MARCH 19, 2015

EXAMINING THE EVOLVING CYBER INSURANCE MARKETPLACE

U.S. SENATE COMMITTEE ON COMMERCE, SCIENCE, & TRANSPORTATION, SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT SAFETY, INSURANCE, AND DATA SECURITY

ONE HUNDRED FOURTEENTH CONGRESS, FIRST SESSION

HEARING CONTENTS:

MEMBER STATEMENTS

WITNESS STATEMENTS

AVAILABLE WEBCAST(S):*

- Full Hearing:
  http://www.commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=df4b3616-0a25-41d1-90dc-ff3734e5d928&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a&MonthDisplay=3&YearDisplay=2015#archiveTab

COMPILED FROM:

- *http://www.commerce.senate.gov/public/index.cfm?p=Hearings&ContentRecord_id=df4b3616-0a25-41d1-90dc-ff3734e5d928&ContentType_id=14f995b9-dfa5-407a-9d35-56cc7152a7ed&Group_id=b06c39af-e033-4cba-9221-de668ca1978a&MonthDisplay=3&YearDisplay=2015*

** Please note: Any external links included in this compilation were functional at its creation but are not maintained thereafter.*

Mar 19 2015

Examining the Evolving Cyber Insurance Marketplace

Chairman Jerry Moran

"Good morning. This hearing is now called to order.

"First, I would like to thank the witnesses for taking the time to provide their valuable knowledge of the cybersecurity insurance market. I would like to also thank the Committee Staff for their hard work in making this hearing possible.

"The purpose of this hearing is to examine the state of the cyber insurance market, identify challenges and opportunities, and learn how cyber insurance may drive improvements to the risk management culture at businesses who purchase these insurance policies. This is our second hearing on the broad topic of data security and to my knowledge the first congressional hearing on the cyber insurance market.

"American consumers and businesses face ongoing and serious cyber threats. As was noted in our last subcommittee hearing, the Privacy Rights Clearinghouse has estimated that over 4,400 data breaches involving more than 932 million records have been made public since 2005. The Verizon 2014 Data Breach Investigations Report reviewed more than 63,000 security incidents and found 1,367 confirmed data breaches in 2013. On average, that means just under four data breaches occur every day across the globe.

"One strategy for businesses to mitigate cyber or privacy-related losses is the purchase of cybersecurity insurance. While some cyber–related losses may be covered under a business's general insurance policy, the increase of publicly-reported cyber incidents and data breaches have lead insurers to begin offering stand-alone policies to cover cyber-related risks and losses. Cyber insurance policies vary greatly, but increasingly new policies are being developed to cover costs ranging from crisis management in response to a data breach of personal or health information, to business interruption or damage to critical infrastructure systems from a cyber attack.

"While an insurer's primary function is to mitigate financial losses – not defend against cyber threats – cyber insurance may be a market-led approach to help businesses improve their cybersecurity posture by tying policy eligibility or lower premiums to better cybersecurity practices. An example of this relationship is an auto insurer offering a "good driver discount" to a customer who avoids accidents or driving violations, providing an additional incentive to a driver to be more cautious and attentive. The insurance company also wins. Even though the premium receipt they receive may be lower, in the end they have fewer claims to pay out.

"The cyber insurance market is one of the fastest growing commercial lines of insurance. Approximately 50 carriers now offer stand-alone cyber policies, and the total written premiums were $1.5-2 billion in 2014. Some estimates show the market could grow as high as $5 billion by the decade's end. In 2014, the number of clients at brokerage Marsh & McClennan who purchased stand-alone cyber coverage – for example – increased by 32% over 2013. Amongst Marsh clients, the highest take-up rates for cyber insurance in 2014 were in health care, education, hospitality, and gaming.

"Challenges in the cyber insurance market exist due to the difficulty of quantifying exposure to cyber risks, liabilities, and losses; the aggregation of losses due to the interconnected nature of IT; and the changing cyber threat environment. Several IT security firms are developing products and assisting insurers in either identifying potential threats and/or offering cyber products or services to better protect the networks. For instance, a startup named BitSight partners with Liberty International Underwriters to externally analyze a company's cybersecurity. In one case,

BitSight helped discover a dormant threat in a company's IT system and the insurer was able to work with the company to avoid a possible breach. Another example is Overland Park, Kansas-based Risk Analytics, which partners with AIG to provide a security product to some of the AIG insurance clients.

"As Congress considers cyber threat information sharing legislation as well as a national data breach notification standard, important questions about the developing state of the private insurance market come to mind. Today, we will focus our attention on some of the key questions on this topic, including:

• How can the private sector – the insurers and insured – work together to not only increase their cybersecurity posture and address their risk, but also to mitigate losses in the event a breach or cyber incident?
• What cyber insurance policies are currently offered and what losses do they cover?
• How does an insurer assess a policy holder's risk?
• What specific factors do insurers consider when developing a policy and premium rate?
• Has the NIST framework had an impact on how insurers communicate with businesses about their cyber posture?
• What factors inhibit companies from purchasing a cyber insurance policy?
• What factors inhibit insurers from offering this insurance?
• What does the future of this market look like?

"I am confident that today's expert panel can share valuable insight to these important questions that can help Congress better understand the marketplace.

"I would like to now turn the Subcommittee's Ranking Member, Senator Blumenthal."

Senate Committee on Commerce, Science, and Transportation
March 19, 2015, Hearing
"Examining the Evolving Cyber Insurance Marketplace"

Testimony of Ben Beeson
Vice President, Cyber Security and Privacy
Lockton Companies®

Chairman Moran, Ranking Member Blumenthal, distinguished members of the Committee, thank you for the opportunity to testify today on behalf of Lockton Companies.

My name is Ben Beeson and I am Vice President for Cyber Security and Privacy at Lockton Companies. Lockton is the world's largest privately held, independent insurance broker. I am based in the Washington, DC, office, where I advise clients on a cyber risk management strategy that addresses people, processes, and technology.

Our clients face a substantial set of cyber threats today that include criminal gangs, disgruntled employees, politically motivated actors, and now nation states. Well-publicized attacks have sought to target and monetize personally identifiable data and protected health information. However, it is also now well understood that the theft of corporate intellectual property is a significant problem, with nontrivial impacts on innovation for companies and countries, and companies also face incidents that can disrupt or destroy information technology and other vital assets.

We believe that cyber insurance is an important market force that can drive improved cyber security for companies—and thus improve protection to consumers and the nation as a whole. It should not just be seen as another insurance transaction. As the cyber insurance market develops, it will provide incentives for companies to understand and mitigate their risks.

