S. HRG. 114–171

EXAMINING THE EVOLVING CYBER INSURANCE MARKETPLACE

HEARING

BEFORE THE

SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT SAFETY, INSURANCE, AND DATA SECURITY

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

MARCH 19, 2015

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PUBLISHING OFFICE

98–475 PDF WASHINGTON : 2016

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

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

JOHN THUNE, South Dakota, *Chairman*

ROGER F. WICKER, Mississippi
ROY BLUNT, Missouri
MARCO RUBIO, Florida
KELLY AYOTTE, New Hampshire
TED CRUZ, Texas
DEB FISCHER, Nebraska
JERRY MORAN, Kansas
DAN SULLIVAN, Alaska
RON JOHNSON, Wisconsin
DEAN HELLER, Nevada
CORY GARDNER, Colorado
STEVE DAINES, Montana

BILL NELSON, Florida, *Ranking*
MARIA CANTWELL, Washington
CLAIRE MCCASKILL, Missouri
AMY KLOBUCHAR, Minnesota
RICHARD BLUMENTHAL, Connecticut
BRIAN SCHATZ, Hawaii
EDWARD MARKEY, Massachusetts
CORY BOOKER, New Jersey
TOM UDALL, New Mexico
JOE MANCHIN III, West Virginia
GARY PETERS, Michigan

DAVID SCHWIETERT, *Staff Director*
NICK ROSSI, *Deputy Staff Director*
REBECCA SEIDEL, *General Counsel*
JASON VAN BEEK, *Deputy General Counsel*
KIM LIPSKY, *Democratic Staff Director*
CHRIS DAY, *Democratic Deputy Staff Director*
CLINT ODOM, *Democratic General Counsel and Policy Director*

SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT SAFETY, INSURANCE, AND DATA SECURITY

JERRY MORAN, Kansas, *Chairman*
ROY BLUNT, Missouri
TED CRUZ, Texas
DEB FISCHER, Nebraska
DEAN HELLER, Nevada
CORY GARDNER, Colorado
STEVE DAINES, Montana

RICHARD BLUMENTHAL, Connecticut, *Ranking*
CLAIRE MCCASKILL, Missouri
AMY KLOBUCHAR, Minnesota
EDWARD MARKEY, Massachusetts
CORY BOOKER, New Jersey
TOM UDALL, New Mexico

CONTENTS

WITNESSES

APPENDIX

EXAMINING THE EVOLVING CYBER INSURANCE MARKETPLACE

THURSDAY, MARCH 19, 2015

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

The Subcommittee met, pursuant to notice, at 10 a.m. in room SR–253, Russell Senate Office Building, Hon. Jerry Moran, Chairman of the Subcommittee, presiding.

Present: Senators Moran [presiding], Blunt, Blumenthal, and Klobuchar.

OPENING STATEMENT OF HON. JERRY MORAN, U.S. SENATOR FROM KANSAS

Senator MORAN. Good morning, everybody. We are delighted that we are here. I call this subcommittee hearing to order.

Let me first of all thank our witnesses for taking the time to provide us with—I have read the testimony—very valuable information on a topic that I think has not received much attention. We are delighted to have you here and appreciate your willingness to share with us.

I also want to thank our committee staff who worked hard at arranging those witnesses and putting this hearing together.

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 that purchase those insurance policies.

This is our second hearing on a broad topic of data security, and to my knowledge, it is the first time, as I said, that a hearing has ever been held on the cyber insurance market.

American consumers and businesses face ongoing and serious cyber threats. Just last week we learned of yet another. Every time we have had a hearing there has been an announcement of a data breach. May be a reason not to have another hearing.

A Washington state-based health insurance company notified 11 million customers that credit card numbers, Social Security numbers, medical records, and other sensitive information may have been compromised.

A data breach, as we know, is all too frequent, and has become common in our digital lives.

One strategy for business to mitigate cyber or privacy-related losses is to purchase cybersecurity insurance. While some cyber re-

lated losses may be covered under a business' general insurance policy, the increase of publicly reported cyber incidents and data breaches have led 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 and response to a data breach, 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 automobile insurer offering 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 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 between 1.5 and $2 billion in 2014. Some estimates show that the market could grow as high as $5 billion by the decade's end.

During last year, 2014, the number of clients at brokerage, Marsh & McLennan, who purchased stand-alone cyber coverage increased by 32 percent over 2013. Among their clients, the highest take up rates for cyber insurance in 2014 were in health care, education, hospitality, and gaming.

The challenges in the cyber insurance market exists due to the difficulty of quantifying the exposure to cyber risk, 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 their networks.

For instance, a startup named BitSite partners with Liberty International Underwriters to externally analyze a company's cybersecurity. In one case, BitSite helped discover a dormant threat in a company's IT system, and the insurer was able to work with the company to avoid the possible breach.

Another example in my home state of Kansas, Overland Park-based risk analysts partner with AIG to provide security products to some AIG insurance products.

This Congress considers cyber threat information sharing legislation as well as a national data breach notification standard.

There are lots of important questions about developing the state of a private insurance market that come to mind. Today, we will focus our attention on some of those key questions, and I am confident today's expert panel can share their valuable insights on these topics.

I would like now to turn to the Ranking Member, my friend and colleague, the Senator from Connecticut, Senator Blumenthal.

STATEMENT OF HON. RICHARD BLUMENTHAL,
U.S. SENATOR FROM CONNECTICUT

Senator BLUMENTHAL. Thank you so much, Senator Moran. I really appreciate your convening this hearing on a topic of huge importance to the entire country, indeed, the world, and certainly to my home state of Connecticut. I want to join you in thanking our staff, but most especially the experts who have come to be with us today.

This topic, I can tell you, is of tremendous interest to my colleagues. I have spoken to them about this issue over the last couple of days. We have a busy day today, so the attendance here may not reflect that interest, but I can tell you there is no topic more important than cybersecurity to the U.S. Senate and maybe to our country.

At this moment, the Armed Services Committee, and I am a member of that committee as well, is having a hearing on the budget for our military cyber warfare activities in part. The two are inextricably linked, the private security and our national defense security.

As you well know, we are struggling now to deal with the problems raised in both spheres, which are very closely linked.

Hartford, Connecticut is home to the Nation's oldest continuously published newspaper, the *Hartford Courant,* but it is also home to many of the world's biggest and greatest insurance companies. It is known colloquially as the insurance capital of the world. Some may dispute whether any place in the world is an insurance capital these days because of their multinational activities. Hartford, I think, has the longest standing claim to that title.

We are a small state but we actually still rank number one in total insurance jobs as a percentage of total employment.

I am particularly pleased to see one our nation's experts, Michael Menapace, of Quinnipiac University joining us here today. Thank you, Michael, for being here.

I am also happy to be here today to learn, and I really do mean learn more about this issue. We all think we know a lot about breaches because they are so common, as Chairman Moran said, but each in many important respects is different from the other, in its consequences and causes, and what can be done to prevent these kinds of breaches.

That is the issue that brings us here today: how to prevent them, how to insure against them, and how to use insurance as an incentive, as a tool, to provide for stronger prevention.

The simple and stark fact is that the Internet was not built for security. The Internet was not built to be secure. It was not intended to be the commercial and financial backbone of the post-industrial world. It was designed as an open system, and it was based and still is based on anonymity, meant to be used among a select group of Government officials and university computer scientists.

Very sadly, it seems like this dynamic has in some ways reinforced the picture we see every time we open the newspaper to read of millions of consumer records stolen from major retailers: Target, Neiman Marcus, Home Depot, Anthem.

Data breaches are hardly a new phenomenon. When I was Attorney General of the State of Connecticut, we tried to deal with them in terms of providing protections to consumers, and consumers have been facing and paying for data breaches for years.

Consumers are hit the hardest, but the growing threats of cyber attacks and data breaches impair more than just our consumers, and it is our critical infrastructure now that has a huge risk, and has so much at stake. They are increasingly hitting the bottom line of our major companies.

The question is whether insurance can play a role in preventing these kinds of breaches, what kinds of insurance are best designed to cover damages from security breach or cyber attack, and why companies do not more commonly choose to have cybersecurity insurance.

