THE ROLE OF CYBER INSURANCE IN RISK MANAGEMENT

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

MARCH 22, 2016

Serial No. 114–61

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PUBLISHING OFFICE

22–625 PDF WASHINGTON : 2016

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

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas
PETER T. KING, New York
MIKE ROGERS, Alabama
CANDICE S. MILLER, Michigan, *Vice Chair*
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
LOU BARLETTA, Pennsylvania
SCOTT PERRY, Pennsylvania
CURT CLAWSON, Florida
JOHN KATKO, New York
WILL HURD, Texas
EARL L. "BUDDY" CARTER, Georgia
MARK WALKER, North Carolina
BARRY LOUDERMILK, Georgia
MARTHA MCSALLY, Arizona
JOHN RATCLIFFE, Texas
DANIEL M. DONOVAN, JR., New York
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
BRIAN HIGGINS, New York
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
DONALD M. PAYNE, JR., New Jersey
FILEMON VELA, Texas
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
NORMA J. TORRES, California

BRENDAN P. SHIELDS, *Staff Director*
JOAN V. O'HARA, *General Counsel*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

JOHN RATCLIFFE, Texas, *Chairman*

PETER T. KING, New York
TOM MARINO, Pennsylvania
SCOTT PERRY, Pennsylvania
CURT CLAWSON, Florida
DANIEL M. DONOVAN, JR., New York
MICHAEL T. MCCAUL, Texas *(ex officio)*
CEDRIC L. RICHMOND, Louisiana
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
BENNIE G. THOMPSON, Mississippi *(ex officio)*

BRETT DEWITT, *Subcommittee Staff Director*
JOHN DICKHAUS, *Subcommittee Clerk*
CHRISTOPHER SCHEPIS, *Minority Subcommittee Staff Director*

CONTENTS

THE ROLE OF CYBER INSURANCE IN RISK MANAGEMENT

Tuesday, March 22, 2016

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES,
Washington, DC.

The subcommittee met, pursuant to call, at 10:14 a.m., in Room 311, Cannon House Office Building, Hon. John Ratcliffe [Chairman of the subcommittee] presiding.

Present: Representatives Ratcliffe, Perry, Clawson, Donovan, Richmond, and Langevin.

Mr. RATCLIFFE. Good morning, everyone. Before we begin today, I want to take a moment and recognize a moment of silence to remember the victims of the terror attacks this morning in Brussels.

Thank you.

You know, attacks like these really cement the need for this committee to move forward with urgency on all fronts to try and prevent and protect Americans from attacks like these here in the United States.

With that, the Committee on Homeland Security, the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies will come to order. The subcommittee today is meeting to examine the potential opportunities to promote the adoption of cyber best practices and more effective management of cyber risks through cyber insurance. I now recognize myself for an opening statement.

The House Homeland Security Committee, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technology meets today to hear from key stakeholders about the role of cyber insurance in managing risk. Just yesterday, the Bipartisan Policy Center came out with a publication on the room for growth in this market and the barriers that it faces. Specifically, today we hope to hear about the potential for cyber insurance to be used to drive companies of all sizes to improve their resiliency against cyber attacks and develop a more effective risk management strategy, thereby leading to a safer internet for all Americans.

The cyber insurance market is in its infancy, but it is easy to envision its vast potential. Just as the process of obtaining home insurance can incentivize homeowners to invest in strong locks, smoke detectors, and security alarms, the same could be true for companies seeking to obtain cyber insurance. It is for that reason that I look forward to hearing from our witnesses today on the cur-

rent state of the cyber insurance market and what can be done to develop and to improve and to expand the availability of cyber insurance in the future.

As news of the recent hacks and breaches and data exfiltrations demonstrates, cyber vulnerabilities impact every American and cause significant concern. The interconnectedness of society exposes everyone to these risks now. The interconnectedness of society—the breaches at Home Depot, Target, and JPMorgan Chase are just a few examples of the cyber incidents that have significantly impacted Americans every day.

According to the World Economic Forum's 2015 Global Risk Report, technological risks in the form of data fraud, cyber attacks, or infrastructure breakdowns, rank in the top 10 of all risks facing the global economy. In light of these risks and their enormous significance to individuals, families, and companies, we really need to be exploring market-driven methods for improving the security of companies that store all of our personal information. I believe cyber insurance to be one such solution.

The very process of considering, applying for, and maintaining cyber insurance requires entities to assess the security of their systems and to examine their own weaknesses and vulnerabilities. The process is constructive, not only for obtaining a fairly-priced policy, but also as a means of improving the company's security in the process. Obtaining and maintaining cyber insurance may be a market-driven means of effecting a rising tide to lift all boats, thereby advancing the security of our entire Nation.

Today, those acquiring cyber insurance largely consist of leading companies that have the most to lose. These market leaders have looked down the road and recognize that the best way to mitigate their own vulnerabilities is to ensure against as many cyber risks as possible. However, we need to explore ways for this marketplace to expand to create a wide array of diverse, affordable products that will benefit small and medium-sized entities as well.

The Department of Homeland Security's Cyber Incident Data and Analysis Working Group, or CIDAWG, has facilitated discussions with relevant stakeholders, including many of the witnesses today, to find ways to further expand the cyber insurance market's ability to address emerging risk areas. The DHS working group has examined the potential value of creating a cyber incident data repository to foster the voluntary sharing of data about breaches, business interruption events, and industrial control system attacks to aid mitigation and risk-transfer approaches. Additionally, they are looking to develop new cyber risk scenarios, models, and simulations to promote the understanding about how a cyber attack might cascade across infrastructure sections.

Last, they are examining ways to assist organizations of all sizes in better prioritizing and managing their top cyber risks.

Over the next several decades, I hope to see a matured insurance ecosystem that incentivizes companies of all sizes to adopt stronger cybersecurity best practices and more effective management of cyber risks against bad actors in cyber space. We look forward to your perspectives on these efforts and what the private sector is doing to make it easier for Americans to more effectively manage cyber risks.

As Chairman of this subcommittee, I am committed to ensuring that legislators help facilitate, but not mandate, solutions to better protect our private-sector networks against cyber adversaries. As I see it, the private sector has always led the way with respect to innovation and investment in this space, and we have an obligation to continue leaning heavily on this wealth of front-line expertise.

I have no doubt that this is only the beginning of our conversation on cyber insurance. This market is growing and it is new. I'm hopeful that we will continue to find ways to facilitate the healthy, market-driven maturation of the cyber insurance market as an effective means of improving our Nation's cybersecurity posture.

[The statement of Chairman Ratcliffe follows:]

STATEMENT OF CHAIRMAN JOHN RATCLIFFE

MARCH 22, 2016

The House Homeland Security Committee, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies meets today to hear from key stakeholders about the role of cyber insurance in managing risk. Just yesterday the Bipartisan Policy Center came out with a publication on the room for growth in this market and the barriers that it faces. Specifically, we hope to hear about the potential for cyber insurance to be used to drive companies of all sizes to improve their resiliency against cyber attacks and develop a more effective risk management strategy, leading to a safer internet for all Americans.

The cyber insurance market is in its infancy. But it's easy to envision its vast potential. Just as the process of obtaining home insurance can incentivize homeowners to invest in strong locks, smoke detectors, and security alarms, the same could be true for companies seeking to obtain cyber insurance. It is for that reason that I look forward to hearing from the witnesses today on the current state of the cyber insurance market, and what can be done to develop, improve, and expand the availability of cyber insurance in the future.

As news of the recent hacks, breaches, and data exfiltrations demonstrates, cyber vulnerabilities impact every American and cause significant concern. The interconnectedness of society exposes everyone to these risks. The breaches at Home Depot, Target, and JPMorgan Chase are just a few examples of cyber incidents that significantly impacted everyday Americans. Further, according to the World Economic Forum's 2015 Global Risk Report, technological risks in the form of data fraud, cyber attacks, or infrastructure breakdown rank in the top 10 of all risks facing the global economy.

In light of these risks and their enormous significance to individuals, families, and companies, we must explore market-driven methods for improving the security of the companies that store our personal information.

I believe cyber insurance may be one such solution. The very process of considering, applying for, and maintaining cyber insurance requires entities to assess the security of their systems and examine their own weaknesses and vulnerabilities. This process is constructive, not only for obtaining a fairly-priced policy, but also as a means of improving the company's security in the process. Obtaining and maintaining cyber insurance may be a market-driven means of enabling "all boats to rise," thereby advancing the security of the Nation.

Today, those acquiring cyber insurance largely consist of leading companies that have the most to lose. These market leaders have looked down the road and recognized the best way to mitigate their own vulnerabilities is to insure against as many cyber risks as possible. However, we need to explore ways for this marketplace to expand to create a wide array of diverse, affordable products that will also benefit small and medium-sized entities.

The Department of Homeland Security's Cyber Incident Data and Analysis Working Group has facilitated discussions with relevant stakeholders, including many of the witnesses today, to find ways to further expand the cyber insurance market's ability to address emerging risk areas. The DHS working group has examined the potential value of creating a cyber incident data repository to foster the voluntary sharing of data about breaches, business interruption events, and industrial control system attacks to aid risk mitigation and risk transfer approaches. Additionally, they are looking to develop new cyber risk scenarios, models, and simulations to promote the understanding about how a cyber attack might cascade across infra-

structure sections. Lastly, they are examining ways to assist organizations of all sizes in better prioritizing and managing their top cyber risks.

Over the next several decades, I hope to see a matured cyber insurance ecosystem that incentivizes companies of all sizes to adopt stronger cybersecurity best practices and more effective management of cyber risks against bad actors in cyber space.

We look forward to hearing your perspectives on these efforts and what the private sector is doing to make it easier for Americans to more effectively manage cyber risks. As Chairman of this subcommittee, I'm committed to ensuring that legislators help facilitate—but not mandate—solutions to better protect our private-sector networks against cyber adversaries. As I see it, the private sector has always led the way with respect to innovation and investment in this space, and we have an obligation to continue leaning heavily on this wealth of front-line expertise.

I have no doubt that this is only the beginning of the conversation on cyber insurance. This market is growing and it is new. I am hopeful that we will continue to find ways to facilitate the healthy, market-driven maturation of the cyber insurance market as an effective means of improving our Nation's cybersecurity posture.

Mr. RATCLIFFE. The Chair now recognizes the Ranking Minority Member of our subcommittee, the gentleman from Louisiana, my friend, Mr. Richmond, for any opening statement that he may have.

Mr. RICHMOND. Thank you, Mr. Chairman, for holding this hearing today on cyber insurance. I want to thank the witnesses for taking their time and their testimony today.

Unfortunately, business and Government in America and across the world have seen increased levels and frequencies of cyber attacks, and the rapidly accelerating sophistication of state-sponsored and privately-organized cyber criminals.

Over the past few years, this subcommittee has conducted Government oversight and produced legislative initiatives and worked diligently to provide the Department of Homeland Security and other Federal agencies with the tools it needs to protect our systems and our databases, and encourage the participation of private industry, both in the critical infrastructure sector and for information sharing.

Today, we are going to hear from private industry and a representative of their State insurance regulatory commissioners about cyber insurance. While the full committee, and particularly this subcommittee, has no oversight or legislative jurisdiction over the cyber insurance activities of those actors and sectors, we do have an interest in how they are doing. The statistics are familiar to us all.

The percentage of U.S. critical infrastructure assets owned by private-sector firms is estimated to be somewhere in the neighborhood of 85 percent. The way these assets are operated and managed has vastly changed over the last few decades, due to the impact of the digital revolution related to computer-based information systems. These changes have increased the efficiency associated with using our infrastructure assets. The digital revolution, however, has also created serious risks to the Nation's critical infrastructure due to actual and potential cybersecurity breaches.

As noted by President Obama in his Executive Order on cybersecurity on February 12, 2013, he stated: Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious National security challenges we must confront.

Last year set a high bar for the size and scope of data breaches, led by the theft of over 20 million Government background checks,

and with that high bar, an increasing interest in how State and local governments and businesses, large and small, can manage their risk and vulnerabilities when they operate in cyber space. For example, recently, on a panel on Lessons Learned From the Real-World Chief Information Security Officers, the University of Virginia's Randy Marchany explained that the increased and sophistication of the level of today's cyber threats forces him to assume that hackers already have access to his network, and the best he can do is to monitor for when the latent threat becomes active.

With that said, let's cut to the chase. What would a cyber insurance policy look like if an experienced chief information security officer of a company or municipal government came to your insurance agency with the proposition that it is likely that his systems had already been hacked and the malware was likely dormant, but he wanted to purchase insurance from you as to mitigation and repercussions? Or to complicate things even more, and to introduce the well-known moral hazard consideration that accompanies many insurance policies, what if a hypothetical chief information security officer knew he had been hacked, but wasn't telling you or anyone else, and he knew or suspected that the hacker intrusion was lying dormant and would activate at some later date?

I am not the first to pose these kinds of questions, and these are questions I am sure all of us have had, if you contemplate the issue of cyber insurance at all. But the worst-case scenarios, going forward, cyber insurance can play a key role in helping businesses, especially small and mid-size businesses, to assess their cybersecurity posture and readiness, and their ability to be resilient and recover from anticipated cyber threats and attacks.