For example, forward-thinking companies invest in workplace safety to reduce their workers' compensation costs. In the same way, sophisticated companies are investing in stronger cyber security, and those companies ultimately will experience fewer losses, insurers will see fewer claims, and their premiums will be lower.

However, we're not there today. The cyber insurance market is still nascent and developing.

CYBER INSURANCE MARKET TODAY

It is estimated that more than 50 insurers domiciled mainly in the US and the Lloyd's of London marketplace provide dedicated cyber products and solutions today. Buyers are overwhelmingly concentrated in the US with little take-up to date internationally. Annual premium spend at the end of 2014 was estimated to be in excess of $2 billion[1] with the potential to grow to $5 billion.[2] Total capacity (the maximum amount of insurance available to any single buyer) is currently at about $300,000,000. Cyber insurance first emerged at the end of the 1990s, primarily seeking to address loss of revenue and data-restoration costs from attacks to corporate networks. However, the underwriting process was seen as too intrusive and the cost prohibitively expensive, and it was not until 2003, and the passage of the world's first data breach notification law in California[3], that demand started to grow.

WHAT DOES CYBER INSURANCE COVER?

It is important to understand that insurers do not address all enterprise assets at risk. The vast majority of premium spent by buyers has sought to address increasing liability from handling personally identifiable information (PII) or protected health information (PHI), and the costs from either unauthorized disclosure (a data breach), or a violation of the data subject's privacy. Insurable costs range from data breach response expenses such as notification,

[1] The Betterley Report - www.betterley.com

[2] The Cyber Liability Insurance Market 2015 - Jim Blinn, Advisen. www.cyberrisknetwork.com

[3] California S.B.1386

Rev. 03_17_15

LOCKTON

forensics, and credit monitoring to defense costs, civil fines, and damages from a privacy regulatory action or civil litigation.

Insurers also continue to address certain first-party risks including the impact on revenue from attacks on corporate networks, extortion demands, and the costs to restore compromised data.

WHAT DOES CYBER INSURANCE NOT COVER?

Theft of corporate intellectual property (IP) still remains uninsurable today as insurers struggle to understand its intrinsic loss value once compromised. The increasing difficulty in simply detecting an attack and, unlike a breach of PII or PHI, the frequent lack of a legal obligation to disclose, suggests that a solution is not in the immediate future.

Much attention in the industry is now being paid to risks to physical assets from a cyber attack. Much of the credit here must go to the federal government for directly engaging the industry initially in 2013 as part of the creation of the NIST Framework and raising awareness about the risks to critical infrastructure industries. In the absence of actuarial risk modeling data, certain innovative insurers and brokers have started to produce solutions that specially address property damage, resultant business interruption loss, and bodily injury from a cyber attack. However, it is early days, and major challenges lie ahead in establishing significant market capacity as well as addressing the current ambiguity embedded in legacy property and casualty insurance policies.

HOW DO INSURERS UNDERWRITE CYBER RISKS?

Historically, underwriters have sought to understand the controls that enterprises leverage around their people, processes, and technology. However, the majority of assessments are "static," meaning a snapshot at a certain point in time through the completion of a written questionnaire, a phone call interview, or a presentation. In the wake of significant insurable losses in 2014 and early 2015 to the retail and healthcare sectors in particular, a consensus is growing that this approach is increasingly redundant. It is Lockton's opinion that insurers will increasingly seek to partner with the security industry to adopt a more threat-intelligence-led capability as part of the underwriting

LOCKTON

process in the face of threats that continue to evolve. The industry (as discussed later) will also increasingly seek to partner with government to access industry loss data and analytics capabilities.

WHAT IS THE ROLE OF CYBER INSURANCE?

In the context of building enterprise resilience to counter evolving cyber threats, insurance should not just be seen as a financial instrument for transferring risk from one balance sheet to another. Importantly, the actual process of seeking cyber insurance coverage should also be viewed as the catalyst for driving an enterprise-wide risk management approach, and ultimately an improved security posture.

It can bring all relevant stakeholders together in IT, Legal, Risk Management, R&D, Finance, Human Resources, Communications, and the Board of Directors for example. Do not view cyber insurance as just a commodity that you may or may not seek at the end of this process.

NIST FRAMEWORK

In the same vein, Lockton also sees the NIST Framework aligning hand in glove with this strategy. Working closely with the Department of Homeland Security to support its implementation, Lockton sees the framework providing the tool that is needed to help boards of directors understand in layman's terms their current security posture, areas for improvement, and desired future status. As insurance brokers who also advise directors and officers on management liability, we can acknowledge that cyber risk has now entered a governance dialogue, and the NIST Framework has proved immensely helpful in facilitating the discussion.

LOCKTON

CONCLUSION—A PUBLIC/PRIVATE PARTNERSHIP

Lockton, and we believe the industry as a whole, would welcome the introduction of legislation that would reduce barriers and incentivize organizations to share threat indicators with government, and each other, while also protecting individual privacy. Actuarial data is extremely thin on the ground and is holding back the growth in market capacity, particularly to address the previously highlighted risks to critical infrastructure industries.

As part of the insurance industry's engagement with the Department of Homeland Security, discussions are ongoing about the possible formation of a data repository to house anonymized enterprise loss information. The ability to access anonymized loss data, shared between industry and government with appropriate privacy protections would also accelerate the growth of the marketplace, but crucially the ability of cyber insurance to act as a market incentive for industry to invest in cybersecurity.

Thank you again for the opportunity to testify, and I will be happy to answer any questions that you may have.

LOCKTON

Catherine Mulligan, SVP Zurich
Testimony before the US Senate Commerce Committee
Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security
Hearing Titled: "Examining the Evolving Cyber Insurance Marketplace."
March 19, 2015

Good morning Chairman Moran, Ranking Member Blumenthal and members of the subcommittee. My name is Catherine Mulligan and I am Senior Vice President of the Management Solutions Group for Zurich (North America). I lead the market facing team of underwriters responsible for working with brokers and customers on the placement of "cyber" insurance. I appreciate the opportunity to speak to the subcommittee on the state of the cyber insurance marketplace and to share thoughts on some of the challenges we are seeing.

As a brief introduction, Zurich Insurance Group (Zurich) is a leading multi-line insurance provider with a global network of subsidiaries and offices. Founded in 1872, Zurich is headquartered in Zurich, Switzerland with approximately 55,000 employees serving customers in more than 200 countries and territories.

