD, within two years I saw these same perpetrators appearing within my private sector clients. Understand that these attackers were skilled enough to give the DoD pause, much less the IT teams within small business and the middle-market. In reality, the situation is even worse than that which I faced within Defense

networks at the time I transitioned. Historically attackers were limited by the extent of their own personal expertise. Now, hacking experts consolidate their skills into pre-packaged "kits" available to anyone who can find their way into the underground market and scrape together a few thousand dollars. Each of these packages comes with full tech support, simplified graphic interfaces, and detailed, easy to follow guides meant to allow a relative newcomer to become "pseudo-elite" virtually overnight. This has significantly lowered the knowledge threshold necessary for someone to act like a world-class hacker, and has increased the number of attackers going after U.S. business by order of magnitude. We are basically facing an army of highly effective "cyber soldiers" who have no actual understanding of what they are doing or how their tools work, but they do know if they point it at an company and click the correct buttons, they almost magically make money.

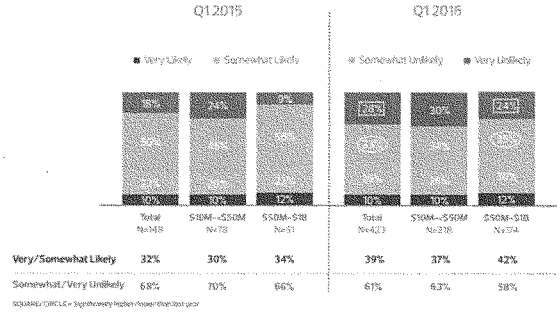
The reality for small and middle-market companies is that the Internet has reached a fundamental, "utility" type status, as it is now a required piece of infrastructure for almost any organization to be successful in our modern economy. However, this powerful asset that is essentially required for branding, sales, management, and growth, is also incredibly hostile and toxic to systems, networks, and users. U.S. small businesses face a situation in which they are required to use an environment that is highly likely to damage, or even destroy, the finances, assets, and reputations of their corporation or those of their customers. Arguably, for the first time in our economic history, a major portion of a business' effort and expense is consumed by something that has very little to do with their core business but is required in order to exist. Small business are being forced to be become IT and cyber experts in addition to trying to establish, deliver, and expand their core services. This model can work for large organizations, but it does not scale to small businesses.

While a wide array of security software, hardware, and frameworks are available, small organizations typically lack the resources to properly acquire and deploy them. Many tools and frameworks are built for large organizations with significant funding and on-hand IT resources. Many of these do not scale down well to fit small and middle-market businesses, and the "lightweight" and open source tools that might be cost-effective for small organizations often require extensive IT and security knowledge to properly deploy.

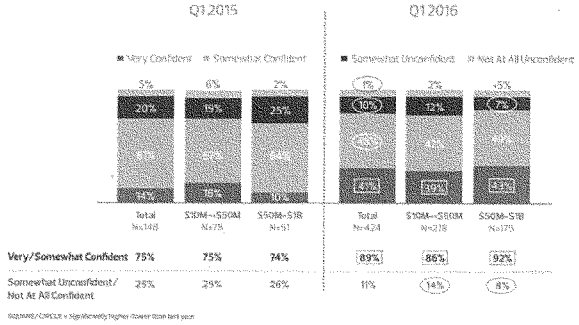
Cyber insurance has gradually assumed an important role in this process, but the current state of security governance within small organizations limits the benefits and uptake of this risk mitigation method. Many organizations simply do not understand the likelihood that they will be breached, and often severely underestimate the damages if such an incident were to occur. Much of this is an issue with education as extensive coverage of "mega breaches" such as Target has led many small and middle-market organizations to

rationalize to themselves that they are too small for attackers to notice. RSM participated in two keystone studies this past year that highlight how drastic the gulf is between perception and reality in regards to cyber threats to small businesses. In the first study, RSM surveyed more than 700 executives within American small and middle-market companies to assess a variety of economic and business factors influencing their planning for the coming year.[ii] Included in that survey was a series of questions regarding cyber security. More than 60 percent of these organizations felt that it was unlikely that an attacker would attempt to attack their business systems, and approximately 90 percent of the respondents felt that their currently deployed controls would be successful in preventing such an attack. This was almost a 15 percent increase over the prior year, which shows that small organizations do not perceive themselves as being targets and do perceive themselves as being relatively skilled at cyber defense.