We are engaged in an exceptionally complex and nuanced policy arena. I am especially interested to see how the States will handle the regulatory responsibilities that surround cyber insurance and how the States can serve as incubators for innovative solutions to the National, international, and industry-wide challenge of cybersecurity for our Nation's businesses and Government agencies.

Mr. Chairman, before I yield back, I would ask unanimous consent to submit for the record a white paper on cyber insurance from the George Washington University Center for Cyber and Homeland Security. The author is Brian E. Finch, a senior fellow, and member of the Center's Cybersecurity Task Force. Mr. Finch is a senior partner at Pillsbury, Winthrop, Shaw, and Pittman, and also serves as a senior adviser to the Homeland Security and Defense Business Council.

Mr. RATCLIFFE. Without objection.

[The information follows:]

SUBMITTED FOR THE RECORD BY HON. CEDRIC L. RICHMOND

STATEMENT OF BRIAN E. FINCH, ESQ., PARTNER, PILLSBURY WINTHROP SHAW PITTMAN LLP

MARCH 22, 2016

Chairman Ratcliffe, Ranking Member Richmond, distinguished Members of the subcommittee, thank you for allowing me to submit a statement for the record addressing the role cyber insurance can play in risk management.

My name is Brian Finch and I am here today testifying in my capacity as a partner with the law firm of Pillsbury Winthrop Shaw Pittman LLP. I am also a senior

fellow with The George Washington University Center for Cyber and Homeland Security, where I am a member of the Center's Cybersecurity Task Force, a senior advisor to the Homeland Security and Defense Business Council, and a member of the National Center for Spectator Sport Safety and Security's Advisory Board.

As I have previously noted to Members of this subcommittee, cybersecurity, cybersecurity best practices, and risk management processes are critical to our Nation's economic security and physical safety. Members of this subcommittee know all too well that our cyber enemies are numerous, growing, and increasingly sophisticated. If we have learned anything over the past few years with respect to the threat posed by our cyber enemies, it is that even our most advanced cyber defenses cannot keep up with the sophistication and innovation of cyber attack methodologies. The result is a steady if not increasing "cyber gap" between defense and offense.

In that vein, we must confront the fact that too much focus has been given to "eliminating" the cyber threat posed to America. Indeed, no company has an "Enterprise Risk Eliminator," so as the title of this hearing implies, our efforts should be concentrated on managing cyber risk.

I will leave it to the Members of this subcommittee and the witnesses at the hearing to discuss critical facts related to what cyber insurance as it currently exists has to offer, including with respect to the amount of insurance that is available to anyone company, much less in total.

What I would like to bring to the attention of the subcommittee instead is that today's cyber insurance products are focused on the wrong end of the problem. Cyber insurers, like many others, have correctly assessed that cyber attacks will successfully strike a company at some point. However, these cyber insurance models suffer a fundamental disconnect in that they operate under the assumption that cyber attacks will be sporadic and will rarely succeed.

The reality is that cyber attacks are a constant threat, seeking to penetrate information systems and technologies from every direction and through every possible entry. I would argue therefore that the insurance market has been using incorrect models and assumptions when developing policies for use in cyber risk management.

Rather than viewing cyber attacks as infrequent events like a fire or natural disaster, I believe cyber risk management would be best served if insurers looked towards policies that use a personal health model. That means cyber insurers should look to establish an infrastructure that supports constant care and promotes wellness, not merely reimbursement for periodic losses. In my mind, it follows then that cyber insurers should develop cyber policies using a health maintenance organization or "HMO" model.

Under that model, the insurer's goal will be to promote the "right" kinds of claims—ones that encourage healthy behavior. This model addresses the reality that inevitably some sort of cyber disease will work its way into the blood stream by supporting interventional care that prevents minor scratches from developing into a serious infection.

Companies would gain access to the cyber HMO by paying monthly premiums along with associated "co-pays", "deductibles", and similar expenses typically associated with a health insurance plan.

That cyber HMO plan would give the insured access to a vast network of cybersecurity vendors and professionals at discounted rates that could be called upon in the event of a problem (the "co-pays" and "co-insurance" equivalents).

The cyber HMO plans would also provide low-cost or even free access to basic "cyber hygiene" care, such as routine diagnostic examination of information technology systems, perimeter defense systems, and other basic defense systems (the annual physical and low-cost or free vaccine equivalents).

More "advanced" defense systems could be subject to a higher co-pay and deductible, and companies could even chose to go "out of network" if they choose, but only by shouldering more of the cost.

I firmly believe that this subcommittee should look for ways to support the concept of a "cyber HMO," as a model that actively promotes and rewards healthy cyber behavior—a Gordian knot that no carrier has been able to untie yet using traditional insurance models. That's a critical piece of the cybersecurity puzzle, as the challenge has been how to get companies to engage in effective cybersecurity rather than the most easily accessible form of it.

Best of all, using the cyber HMO model addresses a presumed obstacle to cyber insurance: A lack of actuarial data. Through its mere existence, the cyber HMO will gather the data needed to assess and underwrite costs. This enables cyber benefits to be more finely tuned, benefitting its members and society writ large.

At the very least, this approach has the benefit of trying to solve the problem at hand, not simply forcing a square peg into a round hole. If nothing else, maybe this

idea will generate more discussion around trying to take proactive security measures.

One other model I would like to present to the Members of the subcommittee is the notion of creating cyber "pools" of insurance. Through risk pooling, companies can work together to purchase more insurance than might otherwise be available to them while also establishing hard liability limits and sharing cyber defense resources.

Risk pooling mechanisms come in a number of forms, including "risk purchasing" and "risk retention" groups. Those groups allow collections of companies (usually similarly situated in terms of industry sector) to jointly purchase or create insurance coverage that would otherwise be unavailable or excessively expensive.

Such pools have been around for some time, and discussions with respect to utilizing them in the context of cyber threats are picking up steam. Where companies can take true advantage of these mechanisms is to layer in additional risk mitigation tools such as threat information sharing and statutory liability protection. Combining those aspects could lead to a very powerful collective defense tool.

Here's how it can work:

(1) A group of similarly-situated companies agree to form a risk purchasing or retention group in order to obtain cybersecurity insurance.

(2) The companies agree to use certain security standards or technologies (for instance SANS 20 controls, "detonation chambers", information sharing via dedicated "private clouds", the recent National Institutes of Standards and Technologies voluntary cybersecurity framework, etc.)

(3) The companies then pool their resources either to jointly purchase an existing cyber insurance policy or to create a pool of insurance that they would collectively maintain.

(4) As part of the agreement, any company that fails to adhere to the security standards will be asked to leave the group at the next renewal period.

This proposal can potentially be extremely valuable to the most vulnerable companies, namely small and medium-sized businesses that do not have the resources to create their own robust cyber defenses. By pooling both their financial resources to buy additional insurance but also their technical capabilities to create a common defense, this concept will work to strengthen the bonds between businesses and allow them to collectively respond to and mitigate otherwise devastating cyber attacks.

Further, this arrangement also potentially allows more of the insurance funds to be used for "first party" losses the company has directly suffered (damaged equipment, lost data, business interruption, etc.) rather than losses suffered by third parties.

The pool arrangement also enables companies to collaborate and establish a baseline of security that each would commit to maintaining, and also allows for regular reviews to determine what security controls need to be adjusted. The companies could even work with public/private partnership resources within the Department of Homeland Security and other Federal agencies such as NIST to help them refine their programs and policies in order to achieve a greater cyber "maturity" level than they might have otherwise reached.

Another benefit of this pool concept is that the insured group can take advantage of the cyber information-sharing platform recently created by the Cyber Information Sharing Act. The pools would be prime candidates to benefit from that platform, and would likewise make excellent candidates to serve as information-sharing and analysis organizations, or "ISAOs," within the CISA framework.

The pooling concept gives companies an excellent opportunity to take charge of their security profile, and do so in a way that both mitigates the likelihood of a successful attack as well as increase resources to respond to or mitigate losses. Further, these pools can serve as an excellent collective effort that can more fully take advantage ofthe public/private partnership benefits offered through the CISA legislation and the ISAO concept.

CONCLUSION

Thank you for the opportunity to present my statement to the subcommittee. I am happy to answer any question you might have regarding my thoughts.

Mr. RICHMOND. With that, I yield back.

[The statement of Ranking Member Richmond follows:]

STATEMENT OF RANKING MEMBER CEDRIC L. RICHMOND

MARCH 22, 2016

Unfortunately, businesses and government in America, and across the world, are seeing increased levels and frequencies of cyber attacks and the rapidly accelerating sophistication of state-sponsored and privately-organized cyber criminals. Over the past few years, this subcommittee has conducted Government oversight and produced legislative initiatives and worked diligently to provide the Department of Homeland Security and other Federal agencies, with the tools it needs to protect our systems and databases, and encourage the participation of private industry both in the critical infrastructure sector and for information sharing.

Today, we are going to hear from private industry, and a representative of their State insurance regulatory Commissioners about cyber insurance. While, the full committee, and particularly this subcommittee, has no oversight or legislative jurisdiction over the cyber insurance activities of these actors and sectors, we do have an interest in how they are doing.

The statistics are familiar to us all, the percentage of U.S. critical infrastructure assets owned by private-sector firms is estimated to be somewhere in the neighborhood of 85 percent. The way these assets are operated and managed has vastly changed over the last few decades due to the impact of the digital revolution related to computer-based information systems. These changes have increased the efficiency associated with using our infrastructure assets.

The digital revolution, however, has also created serious risks to the Nation's critical infrastructure due to actual and potential cybersecurity breaches. As noted by President Obama in his Executive Order on Cybersecurity, February 12, 2013: Repeated cyber intrusions into critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious National security challenges we must confront.

Last year set a high bar for the size and scope of data breaches, led by the theft of over 20 million Government background checks, and with that high bar, an increasing interest in how State and local governments, and businesses large and small, can manage their risks and vulnerabilities when they operate in cyber space.

For example, recently on a panel on "lessons learned" from real-world chief information security officers, the University of Virginia's Randy Marchany explained that the increased and sophistication of the level of today's cyber threats forces him to assume that hackers already have access to his network, and the best he can do is to monitor for when the latent threat becomes active.

With that said, let's cut to the chase—what would a cyber insurance policy look like if an experienced chief information security officer, or CISO, of a company or municipal government came to your insurance company with the proposition that it is likely that his systems had already been hacked and the malware was likely dormant, but he wanted to purchase insurance from you as to mitigation and repercussions?

Or, to complicate things even more, and introduce the well-known "moral hazard" consideration that accompanies any insurance policy—what if a hypothetical CISO knew he had been hacked, but wasn't telling you or anyone else, and he knew or suspected the hack or intrusion was lying dormant and would activate at some later date? I am not the first to pose these kinds of questions, and these are questions I am sure all of us have had, if you contemplate the issue of cyber insurance at all.

But these are worst-case scenarios. Going forward, cyber insurance can play a key role in helping businesses, especially small and mid-sized business, to assess their cybersecurity posture and readiness, and their ability to be resilient and recover from anticipated cyber threats and attacks. We are engaged in an exceptionally complex and nuanced policy arena. I am especially interested to see how the States will handle the regulatory responsibilities that surround cyber insurance, and how the States can serve as incubators for innovative solutions to the National, international, and industry-wide challenge of cybersecurity for our Nation's businesses and Government agencies.

Mr. RATCLIFFE. I thank the gentleman. Other Members of the committee are reminded that opening statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

FEBRUARY 25, 2016

Cyber insurance is a way to share risks so when a cyber data breach event occurs, the insured company receives a payment to compensate for the losses.

The analysis of data breach claims helps cyber insurance companies estimate the probability of a breach and the likely losses that can be covered.

A cyber insurance company might use this experience to recommend cybersecurity improvements to companies it insures.

Some suggest that cyber insurance companies can gather detailed, technical information on breaches and use this knowledge to prevent future breaches at other clients.

Others have had the idea to create insurance "pools" for use by smaller and mid-sized businesses, in certain sectors, which could then collectively purchase a cyber insurance policy. There are lots of innovative ideas on the table.

Over the past 7 years, President Obama has been very involved on the issue of protecting critical infrastructure. In 2013, the President issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity".

The Executive Order called for, what we now know as, the NIST Cybersecurity Framework, developed by the Department of Commerce's National Institute of Standards and Technology.

It is a set of voluntary industry standards and best practices to help companies and entities manage cybersecurity risks, and it has become a central tenant of the idea that cybersecurity insurance might be possible in the real world.

We have been told the cybersecurity insurance market is growing at 30% a year by some estimates, and brokers and underwriters alike agree that mid-size and small businesses are the next sector of business to see a wide-spread adoption of cyber insurance.

I know I hear from many of the main-street businesses in my District when I hold meetings on cyber—that many are struggling with their cybersecurity efforts. They lack the resources, the time, and the expertise to address this issue.

And I imagine they will have a more difficult time qualifying for cyber insurance. I look forward to the testimony today on this complex and necessary component of cyber and information security.