A lot of these companies cite its high cost, lack of awareness about what it covers, uncertainty that they will suffer a cyber attack as reasons for their decisions or non-decisions to have insurance.

I am looking forward to the panel's testimony today to know about what has been changing, the dynamics of this industry, and what can be done to encourage the growth of this very dynamic market, and ultimately increase its positive impact on the security of consumers' sensitive information.

Thank you very much for being here today.

Senator MORAN. Senator Blumenthal, thank you very much. Our witnesses are Mr. Ben Beeson, Vice President for Cyber Security and Privacy at Lockton Companies. Ms. Catherine Mulligan, Senior Vice President of Management Solutions Group for Zurich, North America. Ms. Ola Sage, CEO, e-Management, an IT firm from Silver Spring, Maryland, and Mr. Michael Menapace, Counsel at Wiggin and Dana, who also serves as Adjunct Professor of Insurance Law at Quinnipiac University School of Law.

It is a good thing to have a polling organization so I know how to pronounce the University's name.

Thank you all very much for being here. Mr. Beeson, we will begin with your testimony.

STATEMENT OF BEN BEESON, VICE PRESIDENT, CYBER SECURITY AND PRIVACY, LOCKTON COMPANIES®

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

My name is Ben Beeson. I am Vice President for Cyber Security and Privacy at Lockton. Lockton is the largest privately held independent insurance broker in the world. I am based in the Washington, D.C. office where I advise clients on a cyber risk management strategy that addresses crucially 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 even nation states.

Well-publicized attacks have sought to target and monetize personally identifiable data and protected health information. However, it is also commonly understood that the theft of corporate in-

tellectual property is a significant problem with non-trivial impacts on innovation for companies and countries, and companies also face incidents that can disrupt or destroy information technology and other vital assets, even now physical assets.

The key message I would like to convey today is this, we believe that cyber insurance is an important market force that can drive improved cybersecurity within companies but also importantly thereby improve consumer protection and the nation as a whole.

There is an important link there. It should not just be seen as a financial instrument to transfer risk from one balance sheet to another. As the cyber insurance market develops, it will provide incentives for companies to understand and better mitigate their risks.

For example, forward thinking companies invest in workplace safety to reduce their Workers' Compensation costs, and in the same way, sophisticated companies are investing in strong cybersecurity. Those companies ultimately will experience fewer losses and insurers will see fewer claims and the premiums will be lower.

In addition, and importantly, simply just engaging in the process of seeking cyber insurance coverage can also assist businesses to develop the correct approach to mitigate risks. It is no longer just the domain of the IT Department.

Cyber insurance can also act as a catalyst for driving an enterprise-wide risk management approach. It can bring all the relevant stakeholders together, in IT, Legal, Risk Management, R&D, Finance, Human Resources, Communications, and perhaps now most importantly, the Board itself.

So, do not view cyber insurance as just a commodity that you may or may not see at the end of this process.

However, we are not there yet today. The cyber insurance market is still young and developing. Companies today spend about $2 billion annually on cyber insurance, a fraction of the $1 trillion U.S. insurance market.

Lockton also sees the NIST Framework aligning hand in glove with this enterprise risk management 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, areas for improvement, and desired future status.

As insurance brokers, we also advise directors and officers on management liability, and we see that cyber risk has now entered the governance dialogue. The NIST Framework has proved immensely helpful in driving better board discussions.

Building on a public/private partnership, discussions are ongoing with the Department of Homeland Security 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 accelerate the growth of the marketplace, and crucially accelerate the ability of cyber insurance to act as a market incentive for industry to invest in cybersecurity.

In addition, 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.

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

[The prepared statement of Mr. Beeson follows:]

PREPARED STATEMENT 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 U.S. and the Lloyd's of London marketplace provide dedicated cyber products and solutions today. Buyers are overwhelmingly concentrated in the U.S. 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, 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.

---

[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

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 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.

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.

Senator MORAN. Thank you very much, Mr. Beeson. Ms. Mulligan?

STATEMENT OF CATHERINE MULLIGAN, SENIOR VICE PRESIDENT, MANAGEMENT SOLUTIONS GROUP, ZURICH (NORTH AMERICA)

Ms. MULLIGAN. Good morning, Chairman Moran, Ranking Member Blumenthal, and members of the Subcommittee. My name is Catherine Mulligan. I am a Senior Vice President with Zurich (North America) with our Management Solutions Group.

I lead a market facing team of underwriters who are responsible for working with our brokers and customers on the placement of cyber insurance.

I appreciate the opportunity to speak with the Subcommittee today, and I apologize for my laryngitis as well.

As a brief introduction, Zurich Insurance Group is a global multiline insurance provider with a global network of subsidiaries and offices, 55,000 employees, and customers in more than 200 countries and territories.

We are the fourth largest commercial property and casualty insurer in the United States by gross written premium. Mr. Chairman, as I am sure you are aware, we employ over 400 people in the state of Kansas.

Zurich has had a cyber insurance product for over 10 years, and we have invested heavily in the last few years in thought leadership to address the risk management concerns of our customers.

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, and while sources suggest that the current market is $2 billion in gross written premium, this number is actually hard to verify due to the fact that the coverage can be offered blended with other coverages in addition to stand-alone.

The product was first introduced about 15 years ago and has its roots in technology errors and omissions, a third party financial damage coverage, and as privacy regulations evolved, companies found that they were incurring costs, first party costs, to respond to privacy events and comply with these regulations, so cyber policies were developed to respond to this blend of first and third party costs arising from breaches and privacy events.

In January of this year, the Insurance Information Institute reported that market capacity for cyber is on the rise, and while this optimism is understandable, given the visibility of these issues, the reality is that the shape of the marketplace continues to shift.

Number one, capacity is in flux, so in the Dowling & Partners' report in October, they said that over 60 carriers wrote the coverage, but that number has since decreased as some excess markets are pulling out of the product or reevaluating their appetite, and reinsurers are doing the same.

Pricing is in flux. 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, and in the large company space, over $1 billion in revenue.

Loss experience is developing. Highly publicized breaches have led to direct damages in the hundreds of millions of dollars of costs which continue to rise, and liability costs have yet to be determined, so what these recent breaches show us is that there is a severity potential as well as this unknown element as liability issues are resolved in court.

Coverage and aggregation challenges remain. It is important to understand the history of the product as financial loss insurance, as the total scope of exposures presented by a cybersecurity event currently are beyond the scope of the current coverage.

For example, a cyber attack may cause physical damage, and while some limited coverage is available in the marketplace, current security and privacy forms generally exclude bodily injury and property damage.

The scope of the exposures is too broad to be solved by the private sector alone, not all exposures are transferrable to an insurance policy.

That leads us to the emerging issues of aggregation tracking and emerging exposures. Multiple lines of insurance may be impacted by a security event. For example, if a public company has a significant breach and then has a stock drop as a result, they may face a shareholder derivative suit, which can then come in as a claim under their directors' and officers' liability policy.

That leads us to the public/private sector cooperation. In 2015, the World Economic Forum report stated "The global risks transcend borders and spheres of influence and require stakeholders to work together."

This echoes Chairman Thune's comments from the February 4 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, as Mr. Beeson said, includes working groups at the Departments of Homeland Security and Treasury on the issue of data repositories, which may need to take a couple of different forms—sharing of cyber event data, such as attack vectors, and cyber insurance data, including claims and underwriting information by sector.

While it is too early to assert any definitive conclusions, the potential upside of these repositories would be more comprehensive information could help the insurance industry develop broader coverage and broader risk management solutions for our customers.

Thank you.

[The prepared statement of Ms. Mulligan follows:]

PREPARED STATEMENT OF CATHERINE MULLIGAN, SENIOR VICE PRESIDENT, MANAGEMENT SOLUTIONS GROUP, ZURICH (NORTH AMERICA)

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 percent 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 straightfoward, 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 percent 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.

---

[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)

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. 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.*

  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

[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

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

court. Moreover, we see attack vectors shifting, for example, approximately 30 percent 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.

  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.

Emerging issues

- *Aggregation tracking and emerging exposures*

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 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

---

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

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

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

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

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.