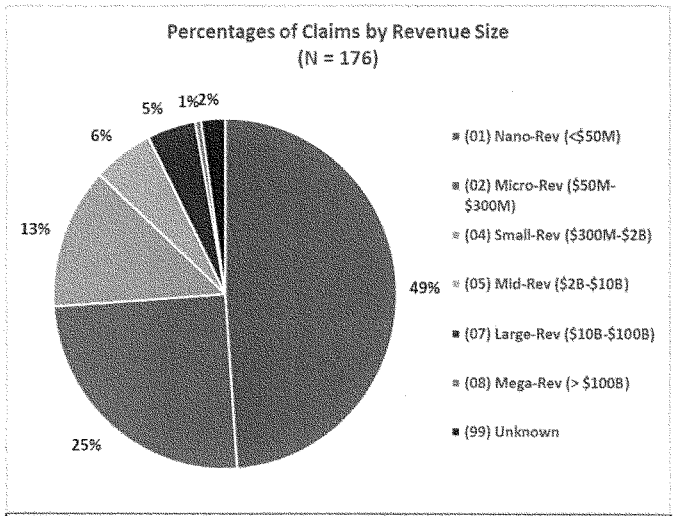
LIKELIHOOD UNAUTHORIZED USERS WILL ATTEMPT TO ACCESS SYSTEMS



CONFIDENCE IN MEASURES TO SAFEGUARD DATA



Regrettably, the reality of the situation cannot be further from this illusion of confidence. In the same time period in which RSM was surveying small business executives, we teamed with the analysis group NetDiligence to perform extensive data mining within a population of cyber insurance claims.[iii] That review showed that approximately 75 percent of cyber insurance claims submitted over the period of the study were for organizations under $300 million in revenue. Approximately 50 percent of the claims were for organizations $50 million in revenue, and the damages reported for these small businesses were similar to the damages occurring in organizations tens, or even hundreds of times larger.



	Total Costs (including SIR)				
	Cases	Min	Median	Mean	Max
(01) Nano-Rev (<$50M)	85	290	49,000	215,297	7,130,000
(02) Micro-Rev ($50M-$300M)	44	1,000	88,154	487,411	6,570,000
(04) Small-Rev ($300M-$2B)	23	4,178	118,671	599,907	5,650,000
(05) Mid-Rev ($2B-$10B)	9	2,662	91,457	173,851	678,000
(07) Large-Rev ($10B-$100B)	8	1,603,800	3,326,313	5,965,571	15,000,000
(08) Mega-Rev (> $100B)	1	11,491,000	11,491,000	11,491,000	11,491,000
(99) Unknown	2	7,338	9,482	9,482	11,625
	172				

These percentages had actually increased over the analysis performed the prior year, which shows that attacks against small business are not an anomaly; they are the norm. This is the key demographic targeted by hackers, and the aggressiveness of their attacks is increasing. Yet at the same time, confidence levels of small organizations were

approaching an all-time high. This leads to a type of cognitive dissonance in which small organizations acknowledge that cyber-attacks have become ubiquitous and highly potent, but, at the same time, they convince themselves that they will not be targeted, and if they are, they feel that their defenses would fend off any malicious actions. This extreme inability to accurately quantify their risk leads many small organizations to determine that allocating precious resources toward security solutions and cyber insurance is unnecessary. This leaves many organizations operating without any type of fiscal safety net meaning they would carry the full brunt of any expenses, bank account thefts, ransoms, civil damages, and fines stemming from an incident. As multiple studies have shown, even a single incident will put approximately 60 percent of small organizations out of business within six months. [iv]

However, even when a small business has acquired insurance, in the event of an incident the generally immature nature of their security controls often greatly compounds costs for both the victim and the insurance carriers. They simply are not ready for the process of going through an incident. They assume that they will know very quickly when they have been breached, but independent research by multiple security firms over the last five years indicates that an attacker will likely be inside an organization for 200-300 days before they are discovered. This means many organizations will build their response plans assuming they can prevent damage, but, in reality, they need to be skilled at performing post-facto accounting of what hackers did while they were within an environment. Lack of proper logging means that an organization might know that an attacker was in their environment but be unable to reconstruct the story of what that attacker touched, where they went, and what they took. This puts many small organizations in the position where they must assume the worst, and perform mass notifications to any individuals that theoretically might have been impacted, where larger, more mature organizations often have the evidence available to properly allocate the hacker's activities and, therefore, greatly reduce the size of the reported breach. Because small businesses often lack formal incident response planning, when they do become aware of an issue, they often attempt to address it themselves using a variety of unplanned activities that usually damages or destroys what little evidence might have existed. These are the major contributing factors why data breaches are inordinately harmful to small organizations, as they often must pay damages based on assumed worst-case events. This also leads to cyber insurance carriers often having difficulty pricing the risk that small organizations represent. It is difficult to justify premiums and deductibles that are tolerable for organizations with small revenue, when those same companies can easily generate damages equal to organizations an order of magnitude larger.