While Zurich is named after the Swiss city where it was founded, we are quite proud of our U.S. roots and our global platform for diversifying risk. In 1912,

Zurich entered the U.S. as the first non-domestic insurance company and quickly became a leading commercial property and casualty insurance carrier.

Over the last 103 years, Zurich has grown and its U.S. companies now employ more than 8,500 people in offices throughout the country with major centers of employment in the metropolitan areas of Chicago, New York City, Kansas City, Atlanta, Dallas, and Baltimore. Mr. Chairman, as I am sure you are aware, we employ nearly 400 people throughout the state of Kansas and write coverage in every single state. Zurich's U.S. insurance group accounts for roughly 40% of its total global business.

As a result, Zurich is the fourth largest commercial property and casualty insurer in the United States by gross written premium. It is the fourth largest writer of commercial general liability insurance, which includes coverages that, among a wide array of other risks, protect U.S. manufacturers, importers and retailers against product liability losses. In addition to this capacity, Zurich also protects many U.S. construction projects throughout the country as the third largest fidelity and surety insurer. Zurich protects hundreds of thousands of U.S. employees and their employers as the fifth largest workers compensation insurer.

With this context as to who Zurich serves, it was two years ago when Zurich's senior leadership decided to act to address the risk management questions and concerns raised by many of our cyber customers. This began a global thought leadership initiative with the Atlantic Council and resulted in a white paper report titled: *Beyond Data Breaches: Global Interconnectedness of Cyber Risk.* This report was released in April 2014, and Zurich has shared its findings and recommendations with its stakeholder community to generate dialog and steps forward to address the cyber threats.

As cyber attacks occur in ever changing forms on business and industry that compromise increasing amounts of sensitive information, this hearing is extremely timely to level set what cyber insurance is, what it is not, and most importantly some of the challenges marketplace actors are seeing.

I will dive into specifics later in my testimony, but overall here is how I see the market. Unsurprisingly given recent high profile breaches, so-called cyber insurance is quickly becoming a need for commercial customers. However, as a new market it faces a number of challenges. Some are somewhat more straight-

foward, such as capacity and pricing, which are in flux as the industry grows and learns of new challenges.

Yet, others reflect the complexity of the challenge. The term cyber insurance is a misnomer. A network security and privacy event - the more accurate term of cyber insurance - can also be caused by something simple such as improper disposal of paper records. At the same time, one cyber event can trigger multiple types of claims, for multiple insureds within one company, and even cause physical damage to a manufacturer or utility.

The lesson can be boiled down to the simple fact that the scope of the challenge is too broad to be solved by the private sector alone. Not all losses from a cyber attack will be or even could be covered by an insurance policy. This market is new and evolving daily which will require time to fully mature.

Market overview:

In October 2014, Dowling and Partners called security & privacy (also known as "cyber") insurance "one of the few growth markets in the U.S. Property and

Casualty Industry" with growth potential up to $10B Gross Written Premium.[1] Sources, including Dowling and Guy Carpenter,[2] suggest the current market is $2 billion with five or six carriers offering primary coverage. Guy Carpenter also states that the six largest carriers have 70% of the market share, a statistic that remained relevant throughout 2014. These premium numbers are difficult to verify. The coverage can be offered on a stand-alone basis or blended with other coverages, such as Errors & Omissions.

Coverage overview and history

The product was first introduced about 15 years ago and has its roots in technology errors & omissions coverage. This is a third party liability coverage designed to respond to financial damages resulting from negligent acts, errors, and omissions in the deliverance of a product or service. As our world and economy became more networked, privacy issues came to the fore, which led to the development of privacy regulations. Companies found they incurred first-party costs to respond to privacy events and to comply with these regulations.

[1] "Cyber Security: with CEO Jobs Now on the Line, It's No Longer Just an 'IT' Issue." Dowling & Partners IBNR Weekly #39, October 20, 2014

[2] Guy Carpenter's State of the Tech/Cyber market report (2012) and Management Liability – Market Overview report (Oct. 2013)

Network Security & Privacy Liability policies were developed to respond to this blend of first and third-party costs.

The product in its current iteration has been in the marketplace since around 2009. There is no industry standard policy language, but the core elements of the coverage are as follows:

- The third-party liability costs arising from network breaches and privacy events as well as some media liability events;
- The first-party or direct costs a company incurs in responding to a breach. These include forensics analysis, legal guidance in compliant breach response, credit and identity monitoring costs, and the costs associated with a call center and public relations.

First-party coverages have further expanded to include Business Interruption and Extra Expense. This is a familiar coverage on most commercial property policies, but here, instead of responding in the event of physical loss or damage, this optional coverage can apply to direct damages arising from downtime caused by a network security breach.

Marketplace shifts

In January of this year, the Insurance Information Institute reported that market capacity for cyber insurance is on the rise.[3] While this optimism is understandable given the visibility of the issues and the attention significant breaches have garnered from Boards of Directors and C-Suite executives[4], the reality is that the shape of the insurance marketplace continues to shift:

- *Capacity is in flux.*

  Dowling & Partners stated more than 60 carriers wrote the coverage as of October 2014. Subsequently, our broker partners tell us a number of excess markets pulled out of the product line or limited their appetite. Business Insurance has reported on major insurers restricting their appetites for challenging industry segments. The London market was tapped out for retailers by December; although capacity refreshed in 2015, the pressure was on to find strong support for growing programs. Reinsurers are also paying careful attention to their aggregations, and some have amended their appetites for supporting the coverage.

- *Pricing is in flux.*

[3] "Insurance Industry Leaders Believe Market Capacity For Cyber Insurance On The Rise, U.S. Economic Growth On the Upswing, I.I.I. Survey Finds." Insurance Information Institute, January 14, 2015
[4] "Cyber Security: with CEO Jobs Now on the Line, It's No Longer Just an 'IT' Issue." Dowling & Partners IBNR Weekly #39, October 20, 2014

The insurance industry lacks robust actuarial data around the loss experience for a product that is still in its nascency. Unlike general liability policies, which all commercial enterprises carry, the buyers of this coverage are largely in a few key industry sectors (such as health care, financial institutions, technology, and retail) and in the larger company space (ie. companies with annual revenues over $1 billion). As loss experience emerges, and underwriters identify new attack vectors, pricing becomes more refined. Some segments, notably retail[5], are experiencing significant increases in premiums as high profile breaches in the past 12 months have generated substantial first party loss dollars, which continue to rise.