Senator MORAN. Thank you very much. Ms. Sage?

STATEMENT OF OLA SAGE, FOUNDER AND CEO, E-MANAGEMENT

Ms. SAGE. Good morning, Chairman Moran, Ranking Member Blumenthal, and to the other members of the Subcommittee. It is an honor for me to be here today, and thank you for the opportunity to testify on behalf of my company, e-Management, as a small business consumer of cybersecurity insurance products.

My company's journey into the cybersecurity insurance market began in 2013. Small businesses had become the fastest growing segment for cyber attacks, and I was advising other small businesses to obtain appropriate business and legal protections, such as cybersecurity insurance.

However, my company, a 15-year-old IT services and cybersecurity firm, was not covered. I decided that needed to change. Working through our insurance broker, we began researching cybersecurity insurance products but could not find products designed specifically for small businesses.

We submitted applications to several large insurance companies, and these applications varied in length and substance with very little consistency in the questions asked.

Comparing the policies against one another 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.

Regrettably, I cannot tell you that our selection of a cybersecurity insurance product was based on a simple and easy analysis of options, and I also cannot say with confidence that we picked the best policy for us.

Our process took 4 months and our policy cost over $10,000. This was a significant investment for a company our size.

We recently passed our one year anniversary, and this time around, the process started with a letter from the insurance company informing us that our coverage would not automatically renew. The abbreviated three page application included one cyber-related question that asked about changes regarding the security and protection of our facility and network.

Three weeks later, our policy was renewed. That was the good news. The surprising news was that our premium increased by 12 percent. Stunned, confused, and frustrated are just a few words that described our reaction.

Our broker explained that there were a variety of factors that went into the underwriting process, and in our case, ironically, because our revenues grew in 2014 over 2013, that appeared to be the primary contributor to our increase.

After a year of using the voluntary NIST Cybersecurity Framework and investing in processes and tools to improve our overall cybersecurity readiness, it was discouraging to be in essence rewarded with an increase in our premium.

My experience though is not unique. As I speak to small business CEOs across the country, many elements of our story resonates.

In addition, there is a general lack of awareness in four areas. One, the need for cybersecurity insurance for small businesses. Two, the availability of insurance products on the market. Three, what the various policies cover, and last, what these insurance products cost.

I would like to offer three recommendations that I believe would encourage more small businesses to take greater advantage of cybersecurity insurance products.

First, increase the awareness of cybersecurity insurance as a risk transfer option for small businesses. According to a recent industry survey, only a third of small and mid-sized businesses are even aware that cybersecurity insurance exists, and of that number, only 2 percent actually hold cybersecurity insurance.

With the average annual cost of cyber attacks to small businesses reported to be close to $200,000 and the median cost of down time reported at $12,500, the majority of small businesses just cannot sustain these costs, leading many to close their doors.

Cybersecurity insurance can be an important tool to help small businesses manage significant financial exposure.

Second, make cybersecurity insurance affordable for small businesses. Cybersecurity insurance needs to provide meaningful coverage that small businesses can actually afford. We believe offering competitive cybersecurity products designed for the small business market will ultimately lead to better deals for small businesses.

We recommend that insurance companies consider a company's use or application of the voluntary NIST Cybersecurity Framework as a best practice factor in their underwriting processes.

Third, reward small businesses who are actively managing their cybersecurity risks and implementing reasonable security measures. Based on our own experience, we strongly believe that any small business that uses the NIST Cybersecurity Framework can significantly reduce their cybersecurity risk exposure and should be preferred candidates for lower premiums.

In closing, I welcome and appreciate the emphasis that Congress, Federal, state, local agencies, and private sector organizations have placed on small business cybersecurity protection. As the threat and challenge to small businesses continues to persist, we at e-Management are committed to continuing to work with all parties to identify and develop simple and affordable solutions.

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

[The prepared statement of Ms. Sage follows:]

PREPARED STATEMENT OF OLA SAGE, FOUNDER AND CEO, E-MANAGEMENT

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 cyberattacks 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 percent 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 percent 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 percent.

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 percent 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 percent were either "very" or "moderately" intrigued, with another 32 percent "minimally" intrigued, giving an overall 84 percent 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 percent 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 Software Advice, only a third of small and midsize businesses are even aware that cybersecurity insurance exists and of that number only 2 percent 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.

---

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

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 percent 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.

Senator MORAN. Thank you very much. Mr. Menapace?

STATEMENT OF MICHAEL MENAPACE, COUNSEL, WIGGIN AND DANA LLP, AND ADJUNCT PROFESSOR OF INSURANCE LAW, QUINNIPIAC UNIVERSITY SCHOOL OF LAW

Mr. MENAPACE. Good morning, Senator Moran, Senator Blumenthal. Thank you for inviting me to today's hearing.

I have submitted written testimony, but I appreciate the opportunity to highlight a few of the issues that I discussed in that testimony, including the evolution of cyber insurance and its cost drivers, breach notification requirements, data breach information sharing, and data protection standards.

As you have heard, in the early 2000s, a small group of insurers did start offering cyber insurance. Those early insurers have now acquired somewhat significant experience and are sophisticated participants in this specialized market, but the market also has smaller insurers who are less experienced and do not necessarily

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

have the same level of expertise as the market leaders, and have less mature books of business.

When cyber insurance was first conceived, we originally thought the cost driver would be third-party litigation against insureds as well as first-party property losses. While litigation is still an important consideration, there was not an appreciation at that time of what would become the cost drivers.

According to several industry sources, data breach response costs, sometimes referred to as "crisis response costs," now account for up to 50 percent of the cost of data breaches. These response costs include technology forensics services, legal guidance, consumer notification, credit monitoring, call centers, public relations.

With regard to the legal guidance and consumer notification, there is an available strategy to lower the costs. Currently, there are 47 states with separate breach notification laws, some of which are inconsistent with each other.

As a result, when a breach occurs, businesses and insurance companies engage lawyers like me to perform 47 legal analyses based on the facts at hand. As you can imagine, 47 separate legal analyses can get expensive. Moreover, the diversity of the 47 states means that a consumer in one state may be notified while a consumer impacted by the same breach who lives in another state may not be notified.

A single Federal standard that preempts the current patchwork could save time and expense and provide for the uniform treatment of consumers.

With regard to data sharing, I mentioned that some insurers have mature books of business, and they rely on their own proprietary analytics to analyze the data they hold. Other market participants, however, could benefit by accessing a nationwide pool of data to help them decide which risks to underwrite and the appropriate premiums to charge.

A nationwide database of cyber breach information, particularly with regard to the origins and causes of the breaches, could also assist non-insurance businesses as they assess their own processes and protocols and look to spot trends with the goal of avoiding loss.

I appreciate the competing positions and interest on this issue, but whether the database is created and maintained by a public agency, the private market, or a public/private partnership, I do believe the market as a whole could benefit from sharing information about data breaches.

Finally, I would like to say a few words about data protection standards. HIPAA provides one model, it provides the model of Government mandated data protection standards. Another model is the development of flexible industry led and voluntary guidance for specific industries, like we have with the NIST Framework.

Now, the existing NIST Framework cannot simply be applied to other industries, but it is an example of what a public/private partnership can look like. That type of framework can inform businesses on their own practices, and even though they are largely subjective in nature and therefore of limited value to insurance actuaries, the goal and guidance in the Framework could be incorporated by insurers as part of their underwriting considerations.

Appropriate data protection practices will likely evolve over time without government involvement, but government involvement or encouragement could be an efficient way to help the standard evolve more quickly across a variety of markets.

I am happy to answer and respond to any questions.

[The prepared statement of Mr. Menapace follows:]

PREPARED STATEMENT OF MICHAEL MENAPACE, COUNSEL, WIGGIN AND DANA LLP; ADJUNCT PROFESSOR OF LAW, QUINNIPIAC SCHOOL OF LAW

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.

A Federal Breach Notification Standard—Reducing the costs of breach responses and treating consumers equally

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 time-frame within which business must notify consumers whose data may have been affected. The time-frame 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.

Nationwide Data Clearinghouse—Assisting underwriting and spotting trends

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 database 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.

Flexible and Industry-Specific Data Protection Guidelines—Assisting Businesses and Underwriters

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.