Requests

To make tangible progress on this issue, small businesses need ready access to resources and information that is currently unavailable to them because they often cannot afford dedicated personnel with the necessary knowledge and skill-sets. Legislation such as H.R. 3170 can start the process to create a cadre of trained personnel within SBDCs who can directly mentor these small businesses that are so critical to the sustainment our economic future. These personnel can essentially become "virtual Chief Information Security Officers" across entire groups of small businesses. Currently, small businesses attempt to acquire security guidance through a variety of security vendors and consultants, but many of these groups have trouble "scaling down" their guidance to be appropriate to environments that do not have the scale and resources of a Fortune 500 organization. Cyber counselors within the SBDCs would be relatively unique within the security community in that they would be solely focused on planning and deploying cyber strategy that is efficient and pragmatic for small businesses. Because their role allows them to interact with a large number of companies, the SBDC counselors become a de facto knowledge sharing center carrying best practices from one business to another. They would see in real-time what technologies and processes are effective within a small business, and which ones are not.

While educating and deploying a "first line" of security advisors within the SBDCs is a critical first step, these facilities hold the promise of a myriad of other benefits that could be made available in the future. Again, to make material progress on this issue we need to move toward clear, concise, pragmatic solutions. While it might seem like an abnormal suggestion, a primary goal of the SBDCs should be to emulate their peers in the hacking community. We are currently lacking the process on the defensive side that exists on the aggressor side, in which relatively non-technical individuals can become highly effective in a short period of time. As mentioned previously, the underground markets have become exceptionally efficient at quickly churning through masses of unskilled individuals with limited technical knowledge and producing a large number of, while not elite, at least functional cyber attackers.

Similar to the methods of our adversaries, small and middle markets need a dedicated hub where they can find useful, cost-effective tools and simple, pragmatic guidance on how to deploy security solutions that, while not elite, are at least complete and effective at a basic level. Existing frameworks from organizations such as the National Institute of Science and Technology (NIST) are high-level and extensive which might be appropriate for large organizations, but they are of little to no value to small organizations that require

low-level, step-by-step guidance on how to achieve some moderate baseline for security. In conversations with executives within the small and middle market regarding my testimony today, this is far and away the most frequent request. What they are looking for is what the security community would describe as "reference environments", which are top-to-bottom, detailed layouts of basic networks with common security controls. As an example, reference environments can be created for networks that are exclusively on-premises, those they rely heavily on cloud solutions, or almost any other model that is common within the small business community. In addition, versions can be quickly adapted to reflect the needs of businesses within specific industries such as retail, manufacturing, and healthcare. These reference environments often detail what security solutions must be deployed, how they must be configured, how data should flow through the network to maximize protection, how users, customers, and third parties should be granted access, and any number of common security requirements. While it sounds relatively simple, these types of assets are not common in the small business community, which often leads to organization cobbling together their security architecture based on their individual interpretations of high-level frameworks that are often more academic in nature than they are prescriptive. The SBDCs could play a critical role in the process of creating and disseminating such models.

The benefits of deploying such common models extends well beyond the immediately visible increase in technical security. As an example, the second most common request during my conversations with executives was for actionable cyber threat intelligence that could be easily consumed and put to use by a small business. This would include notifications of known bad IP addresses and URLs, signatures for new malware and exploits, and Indicators of Compromise (IOCs) that would alert an organization to the presence in their network of known hacking groups. Currently it is extremely difficult to meet this need because information must be shared in high-level, agnostic formats that can be used by a wide variety of organizations. If common reference environments are made available to small businesses, many of these entities would be highly interested in using those frameworks if they knew that it would allow them to access and use real-time threat intelligence in an almost "plug and play" fashion. The development of such reference environments would require extensive cooperation between the government and private sector entities, and a designated coordination and distribution point of threat intelligence, both of which are obvious roles that could be played by the SBDCs. It should be noted that support of this type was included in the prior H.R 5064 legislation that passed in this Committee last year, but has still not been acted upon in the Senate.