Mr. RATCLIFFE. We are pleased to have with us today an incredibly distinguished panel of witnesses on this very important topic. Mr. Matthew McCabe is the senior vice president for network security and data privacy at Marsh FINRPO. Welcome, and as a former counsel to the Committee on Homeland Security, maybe I should say welcome back.

Commissioner Adam Hamm is the North Dakota insurance commissioner and is testifying on behalf of the National Association of Insurance Commissioners. Commissioner Hamm, thank you for being with us here today.

Mr. Daniel Nutkis is the chief executive officer for the Health Information Trust Alliance. We appreciate you coming all the way from the great State of Texas to be with us this morning.

Last but not least, Mr. Tom Finan is the chief strategy officer at Ark Network Security Solutions, and is also a former Department of Homeland Security official. We welcome you back as well.

I now ask the witnesses to stand and raise your right hand so that I can swear you in to testify.

[Witnesses sworn.]

Mr. RATCLIFFE. Let the record reflect that the witnesses have answered in the affirmative. The witnesses' full written statements will appear in the record.

The Chair now recognizes Mr. McCabe for his opening statement.

STATEMENT OF MATTHEW P. McCABE, SENIOR VICE PRESIDENT, NETWORK SECURITY AND DATA PRIVACY, MARSH FINRPO

Mr. MCCABE. Thank you. Good morning, Chairman Ratcliffe, Ranking Member Richmond, and Members of the subcommittee. My name is Matthew McCabe, and I am a senior adviser for Marsh, which is the global leader in risk management and insurance brokering.

Every day around the world, Marsh advisers work with clients to quantify and manage risk. Today, our prayers are certainly with our colleagues in Brussels and, of course, with all the citizenry in the wake of those terrible attacks.

My testimony today focuses on how Marsh helps clients manage risk through cyber insurance. Broadly stated, there are 3 core components. First, a policy can pay costs to respond to a cyber incident. These can be items like forensics, data breach notification and credit monitoring, restoring corrupted data, or even a cyber extortion demand.

Second, cyber insurance will cover fees and damages that arise from litigation triggered by a cyber incident. Third, cyber insurance reimburses revenue lost or expenses incurred from disruption of network operations. However, the benefits of coverage are not simply financial. Cyber insurance actually can strengthen an organization's cyber preparedness.

As a threshold matter, as the Chairman recognized, applying for coverage requires an assessment. Underwriters scrutinize practices such as perimeter defenses, incident response plans, patching software, access privileges, and network monitoring before issuing a policy. In that assessment, we will help determine the premium which incentivizes better practices. Once coverage is bound, tethered to that coverage are vendor services such as threat assessment and vulnerability scanning.

Most prominently, cyber insurance supports incident response plans by providing services like forensics, legal analysis, fraud mitigation, and crisis management. This feature can be especially valuable for small and mid-size businesses that may lack resources to carry their own incident response plans. Notably, research indicates that nearly 60 percent of cyber attacks target small and mid-size businesses.

Interest in cyber insurance is robust and climbing. In 2015, the number of U.S.-based Marsh clients purchasing cyber insurance increased 27 percent when compared to 2014. That 27 percent number follows a 32 percent increase in the prior year, and a 21 percent increase in the year before. Currently, cyber insurance purchasing remains dominated by industries that aggregate customer data, personally identifiable information.

But purchasing is climbing for industries with less data, but which have a significant exposure for network disruptions. Typical industries that can serve as examples would be electric utilities and manufacturers. So this trend signals that more companies see a growing exposure from cyber physical systems where operational technology is remotely controlled via an internet connection.

Marsh and McLennan recently considered this exposure in a report titled "Cyber Resiliency in the Fourth Industrial Revolution,"

which it co-authored with FireEye and Hewlett Packard Enterprise. The report examines how cyber threats are morphing into a realm of physical assets and critical infrastructure. With the escalation of attacks and increased connectivity of devices, there is a clear need for critical infrastructure companies to become more resilient to cyber attacks.

The report concludes that one key for building cyber resiliency is to have distinct cyber risk advisers, such as threat intelligence, forensic assessment, systems architecture, and risk transfer, provide an integrated strategy. They will ask questions as what are your most critical assets? Who are the bad actors targeting your network? What does your on-line activity signal to the hackers out there? The responses to those questions will yield data, and that data should inform every asset of cyber risk management.

For the same rationale, Marsh has participated and supports the DHS Cyber Incident Data Analysis Working Group. The insurance industry is data-intensive, and advising clients relies on our ability to model the likelihood and severity of events. In fact, the strength of our industry is its emergence as a leader in cyber incident analysis. So we believe the repository could have several uses, including strengthening underwriting, developing new products to close gaps in coverage, and could support metrics around information sharing and detecting threats.

In conclusion, cyber risk management depends on our ability to quantify risk and provide analytics that support action items. Thank you, and I look forward to answering any questions that you might have.

[The prepared statement of Mr. McCabe follows:]

PREPARED STATEMENT OF MATTHEW P. MCCABE

MARCH 22, 2016

INTRODUCTION

Good morning Chairman Ratcliffe, Ranking Member Richmond, and Members of the subcommittee. My name is Matthew McCabe, and I am a senior advisory specialist in the field of cyber insurance broking for Marsh. My testimony today will focus on defining the product of cyber insurance, explaining how it supports resiliency to defend against cyber threats, and how analysis of data related to cyber incidents supports the industry. I am grateful for the opportunity to participate in this important hearing.

Marsh & McLennan operates through 4 market-leading brands—Marsh, Guy Carpenter, Mercer, and Oliver Wyman. Each organization provides advice to clients across an array of industries in the areas of risk, strategy, and human capital. As the leading insurance broker in the world, Marsh has a unique perspective on the cyber insurance market.

Marsh's role is to work with clients to analyze their risk exposures and, where appropriate, help our clients implement solutions to address and mitigate the financial impact of a cyber incident.

Over the past decade, our Nation has witnessed an astonishing evolution of cyber risk that continues to grow in size and sophistication. It was aptly described by President Barack Obama as "one of the great paradoxes of our Information Age—the very technologies that empower us to do great good can also be used by adversaries to inflict great harm." Technically-sophisticated actors have the opportunity to carry out attacks at a relatively low cost, and they do so repeatedly by frustrating attribution or enjoying the protection of a jurisdiction where the ability to extradite or prosecute bad actors remains evasive.

That paradigm resulted in an epic crime wave, with enormous consequences for our clients. Companies have lost hundreds of millions of customer records, suffered

rampant pilfering of intellectual property and endured the theft of funds and sensitive financial information.

Many metaphors have been invoked to describe this phenomenon. Is this an epidemic? Is this the modern-day risk of catastrophic fire? My preference is piracy. Simply put, a new generation of raiders committed to plunder have taken to the virtual high seas. These raiders may enjoy tacit or direct support of a nation-state. Victimized merchants expect their government to address this menace and are considering how they can pursue their own recourse. However, even that metaphor has come full circle. This week, security experts found that actual pirates have been hacking into a global shipping company in order to target specific ships with the most valuable cargo.[1] There is no company or industry that is not affected by cyber risk.

For this committee, the paramount concern is that cyber threats have now unquestionably escalated into a genuine threat against the homeland. The growing prominence of cyber physical systems—where operational technology connections become increasingly accessible through the internet—gives rise to an escalated risk to the control physical processes. The threat to U.S. critical infrastructure arising from the exposure of cyber physical systems has quickly morphed from speculative, to rumored, and now actual events. Recent examples include the 2013 attack against a New York dam, last year's attack against a Ukrainian electric utility and railways, and purportedly a recent threat against a South Korean rail system. In short, the stakes in this game have risen quickly.

Marsh & McLennan recently considered this challenge in a report titled "Cyber Resiliency in the Fourth Industrial Revolution", which it co-authored with FireEye and Hewlett Packard Enterprises. (See Appendix A.) As noted in the report, with most experts predicting that the number of internet-connected devices will eclipse 30 million by 2020, there will be a broad expansion of the attack surface against critical infrastructure. Realizing that this boom in connectivity must be met with a better approach for securing the backbone systems that support critical infrastructure, the authors considered the challenge of how the private sector can develop greater resiliency in the face of cyber threats.

Our conclusion is that cyber-risk advisers must come together to create a unified approach for building cyber resiliency of these systems. Much like the NIST Framework presents a process for end-to-end assessment, the different disciplines of cyber-risk management must coalesce into an integrated solution. Each stage of cyber risk advising should inform and reinforce the others. Thus, cyber insurance should not be viewed as a stand-alone solution; it is instead a key component of cyber-risk management around which experts can coalesce and which can provide strong market incentives to pursue greater security.

The many benefits of cyber insurance are apparent to the private sector. The number of Marsh U.S.-based clients purchasing stand-alone cyber insurance increased 27% in 2015 compared with 2014. That followed a 32% increase of clients purchasing cyber insurance in 2014 over 2013, and a 21% increase from 2012 to 2013. This purchasing is supported by more than 50 carriers from around the world that potentially can provide more than $500 million in capacity.

Because of the incessant stream of data breaches that have targeted U.S. companies, purchasing is dominated by industries that aggregate customer data, such as retailers, financial institutions, and health care providers. However, take-up rates are climbing for industries with small amounts of data but that are exposed to significant risk of network outage, such as electric utilities or manufacturers. In short, the sharp increase in cyber insurance purchasing has increased rapidly and continues its growth as a vital part of risk-based cybersecurity management strategies.

THE VALUE OF CYBER INSURANCE

Broadly stated, there are 3 core components of cyber insurance. First, cyber insurance will reimburse the costs that a company pays to respond to a cyber incident. These expenses may come in the form of complying with requirements to notify and protect affected individuals in the wake of a data breach; paying the expense to recreate corrupted or destroyed data; or even paying the demand of an extortionist. Second, cyber insurance covers the fees and damages that a company may pay in response to litigation resulting from a cyber incident. Third, cyber insurance reimburses revenues lost or expenses incurred due to a disruption related to a cyber incident.

---

[1] See [sic] (accessible at *http://www.verizonenterprise.com/resources/reports/rp__data-breach-digest__xg__en.pdf*).

However, the benefits of cyber insurance extend far beyond reimbursement for financial loss. Cyber insurance has evolved into a product that serves as a key touchpoint for an organization to assess its cyber practices and coordinate its incident response plan to cyber incidents. The Department of Commerce Internet Policy Task Force recently commented that cybersecurity insurance is potentially an "effective, market-driven way" of increasing cybersecurity in the private sector.

For demonstrative purposes, the benefits attached to cyber insurance can be explained in the context of the NIST Cybersecurity Framework by mapping the components of a policy to the five cybersecurity domains proposed in the Framework: Assessment, prevention, detection, response, and recover.

As a threshold matter, the very act of applying for insurance forces an assessment of the applicant's cyber practices. The underwriting process will scrutinize a company's technical defenses, incident response plan, procedures for patching software, policies for limiting access to data and systems, monitoring of the vendor network and more. Applying for cyber insurance is therefore an important risk mitigation tool. Further, carriers assess the applicant's security practices and provide premiums based on their interpretation. Thus, cyber insurance premiums provide an important incentive that drives behavioral change in the marketplace.

Once a cyber insurance program is implemented, the insured can avail themselves of services and solutions to further mitigate cyber risk and strengthen cyber hygiene. The insurance marketplace thereby enhances access to detection and mitigation solutions and the large network of vendors that provide threat intelligence, vulnerability scanning, system configuration analysis, and technology to block malicious signatures.

Most prominently, cyber insurance can support an organization's incident response plans. In the example of a data breach, most cyber insurance policies provide the services needed to respond to breaches, including forensics to determine what customer records have been compromised, legal analysis of the insured's responsibilities, notification to affected individuals, and credit monitoring and restoration to protect its customers. A well-executed response plan will actually reduce the overall cost of a data breach and avoid many of the problems that may later surface in resulting litigation or regulatory scrutiny. These services can be especially valuable for small- and mid-size enterprises that will require a cyber incident response plan, but lack the resources to implement one on their own.

In short, using market-driven incentives, cyber insurance serves to build greater resiliency within the private sector. This can be especially critical for small- and mid-size businesses that would experience a significant financial burden to retain and execute all of these services own their own. Notably, recent research indicates that as many as 60% of cyber attacks target small- and mid-size businesses.[2] With cyber insurance, these businesses can rely on experienced cyber security vendors in the wake of a cyber incident and respond and recover more quickly from the incident.

THE ROLE OF DATA ANALYSIS

As this committee has recognized through its important work to pass legislation on the sharing of cyber threat indicators, enhanced information sharing between industry and Government is an important component of a comprehensive risk mitigation strategy. For this purpose, Marsh has participated in and supported the Department of Homeland Security's (DHS) Cyber Incident Data Analysis Working Group, and, prior to that, Cyber Insurance Workshops conducted by DHS.

As the committee is aware, the insurance industry is data-intensive. There are both internal and external drivers for strong modeling to enable more accurate forecasting for the likelihood and severity of events. As a rule of thumb, better data leads to better decisions. For this reason, Marsh has participated in the DHS working groups that have proposed the creation of a repository that would collect anonymized data to track cyber incidents.