Senator MORAN. Thank you very much. We appreciate the testimony. I look forward to the dialogue that now will occur with you.

Let me start with a typical congressional question, which is about legislation. You, Mr. Menapace, talked about the standard, the information sharing. Mr. Beeson, you indicated the industry would be supportive.

As you heard me say and maybe know, this subcommittee had a hearing a few weeks ago on those topics, what the standard should be, how it should be enforced.

Let me ask, if you were in our shoes, and this is really a question to all the witnesses, if you were in the shoes of a Member of Congress, what is the legislative solution that would drive the increase in an insurance market, and what I think would be the consequence of that would be better security practices and less opportunity for breach.

What public policy should we pursue, what legislation should be passed by Congress that would enhance the chances for that scenario to occur?

You do not sound like you are from Kansas City, but we consider you one of us.

Mr. BEESON. Thank you, Chairman. I think as you heard in my testimony, there is a real linkage between improved cybersecurity and potentially the growth of the insurance market itself. I was arguing that more statistics can help drive that, more data can help drive that, but equally, if there was legislation passed that helps industry improve its security posture, which I believe the proposed legislation to do with threat indicator information sharing between industry and Government and between industry.

As we have seen, that has been very effective already in some of these ISACs, information sharing analysis centers, within the private sector. Actually, it would help industry improve its security and thereby help the insurance market sign onto risks, if you like, that it otherwise would not have done. That would in and of itself help grow the market.

Senator MORAN. Anyone else? Ms. Mulligan?

Ms. MULLIGAN. Thank you, Mr. Chairman. I would support what Mr. Menapace said around a national database of information because the breaches right now are really outpacing the usual time it would take for an insurance product and pricing to develop.

That information would help us, as Ms. Sage points out, differentiate the pricing and the coverage for different sizes of insurance and industry segments.

Senator MORAN. You agree with Mr. Menapace about the national standard as compared to 40 some states?

Ms. MULLIGAN. I agree with him actually on both points, the national standard for notification, because that would streamline the process and the cost for insureds, but also on a data repository of sharing information.

Senator MORAN. I am actually surprised that there is enough information in today's current world for you to price an insurance policy. What is out there that allows you to have this market to the degree that it exists today?

Mr. BEESON. As you heard from Mr. Menapace, the cyber insurance market has been around for roughly 15 years, and really since the first breach notifications in California in 2003, the market has built up data.

Specifically, it is important to delineate this, because there are different types of assets at risk here. The cyber insurance market is focused primarily on the risks of handling personal data, consumer, patient, employee. There is quite a bit of data around to model, "data" being statistics, around frequency severity, to model the risk in that area.

The problem at the moment is there is a dearth of information now as the risk has morphed, for example, into the risk of physical assets. On the utility, maybe I am not so worried or that is not my primary concern, handling of personal data. I am more worried about physical damage to the turbine from a cyber attack, for example. That is very challenging right now, and frankly, ambiguous as well for the insurance industry in terms of how to handle that.

Senator MORAN. While the industry is growing, it is growing everywhere, but different from segment to segment, it is coverage to coverage, the type of risk that you are insuring?

Mr. BEESON. As I say, to some extent, this is a symptom of the insurance industry, it is fairly siloed and risks are looked at in different boxes, if you like, with different specialist underwriters.

Cyber is a challenge, of course, because it sits across just about everything, and it is only recently, and thanks really to the Federal Government shining the light on the issue through the creation of the NIST Framework, that cyber is being viewed in a much broader perspective.

It is not just about data breaches. It is actually now also—I think this in many ways should be seen perhaps as a greater concern to

Government. It is a critical infrastructure industry, many of which are more worried about physical damage, business interruption loss, bodily injury, as Ms. Mulligan hinted on as well.

That is where there is a real challenge right now in the marketplace, and where the focus is shifting. I am not saying the handling of personal data is not an issue. It certainly is, and we have seen that over the last year. There is no doubt about that. It is much broader than that now.

Senator MORAN. Do the suggestions that you have made regarding public policy improve the circumstances for all the silos you described?

Mr. BEESON. Certainly, as I mentioned before, I support the threat indicator legislation. I think frankly if you talk to experts in the security industry in particular, they will tell you security has to become more intelligence based to tackle this problem, and clearly threat information is key to that.

There is a whole debate about legacy defenses around firewalls' intrusion detection systems, which is still important, but they are not enough. How do we provide industry with that type of intelligence, and I think public policy or legislation proposed around threat information would be hugely helpful.

Senator MORAN. Across the board?

Mr. BEESON. Yes.

Senator MORAN. Senator Blumenthal?

Senator BLUMENTHAL. Thank you. Just to follow up on that question, Mr. Beeson. What would that threat indicator or intelligence look like? A requirement by the insurance company that there be access to government intelligence or what specifically would that be?

Mr. BEESON. In order to help facilitate an insurance company to underwrite the risk? Is that the premise of your question, Senator?

Senator BLUMENTHAL. Yes.

Mr. BEESON. I will quickly, and then I am going to defer to the underwriter here, but in my opinion, in Lockton's opinion, I think there needs to be a change in the way insurance companies have been underwriting this risk, which has been much more, as I think we have heard from Ms. Sage already, a snapshot or questionnaire, which is a sort of static look at security, which now needs to change to something that is much more dynamic, which is a partnership with both government and probably the security industry to provide that type of intelligence as part of the underwriting process.

Actually, as we heard from the Chairman in his opening remarks, that has already started with this firm BitSite.

Senator BLUMENTHAL. What do you think about that, Ms. Mulligan?

Ms. MULLIGAN. I think Ms. Sage's testimony rightly points out the challenges underwriters have, asking the questions. We are trying to evaluate in an efficient way, people, process, and technology.

Right now, we have an issue where attack vectors are changing more quickly than I think we know how to ask the right questions. Historically, the assumption at the enterprise level was that it was an IT issue, and that is something that has changed in the last 18

months, where now boards of directors are really on notice that there has to be a high level governance of this problem.

We really encourage a culture of awareness from the board room to the mail room. Protection is probably not 100 percent possible for any one company. We really look to help companies move to resiliency rather than just protection.

Are we asking the right questions, can we ask the right questions tomorrow when the attack vector has changed or the attacker has changed, and then are we able to design coverage that can respond to all the consequences of an attack?

The issues are outpacing where we are right now, so the availability of information, underwriters think in trends, so it is not necessarily that I need to know the specifics from a government perspective for just Ms. Sage's industry sector or some other sector. It helps me to think in terms of trends, where is the frequency, where is the severity, and then that helps me design coverage and pricing.

Senator BLUMENTHAL. Let me ask Mr. Menapace, because you emphasized in your testimony the importance of culture, are companies asking the right questions? Obviously, as Ms. Mulligan says, they have been on notice for a while about these threats. Are they doing enough? Are they asking the right questions, and are they acting sufficiently?

Mr. MENAPACE. I think there are two areas where insurers are looking into. One, as we talk about the national database, it would be helpful in a sense to look at industries. Is this potential insured a retailer, are they a health care provider, are they a manufacturer, and a national database will help the insurers identify those trends.

When you get to the specific level of that insured, however, insurers are trying to keep up with what are the right questions that we want to ask of this potential insured, and that is much trickier, there is no doubt about that. I have no doubt that the collection and sharing of data will help in that regard.

A number of underwriters now are looking toward what is the business' culture toward data protection as opposed to do you have this particular piece of software in place. That question is almost useless.

Senator BLUMENTHAL. Software changes and it is so dynamic.

Mr. MENAPACE. Yes.

Senator BLUMENTHAL. Are there not sort of fundamental questions? The question I heard asked repeatedly in the wake of the Anthem breach was, why was there no encryption? In the wake of the Target breach, why are retailers not using chip and PIN rather than swipe technology? Evidently, chip and PIN technology is widely used, maybe almost universally used in Europe.

Costs and the sharing of costs and the allocation of costs has been an obstacle. Lack of agreement on allocation of costs.

It strikes me there are certain elements to protection that are changing. Technology is changing, the type of encryption is changing, but the complete absence of certain techniques maybe is reflected in the culture. Maybe that is what you mean by "culture."