This could eventually lead to the SBDCs acting as the primary coordinator between the small business community, government, and private sector security vendors in creating a

set of approved solutions and services that are "right sized" for small businesses. Potential future legislation could even allow the SBDCs to negotiate with the security industry to purchase solutions "in bulk" for use by pools of small businesses. Currently, each small business individually negotiates with a wide variety of security vendors and consultants, which creates wildly inconsistent pricing and results. While this is always an option for organizations that feel that they are mature, sophisticated buyers of these services, many other organizations would gladly accept assistance from a community of similar consumers. With an entity such as the SBDC doing "pooled" pricing to drive down costs and standardizing the level of services, the small business community would have access to much more cost-effective solutions that would also produce more consistent results. These benefits can be further expanded if the SBDCs coordinate with the private sector security industry so that versions of their cyber solutions can be certified as being compliant with the reference environments. This would allow small businesses to acquire services knowing that they are an appropriate fit for their organizations, while also allowing security vendors to cater to a large pool of potentially new clients. It would be a classic "win/win" situation for all parties involved.

At this point the foundations would be laid for a base level security accreditation program for small business in which they can demonstrate that they have deployed basic cyber security controls and processes. This would be very similar to the UK Cyber Essentials program. The SBDCs, which at that point would be acting as a centralized body in publishing the reference environments and coordinating with private sector security vendors, would be a natural fit to oversee this program. An outcome from this approach would be that the SBDCs could then coordinate between newly accredited small businesses and insurance carriers to facilitate the acquisition of cyber insurance for these organizations. These suggestions create a process that would then naturally flow from a set of standardized security templates, through approved, cost-effective technologies that meet those templates, to an accreditation program that validates that the solutions were deployed correctly, and finalizes with the purchase of cyber insurance to offset the residual risk. This process, in its entirety, represents the most requested types of support by small business executives encapsulated in a clear, concise, and pragmatic approach, and it would materially improve the current security status of approximately 50 percent of the U.S. economy. [v]

While the development of such a standardized process will deliver the most significant results over the long-term, it must be recognized that there are several other immediate, tactical needs that the SBDCs could also address in the near future. Of specific importance is the facilitation of security training within small businesses. Prior legislation, such as H.R 5064, was aimed at starting this process by making security awareness

training available to the employees of small businesses to reduce the likelihood that they would fall for common types of social engineering. While this type of training is extremely beneficial, the concept of performing training through the SBDCs could be greatly expanded. As mentioned previously, the core issue preventing small and middle market companies from becoming properly secured is the inability to acquire access to trained security personnel. While government programs can provide significant assistance to these companies, the beneficial impact will always be limited until small businesses can develop or hire their own security resources. However, the reality of today's jobs market means that these trained individuals are rare, expensive, and difficult to retain for any extended period of time. Recent studies by the U.S Department of Commerce and NIST show that of the entire U.S. workforce considered to be trained cyber security personnel, enough job openings exist that half of that workforce could quit their jobs today and have new employment tomorrow. In further detail, the study showed that the number of positions that request the most respected security certifications outnumber the total population of personnel that have those certifications by as much as 2 to 1 in some cases.[vi] This critical skills gap prevents small and middle market companies from acquiring top security talent, which then drives the need for them to develop their own. H.R. 3170 is written to provide cyber security training to counselors within the SBDCs, but similar future legislation could follow the same model with the goal of providing training directly to the IT personnel within small businesses. This could be as simple as basic "how to" guides for common tasks such as deploying patch management and access control systems, or could be as robust as coordinating with the private sector to offer reduced prices or subsidized versions of critical training programs such as those for incident response and secure network architectures.

My final point is a request meant to address an issue that is easily the most tortuous and aggravating for small business. While this might be through the SBDCs or through some other mechanism, it would be highly useful to have a designated, prescribed method through which small businesses can coordinate with a law enforcement entity that is responsive and functional when it comes to cyber breach matters. Currently, when a small business is compromised, they are often given two potential choices. They can contact their local police departments which are usually willing to help but lacking in the skills to do so, or they can contact the Federal Bureau of Investigations (FBI) or U.S. Secret Service (USSS) who have the ability to help but typically do not have the availability to do so unless the breach has extremely substantial damages. Imagine the frustration felt by a small business owner who has suffered what might be an "end of going concern" level incident, then realizing that they are essentially on their own because the law enforcement entities that will help lack the skill-sets to do so, and the law enforcement entities that have the skill-sets are not willing to do so. This situation has