- *Loss experience is developing*

  One major retailer, who suffered a highly publicized breach in late 2013, is reported to have incurred over $250 million in first-party costs in responding to the attack. Those costs reportedly continue to rise, and the liability costs associated with the breach - including liability to consumers and financial institutions - has yet to be determined. This example demonstrates the severity potential as well as the element of the unknown as the liability issues play out in court. Moreover, we see attack vectors shifting, for example,

[5] "Data breaches prompt insurers to boost cost of retailers' cyber coverage," Business Insurance, Sept. 28, 2014

approximately 30% of breaches originate with a business partner or vendor, presenting challenges to underwriting the exposures and controls and to responding to breaches.

- *Coverage and aggregation challenges remain*

  It is important to understand the history of this product. The total scope of exposures presented by a cyber security event is beyond the current scope of coverage. Richard Clarke's acronym[6] for causes of cyber security events remains applicable. He described them as C.H.E.W.: Crime, Hactivism, Espionage, and War.

  While most security & privacy policies do not focus on attribution, the trigger of coverage must still be a network security breach or privacy event. We eschew the term "cyber" for three reasons:

  1. It is not a defined term in most policies;
  2. Privacy events may be triggered by an analog event such as improper disposal of paper records containing personally identifiable information;
  3. A broad term such as "cyber" erroneously may suggest that the coverage could respond to every type of damage caused by an attack on a network.

[6] Richard Clarke, "Cyber War: The Next Threat to National Security & What to Do About it", published 2012

We understand that customers have a range of exposures that exist beyond the financial loss coverage that is provided under a Security & Privacy policy.

- Top areas of concern include Bodily Injury and Property Damage:

  A cyber attack may cause physical damage to a manufacturer or utility. For example, a December 2014 malware attack to a German iron plant caused fire damage when a furnace's controls were compromised.[7] In 2014, Insurance Service Offices (ISO) issued exclusions on their general liability forms to clarify that cyber events are not meant to be covered on the general liability policy. While some limited coverage is available in the marketplace, current security and privacy forms generally exclude bodily injury/property damage.

The scope of the exposures is too broad to be solved by the private sector. Not all causes of loss can be transferred to an insurance policy.

<u>Emerging issues</u>

- *Aggregation tracking and emerging exposures*

[7] "Cyberattack on German Iron Plan Causes 'Widespread Damage': Report," The Wall Street Journal, December 18, 2014

Multiple lines of business may be impacted as the result of a cyber security event. For example, a significant breach to a public company might result in a stock drop, which leads to a derivative suit that comes in as a claim under a Directors & Officers Liability Coverage.

Also, one event might impact multiple insureds. For example, a recent breach at a large health insurer has resulted in claims under policies for a variety of companies who have business relationships with that insurer.

The current coverage structure and pricing will continue to evolve as carriers gain a more comprehensive understanding of the full scope of the potential. The insurance industry is working with the public sector to shape policies around these issues.

- *Public sector*

The 2015 World Economic Forum report states that "global risks transcend borders and spheres of influence and require stakeholders to work together."[8] The focus of the report on "risk interconnections and the potentially cascading effects they create" echoes the theme of the Atlantic Council's 2014 study on

[8] "Global Risks 2015 – 10th Edition", World Economic Forum, January 2015

cyber risk.[9] The WEF report echoes Chairman Thune's comments from the February 4th hearing on the NIST framework: "Real progress can be made by continuing to enhance public-private cooperation and improving cyber-threat information sharing."

Work in this arena includes working groups at the Department of Homeland Security and the Department of Treasury on the issue of data repositories. Data sharing may need to take a few different forms: sharing of cyber event data, such as attack vectors and scope, and cyber insurance data, such as claim and underwriting information by sector. While it is too early to assert any definitive conclusions, the potential upside of these discussions is that more comprehensive information will assist insurers in developing both coverage and risk management solutions and best practices for our customers.

[9] "Risk Nexus. Beyond data breaches: global interconnections of cyber risk", Atlantic Council, April 2014

Prepared Testimony and
Statement for the Record of

Ola Sage
Founder and CEO
e-Management

Hearing on

"Examining the Evolving Cyber Insurance Marketplace"

Before the

Senate Committee on Commerce, Science, and Transportation
Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security

March 19, 2015

253 Russell Senate Office Building

Examining the Evolving Cyber Insurance Marketplace

Opening Remarks

Good morning Chairman Moran, Ranking Member Blumenthal, and distinguished members of the Committee. It is an honor for me to be here today.

My name is Ola Sage and I am the Founder and CEO of e-Management, a small business provider of high-end IT services and cybersecurity solutions to clients in the private and public sectors, including the largest U.S. federal agencies. Founded in 1999 and headquartered in Silver Spring, Maryland, we employ close to 60 IT professionals who deliver services in our core areas of IT Planning, Engineering, Application Development, and Cybersecurity. In 2013 we were honored to receive the Department of Energy's Cybersecurity Innovative Technical Achievement award, highlighting the expertise of our cybersecurity experts in designing and implementing advanced cybersecurity detection and risk management capabilities. Our newest cybersecurity risk intelligence software solution, *CyberRx*, automates the National Institutes of Standards and Technology (NIST) Cybersecurity Framework (CSF) and is designed to help small businesses easily *measure* their cybersecurity capabilities, *manage* their cybersecurity risks, and *communicate* their cybersecurity readiness to internal and external stakeholders.

I am a champion and advocate for Small and Medium-Sized business (SMB) cybersecurity readiness. I currently serve as an elected member on the *Executive Committee of the National IT Sector Coordinating Council (IT SCC)*. The IT SCC, comprised of the nation's top IT companies, professional services firms, and trade associations, works in partnership with the Department of Homeland Security (DHS) to address strategies for mitigating cybersecurity threats and risks to our nation's critical infrastructure, especially for organizations and businesses that are particularly vulnerable such as SMBs. I am also an 8-year member of Vistage, an international organization of 19,000 CEOs that control businesses with annual sales ranging from $1 million to over $1 billion. I regularly meet with and speak to small business CEOs in Vistage, and other small business forums about why cybersecurity should matter to them and how it can affect their ability to keep business, stay in business, or get new business. In the last 3 months alone, I have spoken to more than 100 SMB CEOs that represent a diverse mix of industries.