Mr. MENAPACE. That is exactly what I mean. When an underwriter can go into a business and speak with the IT, the management, everybody, all the stakeholders, they will be able to get a

sense of that culture in the sense of what they have now is fine, but everyone needs to realize that three months from now, that may not be fine.

Both the insurers and the insureds need to understand this is a continuous process because the technology is advancing so quickly, and the threats are evolving so quickly.

My guess is the questions that insurers like Zurich and others are asking today are going to be different questions that they will be asking 6 months or 12 months from now of their applicants.

Senator BLUMENTHAL. I have other questions which I hope to ask on a second round, but I am going to defer to my colleagues who are here, because they are on schedules as well.

Senator MORAN. Senator Blunt?

STATEMENT OF HON. ROY BLUNT,
U.S. SENATOR FROM MISSOURI

Senator BLUNT. Thank you, Chairman. Thank you and the Ranking Member for holding this hearing.

Obviously, cyber and all elements of cyber need to get a lot of attention. I am hopeful this Congress can move forward in a couple of different areas, data breach, as well as information sharing.

My view on this is if we have a dramatic cyber event and have not legislated, we will overreact, so this is an important time for us to be having this discussion so we have something in place when this happens.

Mr. Menapace, one of the things in the bill we voted out of the Intelligence Committee that I serve on last week, and I am not sure how available that bill is, but I do know one of the topics in the bill is allowing competitors to share information in this area, with no concerns about price fixing or any of the things we would normally be concerned about there, but for them to be able to share with others in the industry the kinds of attacks they are having, fighting off successfully or not.

Do you want to make a brief comment on that as a concept?

Mr. MENAPACE. Certainly, Senator. The idea of sharing would be helpful in several areas. Insurers generally are not in the game of guessing. They rely on actuarial analyses. Without the data to back that up, that is impossible to do.

Some insurers have robust and mature books of business but newer entrants do not. The sharing of the data would allow new entrants into the market, and for those existing insurers would provide more certainty and more available data to incorporate into their own underwriting to make sure that the premiums charged are appropriate.

The other area where the sharing can be helpful is for non-insurance businesses. They, too, if they had access to the data would be able to test what is going on, what are the trends, spot the trends, and then compare that to what are we doing right now. If we see this trend, are our protections robust enough that we would be able to respond, mitigate, or even avoid that kind of loss.

Senator BLUNT. Mr. Beeson, one of the things we have consistently talked about here is some liability protection if you followed the standards that a new Federal law would set forth for cyber protection, and that would be one of the elements I am sure we want

to look at, but another thing I am wondering about, is there any evidence yet of insuring against the actual loss?

Is there anything publicly available frankly that any of you know about these data breaches that we have already had that would give us a sense of how much might be lost in terms of the destruction to your internal system, the equipment, the information, the cost it takes to replace that, and is this something you are seeing people interested in trying to insure against as well?

Mr. BEESON. Yes. The insurance market outside of insuring the costs of a data breach or a violation of an individual's privacy has also provided coverage for what is called "non-physical damage business interruption."

Attacks that bring down corporate networks or impact corporate networks, impact revenue, and other related costs such as the cost to restore data. Those types of attacks we know now exist.

The actual costs, as you asked, is not public knowledge, I think, other than between a client and its insurance broker. When you see some of these losses disclosed in 10-Ks, what have you, as public filings, typically they seem to appear as a total amount. It does not seem to break down those costs, unfortunately.

In my experience, I will say at least to date, the biggest component of a cost from a breach that involves personally identifiable data, protected health information, is dealing with that itself, rather than the cost on your infrastructure.

I think that is starting to change, and we have seen a precedent from that last year where the attacks were becoming more destructive or could certainly become more destructive, rather than just about what they call "exfiltrating," stealing data to monetize it. This goes back to how the attacks are changing and what will be the consequential losses from that.

Senator BLUNT. Exactly. I think that is something that we are seeing as a growing problem. Mr. Chairman, I am already out of time.

Senator MORAN. Thank you. Senator Klobuchar, welcome.

STATEMENT OF HON. AMY KLOBUCHAR,
U.S. SENATOR FROM MINNESOTA

Senator KLOBUCHAR. Thank you very much, Mr. Chairman, for holding this important hearing. I think we all know this is an issue whose time has come, and we also need to spur the private sector to increase the securities and protections.

I want to start out with actually a small business question. We have a lot of big businesses in my state, some of which has been kind of notable for having some cybersecurity attacks, as you may know. While those kinds of attacks get attention in the headlines and affect millions of customers, many small businesses and community banks are also the victims of these kinds of cyber attacks.

Ms. Sage, how would the insurance agency help these businesses manage the risk of cyber attacks and provide insurance at a reasonable rate? What do you see as the unique challenges facing small and medium-sized businesses, and what can we do to help them?

Ms. SAGE. Thank you, Senator. I agree with a number of the comments that have been made about company culture, and the

need to really understand what the perspective is of the management of these small businesses toward cybersecurity risks.

In my submitted testimony and also in my oral testimony this morning, there were a number of themes that I have been hearing in my travels and talks with small businesses. For example, there is a segment of the small business community that just does not believe this applies to them and have the sense that they do not have information that anybody would want.

I think it really does speak to culture. I think this is where insurance can have a role in making it a priority for small businesses to think about.

Senator KLOBUCHAR. OK. Ms. Mulligan, even larger companies with policies from several different insurance providers cannot find policies to cover their cybersecurity needs. I know some of our companies may often have to purchase multiple policies with different retention levels and still have to partially self-insure.

How does the lack of the availability of a comprehensive cyber insurance policy affect a company's ability to manage risk?

Ms. MULLIGAN. Every company will manage their risk differently, so the idea of risk transfer is really only one element of a risk manager's tool, available in their toolbox.

There will be decisions to self-insure, but this is where we get back to the information sharing. The availability of information that would help a company like Zurich determine appropriate pricing for capacity would then allow for an expansion of capacity, and as Mr. Menapace pointed out, for new entrants to come into the marketplace to build out more robust programs. We are not there yet.

Senator KLOBUCHAR. Also, 90 percent, Mr. Beeson, of the critical infrastructure in our country is privately held, and these companies are on the front line, and every exercise we have ever had where we talked with our national security people, it is always about some kind of a private infrastructure company. I believe it is in their own best interest to establish robust policies.

In general, do you believe critical infrastructure sectors in the economy and companies are taking appropriate steps? What more do you think they should be doing?

Mr. BEESON. I think there are a lot of challenges there. I have spent quite a bit of time looking at certain industries, such as energy, for example, over the last couple of years. The more you dive into that, the more you see the challenge.

I think number one is risk awareness, education on these risks throughout the organization. Does the board realize the differences between, for example, corporate information technology and what is called "industrial control systems," operational technology. They are very different. One is built to be available and one is built to be secure, but they are interlinked, and the challenges that go around that.

I would say there is a lot of work to be done in this area, and it goes back to what I said earlier about cyber risk, cyber insurance needs and can be an incentive to help that process, but to do that, if we are going to look at other enterprise assets that the insurance industry can address, and if you look at critical infrastructure, you are now talking about physical damage, business interruption loss.

I agree with my fellow witnesses here we need more data and more information to help drive that process.

Senator KLOBUCHAR. For the first time, some of our smaller rural electric companies raised cybersecurity with me, which I think is a sign that people are starting to see it and understand they need to start preparing for it.

Thank you very much.

Senator MORAN. Thank you, Senator. Ms. Sage, do you know, and in a broader question to the panel, do the insured know what is covered? Can you tell from your policy that if something happens, it is either included or excluded in coverage?

Ms. SAGE. Chairman, the answer is no. It is very difficult, and not just the cost of the policy, but legal assistance to help us understand the policy, so now you have costs on top of the policy itself to understand what your policy covers and does not cover.

Senator MORAN. What do you think your policy covers? What events, what might happen to your company that you feel pretty certain are covered and ones you have doubt about?

Ms. SAGE. I think some of the costs associated with let's say there was an attack and there was equipment potentially that was compromised, those costs might be covered. I believe costs associated with notification and things like that might also be covered.