Importantly, the committee should not interpret the desire to collect more actuarial data or to strengthen modeling as an indication that the cyber insurance industry is currently without tether to a strong appreciation of the underlying risk. One strength of the cyber insurance industry is that the underwriting process generates data on threats, vulnerabilities, and potential consequences for each applicant. Indeed, the cyber insurance industry has risen to become a leader in incident analysis for informing trends in cyber threats and correlate best practices with the amount of loss.

---

[2] See Symantec Internet Security Report 2014 (accessible at *http://www.symantec.com/content/en/us/enterprise/other__resources/b-istr__main__report__v19__21291018.en-us.pdf).*

However, a centralized repository could offer several benefits to both Government and industry. As proposed, the data repository would provide a centralized platform to share the information that many companies retain about hacking activity.

Making this data available centrally can inform analysis of long-term trends for insight into the effectiveness of security practices. For example, companies, carriers, and regulators could potentially analyze whether certain security protocols or practices have effectively mitigated cyber risk. For example, Government and industry could undertake an analysis as to whether organizations that have implemented cyber practices using the NIST Framework have proven more resilient in withstanding cyber attacks. Further, in the wake of the recent passage of information-sharing legislation, Government, and industry, could explore whether the greater availability of cyber threat indicators has enabled organizations to fend off malevolent actors.

From the perspective of Government, analyzing the successes and challenges related to cyber risk strategies could provide a basis for shaping future Federal policy. Increasingly, network systems tie together an ever broader and more sophisticated global supply chain, yielding greater complexity and more latent risk. Accordingly, any new requirement for protecting supply chains should be founded in data analysis and consider potential consequences of regulations on the marketplace and the likelihood for accomplishing intended security goals.

From the perspective of the insurance industry, the greater availability of cyber incident data to strengthen underwriting may also facilitate market forces to address current and future risks, and eventually encourage further carrier participation. Better data could also enable the insurance industry to introduce solutions to close gaps in current coverages and to determine how to best to detect and mitigate future incidents, or to reduce incident response times and facilitate recovery.

Thank you for allowing me to present this testimony. I am happy to take your questions.[3]

Mr. RATCLIFFE. Thank you, Mr. McCabe. The Chair now recognizes Commissioner Hamm for his opening statement.

STATEMENT OF ADAM W. HAMM, COMMISSIONER, NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS

Mr. HAMM. Good morning, Chairman Ratcliffe, Ranking Member Richmond, and Members of the committee. Thank you very much for the opportunity to testify today.

So to begin, State insurance regulators are keenly aware of the potentially devastating effects that cyber attacks can have, and we have taken a number of steps to enhance data security expectations across the insurance sector. We understand the pressure these increased risks put on other industries, creating unprecedented demand for products to manage and mitigate some of their cybersecurity risks through insurance.

Most businesses carry commercial insurance policies, but may not realize cybersecurity risks are not covered. To cover these unique risks, businesses need to purchase a special, customized cybersecurity policy. My written testimony details the structure of financial and market regulation for U.S. insurers writing these types of policies.

Ours is a Nationally-coordinated, State-based system that relies on extensive peer review, communication, and collaboration among regulators to produce checks and balances in oversight, always with the fundamental tenet of protecting policy holders by ensuring that companies are solvent and can pay claims when they come due.

---

[3] Appendix to Marsh & McLennan Companies Testimony A. Report: "Cyber Resiliency in the Fourth Industrial Revolution" is available at: *http://info.resilientsystems.com/ponemon-institute-study-the-cyber-resilient-organization-ppc?utm__campaign=CyberResiliencePonemonReport-&utm__source=google&utm__medium=cpc&gclid=CP3F2Lf61MsCFRNahgodl98LrA*.

When it comes to regulation, cybersecurity policies are scrutinized just as closely as other insurance contracts. Their complexity and new product language will present some novel issues, but policy forms and rates are still subject to review to ensure the contracts are reasonable and not contrary to State laws. We also have market conduct authorities to examine insurers and policies, as well as strong enforcement powers.

Cybersecurity risk remains difficult for insurance underwriters to quantify, due in large part to a lack of actuarial data. Today, in the absence of that data, insurers compensate by pricing that relies on qualitative assessments of an applicant's operations, vendors, risk management procedures, and security culture. As a result, the policies for cyber risk tend to be more customized than others, and therefore more costly.

From a regulatory perspective, we would like to see these qualitative assessments coupled with a more robust actuarial data system based on actual incident experience. As it is still developing, accurately assessing the exposure or the size of the cybersecurity insurance market is a work in progress. That is why the NAIC has developed a new mandatory data supplement. This supplement requires all insurance carriers, writing either identity theft insurance or cybersecurity insurance, to report on their claims, premiums, losses, expenses, and in-force policies in these areas.

With this data, regulators will be able to more definitively report on the size of the market and identify trends that will inform whether more tailored regulation is necessary. As with any new requirement, we expect that the terminology and reporting will mature over time.

State insurance regulators are also ramping up our efforts to tackle other cybersecurity issues and reduce risk in the insurance sector through a number of initiatives. In the past year, the NAIC has adopted 12 principles for effective cybersecurity, a roadmap for consumer cybersecurity protections, updated guidance for examiners regarding IT systems and protocols. Most recently, we exposed for public comment a new insurance data security model law. We have done all of this through the NAIC's open and transparent process, and we continue to welcome all stakeholder input on these projects.

The expansion of cyber risks and the growth of the cybersecurity insurance market are a tremendous opportunity for the insurance sector to lead in the development of cyber hygiene across our National infrastructure. Insurance has a long history of driving both best practices and standardization. It creates economic incentives through the pricing of products, and the underwriting process can test risk management techniques and encourage policy holders to make their businesses more secure.

As insurers develop more sophisticated tools for underwriting and pricing, State regulators will continue to monitor and study cybersecurity products, always remembering that our fundamental commitment is to ensuring that policy holders are protected and treated fairly by financially sound insurance companies.

In conclusion, State insurance regulators remain extensively engaged to promote an optimal regulatory framework, and cybersecurity insurance is no exception. I want to thank you again, Chair-

man Ratcliffe, for the opportunity to testify today, and I look forward to answering your questions.

[The prepared statement of Mr. Hamm follows:]

PREPARED STATEMENT OF ADAM W. HAMM

MARCH 22, 2016

INTRODUCTION

Chairman Ratcliffe, Ranking Member Richmond, and Members of the subcommittee, thank you for the invitation to testify today. My name is Adam Hamm. I am the commissioner of the Insurance Department for the State of North Dakota and I present today's testimony on behalf of the National Association of Insurance Commissioners (NAIC).[1] I am a past president of the NAIC, and I have served as the chair of the NAIC's Cybersecurity Task Force since its formation in 2014.[2] On behalf of my fellow State insurance regulators, I appreciate the opportunity to offer our views and perspective on cybersecurity challenges facing our Nation and the role cybersecurity insurance can play in risk management.

THE CYBER THREAT LANDSCAPE CREATES DEMAND FOR COVERAGE

On one hand, threats to data privacy are not new for businesses, regulators, or the consumers we protect. Regulators and legislatures have required businesses to protect consumer data for decades. On the other hand, the modern size, scale, and methods of data collection, transmission, and storage all present new challenges. As society becomes more reliant on electronic communication and businesses collect and maintain ever more granular information about their customers in an effort to serve them better, the opportunity for bad actors to inflict damage on businesses and the public increases exponentially. Rather than walking into a bank, demanding bags of cash from a teller, and planning a speedy getaway, a modern thief can steal highly-sensitive personal health and financial data with a few quick keystrokes or a well disguised phishing attack from the comfort of his basement couch. Nation states also place great value on acquiring data to either better understand or disrupt U.S. markets, and are dedicating tremendous resources to such efforts.

As these cyber threats continue to evolve, they will invariably affect consumers in all States and territories. State insurance regulators are keenly aware of the potential devastating effects cyber attacks can have on businesses and consumers, and we have taken a number of steps to enhance data security expectations across the insurance sector, including at our own departments of insurance and at the NAIC. We also understand the pressure these increased risks are putting on other industries, creating unprecedented demand for products that allow purchasers to manage and mitigate some of their cybersecurity risks through insurance. Whether attacks come from nation states, terrorists, criminals, hacktivists, external opportunists or company insiders, with each announcement of a system failure leading to a significant business loss, awareness grows, and companies will seek additional coverage for security breaches, business interruptions, reputational damage, theft of digital assets, customer notifications, regulatory compliance costs, and many more liabilities that arise from doing business in the modern connected universe.

Most businesses carry and are familiar with their commercial insurance policies providing general liability coverage to protect the business from injury or property damage. What they may not realize is that most standard commercial lines policies do not cover many of the cyber risks mentioned above. To cover these unique cyber risks through insurance, businesses need to purchase a special cybersecurity policy.

I want to urge some caution regarding the term "cybersecurity policy" because it can mean so many different things—while it is a useful short-hand for purposes of today's conversation, I want to remind the committee that until we see more standardization in the marketplace, a "cybersecurity policy" will really be defined by what triggers the particular policy and what types of coverage may or may not be included depending on the purchaser and insurer. Commercial insurance policies are

[1] The NAIC is the United States standard-setting and regulatory support organization created and governed by the chief insurance regulators from the 50 States, the District of Columbia, and 5 U.S. territories. Through the NAIC, we establish standards and best practices, conduct peer review, and coordinate our regulatory oversight. NAIC members, together with the central resources of the NAIC, form the National system of State-based insurance regulation in the United States.

[2] Attachment A—NAIC Cybersecurity (EX) Task Force Membership List.

contracts between 2 or more parties, subject to a certain amount of customization, so if you've seen 1 cybersecurity policy, you've seen exactly 1 cybersecurity policy.

All these nuances mean securing a cybersecurity policy is not as simple as pulling something off the shelf and walking to the cash register. Insurers writing this coverage are justifiably interested in the risk-management techniques applied by the policy holder to protect its network and its assets. The more an insurer knows about a business's operations, structures, risks, history of cyber attacks, and security culture, the better it will be able to design a product that meets the client's need and satisfies regulators.

INSURANCE REGULATION IN THE UNITED STATES—"COPS ON THE BEAT"

The U.S. insurance industry has been well-regulated at the State level for nearly 150 years. Every State has an insurance commissioner responsible for regulating that State's insurance market, and commissioners have been coming together to coordinate and streamline their activities through the NAIC since 1871. The North Dakota Insurance Department, which I lead, was established in 1889 and employs approximately 50 full-time staff members to serve policy holders across our State. It is our job to license companies and agents that sell products in our State, as well as to enforce the State insurance code with the primary mission of ensuring solvency and protecting policy holders, claimants, and beneficiaries, while also fostering an effective and efficient marketplace for insurance products. The strength of our State-based system became especially evident during the financial crisis—while hundreds of banks failed and people were forced from their homes, less than 20 insurers became insolvent and even then, policy holders were paid when their claims came due.

Conceptually, insurance regulation in the United States is straightforward. Americans expect insurers to be financially solvent, and thus able to make good on the promises they have made. Americans also want insurers who treat policy holders and claimants fairly, paying claims when they come due. In practice, the regulation of an increasingly complex insurance industry facing constantly-changing risks and developing new products to meet risk-transfer demand becomes challenging very quickly. The U.S. State-based insurance regulatory system is unique in that it relies on an extensive system of peer review, communication, and collaboration to produce checks and balances in our regulatory oversight of the market. This, in combination with our risk-focused approach to financial and market conduct regulation, forms the foundation of our system for all insurance products in the United States, including the cybersecurity products we are here to discuss today.

Treasury Deputy Secretary Sarah Bloom Raskin stated at an NAIC/CSIS event last fall that "State insurance regulators are the cops on the beat when it comes to cybersecurity at insurance companies and the protection of sensitive information of applicants and policy holders." We take very seriously our responsibility to ensure the entities we regulate are both adequately protecting customer data and properly underwriting the products they sell, and we continue to convey the message to insurance company C-suites that cybersecurity is not an IT issue—it is an Enterprise Risk Management Issue, a board of directors issue, and ultimately a CEO issue.

REGULATION OF CYBERSECURITY POLICIES

Having discussed increasing demand for coverage, we can turn to the role my fellow insurance commissioners and I play as regulators of the product and its carriers. Let me start by putting you at ease: When it comes to regulation, cybersecurity policies are scrutinized just as rigorously as other insurance contracts. While they may be more complex than many existing coverages and new product language will present some novel issues, when insurers draft a cybersecurity policy, they are still required to file forms and rates subject to review by the State Department of Insurance. State insurance regulators review the language in the contracts to ensure they are reasonable and not contrary to State laws. We also review the pricing and evaluate the benefits we expect to find in such policies. State regulators also retain market conduct authorities with respect to examinations of these insurers and policies in order to protect policy holders by taking enforcement measures against bad actors.

Insurance regulation involves front-end, on-going, and back-end monitoring of insurers, products, and insurance agents (or producers). The system's fundamental tenet is to protect policy holders by ensuring the solvency of the insurer and its ability to pay claims. Strict standards and keen financial oversight are critical components of our solvency framework. State regulators review insurers' material transactions for approval, restrict key activities, have explicit financial requirements, and monitor compliance and financial condition through various solvency surveillance

and examination mechanisms, some of which we recently updated to incorporate cybersecurity controls. We can also take corrective action on insurers when necessary through a regulatory intervention process.