Thank you for the opportunity to testify today on behalf of e-Management as a small business consumer of cybersecurity insurance products. In my testimony today, I will discuss:

- My company's involvement with cybersecurity insurance including our application and renewal process
- Perspectives that I have as a CEO and from other CEO's relative to cybersecurity insurance
- Opportunities for the cybersecurity risk insurance industry
- Concluding thoughts

Our Driver

My company's foray into the cybersecurity insurance market began in November 2013 as I prepared for a webinar on cybersecurity titled "We've Tipped: 5 Ways to Increase Your Cybersecurity Resiliency." The webinar discussed the wave of cyber-attacks that were occurring across all industries, highlighting the significant increase in attacks on small businesses and the impacts – including financial, legal, and reputational – that they were having on all sizes of business, including the disproportionate and negative impact to small business. According to the Cyber Security Alliance, 60% of small businesses go out of business within 6 months of a significant cybersecurity event.

Among the five key recommendations I made in the webinar was for businesses to make sure they had appropriate business and legal protections (e.g., business policies, insurance, etc.). I thought about my own company and whether we had taken appropriate steps to include business and legal protections in the area of cybersecurity. As a company, we had participated for more than a year with NIST as they worked with thousands of security professionals in government and private industry to develop the CSF. Upon release of the Preliminary Draft of the CSF, NIST encouraged companies and organizations to try it and provide feedback that could inform the final version (v 1.0 which was ultimately published in February 2014). We took the challenge.

Methodology

In our "test drive" of the CSF, we used the Framework as a way of assessing our cybersecurity readiness in the five core cybersecurity functions (Identify, Protect, Detect, Respond, and Recover) and mapped the results to the four Implementation Tiers to help us to understand how our current cybersecurity risk-management capabilities measured up against the characteristics described by the Framework and to assess the degree of risk management rigor we were applying to each of the five core functions. Overall, the CSF provided a common language that I could use with my management and IT teams in organizing our thinking around cybersecurity. We were able to distill where we needed to prioritize our efforts and focus our dollars. We found it to be a very effective and useful tool.

Our Cybersecurity Insurance Experience

In addition to technical and operational changes we made after our initial CSF readiness assessment, we decided to move forward with researching what cybersecurity insurance products were available on the market, specifically available offerings for SMBs. As I'm sure it will come as no surprise to anyone here, we could not find cybersecurity insurance products designed specifically for SMBs. The cybersecurity insurance industry was and is still in a nascent stage.

Working through our insurance broker, we submitted applications to several large insurance companies. The applications varied in length and substance, with very little consistency in the questions asked. When the quotes arrived, they ranged from a couple thousand dollars from one insurer to twelve thousand plus for another. Comparing the policies against one other was virtually impossible as the language used in one policy was quite different from the next and it was unclear whether or not they covered the same conditions. As expected, all of the policies contained exclusion clauses, however it was not clear from policy to policy whether the exclusions were similar or not.

Regrettably I cannot tell you that our selection of a cybersecurity insurance product was based on a simple and easy analysis of options. We ended up with a policy that combines cybersecurity liability and errors and omissions, but honestly, as I sit here today, I cannot say with confidence we have the right policy for us. All told, the process from start to finish took four months and cost over ten thousand dollars. This was a significant investment for a company our size.

We continue to regularly monitor and manage our cybersecurity risks, and implement preventative measures based on the results of our Framework assessment. We call it "operationalizing" the CSF. We understand it is not possible to achieve 100% cybersecurity, but as a provider of IT and cybersecurity services, we believe it is important to convey to our employees, customers, and vendors that we take cybersecurity seriously and understand the potential damage it could cause to them. In addition to doing it for the right reason, we also see it as a competitive advantage.

We have taken it a step further. Understanding the value the CSF gave us, we wanted to share our experience with other small businesses. Drawing on our entrepreneurial instincts, we created and brought to market a software solution that automates the CSF in a way that is simple and affordable for other small businesses to use. In two hours or less, a small business can conduct a "fitness" review of their cybersecurity readiness in the CSF's five core areas. In addition, the small business CEO receives information unique to their company that provides them insight into their level of technical, operational, and financial exposure. It is actionable risk intelligence. We call it CyberRx. CyberRx makes it easy for a small business to understand how prepared their business is to identify, protect, detect, respond, and recover from cybersecurity attacks and alerts them to areas that need attention. They quickly know what areas to focus on and what their next steps should be. We use CyberRx in our company today to continuously manage our own cybersecurity risks.

Renewing our Cybersecurity Insurance

This brings me back to our cybersecurity insurance experience. We have just passed our one year anniversary and this time around the process started with a letter from the insurance company informing us that our coverage wouldn't automatically renew. We received an abbreviated application (3 pages vs 15) which we completed and sent back. There was only one question around cybersecurity asking whether there had been any changes regarding the security and protection of our facility and network. The instructions indicated that if the response was "Yes", we needed to indicate if we had experienced a security breach? As we thankfully did not experience a breach (that we know of) we were able to answer no. We received our renewed policy in approximately three weeks, which was the good news. The surprising news was that our premium increased by 12%.

Stunned, surprised, frustrated, confused, discouraged, etc. are all words that would accurately describe our reaction. After a year of investing in processes and tools to strengthen our cybersecurity posture, the result was an increase in premiums. Doing the right thing didn't seem to pay, literally. We went back to our broker to better understand how this could have happened and were informed that there were a variety of factors that went into the underwriting process. In our case, ironically, because our revenues grew in 2014 vs 2013, that appeared to be the primary contributor to the increase. When we asked whether or not using the CSF could be a factor, our broker wrote that "although they do not specifically inquire as to whether or not an insured is following the voluntary cyber security framework provided by NIST, they obviously take into consideration any preventative measures an insured implements when underwriting a risk."

SMB CEO Perspectives

My experience is not unique. As I speak to small business CEOs across the country, there is a general lack of awareness about (1) the need for cybersecurity insurance; (2) what cybersecurity insurance products exist on the market; (3) what the various polices cover; and (4) what the costs are.