What is more unclear is what is not covered. We keep hearing, well, it is claim-specific. Well, you do not know what your claim is going to be until you have that, and hopefully you never have that. That is a little bit of a challenge in understanding.

Senator MORAN. I do not know your business, but would you be subjected to litigation by those damaged by the cybersecurity, your customers or clients?

Ms. SAGE. Possibly. We provide services to the Government as well as the private sector. I think there is exposure, we hold information that is perhaps sensitive, business sensitive, et cetera.

In terms of what we are seeing in our Government contracts, it is really a mix. Some agencies are more focused on cybersecurity and including language in contracts that address that. Others do not have anything that speaks specifically to cybersecurity and just speak to security in general, and in protecting the Government's information. I think really right now it is a mix.

Senator MORAN. You have heard Ms. Sage's testimony plus her response to me. My question to the rest of the panel, are the policies any more standardized now than when Ms. Sage described what she went through with different companies? Mr. Menapace?

Mr. MENAPACE. No, there is no standardized policy language. You may be aware, there is an organization called ISO, the Insurance Services Office, that does provide standardized wording for a whole line or many lines of insurance.

ISO recently did issue cyber policy wording. However, I know of no insurer who has adopted the ISO form, and I know of no insurer who plans to adopt the ISO form.

What we have out in the marketplace are 40 or 50 different policy wordings for these coverages. I have to say this is an area where brokers are important, and this is where they earn their money, to help the insureds assess their own risks and then match those up to the different protections that are being offered.

Senator MORAN. Do agents know—does the agent in my home town know when the businessman or woman came to him or her—would they be knowledgeable about this topic?

Mr. MENAPACE. Certainly, the big insurers do. Excuse me, the big brokers do, certainly. The smaller brokers, if they have taken the time to educate themselves, are valuable, and certainly there is a group of smaller brokers who I refer clients to for this very reason, because they have taken the time to understand the coverages, and they take the time to go into the businesses and assess what their risks really are, rather than pulling something off the shelf and saying here is cyber insurance.

Senator MORAN. You said 40 or 50 companies, the market is not yet sophisticated enough to say these are the companies that have the best policies. Have we narrowed this down to those who know what they are doing and those that do not?

Mr. MENAPACE. I am even underestimating the 40 to 50 companies, because each of those companies offer different policy coverages depending on the size of the business, what sector of the business they are in, and what their needs are.

The matching up of the risks and the needs will continue to be a problem, and it is certainly something that large businesses look at extensively, but with smaller businesses, it takes resources to do this kind of analysis, and it takes resources on the insurance companies as well to do individual underwriting. That is really hard to look at individual small businesses one at a time.

Ms. MULLIGAN. Mr. Chairman, the data that I have says that five or six carriers write the coverage on a primary basis, and those five or six carriers write approximately 70 percent of the gross written premium, so while there is 40 or 50 markets who may offer the coverage, it is really sort of centralized with those markets.

The other thing I would say on your coverage question is this is where the history of the product becomes useful and understanding what may be covered in the event of a claim.

It was designed originally to respond to third party liability costs arising from a network breach or a privacy event, and now there has been the inclusion of first party costs to a privacy breach remediation and response, which can include some business interruption costs in the event of a network security breach. That is really where it stands right now.

Senator MORAN. Is the market mature enough that there has been litigation related to the coverage issue?

Ms. MULLIGAN. Yes. Well, I am not sure to the coverage issues, but the litigation around liability has been evolving. If we had been having this conversation three years ago, I would have told you the cases were not getting through to discovery. That is not the case now. The plaintiff's bar is asserting new theories of liability; they will continue to do that.

Senator MORAN. That would be in instances maybe where it was not even necessarily the intention of the insured to have that coverage, but you look at the policy and maybe this is covered and then you litigate it?

Ms. MULLIGAN. Well, no. I am thinking specifically around security and privacy liability policies, meaning the liability is arising from alleged mishandling of data or breached personal data.

Those are still evolving in courts. We do have some publicly available information about the significant breaches that have happened in the last 12 to 18 months.

One major retailer reported recently that their first party costs are over $250 million and rising right now, but their liability costs to their customers and potentially to financial institutions are still playing out in the courts. We do not know where that will land at the moment.

Senator MORAN. Do the policies provide limitations on coverage, an amount not to exceed something?

Mr. BEESON. Could I just make an additional comment? I do not want the Committee to get the perception that all these insurance policies are different, some are covering one thing, and some are covering another. That is not actually the case.

Yes, I absolutely agree the actual policy language is different from one insurance company to another, but if you really boil it down, the specialist policies are trying to cover fundamentally three things.

Number one, costs of dealing with the breach response, notification, forensics, credit monitoring, that type of thing. The other two buckets really fall into liability coverage, to your point, Chairman, the second one being privacy regulatory action, you are sued by a regulator, and it is the cost of defending yourself against that and any civil fine you could be hit with.

Finally, the third one being civil action, for example, a suit in class. It could be from the banks, the individuals who own the data.

Really most of the policies in the marketplace are trying to address those three things. Yes, they are doing it sometimes in different ways. Yes, there are exclusions here where there might not be in another, and a broker has to navigate that on behalf of their client, and that is where one broker is better than another.

I think it is important just to say although it is not commoditized and it is not commoditized because frankly it is still a new area of risk, there is some sort of streamlining in that regard.

Senator MORAN. Thank you. Senator Blumenthal?

Senator BLUMENTHAL. Thank you. Those three areas, the first two areas seem very much alike in terms of both being responses, that is to say notification, aid for consumers who may be harmed, and then the regulatory response. The third is somewhat different. Is that correct?

Mr. BEESON. The biggest difference between one and two and three is that one is a first party loss, so it is under your legal obligation typically at state level to notify individuals. The first party, costs you have associated with that, follow on from that.

The other two are liability. A third party, whether that is a regulator or somebody else, has to come along and take action against you. That is the fundamental difference between one and two and three, if that makes sense.

Senator BLUMENTHAL. How would you define the third?

Mr. BEESON. It is a civil action, so it could be a bank suing a merchant for the cost of canceling and reissuing credit cards. It could be the victims who own the credit cards who sue in a class action to recoup their costs.

There is another area that is emerging, but it is starting to emerge, which is of course the board now gets sued potentially as well under a derivative action from the shareholders. That is something that is starting to emerge as well.

Senator BLUMENTHAL. Mr. Menapace, I do not know whether you had the same kind of analysis in your statement, and I do not have it in front of me, that more than half the costs of a breach involve the responses like technical forensics investigations, attorney oversight, breach notification, credit monitoring, call centers, public relations services, and the other half being legal defense, settlement, regulatory response.

In effect, you are saying half the costs are in that first category of responses?

Mr. MENAPACE. The industry surveys that I have seen have it ranging anywhere from 45 to 50 percent, and some slightly more than 50 percent, but that is what we have seen to be the cost drivers.

I am not sure that amount or those statistics cover what Mr. Beeson was talking about, however, which is the cost of damaged infrastructure, which there is not public information about that, but certainly with the reportable and the discoverable data that we have been able to find, that is accurate, Senator.

Senator BLUMENTHAL. I understand that in talking about captive insurance, it is basically self-insurance or very much like self-insurance, because a company establishes in effect a wholly-owned subsidiary or an entity to protect itself from risks, and it is insured through that captive entity.

My concern is that these types of arrangements could result in private companies in effect reaping the financial benefits of collecting personal data, but the costs could still be spread or socialized among consumers and taxpayers if they underestimate the risks. In other words, the benefits go to the company but the costs hit the consumers.

If companies use this self-insurance approach, cyber insurance, but do not have the funds to adequately cover the costs of cyber incidents, the companies would not have funds available to compensate consumers whose information has been stolen. In other words, in that sort of category of costs where consumers, third parties, are impacted.

Are you aware of captive insurance being used in the cyber insurance market?

Mr. MENAPACE. That is an interesting issue with the captive insurance companies, as you have stated it. Certainly, for companies that have difficulty placing their risks or need additional capacity or perhaps have a large self-insured risk before insurance attaches, and those companies have or will set up captive insurers.