Financial Regulation

Financial regulation is focused on preventing, detecting, and resolving potentially troubled insurers. Insurance regulators carefully monitor insurers' capital, surplus, and transactions on an on-going basis through financial analysis, reporting requirements, actuarial opinions, and cash flow testing. State insurance laws also restrict insurers' investments and impose capital and reserving requirements.

The monitoring of insurers is done through both on-site examinations and analysis of detailed periodic insurer reporting and disclosures. Insurers are required to prepare comprehensive financial statements using the NAIC's Statutory Accounting Principles (SAP). SAP utilizes the framework established by Generally Accepted Accounting Principles (GAAP), but unlike GAAP which is primarily designed to provide key information to investors of public companies and uses a going-concern concept, SAP is specifically designed to assist regulators in monitoring the solvency of an insurer. The NAIC's Accounting Practices and Procedures Manual includes the entire codification of SAP and serves as the consistent baseline accounting requirement for all States. Each insurer's statutory financial statements are filed with the NAIC on a quarterly and annual basis and include a balance sheet, an income statement, and numerous required schedules and exhibits of additional detailed information.

The NAIC serves as the central repository for an insurer's financial statement data, including running automated prioritization indicators and sophisticated analysis techniques enabling regulators around the country to have access to National-level data without the redundancy of reproducing this resource in every State. This centralized data and analysis capability has been cited by the IMF as world-leading.

Cybersecurity risk remains difficult for insurance underwriters to quantify due in large part to a lack of actuarial data. This has potential implications for on-going regulation and the market for the product. If a product is priced too low, the insurer may not have the financial means to pay claims to the policy holder. If too high, few businesses and consumers can afford to purchase it, instead opting to effectively self-insure for cyber incidents, limiting the ability of the insurance sector to be used as a driver of best practices. Today, in the absence of such data, insurers compensate by pricing that relies on qualitative assessments of an applicant's risk management procedures and risk culture. As a result, policies for cyber risk tend to be more customized than policies for other risks, and, therefore, more costly. The type of business operation seeking coverage, the size and scope of operations, the number of customers, the presence on the web, the type of data collected, and how the data is stored will all be among the factors that dictate the scope and cost of cybersecurity coverage offered. From a regulatory perspective, though, we would like to see insurers couple these qualitative assessments with robust actuarial data based on actual incident experience.

Prior to writing the policy, the insurer will want to see the business' disaster response plan and evaluate it with respect to network risk management, websites, physical assets, intellectual property, and possibly even relationships with third-party vendors. The insurer will be keenly interested in how employees, contractors, and customers are able to access data systems, how they are trained, and who key data owners are. At a minimum, the insurer will want to know about the types of antivirus and anti-malware software the business is using, the frequency of system and software updates performed by the business, and the performance of the firewalls the business is using.

Examination Protocols and Recent Updates

Last year, the NAIC, through a joint project of the Cybersecurity Task Force and the IT Examination Working Group, undertook a complete review and update of existing IT examination standards for insurers. Prior to this year, regulatory reviews of an insurer's information technology involved a 6-step process for evaluating security controls under the COBIT 5 framework. Revisions for 2016 to further enhance examinations are based in part on the NIST framework "set of activities" to Identify, Protect, Detect, Respond, and Recover. Specific enhancements were made to the NAIC *Financial Examiner's Handbook* regarding reviews of insurer cybersecurity training and education programs, incident response plans, understanding cybersecurity roles and responsibilities, post-remediation analyses, consideration of third-party vendors, and how cybersecurity efforts are communicated to the Board of Directors.

Also evolving are regulators' expectations of insurance company C-suites—specifically chief risk officers and boards of directors. Regulators expect improved incident response practice exercises, training, communication of cyber risks between the board and management, and incorporation of cybersecurity into the Enterprise Risk Management processes. There is now an expectation that members of an insurer's board of directors will be able to describe how the company monitors, assesses, and responds to information-security risks.

Market Regulation

Market regulation is focused on legal and fair treatment of consumers by regulation of product rates, policy forms, marketing, underwriting, settlement, and producer licensing. Market conduct examinations occur on a routine basis, but also can be triggered by complaints against an insurer. These exams review producer licensing issues, complaints, types of products sold by insurers and producers, producer sales practices, compliance with filed rating plans, claims handling and other market-related aspects of an insurer's operation. When violations are found, the insurance department makes recommendations to improve the insurer's operations and to bring the company into compliance with State law. In addition, an insurer or insurance producer may be subject to civil penalties or license suspension or revocation. To the extent that we see any of these issues arising from claims made on cybersecurity policies, regulators will be able to address them promptly through our suite of market conduct tools, and enhancements made to the *Financial Examiner's Handbook* are expected to be incorporated into the *Market Conduct Examiner's Handbook* this year.

Surplus Lines

It is worth mentioning that some cybersecurity coverage is currently being written in the surplus lines markets. A surplus lines policy can be issued only in cases where the coverage cannot be found in traditional insurance markets because the coverage is unique or otherwise difficult to underwrite. Surplus lines insurers that are domiciled in a U.S. State are regulated by their State of domicile for financial solvency and market conduct. Surplus lines insurers domiciled outside the United States may apply for inclusion in the NAIC's Quarterly Listing of Alien Insurers. The carriers listed on the NAIC Quarterly Listing of Alien Insurers are subject to capital and surplus requirements, a requirement to maintain U.S. trust accounts, and character, trustworthiness, and integrity requirements.

In addition, the insurance regulator of the State where the policy holder resides (the home State of the insured) has authority over the placement of the insurance by a surplus lines broker and enforces the requirements relating to the eligibility of the surplus lines carrier to write policies in that State. The insurance regulator can also potentially sanction the surplus lines broker, revoke their license, and hold them liable for the full amount of the policy.

Like any other insurance market, as the cybersecurity market grows and more companies offer coverage, we anticipate the regulation will continue to evolve to meet the size and breadth of the market as well as the needs of consumers. State insurance regulators have a long history of carefully monitoring the emergence and innovation of new products and coverages, and tailoring regulation over time to ensure consumers are appropriately protected and policies are available.

CYBERSECURITY INSURANCE MARKET—NEW REPORTING REQUIREMENTS

As a still nascent market for coverage, accurately assessing exposure or the size of the cybersecurity insurance market is a work in progress. To date, the only analyses of the cybersecurity market come from industry surveys and estimates that consistently place the size of the market in the neighborhood of $2–3 billion. In light of the uncertainty and many questions surrounding these products and the market, the NAIC developed the new *Cybersecurity and Identify Theft Coverage Supplement*[3] for insurer financial statements to gather financial performance information about insurers writing cybersecurity coverage Nation-wide.

This mandatory new data supplement, to be attached to insurers' annual financial reports, requires that all insurance carriers writing either identity theft insurance or cybersecurity insurance report to the NAIC on their claims, premiums, losses, expenses, and in-force policies in these areas. The supplement requires separate reporting of both stand-alone policies and those that are part of a package policy. With this data, regulators will be able to more definitively report on the size of the market, and identify trends that will inform whether more tailored regulation is necessary. We will gladly submit a follow-up report to the committee once we have re-

[3] Attachment B [This attachment is retained in the committee files].

ceived and analyzed the first batch of company filings, which are due April 1, and will keep all stakeholders apprised as we receive additional information. As with any new reporting requirement, we expect the terminology and reporting to mature over time as carriers better understand the specific information regulators need.

Having this data will enable regulators to better understand the existing cybersecurity market, and also help us know what to look for as the market continues to grow, particularly as we see small and mid-size carriers potentially writing these complex products.

NAIC EFFORTS BEYOND CYBERSECURITY INSURANCE

The NAIC and State insurance regulators are also ramping up our efforts to tackle cybersecurity issues in the insurance sector well beyond cybersecurity insurance. We understand that the insurance industry is a particularly attractive target for hackers given the kind of data insurers and producers hold, and to that end we are engaged on a number of initiatives to reduce these risks.

The NAIC adopted 12 *Principles for Effective Cybersecurity: Insurance Regulatory Guidance* in April 2015.[4] The principles set forth the framework through which regulators will evaluate efforts by insurers, producers, and other regulated entities to protect consumer information entrusted to them.

We also adopted an NAIC *Roadmap for Consumer Cybersecurity Protections* in December 2015 to describe protections the NAIC believes consumers should be entitled to from insurance companies and agents when these entities collect, maintain, and use personal information and to guide our on-going efforts in developing formal regulatory guidance for insurance sector participants.[5]

Most recently, on March 3, the Cybersecurity Task Force exposed its new *Insurance Data Security Model Law* for public comment—written comments should be submitted by Wednesday, March 23, and feedback will be discussed at the open meeting of the task force on April 4 in New Orleans.[6] The purpose and intent of the model law is to establish the exclusive standards for data security, investigation, and notification of a breach applicable to insurance licensees. It lays out definitions and expectations for insurance information security, breach response, and the role of the regulator. Recognizing that one size does not fit all, the model specifically allows for licensees to tailor their information security programs depending on the size, complexity, nature, and scope of activities, and sensitivity of consumer information to be protected. Perhaps most importantly, the model is intended to create certainty and predictability for insurance consumers and licensees as they plan, protect information, and respond in the difficult time immediately following a breach. We welcome all stakeholders' input as we continue the model's development through the open and transparent NAIC process.

Related to the NAIC's new model, we are aware Congress is considering a number of Federal Data Breach bills. While Congress held its first hearings on data breaches 20 years ago, there has been no successful legislation on the issue. Meanwhile, 47 States have acted to varying degrees, and some are on the fourth iteration of data security and breach notification laws. Some of these bills, including S. 961/H.R. 2205, the Data Security Act, would lessen existing consumer protections in the insurance sector and could undermine our on-going and future efforts to respond to this very serious issue.

COORDINATING WITH OUR FEDERAL COLLEAGUES

Lastly, we understand that State insurance regulators are not alone in any of our efforts. We work collaboratively with other financial regulators, Congress, and the administration to identify specific threats and develop strategies to protect the U.S. financial infrastructure. State insurance regulators and NAIC staff are active members of the Treasury Department's Financial Banking and Information Infrastructure Committee (FBIIC), where I recently gave a presentation on insurance regulators' efforts in this space.

We are also members of the Cybersecurity Forum for Independent and Executive Branch Regulators, where we meet with White House officials and other regulators to discuss best practices and common regulatory approaches to cybersecurity challenges across very different sectors of the U.S. economy. While we certainly do not have all the answers yet, rest assured that regulators are communicating and collectively focused on improving cybersecurity posture across our sectors.

---

[4] Attachment C [This attachment is retained in the committee files].
[5] Attachment D [This attachment is retained in the committee files].
[6] Attachment E [This attachment is retained in the committee files].

CURRENT STATE OF PLAY

I recently met with a group of insurance CEOs to discuss the NAIC's on-going efforts in data and cybersecurity. Several baseball metaphors were used in the meeting, so when the discussion pivoted to cyber insurance, I asked how far along they felt that market was in its development. One CEO said it was only the top of the first inning, and the lead-off batter has just grabbed a bat from the rack before the first pitch has even been thrown—the rest of the room nodded in agreement. We are on the first leg of a long race when it comes to cybersecurity insurance.

There is no question that the expansion of cyber risks and the maturation of the cybersecurity insurance are a tremendous opportunity for the insurance sector to lead in the development of risk-reducing best practices and cyber hygiene across our National infrastructure. Insurance has a long history of driving best practices and standardization by creating economic incentives through the pricing of products, and the underwriting process can test the risk management techniques and efficacy of a policy holder making a broader range of businesses secure. As insurers develop more sophisticated tools for underwriting and pricing, State regulators will continue to monitor and study cybersecurity products, always remembering that our fundamental commitment is to ensuring that policy holders are protected and treated fairly, and that insurance companies are able to pay claims when they come due.

CONCLUSION

As insurance markets evolve, State insurance regulators remain extensively engaged with all relevant stakeholders to promote an optimal regulatory framework-cybersecurity insurance is no exception. As the cybersecurity insurance market develops, we remain committed to effective regulation and to making changes when necessary. State insurance regulators will embrace new challenges posed by a dynamic cybersecurity insurance market and we continue to believe that well-regulated markets make for well-protected policy holders. Thank you again for the opportunity to be here on behalf of the NAIC, and I look forward to your questions.