created the mindset within the small business community that, when it comes to cyber matters, they have essentially been abandoned in the "wild west" where the rule of law does not apply. It would be extremely beneficial for a process to be put in place to give small businesses rapid access to a law enforcement entity that can, and will, support their response. This is not to suggest that the goal of this support is to end every incident with an arrest and prosecution. With the simple reality that many attackers are operating out of geographies where the U.S. has no jurisdiction, it is not reasonable to assume that arrests would be common. The goal of this law enforcement involvement is to facilitate rapid and complete investigations of issues so that damages can be reduced as much as possible. As an example, it is common during an incident investigation to discover that attackers were coming from another system within the U.S.. If a small business does not have the proper logging and other sources of evidence necessary to reconstruct the entirety of a breach, and therefore know the true extent of data loss, there is often the chance that the necessary evidence is located on the system from which the attacker entered the environment. The ability to get a law enforcement entity involved quickly can mean search warrants might be used to gather logs, files, or other artifacts from internet service providers (ISPs), systems in other companies, or systems owned by individual citizens. We often try to perform these actions today, but the process is so time consuming that viable evidence is often lost before we can acquire it.

Legislation that addresses the points I have described above would greatly improve the security and longevity of U.S. small and middle market businesses. These entities are the core of U.S. growth and job creation, but they are under daily siege from cyber adversaries. If our political institutions cannot find a way to assist these organizations, the U.S. economy, and arguably our role as the premier member of the global economy, will be under dire threat for the foreseeable future.

Conclusion

Mr. Chairman, this concludes my statement. I would be happy to answer any questions you or other members of the Committee might have.

The views expressed herein are those of Mr. Geopfert, and are not necessarily those of RSM US LLP.

RSM

Daimon E. Geopfert

National Leader and Principal, Security, Privacy, and Risk Consulting
Risk Advisory Services
RSM US LLP
Chicago, Illinois
daimon.geopfert@rsmus.com
+1 312 634 4523

Summary of experience

Daimon Geopfert specializes in penetration testing, vulnerability and risk management, security monitoring, incident response, digital forensics and investigations, and compliance frameworks within heavily regulated industries. Daimon has over 20 years of experience in a wide array of information security disciplines. He serves as the firm's national leader for the security, privacy, and risk practice, responsible for the development of the firm's overall strategy related to security and privacy services and applicable methodologies, tool kits and engagement documentation.

Daimon is a regular presenter for organizations such as Information Systems Audit and Control Association (ISACA), InfraGard, the Certified Fraud Examiners and SC Magazine's World Congress. He has been quoted in a variety of publications, including The Wall Street Journal, Fortune Magazine, The Washington Post and the Kansas City Business Journal.

Representative experience

- Information systems security assessment
  Daimon has served as the manager and lead technician for security assessments performed on some of the largest corporations and government entities in the world. He has designed and implemented testing frameworks and methodologies used to properly capture and communicate the technical, operational and regulatory impact of identified security weaknesses.

  Daimon's experience in this area includes analyses and reviews of the following:

  - Security testing across the enterprise: network, host, application and database
  - Wireless, Voice over Internet protocol (VoIP), cellular, modem/telco assessment
  - Security operations structure and effectiveness
  - Social engineering testing, including phishing/pharming, phone and physical
  - Corporate security policies and procedures
  - Application secure architecture and coding analysis

- Incident response, forensics and security monitoring
  Daimon acts as the lead developer for RSM's forensic and monitoring service offerings, and has designed and deployed incident response and security monitoring programs within several highly regulated clients. These frameworks are based on customized versions of National Institute of Standards and Technology (NIST) SP800-81, ISO 18044:2004 and the SANS IR 6 Step. Daimon previously served as a special agent with the Air Force Office of Special Investigations as a researcher with the CIA's Directorate of Science and Technology, and deployed and ran Security Operations Centers for the Department of Defense (DoD).

- Security program management
  Daimon has managed and performed a myriad of security program engagements across a variety of industries. The purpose of these projects was to assist organizations in deploying efficient, manageable and cost-effective solutions and processes that would address the wide ranging business and regulatory aspects of IT security. Daimon has deep experience in Payment Card Industry (PCI), HIPAA/Health Information Technology for Economic and Clinical Health (HITECH), FFIEC/Federal Deposit Insurance Corporation (FDIC), Federal Information Security Management Act (FISMA), NIST SP800 series, ISO 2700X, National Information Assurance Certification and Accreditation Process (NIACAP)/DoD Information Assurance Certification and Accreditation Process (DIACAP), American Electric Reliability Corporation(NERC)/Critical Infrastructure Protection (CIP), EU Data Privacy Directive, and various state security and privacy laws.