I would be interested to see how that plays out, and I think that is an area where state regulators who do regulate these captives as they do what we think of as regular insurance companies—we will have to take a look at that to see if companies are shifting this risk to their captive insurers.

As insurers have difficulty, both pricing and setting reserves for losses, captives who would necessarily have even less data to go on, this would have to be taken very seriously by the regulators if we

do see a trend in people or businesses transferring the risk via the captive insurer.

Senator BLUMENTHAL. Is there active discussion of the use of captive insurance for cyber?

Mr. MENAPACE. I know that the NAIC is looking at the cyber insurance marketplace in general. I do not know if there is specific discussion within that group with the captive insurers.

It would be interesting to know if some of the large—I do not know but I would be interested to know if the regulators, the individual state regulators, who have large captive populations domiciled in their states are looking at that.

We also know many captives are regulated offshore in other countries. I do not have statistics on that, but it does raise a good point, an important point, which is are these captives set up and appropriate for that kind of risk.

Senator BLUMENTHAL. Right, exactly. Thank you, Mr. Chairman.

Senator MORAN. Thank you, Senator Blumenthal. On a national database, on that concept, there are some who have general concerns about the Federal Government running that database, and then if you reach the conclusion they should, then the question becomes who is that, is that the Department of Homeland Security or Treasury. Is there a public/private partnership.

Is there an outsider that could effectively run a database that we could then rely on? I think the National Association of Insurers is working on this topic. Is there a conclusion or direction they are going?

Ms. MULLIGAN. I can comment that the Department of Homeland Security has had three different working groups over the last 2 years, and now has commenced another group. We have had one meeting so far. We are just starting off.

Because your questions are exactly right, these are the details that need to be ironed out really. In theory, the idea of a data repository is a good one, but the question of ownership, who has access, what kind of information would be put in there, how would it be anonymized, and then how would it be made most useful to the insurance community and the non-insurance community.

These are all the questions that we have on the table right now as part of the working group.

Senator MORAN. On information sharing analysis centers, does the insurance industry have one?

Ms. MULLIGAN. We do not have one centralized place for this line of business. Mr. Menapace mentioned ISO. ISO is an organization that has information about a multitude of insurance.

As I mentioned in my testimony, this line of business is something that is largely purchased by specific industry segments, so we do not have data for every single company irrespective of industry, irrespective of size. We just do not have that data that way, so we are unable to really create those trends from ISO or anywhere else.

Individual insurers are relying on the data that we have about our cyber customers, and we can use information and extrapolate it from general liability and other lines of business where we have experience. That is quite fragmented.

Senator MORAN. Should it be a public policy goal of having ISACs in a wide array of arenas, industries, businesses?

Ms. MULLIGAN. Well, to the extent that it would help us differentiate coverage, and as Ms. Sage pointed out, price, by industry segment, that might be useful. Again, I think we have an issue of a lot of details that would need to be ironed out.

Senator MORAN. Ms. Sage, do you participate in an ISAC?

Ms. SAGE. Not officially. I think one of the challenges for a lot of small businesses is we do not fit neatly into specific industry segments. I know that was part of the discussion around the ISAOs, of which ISACs are considered a type.

As a small business, we are on the ground. We are really just trying to get new customers, keep our customers, et cetera. Some of these activities that require a lot of resources, participating in working groups, attending meetings, these are things that typically we just do not have a lot of time and resources for.

Senator MORAN. Senator Gillibrand and I have discussed legislation that would create a tax credit for the participation in an organization like that. Does that have any appeal to you or to the industry?

Ms. SAGE. Absolutely. As I mentioned in my testimony, even things like the voluntary NIST Cybersecurity Framework, if insurers could even consider that, like the other ISO, the international standards organization, that sometimes is used as a way of understanding what areas of emphasis an organization has, whether it is quality, risk management, et cetera.

Using something like the Cybersecurity Framework could be a factor, so we do not have to worry now about what specific questions do we have to ask this company or that company. At least it could begin to move us in that direction. Offering incentives for small businesses to use the Framework, for example, would really be helpful.

Senator MORAN. Thank you. I am going to see if Senator Blumenthal has any additional questions in another round, and before we conclude, I want to give you a chance to tell us things you wish you would have said or you wish we would have asked you.

Senator BLUMENTHAL. I do not have any further questions, but I may follow up in writing with some, and I want to simply thank everyone on the panel for being here and contributing so well today.

Senator MORAN. Anything you would like to make certain that we know?

Mr. BEESON. I would just leave the thought that certainly at Lockton we view the opportunity as a market incentive as much as anything to where the insurance industry has a role right now to help drive better security. That is the key component, I think, as far as we are concerned.

Thank you for the opportunity to testify today.

Senator MORAN. Thank you for your testimony. Anyone else?

Ms. MULLIGAN. Thank you. I would just comment the importance of the public and private sector cooperation in this arena, this problem is just too large to be solved by just an insurance solution.

Having said that, the insurance community really is in a great position to contribute to the risk management conversations and issues, and I think it is essential to get the conversation out of the

IT focus only, so we can really help companies move to a place of a culture of awareness and resiliency rather than protection.

Senator MORAN. Thank you.

Ms. SAGE. I would just thank you again for this opportunity. There is a saying, if you are not at the table, you might be on the menu. As small businesses, we appreciate the attention and consideration of small businesses in any legislation that you are considering.

Senator MORAN. Ms. Sage, I felt very guilty when you told me that in a sense your every day effort is to survive, get new customers, and grow, which I very much support. I feel badly that we invited you to Washington, D.C.

Ms. SAGE. I actually live locally.

Senator MORAN. Very good. Mr. Menapace, anything?

Mr. MENAPACE. Senator, I appreciate the fact that you commented before that you had taken a look at our written testimony, which is obviously more extensive than we were able to present here today. I stand on that testimony, but I am willing to provide answers to any written questions that the Committee may have afterwards.

Senator MORAN. Thank you very much. In that regard, the record will remain open for 2 weeks for members to submit questions, and we would ask you to respond to those as quickly as possible.

With that, the Subcommittee hearing is adjourned.

[Whereupon, at 11:19 a.m., the hearing was adjourned.]

A P P E N D I X

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JERRY MORAN TO BEN BEESON

Question 1. What challenges do brokers like Lockton face when determining whether to participate in the cyber insurance marketplace? What types of information would be helpful to better analyze risk?

Answer. The primary barrier to entry for a broker seeking to advise their client is education. Driven by the fear of lost business and the high profile of cyber risks that now exists many brokers are developing a greater knowledge base and understanding. However, it is probably fair to say that you can still count on one hand those brokers that have the resources to handle a Fortune 500 client.

The biggest challenge to brokers once they begin to advise clients is risk quantification. What is the consequential loss value to the client following some form of cyber event? There is some ability to quantify losses that involve personally identifiable information or protected health information. However, no actuarial data exists at all for losses involving property damage, business interruption or bodily injury.

The insurance industry also a very little information on the frequency and severity related to the types of attack vectors, and the mitigation tools used that were or were not successful.

The net result means that brokers have a difficult time explaining to clients how much money they should invest in cyber security, particularly the cost of transferring residual risk through insurance.

Question 2. Are there countries outside of the U.S. who have developed a functioning cyber insurance market? What lessons can we learn from those countries?

Answer. No. The U.S. is really the only fully functioning cyber insurance market driven by mandatory data breach notification laws. Internationally the requirement to disclose is sporadic and businesses do not yet perceive enough of a severity risk to warrant buying insurance. However, the emergence of physical damage risks from cyber attacks suggest that international take up could now accelerate.

Question 3. How has the NIST framework helped your company to participate in the cyber risks insurance marketplace?

Answer. Yes very much so. The NIST framework has helped Lockton articulate a governance and enterprise wide risk management approach to boards of directors and senior executives. Cyber insurance forms part of that discussion.

Question 4. One cost in addressing a data breach is legal support to comply with the patchwork of state data breach notification laws. Would a uniform national data breach notification standard improve the cyber insurance marketplace? Why or why not?