1. ***The need for cybersecurity insurance***
   Many SMB CEOs just don't believe they have anything cyber hackers would want. "We're too small," some will say, believing that hackers are only interested in the large companies where they can get more "bang for their buck." Interestingly, another subset of SMB CEOs believe that cybersecurity insurance is already included in their professional liability coverage, and therefore do not see the need for additional or separate coverage.
2. ***Availability of cybersecurity insurance products***
   Of the 100 or so SMB CEOs I have spoken to over the past three months, easily 70% were not aware of what cybersecurity insurance products are available on the market. Once informed they were curious to learn more. This aligns with a recent 2015 survey by Gartner company, Software Advice, who reported that after defining cyber insurance to the SMB decision-makers in their survey, they found that a combined 52% were either "very" or "moderately" intrigued, with another 32% "minimally" intrigued, giving an overall 84% who expressed some level of curiosity. [1]
3. ***Policy Coverage***
   Understanding what the different cybersecurity insurance policies cover can be a challenge, not just for SMBs, but also for many brokers. There does not appear to be any common terminology or contract organization amongst carriers, thus making it difficult and costly to truly understand what an individual policy covers and to compare competing insurance products.
4. ***Cost of Coverage***
   The cost of cybersecurity insurance varies widely. Our own experience with a range of quotes from $2,000 - $13,000 is not uncommon. This large variance can discourage SMB CEOs from making needed investments in cybersecurity insurance. In addition, for many SMBs, such rates are cost prohibitive for what they might consider "elective" insurance. Given the challenges with understanding and comparing the scope and coverage of various insurance products on the market, SMBs may incur additional costs in connection with the placement or renewal of insurance in addition to the cost of the insurance itself.

Opportunities for the Cybersecurity Risk Insurance Industry to Assist SMBs

There is no 100% level of cybersecurity. At e-Management, we strongly believe cybersecurity readiness is about risk management. We offer the following straightforward recommendations that we believe would encourage SMBs to take greater advantage of cybersecurity insurance products.

1. ***Increase awareness of cybersecurity insurance as a risk transfer option for small businesses.***
   Cybersecurity insurance can be an effective tool to help small businesses manage their financial risk and should be a key part of a company's cyber and information security practice. Several years ago, Symantec reported that the average annual cost of cyberattacks to small businesses was $188,242 with median cost of downtime for an SMB reported at $12,500 per day. These costs can be devastating, in many cases leading small businesses to shut their doors. However, a majority of small businesses are not aware of cybersecurity insurance. According to the 2015 survey by

[1] http://www.softwareadvice.com/security/industryview/cyber-insurance-report-2015/

Software Advice, only a third of small and midsize businesses are even aware that cybersecurity insurance exists and of that number only 2% actually hold cybersecurity insurance. I understand that in the last year there have been extensive discussions among government, private companies, insurance groups, and other relevant stakeholders about expanding the role of cybersecurity insurance in public and private industry business agreements. While I think this is a necessary and important conversation to have, I encourage these discussions to continue to be as thorough and transparent as possible including a full review of potential impacts or consequences that particular policy decisions could have, particularly to SMBs.

2. ***Make cybersecurity insurance affordable for SMBs***
   Cybersecurity insurance needs to provide meaningful coverage that SMBs can actually afford. Various industry reports indicate that SMBs continue to be the fastest growing segment of cyberattack victims, creating a huge vulnerability, not just for the SMBs, but for their customers, vendors, and suppliers. We believe offering competitive cybersecurity insurance products designed for the SMB market can lead to better deals for SMBS. We recommend that insurance companies consider a rating system based on the CSF that underwriters could consider as a factor in the underwriting process. SMBs that demonstrate use of the CSF could receive a higher rating as they have mitigations in place which line up with industry standards and best practices.
3. ***Reward SMBs who are actively managing their cybersecurity risks and implementing reasonable security measures.*** In 2014, the Online Trust Alliance indicated in a report that 90% of the year's breaches could have been prevented if organizations implemented basic cybersecurity best practices[2]. The CSF is a model cybersecurity best practice and offers a defensible way to assess and manage cybersecurity risks. Based on our own experience, we strongly believe that any small business that uses the CSF can significantly reduce their cybersecurity risk exposure. Small businesses that are actively managing their cybersecurity risks should be preferred candidates for lower premiums and tax incentives.

Conclusion

At e-Management, we continue to find the CSF to be a useful tool in helping us and other SMBs organize the way we think about cybersecurity risks and the best practices we need to implement to reduce our overall cybersecurity risk exposure. We appreciate the emphasis that Congress, NIST and the DHS have placed on educating SMBs about the increasing cybersecurity threat and raising awareness of the CSF. We welcome continued efforts in this area and encourage the addition of cybersecurity insurance in the discussion as another tool that SMBs can consider along with other risk management solutions.

While simply obtaining cybersecurity insurance cannot be viewed as a silver bullet, I believe cybersecurity insurance can be an important tool in helping SMBs manage significant financial exposure associated with a successful cyber attack. As the cybersecurity threat and challenge to small business continues to persist, we at e-Management are committed to working with government and industry to identify and develop simple and affordable solutions that enable small businesses to strengthen their cybersecurity readiness and posture.

Thank you again for the opportunity to testify, and I am ready to answer any questions you may have.

[2] https://www.otalliance.org/news-events/press-releases/ota-determines-over-90-data-breaches-2014-could-have-been-prevented

Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security
Hearing entitled "Examining the Evolving Cyber Insurance Marketplace."
Thursday, March 19, 2015

Written Testimony of Michael Menapace

Sen. Jerry Moran, Sen. Blumenthal, and other members of the Subcommittee -

I am pleased to provide testimony today concerning this Committee's interest in the growing cybersecurity insurance market, the evolution of the insurance coverage, opportunities to strengthen the insurance industry, and the insurance market's impact on cybersecurity.

I would be pleased to respond to specific questions posed by the Committee and I would like to cover in my testimony several specific issues concerning the evolving cyber insurance marketplace. Specifically, I would like to discuss the cost-drivers for cyber insurance, the role that the insurance industry and the government can play in helping in the development and evolution of standards for breach notification, the sharing of data breach information, and flexible, industry-specific standards for protecting consumer data.

The testimony I provide is my own and not necessarily that of any of my firm's clients.

Background and Introduction

I practice law at the law firm of Wiggin and Dana after having previously practiced at a large international law firm. In addition, for the past 6 years, I have taught Insurance Law at the Quinnipiac University School of Law and have published articles and books on a variety of property and casualty insurance issues. In my law practice, I, along with my colleagues, represent companies in a broad spectrum of industries by helping them develop data security and privacy protocols and procedures, and I represent insurance companies in several areas, including cybersecurity. In both my academic role and in private practice, I have the opportunity to work closely with businesses in many market segments, insurance companies, and regulators.

Examining the intersection of insurance and cybersecurity is an important and timely topic for this Committee. Insurance often evolves slowly, but we are in the midst of a period in which technological advancements and the development of a relatively new product are occurring simultaneously. No doubt, we are living through a dynamic period in the insurance industry and we should not underestimate the importance of the insurance industry in terms of risk transfer and the information insurers provide to insureds on loss mitigation strategies and loss trends.