Professional affiliations

- Information Systems Audit and Control Association (ISACA)
- International Information Systems Security Certification Consortium (ISC)²
- FBI InfraGard, Michigan Chapter—Member, Presenter, Speaker Committee
- The SANS Institute—Global Information Assurance Certification (GIAC)
- The Ethical Hacker Network

Professional certifications

- Certified Information Systems Security Professional (CISSP)—(ISC)²
- Certified Information Security Manager (CISM)—ISACA
- Certified Information Systems Auditor (CISA)—ISACA
- GIAC Certified Incident Handler (GCIH)—The SANS Institute
- GIAC Certified Reverse Engineer of Malware (GREM)—The SANS Institute
- Certified Ethical Hacker (CEH)—EC-Council

Education

- Master of Science, computer science, University of Michigan
- Bachelor of Science, computer science, United States Air Force Academy
- Numerous technical and industry courses and seminars

---

[i] IASME Consortium, "Automatic Insurance Cover "https://www.iasme.co.uk/cyberessentials/automatic-insurance-cover/

[ii] RSM, "US Middle Market Leadership Council Survey Report" (http://rsmus.com/pdf_download/rsm_middle_market_leadership_council_survey_may_2016.pdf)

[iii] NetDiligence, AllClear ID, RSM "2016 Cyber Claims Study" (https://netdiligence.com/wp-content/uploads/2016/10/P02_NetDiligence-2016-Cyber-Claims-Study-ONLINE.pdf)

[iv] U.S. Securities and Exchange Commission, "The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses" - Commissioner Luis A. Aguilar, Oct. 19, 2015 (https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html#)

[v] Small Business Administration, "Small Business Trends" (https://www.sba.gov/managing-business/running-business/energy-efficiency/sustainable-business-practices/small-business-trends)

[vi] National Initiative for Cybersecurity Education (NICE), National Institute of Standards and Technology in the U.S. Department of Commerce, "Cybersecurity Supply/Demand Heat Map" (http://cyberseek.org/heatmap.html)

House Small Business Committee

"Protecting Small Businesses from Cyber Attacks: the Cybersecurity Insurance Option"

AIA STATEMENT

July 26, 2017

In today's increasingly interconnected world Cybersecurity is a risk that no business is immune from regardless of industry or size. We appreciate the House Small Business Committee (Committee) holding the hearing. "Protecting Small Business from Cyber Attacks: the Cybersecurity Insurance Option." The comments below are intended to provide a brief overview of cybersecurity insurance and some potential challenges for this market.

As with many other emerging and complex risks, insurance is, first and foremost, a useful targeted risk transfer mechanism. A cyber event can be costly for any business, including small and medium businesses, so minimizing that financial impact through cyber insurance is beneficial. And, just as cyber risks continue to evolve and develop, so has the cyber insurance market. Therefore, a key point is that the insurance market is developing responsibly to meet changing client demands and offering produts tailored to meet small, medium and large business needs.

Approximately 15 years ago, "cyber insurance" originated as a technology errors and omissions product that provided coverage for negligent acts, errors, and omissions in the deliverance of technology products and services. Today, stand-alone "cyber insurance" products may include coverage for forensic activities, legal fees associsated with determining how best to comply with each state or territory's notification rules, notification and credit monitoring costs, business interruption, and damages and expenses incurred in connection with claims brought against a third party, such as costs associated with responding to or defending against regulatory inquires, payment of fines, and lawsuit liability. More recently, some insurers may also offer dedicated cyber coverage for bodily injury or property damage.

Importantly, cyber risk should be considered a peril. Coverage for the cyber peril can be addressed, in whole or part, in a dedicated, stand-alone product or embedded in a multi-risk policy that might include cyber as one of the many causes of loss, for instance a commercial property policy or a directors and officer's policy.

Moreover, cyber insurance can serve as a valuable tool in crafting a risk management program. Hence, communication is an important aspect of the cyber insurance purchasing process. The process typically begins with a conversation with the insurance carrier and with the advice of an insurance agent and broker whose expertise guides the insured in evaluating its coverage needs and

existing insurance products to determine whether insurance gaps exist and how best to address those gaps.

Additionally, cyber insurers continually innovate and offer add-on products and access to strategic partnerships that small business may find invaluable. For instance, many insurers have partnerships with computer forensic firms, public relation coaches, and expert legal counsel. Timing is critical in the event of a breach, therefore, having a list of identified resources could be crucial. As well as post-event resources, pre-event resources may also be important to a small business. For example, risk assessments, employee training, and table-top exercises are useful tools that an insurer may offer.