ATTACHMENT A.—CYBERSECURITY (EX) TASK FORCE

Adam Hamm, Chair, North Dakota
Raymond G. Farmer, South Carolina
Jim L. Ridling, Alabama
Lori K. Wing-Heier, Alaska
Allen W. Kerr, Arkansas
Dave Jones, California
Marguerite Salazar, Colorado
Katharine L. Wade, Connecticut
Karen Weldin Stewart, Delaware
Stephen C. Taylor, District of Columbia
Kevin M. McCarty, Florida
Gordon I. Ito, Hawaii
Dean Cameron, Idaho
Anne Melissa Dowling, Illinois
Ken Selzer, Kansas
Brian Maynard, Kentucky
Eric A. Cioppa, Maine
Al Redmer, Jr., Maryland
Mike Hothman, Minnesota
John M. Huff, Missouri
Monica J. Lindeen, Montana
Bruce R. Ramge, Nebraska
Barbara Richardson, Nevada
Roger A. Sevigny, New Hampshire
Peter L. Hartt, New Jersey
John G. Franchini, New Mexico
Maria T. Vullo, New York
Wayne Goodwin, North Carolina
Mary Taylor, Ohio
John D. Doak, Oklahoma
Teresa D. Miller, Pennsylvania
Angela Weyne, Puerto Rico
Elizabeth Kelleher Dwyer, Rhode Island
Larry Deiter, South Dakota
Julie Mix McPeak, Tennessee

David Mattax, Texas
Todd E. Kiser, Utah
Susan L. Donegan, Vermont
Jacqueline K. Cunningham, Virginia
Mike Kreidler, Washington
Ted Nickel, Wisconsin
NAIC Support Staff: Eric Northman/Sara Robben/Tony Cotto/Cody Steinwand

Mr. RATCLIFFE. Thank you, Commissioner Hamm.

The Chair now recognizes Mr. Nutkis for his opening statement.

STATEMENT OF DANIEL NUTKIS, CHIEF EXECUTIVE OFFICER, HEALTH INFORMATION TRUST ALLIANCE

Mr. NUTKIS. Good morning, Chairman Ratcliffe, Ranking Member Richmond, and the distinguished Members of the subcommittee. I am pleased to appear today to discuss the role of cyber insurance in risk management, and initiatives underway by HITRUST and the health care industry to expand and leverage its role.

I am Dan Nutkis, CEO and founder of the Health Information Trust Alliance, or HITRUST. While I prepared my written statement for the record, I would like to share with you a few of the highlights.

HITRUST helps elevate the health care industry's cyber awareness, improve cyber preparedness, and strengthen risk management posture. In particular, I want to point out how cyber insurance is integral to this process.

There should be no question as to the significance of managing cyber risk, and an organization's ability to respond efficiently and effectively to cybersecurity incidents plays in cyber resilience. To aid industry in cyber risk management, threat preparedness, and response, HITRUST implemented numerous programs in coordination with industry stakeholders, including our risk management framework, or HITRUST RMF.

Our perspective on evolving cybersecurity threats facing the health care industry is formed based on our deep engagement with the industry around information protection. That engagement includes data from over 14,000 security assessments done in 2015 alone, leveraging the HITRUST RMF, as well as operating the industry's information-sharing and analysis organization, or ISAO, and running CyberRX, now in its third year, which is a series of industry-wide exercises developed by HITRUST to simulate cyber attacks on health care organizations, and evaluate the industry's preparedness against attempts to disrupt U.S. health care industry operations. In 2015, over 1,000 organizations participated in CyberRX.

The HITRUST RMF incorporates a risk-based control framework, specifically the HITRUST CSF, which is a scalable, prescriptive, and certifiable, risk-based information, privacy, and security control framework. It provides an integrated, harmonized set of requirements tailored specifically for the health care industry. The HITRUST RMF is adopted by approximately 80 percent of the hospitals and health plans, making it the most widely adopted in the industry.

Leveraging HITRUST's knowledge and role in understanding and aiding industry in risk management, HITRUST approached Willis

Towers Watson, a leading insurance brokerage, to explore ways to leverage the HITRUST RMF to allow insurers to better and more effectively evaluate cyber risk. HITRUST and Willis established a detailed approach to educate and substantiate the value of leveraging the HITRUST RMF as the basis for their cyber underwriting programs in the health care industry. I have outlined 8 points in my written testimony that provides details on this approach and process.

Over the last 5 months, HITRUST and Willis have worked to educate cyber insurers regarding the use of the HITRUST RMF in supporting the cyber risk underwriting process. Insurers have found the HITRUST CSF to offer many advantages over the existing approaches, including providing a comprehensive and mature controls framework, aligning strong controls with risk, and accurately and consistently measuring residual risk.

Allied World was the first company to offer preferred terms and conditions based on meeting the HITRUST CSF certification standards. After review and analysis, Allied World has determined that the CSF framework and CSF insurance methodology will insure its underwriting program in terms of efficiency, consistency, and accuracy, allowing it to better align the effectiveness of an organization's security controls with cyber insurance premium levels.

The review also concluded that organizations that had obtained a HITRUST CSF certification posed lower cyber-related risks than organizations that had not. The comprehensiveness and improved risk reporting enabled by the HITRUST CSF and the CSF assessment summary scores in place of many of the standard information security application questions creates a more streamlined and consistent application process. Allied World will also provide HITRUST with loss data in order to ensure the HITRUST CSF control guidance accurately reflects the associated risks.

In addition, we are in discussions with 5 other cyber underwriters regarding leveraging this approach with an expectation that 2 more will be participating by mid-year. It is clear that this approach is a win-win for the health care industry, underwriters, and, of course, the members and patients whose information they are responsible for safeguarding.

For health care organizations, it drives better behavior in the industry, supports better control selections, and helps prioritize remediation activity, which ultimately provides better protection for patients. For cyber insurance underwriters, it ensures premium costs are proportionate to risk, provides more targeted coverage relevant to actual risks, and ultimately provides a more sustainable underwriting model.

HITRUST also believes this current cyber insurance platform could provide the risk management focus to encourage health care organizations to invest in maturing their information protection programs, once they understand the impact residual risk has on cyber insurance premiums.

With that, Mr. Chairman, I am pleased to answer any questions.

[The prepared statement of Mr. Nutkis follows:]

PREPARED STATEMENT OF DANIEL NUTKIS

MARCH 22, 2016

Chairman Ratcliffe, Ranking Member Richmond, and distinguished Members of the subcommittee, I am pleased to appear today to discuss the role of cyber insurance in risk management, and initiatives underway by HITRUST and the health care industry to ensure its role is enhanced. I am Daniel Nutkis, CEO and founder of the Health Information Trust Alliance, or HITRUST. I founded HITRUST in 2007, after recognizing the need to formally and collaboratively address information privacy and security for health care stakeholders representing all segments of the industry, including insurers, providers, pharmacies, PBMs, and manufacturers. HITRUST endeavored—and continues to endeavor—to elevate the level of information protection in the health care industry, ensuring greater collaboration between industry and Government, and raising the competency level of information security professionals.

In my testimony today, I would like to highlight how HITRUST helps elevate the industry's cyber awareness, improve cyber preparedness and strengthen the risk management posture of the health care industry. In particular, I want to point out how cyber insurance is integral to this process.

There should be no question as to the significance that managing cyber risk and an organization's ability to respond efficiently and effectively to cybersecurity incidents plays in cyber resilience. To aid industry in cyber risk management, threat preparedness, and response, HITRUST has implemented numerous programs in coordination with industry stakeholders as part of its overall risk management framework (RMF).

The HITRUST RMF provides a risk-based control framework, specifically the HITRUST CSF, which is a scalable, prescriptive, and certifiable risk-based information privacy and security control framework. It provides an integrated, harmonized set of requirements tailored specifically for health care.

Health care organizations are subject to multiple regulations, standards, and other policy requirements, and commonly-accepted best practice standards, including implementing the NIST Cybersecurity Framework. However, these "authoritative sources" often overlap in the depth and breadth of their requirements, which, when integrated and harmonized, can often be mutually reinforcing when intelligently applied in the intended environment.

To ensure the HITRUST CSF remains relevant, it is reviewed and updated at least annually. The review not only takes into account changes in underlying regulations and standards, but it also considers best practices and lessons learned from security incidents, incident response exercises, and industry post-data breach experiences.

This level of comprehensiveness, relevance, and applicability is why over 80 percent of hospitals and health plans, as well as many other health care organizations and business associates, have adopted the HITRUST CSF, making it the most widely adopted privacy and security framework in health care.

Also distinctive to the HITRUST RMF, the HITRUST CSF Assurance Program delivers a comprehensive, consistent, and simplified compliance assessment and reporting program for regulatory requirements, such as HIPAA, HITECH, and other Federal and State requirements, and the sharing of assurances between and amongst covered entities and business associates. Specifically designed for the unique regulatory and business needs of the health care industry, the HITRUST CSF Assurance Program provides health care organizations and their business associates with a common approach to manage privacy and security assessments that enables efficiencies and contains costs associated with multiple and varied information protection requirements. The CSF Assurance Program incorporates specific guidelines to allow a broad array of leading industry professional services firms to perform services, while allowing HITRUST to oversee quality assurance processes to ensure assessments are rigorous, consistent, and repeatable.

An additional benefit of using the HITRUST RMF is that it supports assessment and reporting for multiple and varied purposes,[1] such as the evaluation of AICPA's Trust Services Principles and Criteria and SSAE–16 SOC 2 reporting "scorecards" against regulatory requirements and best practice frameworks, such as HIPAA, the

[1] Health care organizations have been saving roughly 25–30% of audit costs when leveraging a HITRUST RMF Certification and a SSAE–16 SOC2 audit. Similar underwriting and auditing savings are also envisioned as the cyber insurance industry matures.

NIST Cybersecurity Framework, and State-based covered entity privacy and security certifications like the SECURETexas program.[2]

Just last month, HITRUST announced the availability of a new guide to assist health care organizations in implementing the NIST Cybersecurity Framework. This new guide was developed in consultation with the Healthcare and Public Health (HPH) Sector Coordinating Council (SCC) and Government Coordinating Council (GCC), along with input from other sector members and the DHS Critical Infrastructure Cyber Community (C3), to help HPH Sector organizations understand and use the HITRUST RMF to implement the NIST Cybersecurity Framework in the HPH Sector and meet its objectives for critical infrastructure protection.

I would also note that the availability of the HITRUST CSF, HITRUST CSF Assurance program and this implementation guide also provides an excellent basis for the Department of Health and Human Services (HHS) to leverage "voluntary, consensus-based, and industry-led guidelines, best practices, methodologies, procedures, and processes that serve as a resource for cost-effectively reducing cybersecurity risks for a range of healthcare organizations."

HITRUST has spearheaded initiatives in other areas of cybersecurity as well. In 2012, after identifying the need for coordination among stakeholders, HITRUST launched a cyber-threat intelligence-sharing and analysis program to provide threat intelligence, coordinated incident response and knowledge transfer specific to cyber threats pertinent to the health care industry. This program facilitates the early identification of cyber attacks and the creation of best practices specific to the health care environment and maintains a conduit through the Department of Homeland Security (DHS) to the broader cyber-intelligence community for analysis, support, and the exchange of threat intelligence. HITRUST was also the first to track vulnerabilities related to medical devices and electronic health record (EHR) systems, which are both emerging areas of concern.

This program became the foundation for the HITRUST Cyber Threat XChange (CTX), which significantly accelerates the detection of and response to cyber threat indicators targeted at the health care industry. HITRUST CTX automates the process of collecting and analyzing cyber threats and distributing actionable indicators in electronically-consumable formats (e.g. STIX, TAXII, and proprietary SIEM formats) that organizations of almost all sizes and cybersecurity maturity can utilize to improve their cyber defenses. HITRUST CTX acts as an advanced early warning system as cyber attacks are perpetrated on the industry. The HITRUST CTX is now offered free of charge to the public and has gained wide acceptance within the health care industry. HITRUST is also a Federally-recognized Information Sharing and Analysis Organization (ISAO), has strong relationships with DHS and the Federal Bureau of Investigation (FBI), and considers them integral partners in better addressing the threat landscape facing health care today and strengthening the continuum of care.

HITRUST also developed CyberRX, now in its third year, which is a series of industry-wide exercises developed by HITRUST to simulate cyber attacks on health care organizations and evaluate the industry's preparedness against attempts to disrupt U.S. health care industry operations. These exercises examine both broad and segment-specific scenarios targeting information systems, medical devices, and other essential technology resources of the HPH Sector.[3] CyberRX findings are analyzed and used to identify general areas of improvement for industry, HITRUST, and Government and to understand specific areas of improvement needed to enhance information sharing between health care organizations, HITRUST, and Government agencies.

I only share this information to provide context on our engagement, experience, knowledge, and commitment in supporting the health care industry around cyber risk management.

Now to the specifics of the topic at hand. We can all agree that managing the risks associated with cyber threats requires a comprehensive approach to risk management, including the implementation of strong security controls such as the HITRUST CSF, continuous monitoring of control effectiveness, and routine testing of cyber incident response capabilities, such as in CSF Assurance and CyberRX. Commonly applied "network hygiene" only covers what is referred to as "basic blocking and tackling." Cyber information sharing, such as that facilitated by HITRUST CTX, is designed to help organizations go beyond basic "hygiene" by alerting organizations to potential cyber threats, however, information sharing is very much de-

[2] SECURETexas is the first State program of its kind in the country offering privacy and security certification for compliance with State and Federal laws that govern the use of protected health information (PHI).

[3] See *https://www.dhs.gov/healthcare-and-public-health-sector*.

pendent on the maturity of participating organizations and their ability to consume and respond to the potential threat indicators that have been identified.

While there is not a perfect solution to cybersecurity; the best strategy is to prevent, detect, and respond before the adversary achieves their objective.