The insurance industry is in a unique position to help regulators, businesses, and consumers assess and respond to the ever-growing threat of data breaches. Insurers can help businesses

and consumers respond quickly and efficiently when breaches unfortunately, but inevitably, occur. Insurers have first-hand experience with large amounts of consumer data. Moreover, insurers are in the business of examining and responding to risks, tracking emerging trends, and finding ways to mitigate their impact. Indeed, insurers often provide information and best practices to their insureds to help avoid losses.

By definition, insurers deal with events that are uncertain from the viewpoint of the insured. There is an element of fortuity at the heart of insurance that insureds cannot predict. While this element of uncertainty is present to insureds, insurers can pool large amount of data and experience to see trends as they evolve – this helps them price insurance policies appropriately and remain in a financial position to pay claims.

In addition to the traditional goal of providing risk transfer, insurers can help insureds avoid loss in the first instance. For example, insurers have traditionally helped in the development of safety programs to help employers and employees avoid workplace injuries. Obviously, such programs help workers, but they also assist the purchasers of insurance by bringing down premiums. In all, the goal of the insurer is for their insureds to avoid losses and to make those losses that inevitably occur smaller and easier to rectify.

The insurance market can play a similar role in cybersecurity with risk transfer products and sharing information and experience with their insureds.

Evolution of Cyber Coverage

There are some insurers, particularly the large insurers, who have been writing some form of cyber coverage for well over a decade. They have become quite sophisticated and efficient in providing excellent risk transfer products to a variety of markets. However, there are approximately 40 insurers in the U.S. that are currently providing cyber coverage, and among those insurers are some that are relatively small by comparison to the market leaders and who are less experienced and sophisticated in providing cyber insurance. While the insurance market as a whole could benefit from the topics we are discussing today, it is the smaller companies and those with a less mature book of business that would likely benefit the most – and, by extension, their insureds would see benefits in the form of lower premiums and thriving insurance marketplace.

I will discuss breach notification standards, the sharing of data, and the development of data protection standards in a few moments, but I would first like to discuss how the cyber insurance market has evolved to where we find it today.

During the “dot com” boom of the early 2000s, some insurers started offering insurance products for technology companies. Originally, those insurers provided first party property loss coverage along with some third party liability coverage. The first party property loss coverage was designed to cover, for example, losses the policyholder experienced for damage to its own

technology equipment and infrastructure. The third party liability coverage was designed for exposure to third party lawsuits against the insureds.

The early coverage was written that way because, in those nascent years, the insurance market believed that the liability losses would be driven by the cost of defending lawsuits and paying settlements or judgments as a result of those lawsuits. But the predictions on the cost-drivers were not entirely accurate and today's products have developed to reflect this reality.

While third party lawsuits are still one factor insurers consider how they draft policy wordings and price the coverage they offer, we have seen that data breach response costs have come to the forefront in the minds of insurers and insureds alike.

Neither insurers nor insureds anticipated that these breach response costs, sometimes called crisis service costs, would be the significant cost drivers that they have become. These breach response expenses have become costs drivers for several reasons, including the fact that many data breach lawsuits are dismissed in the early phases of litigation. These lawsuits are often dismissed because the plaintiffs cannot show or even plead concrete damages – in response to breaches, businesses or their insurers often provide credit monitoring at no cost to consumers and until actual damage to the consumer can be alleged as a result of the data breach, the damages are speculative. Obviously for those cases that are dismissed, there are no settlement or judgment costs borne by insurers and the defense costs are extinguished, whereas every breach will have breach responses expenses.

According to a recent insurance industry survey, the initial crisis service costs account for about half of all data breach costs. Those breach response services include technical forensic investigations, attorney oversight, breach notification to and credit monitoring for affected consumers, call centers, and public relations services. The other half of the costs go towards legal defense and settlement, regulatory response and defense, regulatory fines, and fines imposed by credit and debit card issuers.

<u>A Federal Breach Notification Standard – Reducing the costs of breach responses and treating consumers equally</u>

As of today, the are 47 states, plus Puerto Rico, Washington D.C., and the Virgin Islands, that have requirements for notifying customers after the unauthorized access of personally identifiable information or protected health information. Many of these state requirements also require notification of the state attorney general when a certain number of residents have been impacted.

But, these state requirements are not uniform in terms of when they are triggered and what information must be contained in the consumer notices. Therefore, when responding to a nationwide incident, lawyers like me must assess the impacted data and consumers under 47 different sets of requirements. Among the questions we must ask for each state are:

Has the breach notification standard been triggered?

Must the consumer(s) be notified under the facts of the incident?
What information must be contained in the notification?
Must we notify state regulators or attorneys general?
Must notice be given in a specific timeframe?
Are we required to provide specific consumer protection services such as identify theft insurance and/or credit monitoring?

This 47-state exercise can be a costly endeavor and, frankly, can result in a situation where some consumers and state officials are notified in one state while consumers and officials in other states are not notified about the very same incident. As both industry members and regulatory authorities have noted, this current patchwork quilt of state breach notification requirements creates gaps in consumer protection as well as additional burdens for businesses that experience cyber-attacks

A nationwide standard for breach notification that preempts state law requirements would eliminate the time, expense, and inconsistencies involved in the 47-state analysis for each breach and would provide for uniform treatment of consumers. I note, however, that any such federal standard must carefully consider the timeframe within which business must notify consumers whose data may have been affected. The timeframe must balance the needs of timely notice to consumers with the concern of providing consumers with accurate information. Increasingly, large breaches involve complex attacks that require equally complex forensic investigations to determine the actual scope of data losses.

<u>Nationwide Data Clearinghouse – Assisting underwriting and spotting trends</u>
There are many lines of insurance that have fairly standardized coverage terms and conditions regardless of which insurer is issuing the coverage. For example, the vast majority of general liability policies purchased by businesses are based on standardized policy language. The Insurance Services Offices, Inc. (ISO), publishes standard liability policy language for many lines of property and casualty insurance. Insurers can choose to adopt the ISO forms and, in the case of general liability policies, most insurers do adopt the ISO policy or use policy wording that is very similar.

However, there is no standard insurance policy language for cyber insurance. ISO did recently publish cyber coverage terms, but I know of no insurer that has adopted the ISO policy terms or has plans to do so in the near future.

Among the approximately 40 insurers that offer cyber insurance, there are some with significant experience and who have policy language that they have developed over the course of more than a decade of experience. Those insurers are comfortable with their policies even though they will undoubtedly continue to evolve. Other insurers, some who are newer entrants into the cyber insurance market and others who are looking to differentiate themselves from their competitors, have their own policy language that has not been tested to the same extent as the policy terms used by the insurers with more mature books of business.