It is important to note that there are clear business benefits to cyber insurance, as identified above, but cyber insurance should not be seen as a driver of behavior, guarantor of cyber security, or a standard-setting vehicle. Regardless of a business's size, cybersecurity requires an ever-evolving adaptable approach that is incorporated into an entity's overall risk culture and each individual company is uniquely and best able to assess its own risk and global approach to managing cyber exposures and deciding what role insurance will play.

We recognize that small and medium businesses have limited resources and the decision to purchase cyber insurance is one that should remain within the businesses sole discretion. As such, our industry is committed to responsibly meeting market demand and offering innovative solutions that best suit our client's needs.

Therefore, the cyber insurance market should be allowed to grow organically without undue pressure that could stifle innovation and market growth. Rather, through public-private partnerships we should explore solutions for addressing the challenge that confront market growth. Some of these challenges include the following:

- Education - Businesses are not always convinced that they are at risk of a cyber-event. Size and industry may be factors that convince an entity they are not at risk, but unfortunately, today's connected society and supply chain interdependencies makes everyone a target for unscrupulous actors.

- Data and Risk Modeling - The risks presented by the cyber age are new and more rapidly evolving compared to more traditional risks that insures have been underwriting for hundreds of years. Thus, sufficient loss data and risk modeling capabilities, which are critical to responsible underwriting, will need time to develop. Moreover, the risk is continually evolving as bad actors look for new ways to expropriate information and process it for their own purposes.

- Aggregation and Accumulation - As indicated above, coverage for cyber events may be embedded in a number of insurance policy types. Further, cyber is also a global challenge, sometimes without geographic borders or predictable locational centers, thereby increasing the geographic risks broadly. The increasingly interconnected business environment and the ubiquitous presence of cyber in our commercial world also

serves to increase the aggregation and accumulation risks insurers must manage.

- Forensic Review - A lack of actuarial data is not the only data gap that insurers may face. Often times insureds may avoid sharing data such as forensic reports with their insurer in an effort to avoid an assertion that they have waived the attorney client or work product privilege. Though these concerns are understandable, failing to provide forensic information hurts insurance carriers and their clients in two ways: (i) it makes it more difficult to evaluate claims triggered by a cyber-event given that critical information is withheld from the carrier; and (ii) there will be less information available to insurance carriers to aid in risk management and risk transfer solutions for the client and more broadly for the benefit of the cyber insurance market.

Insurers are committed to meeting the challenges of market growth so that they can continue to evolve their product offerings in order to provide risk transfer solut8ions that benefit businesses of all sizes. Thank you for your interest in this subject matter. Our membership is an active participant in the cyber insurance market and we would be happy to discuss this issue and answer any questions that vou mav have.

Respectfully,

Angela Gleason

Angela Gleason
Senior Counsel
American Insurance Association
555 12th Street, N.W.
Suite 550
Washington, DC 20037
202-828-7181

STATEMENT ON BEHALF OF WILLIS TOWERS WATSON

BEFORE THE

UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON SMALL BUSINESS

HEARING ENTITLED, "PROTECTING SMALL BUSINESSES FROM CYBER ATTACKS: THE CYBERSECURITY INSURANCE OPTION"

JULY 26, 2017

On behalf of Willis Towers Watson, we submit the following statement in response to the above-referenced hearing.

Small businesses (SBs) tend to be less concerned about their technology/cyber risks than their publicly traded counterparts. This view may be due primarily to a limited understanding of the scope of risks these organizations face. According to the Verizon Data Brach Repot, approximately 61% of data breach victims are businesses with less than 1,000 employees. With this in mind, here are some of the common misconceptions we found among SBs:

a. ***We're not a target for attackers because we don't have valuable data:*** Any business that processes data and is connected to the internet has cyber risk. While SBs often do not have large 'troves' of data, they still have data. Attackers view access to SB networks as a 'path of least resistance.' Compared to large publicly traded companies, SBs may not have significant resources invested and dedicated to protecting their critical assets. As such, it is easier for a hacker to infiltrate a high volume of SBs than one large organizations with stronger controls.

b. ***We outsource the storage/processing of data:*** Most SBs think outsourcing data storage and processing will completely transfer their risk and potential liability to the outsource provider. However, the organization that owns the data ultimately has reasonability for it. While there may be some shared liability with outsource providers, most have limit of liability provisions in their contracts. Further, determining liability is a lengthy process and something an organization will be challenged to devote time to while responding to a breach.

c. ***We have adequate technology security controls:*** While technology controls are important and part of the solution, cyber risk at its core is a people risk. Willis Towers Watson claims data reveals that 69% of cyber breaches can be attributed to an organization's employees and can stem from a lost laptop, a disgruntled employee, inadequate cyber awareness training or hiring of non-qualified employees. Therefore, to ad-

dress these vulnerabilities, it is important organizations to also devote attention and resources to people solutions, such as employee engagement, awareness and hiring the appropriate IT talent.