A data breach in the health care industry not only has financial and reputational effects on the company targeted by the threat actors, but the effects could be dramatic for members, patients, and their families due to the nature of the data disclosed. Personal health information or identities could be stolen directly from hospitals, insurance companies, pharmacies, and from any business associate supporting these organizations. Beyond the privacy implications of data breach incidents, these breaches have the potential to disrupt operations of a health care facility or affect patient care. The various complexities, interdependencies, and unique attributes all create various risk levels that need to be considered across the continuum of care.

And HITRUST firmly believes cyber insurance and cyber insurance underwriters can play a key role in supporting an organization's overall risk management strategy and help provide for the "adequate protection" of patient information.

Organizations have relied heavily on cyber insurance as one of the means to reduce the overall financial impact of cyber-related incidents or breaches. But after numerous cyber-related breaches affecting health care organizations over the past few years, it is clear that health care data is one of the prime targets of malicious cyber threat actors who strive to monetize the data they seize. As a result of increased targeting by threat actors and recent incidents, underwriters have determined the risks were greater than they had anticipated given the methods leveraged to evaluate risk and, subsequently, health care organizations' cyber insurance premiums have increased dramatically.

In many cases, companies who underwrite cyber insurance struggle with an effective way to evaluate cyber risk and the full extent of a company's cybersecurity controls.

Every cyber insurer customarily uses a specific application for insurance, and each application differs substantially. These tools are intended to be used to help insurers gain an understanding of key risk controls, but are not intended to be used as part of a comprehensive assessment. Additionally, many cyber insurance carriers rely on a wide array of supplemental questionnaires intended to provide them with additional insight to support coverage and pricing decisions. However, the industry lacks a consistent underwriting process, given that the questions and applications can vary significantly from one carrier to the next.

Insurance underwriters have always been investigating ways to efficiently and accurately evaluate risk and help health care organizations ensure health information systems and services are adequately protected from cyber risks.

Leveraging HITRUST's role in aiding industry in risk management, HITRUST approached Willis Towers Watson (Willis), a leading insurance broker, to explore ways to leverage the HITRUST RMF to allow insurers to better evaluate cyber risk and to also address 3 concurrent needs:

(1) Ensure people, processes, and technology elements completely and comprehensively address information and cybersecurity risks;

(2) Identify risks from the use of information by the organization's business units; and

(3) Facilitate appropriate risk treatments, including risk avoidance, transfer, mitigation, and acceptance.

HITRUST and Willis established the following approach to educate and substantiate the value of leveraging the HITRUST RMF as the basis for their cyber underwriting programs in the health care industry:

(1) Compare the use of the HITRUST RMF, and the HITRUST CSF in particular, to current application-based risk evaluation and pricing methodology;

(2) Map the HITRUST CSF to insurer applications to demonstrate how it addresses the current application process and the additional depth it provides;

(3) Show how superior risk evaluation efficiency and consistency can be achieved using assessment scores and summaries without sacrificing detail;

(4) Identify where the HITRUST CSF assessment scores and summaries can replace current application elements and other risk management-gathering methods;

(5) Use test cases to substantiate accuracy and efficiency of the HITRUST CSF as a key underwriting resource in risk evaluation that allows an underwriter to compare an application-based risk evaluation to HITRUST CSF assessment-based risk evaluation;

(6) Correlate claims with HITRUST CSF scores for test cases in support of a pricing framework aligned with the scores;

(7) Provide feedback to HITRUST on successful attack scenarios to bring underwriter experience and any key concerns into the HITRUST CSF development process to improve risk management; and
(8) Explore a pricing framework based on HITRUST CSF certification and various levels of control maturity in the certification process.

By leveraging a standardized approach to control selection and risk assessment and reporting, underwriters and other stakeholders can obtain risk estimates that are accurate, consistent, repeatable, and evolving, that is, risk estimates that take evolving risks and threats into consideration.

The goal is to integrate risk management into the underwriting process without adding confusion or unneeded complexity. HITRUST and Willis studied the relationship between HITRUST CSF and CSF Assurance control assessment scores, risk, coverage, and premiums to provide a simple, but effective data point to complement existing underwriting models.

After many months analyzing the benefits of an underwriting program leveraging a robust risk management framework, both HITRUST and Willis saw immediate value in the approach and began educating underwriters on a cybersecurity assessment methodology that would provide the industry with consistent, repeatable, reliable, and precise estimates of cyber-related risk. The HITRUST CSF and CSF Assurance program would provide underwriters with the information they could use to better understand an organization's residual cyber risk, and apply to their underwriting process.

The benefits of the HITRUST RMF-based underwriting model for cyber insurance in the health care industry allows organizations to maximize the benefits of demonstrating an enhanced information security posture. Ultimately, the better controls you have in place, the less likely you are to experience a breach. If a breach does occur, the potential impact will likely be contained and mitigated. This will translate into lower premiums and broader coverage for organizations who meet certain criteria defined by the HITRUST CSF. This is in many respects analogous to a "good driver discount program".

In addition to streamlining the underwriting process by leveraging their existing risk assessment, it also encourages organizations to consider the financial implications of cyber-related risks. Specifically, analyzing the impact on premium from investments reducing their cyber risks. Which is the mindset and behavior we would like to see organizations engage.

Over the past 5 months, HITRUST and Willis have worked to educate cyber insurers regarding the use of the HITRUST CSF and CSF Assurance program in supporting the cyber risk underwriting process. Insurers have found the HITRUST CSF to offer many advantages over the existing approaches, including providing a comprehensive and mature controls framework, aligning strong controls with risk, and accurately and consistently measuring residual cyber risk.

Allied World was the first company to offer preferred terms and conditions based on meeting the HITRUST CSF certification standards. After review and analysis, Allied World U.S. has determined that the HITRUST CSF framework and CSF Assurance methodology, will enhance its underwriting program in terms of efficiency, consistency, and accuracy, allowing it to better align the effectiveness of an organization's security controls with cyber insurance premium levels.

The review also concluded that organizations that had obtained a HITRUST CSF Certification generally posed lower cyber-related risks than those organizations that have not. The comprehensiveness and improved risk reporting enabled by the HITRUST CSF and the CSF Assessment summary scores in place of many of the standard information security application questions create a more streamlined and consistent application process. Allied World will also provide HITRUST with loss data in order to ensure the HITRUST CSF control guidance accurately reflects the associated risks.

In addition, Willis and HITRUST are in discussions with 5 other cyber underwriters regarding leveraging this approach, with an expectation that 2 more will be participating by mid-year. It is clear that this approach is a win-win for the health care industry, underwriters, and of course, the members and patients whose information they are responsible for safeguarding.

For health care organizations, it drives better behavior in the industry, supports better control selection, and helps prioritize remediation activity, which ultimately provides better protection for patients. For cyber insurance underwriters, it ensures premium costs are proportional to risk, provides more targeted coverage relevant to actual risks, and ultimately provides a more sustainable underwriting model.

As you can see, the cybersecurity and risk management challenges facing the health care industry are complex and in some cases daunting, in many cases unique

to industry dynamics, and they evolve at a pace that is unrealistic to manage by regulations and strict Governmental policy or high-level policy document.

HITRUST, in partnership with industry, has been constantly working to establish programs to aid industry in mitigating cyber risks and is committed to be the link between the public and private sector that will continue to provide value and strengthen our industry, our Government, our economy, and our Nation as a whole against the growing cyber threats we face.

HITRUST saw an opportunity to bring relevant industry stakeholders together to help health care organizations better manage cyber risk and help the insurance industry better align cyber insurance premiums with this risk by leveraging a formal framework, like the HITRUST RMF. Risk management methodologies help companies address applicable regulations, standards, and best practices, and health care and insurance industry threat data helps identify high-risk controls requiring executive attention and link incidents to controls guidance. In many ways, this breach data helps inform insurance loss experience and allows cyber underwriters to play a key role in understanding where losses are occurring.

HITRUST also believes this current cyber insurance platform could provide the risk management focus to further drive innovation and encourage health care organizations to invest in maturing their information protection programs. HITRUST is working with underwriters to improve actuarial data and provide better estimates of risks while using threat and incident data to improve control selection within the HITRUST RMF. While we believe we have a novel approach and are leveraging new partners to grow its acceptance, mandates have the potential to stifle the innovations taking place in the marketplace. This market-based approach will provide a better insurance product for policy holders while allowing organizations to grow and mature their information security programs.

HITRUST, through its many tools and programs, remains committed to ensure that the health care industry can properly address these challenges. Cyber insurance will be a key component in HITRUST's approach to cybersecurity and cyber risk management, and we are excited about pioneering this approach to strengthen risk management.

Thank you again for the opportunity to join you today and share these insights. I look forward to your questions.

Mr. RATCLIFFE. Thank you, Mr. Nutkis. The Chair now recognizes Mr. Finan for his opening statement.

STATEMENT OF THOMAS MICHAEL FINAN, CHIEF STRATEGY OFFICER, ARK NETWORK SECURITY SOLUTIONS

Mr. FINAN. Chairman Ratcliffe, Ranking Member Richmond, and Members of the subcommittee, thank you very much for inviting me to address the role of cybersecurity insurance in risk management. I am greatly honored to share my perspectives with you about this very important topic.

I am the chief strategy officer with Ark Network Security Solutions in Dulles, Virginia, but until recently I served as a senior cybersecurity strategist and counsel with DHS's National Protection and Programs Directorate, where I led the Department's Cyber Incident Data and Analysis Working Group for the last 4 years.

DHS engaged the cybersecurity insurance market early on because of its tremendous potential to incentivize better cyber risk management, and our starting point really was the fire insurance market. Through years of collective claims information, insurers have been very successful in identifying the fire safety controls that need to be in place to protect lives and property. Those controls have become the gold standard. You can't get a permit to build a commercial building, and you can't get fire insurance for that building unless you have those controls in place.

We wanted to know if the cybersecurity insurance market could do the same thing. Specifically, could it help identify the cyber risk control equivalents of sprinkler and other fire suppression systems?

We discovered that while the insurance industry will certainly get there, there is still more work to do.

DHS initiated a series of public workshops from October 2012 through the spring of 2014, to determine what obstacles are impeding the market's progress. Brokers and underwriters identified 4, including a lack of actuarial data: The absence of common cybersecurity standards, best practices and metrics; a lack of knowledge about critical infrastructure dependencies and interdependencies; and an on-going failure by many companies to include cyber risk within their existing enterprise risk management programs.

In response, brokers and underwriters look to see if a company has an effective cyber risk culture to determine if it is a safe insurance bet. They identified 4 pillars of such a culture, including what roles executive leadership, education and awareness, technology, and relevant information sharing play in securing the business environment. Given these findings, we asked our insurance participants what we could do to help advance the cyber insurance market. They told us that we should turn our attention to the concept of a cyber incident data repository, one where companies could anonymously share their cyber incident data so it could be aggregated and analyzed for maximum risk management benefit.

In December 2014, DHS accordingly established the CIDAWG to bring together brokers, underwriters, CISOs, and other cybersecurity professionals to discuss the repository idea. Throughout 2015, the group discussed 3 major topics: The value proposition for a cyber incident data repository, the kinds of data a repository would need to be successful, and how to overcome likely obstacles to repository sharing. A fourth topic, how a repository should actually be structured, will be the subject of a DHS workshop next month.

We published 3 white papers last year that detailed the CIDAWG's findings. The first, on the value proposition, identified 5 kinds of analysis that would benefit brokers, underwriters, CISOs, and others. Specifically, analysis that identifies top cyber risks and the controls that are most effective in addressing them; analysis that informs peer-to-peer benchmarking, promotes sector differentiation, supports cyber risk forecasting, trending and modeling, and advances cyber risk management culture. The group then spent several months identifying 16 data categories that the CIDAWG believed would help deliver on that value, and we released them publicly in September of last year.

In December, the CIDAWG published its third white paper on likely obstacles to repository sharing and ways to overcome them. They included assuring anonymization of the repository, ensuring the security of the data it holds, cultural and regional challenges that could result in skewed data contributions, perceived commercial disadvantage to repository participation, internal process hurdles, the perceived value of a repository, assuring appropriate, adequate, and equitable participation, and technical design issues.

The CIDAWG was very successful in breaking down barriers between the insurance industry and technical cybersecurity professionals. I strongly believe that the same model could be adopted to help address the cybersecurity needs of mid-size and small businesses that today are struggling to keep up. Although they are often key players in the global supply chain, and a source for the

continued growth of the cybersecurity insurance market, they too often lack the budgets, expertise, staff, and time to adequately and consistently address their cyber risks. As a result, mid-size and small businesses tend to have weaker security that makes them not only easier to attack, but also a prime launching point for attacks against others.

Cybersecurity expert exchanges, best practice knowledge sharing, compliance, automation, and coordination of cybersecurity investments are just a few topics of conversation that a CIDAWG-like group could initiate to address this key area of vulnerability that affects us all.

Thank you, and I look forward to your questions.