Understanding these differences in policy language from one insurer to another can be a challenge to insurance purchasers and brokers, but the diversity in the market also gives purchases more choice to purchase insurance tailored to their specific needs.

In and of itself, this diversity of policy terms and conditions is not problematic for individual insurers. What can be challenging for some insurers is making sure they have enough data to make prudent underwriting decisions when they sell policies.

For insurers to have good underwriting in terms of deciding what risks to insure and how to price the coverage, it is important for them to have a good data set of past experience and loss information. There are some insurers who have been active in the cyber insurance space for a long time, they have developed their own data base of loss experience, have a mature book of business, and have refined their criteria for underwriting decision. But, for the smaller insurers and for new entrants into the market, they do not necessary have the same foundation from which to make underwriting decisions.

A nationwide database or clearinghouse for data breach information, specifically recording how each breach occurred and who was responsible for the breach, could be helpful to the insurance market generally and for businesses that are implementing their own data protection practices, processes, and protocols. Insurers could use the information to supplement their existing underwriting criteria. In addition, businesses in many industries could use the data to learn about the causes of other breaches and apply that information to improve their own efforts to keep consumer information safe. All market participants would be able to use the data, for example, to spot trends in cyber-attacks and hopefully respond before those attacks are repeated.

I do not intend to imply that insurers are making underwriting decisions in a cavalier or uninformed manner. But there is no doubt that not all breach incidents receive national attention in the press and a nationwide database to which business could report information and from which they could learn from others could be a positive force in combating the evolving threat of cyber intrusion and data misappropriation. The federal government could play a role in encouraging the creation of and participation in such a clearinghouse.

I can envision several ways the database or clearinghouse could be established and administered, either by private market participants, the federal government, or a public-private partnership. I do not have a view on the best method to accomplish this, and I concede there is debate on whether this kind of sharing is prudent, but there is a valid argument that more information can be a net positive for the market in general.

<u>Flexible and Industry-Specific Data Protection Guidelines – Assisting Businesses and Underwriters</u>

As this Committee and the other witnesses here today know, there are data protection standards that have been imposed on, or adopted by, certain business segments. For example,

HIPAA provides, among other things, a set of national standards to protect personal health information and applies to "covered entities" and "business associates." This is an example of government imposed standards. On the other hand, the NIST Cybersecurity Framework that was published about a year ago provides a different model from HIPAA. As this Committee is aware, the NIST Cybersecurity Framework was a collaborative effort between industry and government and consists of processes, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the Framework helps owners and operators of critical infrastructure to manage cybersecurity-related risk. The Framework is not a fixed, uniform standard, but instead is a generalized framework for managing cyber-risk based on a continuous cycle of threat assessment and risk mitigation measures which can be customer by industry sector and by each organization. While still evolving, the Framework may over time become a baseline or benchmark of cybersecurity preparedness in some sectors.

There are other markets and industries that have neither legally-mandated nor widely-adopted voluntary security standards and guidance. For example, the mobile apps industry, education institutions and retailers do not yet have industry-specific guidance on what protections they should employ to protect the data they collect, use, and store. As a result of recent 'mega' data breaches, such as Target and Home Depot, we may see more coordinated industry efforts in this regard.

Industry guidance, even if voluntary, can serve several purposes. One, it could provide a standard that businesses can use to gauge their own policies, protocols, and procedures. Two, the insurance market can look to that industry-specific guidance during the underwriting process to assess whether to underwrite a specific business and what price is appropriate for coverage. The NIST Framework contains subjective criteria – it is not a list of quantifiable metrics. Nevertheless, businesses can look to such frameworks as they examine their own business practices and as they consider what to expect when applying for cyber insurance. Insurance company actuaries may find the Framework less helpful, but guidance like the NIST Framework can provide some common expectations that insurers and insureds alike can use. Three, when government sponsored guidelines are industry-led, market participants can have some confidence in the standard that will be applied by a regulatory body in a post-breach inquiry. And, four, the standards could be a useful tool as private litigants and courts look to the appropriate standard of care that a business should be held to.

It seems that the intent of any guidance or standards is to provide businesses with data protection expectations or best practices. But as a secondary benefit, insurers could choose to use the guidance as part of the criteria considered during the underwriting process.

Any data protection guidance or framework, however, consistent with the approach of the NIST Framework, must be industry specific. For example, the data protections guidelines applicable to retailers are different than those applicable to entertainment companies, banks, education institutions, or health care providers to name just a few industries with uniquely specific needs.

In addition, the industry standards must remain flexible to accommodate the size of the company, the data at issue, and technology as it emerges. Software will change, existing technology will continue to evolve, and we will see the use of wearable technology, drones, and the Internet of Things expand in use. Therefore, any government-sponsored or encouraged security guidance must be able to adapt in real time and should be technology-neutral and risk-based.

Insurers understand already that business should not be required to use specific software or hardware. Instead, when deciding whether to cover a particular business or how much the coverage should cost, insurers sometimes are more interested generally in the business's culture towards data protection. If a company is committed to securing the data it holds, that company will likely update its software, its procedures, and its processes, making insurers more likely to underwrite coverage for that business. In examining the data protection culture of a business, cybersecurity frameworks, like the NIST Framework, can be useful tools even though, as stated earlier, they will not provide the actuaries with objective metrics on a particular insured or industry.

If the government decides not to move forward with security guidelines for particular industries, such industry-specific standards and expectations will nevertheless likely develop over time in the marketplace. But, a partnership between the government and private industry could accelerate the development and adoption of flexible guidelines that will, ultimately, benefit consumers without restricting innovation.

Getting businesses to examine their own practices in the course of purchasing insurance does have a recent precedent. Several years ago, when insurers started asking their business customers how they viewed their susceptibility to climate change impacts and what they were doing to address those risks, some business began looking at those issues for the first time and responded accordingly. There was no government mandate for insurers to ask these questions, but insurers did so because they saw that climate change risks could impact their customers and, by extension, themselves. The insurance market could spur the type of self-examination by businesses with cybersecurity measures and there does seem to be a role that the government can play to encourage this outcome. In the end, if insurers are confident that their concerns have been incorporated into any cyberssecurity guidance that is developed and they adopt that guidance as part of their underwriting processes, businesses will be encouraged and incentivized to address those issues even if security standards are not mandated by the government.

I thank you for the opportunity to provide this testimony and am available to try to address any specific questions the Committee has for me on these or related topics.