Answer. Yes. It would help our clients—businesses—respond faster to those whose data has been compromised. Improved incident response should also help our clients mitigate both their regulatory and civil liability, leading to fewer losses to insurers and ultimately a more competitive premium structure for buyers.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JERRY MORAN TO CATHERINE MULLIGAN

Question 1. Are there countries outside of the U.S. who have developed a functioning cyber insurance market? What lessons can we learn from those countries?

Answer. There are a number of countries in addition to the U.S. that have functioning cyber insurance markets. The UK, France, and Australia have experienced moderate Gross Written Premium growth over the past few years due to an increase in interest and buying behavior from companies operating in highly exposed industries such as finance/banking, retail, healthcare and hospitality. Markets are also beginning to take shape, albeit more slowly, in a number of other countries such as Canada, Hong Kong, Singapore, Spain, Germany, Switzerland, Italy, and Mexico

just to name a few. Buyers of cyber insurance outside the U.S. tend to place more value on first party coverage grants such as privacy breach costs and business income loss as opposed to third party liability coverage. This is generally due to lower frequency of litigation resulting from data breach incidents. However, this may change as more and more countries pass more stringent data privacy laws. Ex-US buyers also perceive significant value in pre and post breach service capabilities offered by each carrier, or service providers with whom carriers partner, relative to risk assessments, forensic investigations, fraud remediation, legal advice, and public relations.

Question 2. How has the NIST framework helped your company better understand the preparedness of the companies you seek to insure?

Answer. The NIST framework is a useful tool for risk managers to use in identifying their exposures and any gaps in best practices. This mapping process may help them take corrective action if necessary and make decisions around risk transfer. It creates a common vernacular for IT professionals, risk managers, and underwriters to use in the discussion of cyber security and privacy event exposures and controls. To the extent this tool brings forth information about a company's awareness of their risk landscape, it creates a good dialogue with underwriters. But good cyber security and privacy practices are not just an IT issue; an underwriter must review people, process, and technology. We look for an overall culture of awareness, which cannot be summarized in any one document or tool. Moreover, the exposure landscape is moving too fast for the underwriting community rely on one single tool or method. Still, the NIST framework has established an effective methodology for building our collective understanding of the exposures and controls in this space.

Question 3. One cost in addressing a data breach is legal support to comply with the patchwork of state data breach notification laws. Would a uniform national data breach notification standard improve the cyber insurance marketplace? Why or why not?

Answer. A company cannot rely on one single approach to responding to data breaches due to the variety of reporting requirements under the various state statutes. There is no single definition of Personally Identifiable Information, nor is there a standard requirement around the way notification must be sent, to whom it must be sent (including the States' Attorneys General), and in what time frame. Companies express confusion around which laws apply to them in different circumstances. There is also confusion about when and how to report an event to their insurers under the policy requirements. A uniform standard could streamline process for the enterprise, consumers, and the insurance community. This would help get information to consumers in a timely fashion as well as mitigating tools such as credit and identity monitoring. There could be cost benefits to the company and their underwriters, which could contribute to the development of improved pricing methodology for this line of insurance.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. JERRY MORAN TO OLA SAGE

Question 1. What are the biggest challenges for a small or medium-sized business like yours in determining whether or not you need cyber risk insurance?

Answer. There are three primary questions that a small business like e-Management should answer in considering cybersecurity insurance.

(1) Do We Really Need It?

According to a threat awareness poll of small businesses conducted by Symantec, 50 percent of small to medium-sized businesses don't feel they are at risk because they are a small business and are therefore not a target for cyberattacks. The reality is very different. Over the past few years, small businesses represent the fast growing segment for cyber-attacks according to data from Verizon's annual data breach report. There are many reasons that small businesses are richer targets for cyber criminals. A very common experience is that many small businesses do not have the resources to invest in the same level of protection that some larger organizations do, thereby making them easier targets to compromise. At the core is the question, "what do small businesses have that cyber criminals want?" The answer is data. This data can be about the small business itself (*e.g.,* employee information, personal information about the principals of the business, confidential or proprietary business information, etc.) or it can be data about people or companies that the small business is connected to (*e.g.,* professional colleagues, high profile customers or celebrity clients, vendors or suppliers, professional organizations, etc.). Armed with this

knowledge, every small business must then ask the question, *what would our legal and financial exposure be if the data we hold or have access to is compromised?* Industry reports indicate that the average cost to a small business to recover from a significant cybersecurity attack is estimated at $300,000. For many small businesses the cost exceeds their ability to cover such exposure and significantly increases the likelihood that a small business shuts its doors.

Cybersecurity insurance can be an effective tool in helping to mitigate financial risks associated with a cyber-breach. Small businesses are wise to at least learn what cybersecurity insurance products are available and consider whether or not it make sense for their business. While this type of insurance is relatively new, several leading insurance providers now offer separate cybersecurity insurance policies that small businesses can take advantage of.

(2) Does It Cover What We Need?

During our process of comparing policies, we found it virtually impossible to compare policies against one another as the language used in one policy differed from the next. An experienced and knowledgeable broker is a must have to help interpret what the different insurance products cover. *Having a multi-faceted cybersecurity policy is ideal.* This type of policy covers costs associated with notification, incident response, legal, regulatory fines, etc. Keep in mind that costs associated with equipment replacement or refurbishment may already be covered by other general liability or business insurance. Importantly, small businesses must understand that cybersecurity insurance is not a silver bullet and cannot cover things like company downtime, reputational damage, loss of business, or intellectual property theft.

(3) Can We Afford It?

The cybersecurity insurance market is in its infancy with only about 50 insurance carriers issuing policies.[1] As a result, the cost to purchase a policy can range from a couple thousand dollars to tens of thousands for a small business. This is out of range for a large number of small businesses. However, we believe cybersecurity is about risk management. It boils down to how much risk a small business willing or able to take. The question small businesses should ask is *"can we afford NOT to invest in cybersecurity insurance?"* As small businesses answer this question, they should consider, at a minimum, what industry or sector their business is in (*e.g.*, critical infrastructure like energy, financial services, healthcare), what valuable data could be compromised, are there other alternatives to cybersecurity insurance to reduce or transfer some of the financial risk?

In addition, small businesses should make sure they communicate to their insurance underwriters, directly or through their brokers, what they are doing to implement reasonable cybersecurity measures or what steps they have taken to strengthen their cybersecurity posture. These are factors that insurance underwriters can take into consideration when evaluating an application, and may result in more affordable pricing.

Summary

At e-Management, we considered these three questions and came to the conclusion that for our business, cybersecurity insurance was a necessary business investment. We recognize that for a variety of reasons, cybersecurity insurance may not be the right solution for all small businesses. However we encourage small businesses from start-up phase to those who are planning an exit, to at least start the conversation about whether or not cybersecurity insurance is right for their business based on their answers to these three straightforward questions.

Question 2. Has the process of seeking cyber risk insurance helped your company improve its cyber posture? If so, how?

Answer. At e-Management, we are using the NIST Cybersecurity Framework to improve our cyber posture. We view improving our posture as good cyber hygiene, a competitive differentiator, and an indication to our clients and partners that we take protecting their information seriously. Cybersecurity insurance is one of several tools in our risk mitigation portfolio to help reduce or transfer some of the financial risk associated with a potential breach.

We believe cybersecurity risk insurance can play an important role in driving companies to improve their cyber posture by stipulating specific requirements. Examples could include policies and procedures that address cybersecurity, baseline

[1] Cyberattack Insurance a Challenge for Business, *The New York Times,* June 8, 2014

technical requirements for company network infrastructures, and demonstration of a company's ongoing cybersecurity risk management approach.

Question 3. One cost in addressing a data breach is legal support to comply with the patchwork of state data breach notification laws. Would a uniform national data breach notification standard improve the cyber insurance marketplace? Why or why not?

Answer. It is unclear how much a national data breach notification standard would "improve" the cyber insurance marketplace. Conceivably, having some degree of consistency among the approximately 48 current state notification breach laws could help companies doing business in multiple states lower legal costs associated with interpreting and complying with the various notification requirements. Over time, this could provide insurance carriers with better data about the costs associated with breach notifications which are covered by most cybersecurity insurance policies today. Ultimately better data should lead to better decision-making, resulting in better pricing of cyber insurance products over the long term.

This page intentionally left blank.