Both Business to Business (B2B) and Business to Consumer (B2C) organizations should understand their cyber risk and consider cyber insurance as a method of risk transfer. For B2B organizations, it's easier to understand why cyber insurance is important. When dealing with other businesses, there may be contractual requirements that require organizations to carry cyber insurance or technology professional services coverage.

If an organization is providing technology professional services, it is important for them to put together technology professional services coverage with cyber liability insurance, as there is an overlap in coverage. Even if an organization is not providing a technology professional service, cyber insurance should be considered as it can provide balance sheet protection for both first-party coverage (out of pocket expenses - i.e., business interruption, data restoration, and cyber extortion) and third-party liabilities (lawsuits alleging financial harm as a result of an organization's errors or omissions).

For B2C organizations, historical buyers of cyber insurance were industries that held a lot of records (i.e., retail, healthcare and education); however, the more recent cyber claims have affected other industries such as manufacturing, nonprofits and critical infrastructure.

One of the best practices for SBs seeking to understand their cyber exposures is to review cyber claims and losses scenarios, such as the following:

Retail

An online retailer noticed unusual activity on its server, which prompted an investigation. They discovered that hackers had stolen an employee's credentials and used them to access the names, billing addresses and credit card numbers of approximately 50,000 customers during checkout.

Outcome: The insurer retained the appropriate vendors and notified the necessary individuals and agencies. The retailer incurred approximately $1M in first-party costs.

Healthcare

A hospital office employee stole medical profiles, histories and detailed personal information on approximately 125,000 patients.

Outcome: The insurer provided the client hospital with crisis support team, made up of outside vendors, to help resolve the breach and reimbursed the hospital approximately **$800,000** for the crisis team's expenses.

Manufacturing

A consumer products company underwent a software system upgrade performed by a vendor. The system upgrade failed, which caused all of the manufacturer's systems to malfunction on the

same day. This caused an unintentional and unplanned outage, which resulted in the suspension of the manufacturer's operations.

Outcome: $2M was paid by the insurer for extra expenses associated with the business interruption, including expenses to continue normal business operations.

Technology Professional Services

A technology services provider of software applications, implementation services and support contracted with a social welfare organization to consolidate and update its legacy IT systems. The social welfare organization filed suit against insured, claiming it failed to meet contractual deadlines, delivered a poorly performing system and failed to properly staff the project.

Outcome: The social welfare organization sought damages in excess of $15M.

Cyber Extortion

A client's computer server was maliciously attacked by a virus that encrypted their data and demanded a $5,000 ransom to unencrypt. The insured reported the matter to the FBI and local authorities, and refused to pay the ransom.

Outcome: The insurer engaged ex expert to perform a forensic analysis of the client's system. The expert found the impacted server didn't contain any confidential information. They removed the virus and strengthened the client's data security protections. The insurer reimbursed the insured $45,000 for **forensic costs** incurred.

Handling cyber breaches can be complex and expensive, and costs can easily amount to thousands of dollars or millions if an organization is not proactive. SBs need to take advantage of cyber insurance, as it provides a risk transfer, as well as a partnership with the various experts (such as forensics, attorneys and public relations) that need to be involved in the event of a breach. Most cyber insurers offer their policyholders a choice of breach response services, typically from a list of pre-approved vendors. Many allow the policyholders' own choice of vendor. Most insurers also grant policyholders access to a complimentary cyber risk management portal that includes the most updated information on emerging cyber threats and the latest reports on risk mitigation measures and practices. Moreover, premiums and other terms and conditions are extremely competitive as market conditions are relatively soft with slight rate decreases. This is likely due to additional capacity in the market and underwriters being able to better quantify exposure.

In sum, SBs need to be as proactive as their larger counterparts by: (1) conducting proper risk assessment and quantification; (2) investing in a cyber-savvy culture; (3) insuring cyber threats they can't mitigate and; (4) allocating enough capital to technological cyber defenses.

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to

1828, Willis Towers Watson has 39,000 employees in more than 120 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas - the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

○