[The prepared statement of Mr. Finan follows:]

PREPARED STATEMENT OF THOMAS MICHAEL FINAN

MARCH 22, 2016

Chairman Ratcliffe, Ranking Member Richmond, and Members of the subcommittee, thank you for inviting me to address the role of cybersecurity insurance in risk management. I am the chief strategy officer at Ark Network Security Solutions, a private company that provides software and services to accelerate standards compliance for enhanced security. Until this past December, I served as a senior cybersecurity strategist and counsel with the U.S. Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD), where I launched and led DHS's Cybersecurity Insurance Initiative. I will describe the role that DHS has played in identifying and overcoming obstacles to a more robust cybersecurity insurance market. I will also discuss how the private-public engagement model that DHS has followed as a convener of the insurance conversation could be extended to address the cyber risk management needs of mid-size and small businesses nationally.

DHS'S CYBERSECURITY INSURANCE INITIATIVE

As a largely operations-focused organization, NPPD may not immediately come to mind as a likely candidate to lead a sustained discussion with stakeholders about cybersecurity insurance. NPPD has a more general mandate beyond its day-to-day cybersecurity mission, however, and its mission statement says it all:

"NPPD's vision is a safe, secure, and resilient infrastructure where the American way of life can thrive. NPPD leads the national effort to protect and enhance the resilience of the nation's physical and cyber infrastructure."

That means DHS must do more than just help its partners extinguish rapidly-developing cyber risk "fires." It also requires DHS to think more strategically and to figure out what cyber risk fires—and what potential solutions to them—may be ahead and then determine how to address both as part of its overall resilience mission. Ultimately, DHS is in the risk management business. It is increasingly called to think about risk management not just 3 to 5 minutes, hours, or days ahead but—like its external partners—3 to 5 years ahead.

Insurance, we learned, is a key part of that process. When we began DHS's inquiry into the cybersecurity insurance market, we asked whether cybersecurity insurance could—as a market force—raise the cybersecurity "floor" by getting more critical infrastructure owners to manage their cyber risk better in return for more relevant and hopefully more affordable policies. At the time, our point of reference was the fire insurance market. We knew that insurers had been very successful in identifying specific fire safety controls that today are not only conditions for coverage within fire insurance policies but also prerequisites for obtaining a building permit. Our hope was that brokers and underwriters together could help identify the cybersecurity equivalents of sprinkler and other fire suppression systems. What we discovered is that while they may get there one day, they are not there yet.

Challenges

From 2012 through 2014, DHS engaged a wide range of partners through a series of public workshops on the cybersecurity insurance topic. Our participants included brokers and underwriters, chief risk officers, chief information security officers, critical infrastructure owners and operators, and members of the academic community. During the course of our conversations, we asked them whether now or in the future

insurance could help incentivize better cyber risk management. DHS was especially interested in finding out if the market already provided coverage—or could eventually provide coverage—for physical damages and bodily injuries that might result from a successful cyber attack against critical infrastructure. What we heard back is that several major obstacles continue to prevent insurers from providing more cybersecurity insurance coverage—specifically, higher limits—than they currently do. Chief among them are:

- First, the market suffers from an on-going lack of actuarial data. Unlike fire insurance, insurers do not have 100 years' worth of cyber loss data that they can use to build out new policies. This has inhibited them from providing more than the $10 to $15 million in primary coverage that they historically have offered customers for data breach and network security-related losses. Despite some recent progress, moreover, very few insurers provide discrete coverage for cyber-related critical infrastructure loss. When we asked why, the insurers explained that for obvious reasons, they do not receive claims against policies that do not yet exist. Without such claims, however, they have no way to build out the actuarial tables they need to expand their offerings. In short, they are left with little insight into the growing number of SCADA and other industrial control system attacks that are occurring world-wide. They insurers further advised that they similarly lack a consistent source of raw cyber incident data that they could alternatively use to get their underwriting bearings in this area.
- Second, brokers and underwriters cited the absence of common cybersecurity standards, best practices, and metrics as a further hurdle to a more robust market. They nevertheless cited the advent of the NIST Cybersecurity Framework in 2014 as a very positive development. Many advised that the Framework's common vocabulary for cyber risk management topics was helping them have more in-depth conversations with their current and potential clients about their cyber risk profiles than otherwise would be the case. They also told us that they would like to see tailored versions of the Framework emerge for each of the Nation's 16 critical infrastructure sectors that provide more particularized risk management information to their clients in those sectors. The ultimate utility of the Framework, they added, remains to be seen. Several underwriters explained that they continue to seek answers to two key questions: (1) Are companies that use the Framework having a better cyber loss experience than their peers that don't; and (2) what Framework-inspired controls should be incorporated into cybersecurity insurance contracts as conditions for coverage—like sprinkler systems for fire insurance?
- Third, the workshop participants noted an on-going lack of understanding about critical infrastructure dependencies and interdependencies as another major obstacle. Like most of the population, brokers and underwriters do not know much about how a cyber-related critical infrastructure failure in one sector might cascade across multiple other sectors. Until they have a better idea about how big and bad related losses might be—and where a strategically-placed risk control might make a difference—they are reluctant to develop new insurance products to cover this loss category. Without more insight, one underwriter explained, one big loss affecting hundreds of clients could effectively put them out of business.
- Fourth, a final challenge to the cybersecurity insurance market is the on-going failure by many companies to include cyber risk as part of their traditional enterprise risk management—or ERM—programs. Despite the growing threat, many companies continue to treat cyber risk as an IT problem, separate and apart from the other business risks they face. Without including cyber risk within existing ERM programs, however, they really are not "doing ERM." Consequently, they often are blind to their true risk profiles and may not be prioritizing their risk management resources most effectively.

Cyber Risk Culture

Given these obstacles, brokers and underwriters told us that they generally consider 2 major risk management factors when assessing a company's qualifications for coverage: Its compliance with available cybersecurity standards and its risk culture. In so doing, they pay particular attention to the internal cybersecurity practices and procedures that a company has adopted, implemented, and enforced. Several underwriters advised that they focus primarily on risk culture when assessing a potential insured for coverage—leading them to draft custom policies for clients rather than more generic "template" policies that can be marketed more broadly. Regardless of their particular practices, practically all of the participants suggested that DHS should turn its attention next to how companies should go about building more effective cyber risk cultures.

This made a lot of sense. We started thinking: If a core group of brokers and underwriters is looking to how companies individually manage their cyber risk, then maybe we could discover some lessons learned that might be more broadly applicable to others. We therefore identified 4 "pillars" of an effective cyber risk culture that appeared to merit a deeper dive. Those pillars included the roles of:

- *Executive Leadership*.—What should boards of directors be demanding—and doing themselves—to build corporate cultures that manage cyber risk well?
- *Education and Awareness*.—What messages, training, and accountability mechanisms need to be in place internally in companies, among partnering companies, and at a National level to help create a culture of cybersecurity?
- *Technology*.—How should technology be leveraged to encourage better cybersecurity practice?
- *Relevant Information Sharing*.—Who within a company needs what information, and in what formats, to help drive more effective cyber risk management investments?

Several core conclusions emerged from our discussions:

- First, for many companies, the business case for more effective cyber risk management investment still has not been made. The key reason for this appears to be that cyber risk by and large has not been reduced to terms that non-technical business leaders can readily understand—namely, the financial costs of cyber events and the potential damages to reputation for failing to mitigate them adequately. Many of our participants suggested that to overcome this, companies should adopt ERM programs that incorporate cyber risk into the vast pool of other business risks they face.
- Second, many of our participants called for more research when it comes to the costs and benefits of existing and future cybersecurity solutions. Once corporate leaders engage, they explained, they will want to know what investments to make to best manage their cyber risk. In other words, which controls offer the most cybersecurity bang for the buck?
- Third, the participants explained that it probably is unrealistic to expect the insurance industry to come up with a one-size-fits-all suite of cyber risk controls that everyone should adopt in return for more coverage and (eventually) lower premiums. What the underwriters told us is that they typically do not spend weeks with potential insureds reviewing and red-teaming every aspect of their organizations to see what is happening with their information security. Moreover, they no longer subject corporate IT professionals to hundreds of detailed questions getting at the technical and human-based control aspects of this information. Instead, they usually survey the companies—asking just 20–25 questions directed at basic, high-level information security issues to eliminate only the most ill-prepared companies from coverage consideration.

This third point, however, does not mean that the insurance industry does not have an important cyber risk management role to play. On the contrary, what a growing number of strategically-focused brokers and underwriters look for during the underwriting process, separate and apart from the insurance application, is how well companies understand where they uniquely sit in the cyber risk landscape and what they are doing about their particular circumstances. Put simply, this means:

- Do they know what cyber incidents are actually happening to them based on their own data and reports from outside sources?
- Do they know—through public sources and private conversation—what kinds of cyber incidents are happening to other companies like them; and
- What cyber risk management investments are they making based on this information?

In other words, these brokers and underwriters are assessing whether a company exhibits an engaged cyber risk culture—one where corporate leaders support risk mitigation efforts aimed at the cyber risks most relevant to their companies. Such engagement serves as a critical point of differentiation between companies that represent a safer versus unsafe cyber risk.

ACTION OPTIONS

During DHS's fourth and final public workshop in April 2014, we asked our insurance participants how we could best help them work through some of the cybersecurity insurance market's persistent challenges. They identified 3 topic areas for further discussion:

- Cyber incident information sharing (as opposed to cyber threat sharing), with a specific focus on the value of creating an anonymized cyber incident data repository;
- Cyber incident consequence analytics; and

• Promotion of comprehensive ERM strategies that incorporate cyber risk.

When we asked how to prioritize this list, the insurance participants agreed that DHS should focus first on the concept of a cyber incident data repository—specifically, one that helps meet the cyber risk analysis needs of the insurance industry, chief information security officers (CISOs), chief security officers (CSOs), and other cybersecurity professionals.

From the start, the brokers and underwriters described a repository notionally as a place where companies could anonymously share their cyber incident data. That data, they explained, could then be aggregated and analyzed to increase awareness about current cyber risk conditions and longer-term cyber risk trends. They explained that this information could benefit not only the insurance industry with its risk transfer efforts but also CISOs, CSOs, and other cybersecurity professionals with their complementary cyber risk mitigation efforts. The brokers and underwriters emphasized that these professionals should be central to any future repository discussion. They felt strongly that if the men and women on the front lines of cybersecurity are not "bought in" on the idea, then all the talking in the world would be for naught. We agreed and endeavored to engage not only insurance experts but also these day-to-day practitioners who had hands-on knowledge about cyber incidents and the kinds of analysis that would help them better prepare, respond, and recover from them. The results from our initial follow-up conversations testing the waters were promising:

- From the insurance side, we heard that a repository could help the industry build up the information stores it needs to better understand the impacts of cyber events, their frequency, and the optimal controls for mitigating particular kinds of cyber incidents. Various brokers and underwriters told us that this knowledge could help them scope and price policies that contribute more effectively and more affordably to a company's overall corporate risk management strategy. Many of them believed, moreover, that a repository one day could help them provide more cybersecurity insurance at lower rates to clients that invest in so-called "best-in-class" controls. Repository-supported analysis, they explained, would be essential for identifying those controls.
- For their part, the CISOs and CSOs told us that repository-supported analysis could help them conduct much-needed peer-to-peer benchmarking and other activities that could bolster their in-house cybersecurity programs.
- Cybersecurity solutions providers reported that they also have a critical stake in any future repository. They explained that repository-supported analysis would likely influence how the market for new solutions develops. Specifically, they told us that greater knowledge about longer-term cyber incident trends will inform the kinds of products and services that they create to meet the risk mitigation needs of clients across every industry sector.

THE CIDAWG

In late 2014, DHS approached the Critical Manufacturing Sector Coordinating Council (CMSCC) to sponsor and identify willing CISOs to participate in the newly-initiated Cyber Incident Data and Analysis Working Group (CIDAWG). The CMSCC was immediately supportive of the repository concept and named several CISOs to the group. DHS also was very fortunate to be joined by a number of brokers and underwriters from the previous public workshops who had been strong proponents of the idea. At the outset, the CIDAWG included about 10 brokers and underwriters that were among the top thought leaders in the cyber insurance industry. DHS paired them with approximately 25 CISOs, CSOs, and other cybersecurity professionals to enter into a sustained dialogue about 4 main agenda items:

- The value proposition for a cyber incident data repository;
- The data categories necessary to support repository-supported analysis that helps companies manage their cyber risk better;
- How to encourage the voluntary sharing of cyber incident data repository into a repository; and
- How a repository should be structured in any proof of concept stage.[1]

To be clear, DHS is not building a repository. Instead, it is creating a safe space for people to discuss how a repository notionally should come together as a place where companies feel comfortable sharing their cyber incident information anonymously. To do so, DHS established several ground rules that have been critical to the success of the project to date:

[1] The CIDAWG's conclusions about the first 3 of these topics are included in a series of white papers available on DHS's Cybersecurity Insurance webpage, accessible at *https://www.dhs.gov/cybersecurity-insurance.*

- During DHS's previous public workshops, we learned that hosting our discussions on a confidential basis helped promote rigorous debate. We therefore followed suit with the CIDAWG and held all of our meetings under the auspices of the Critical Infrastructure Partnership Advisory Council (CIPAC), a mechanism that allowed us to keep them closed to the public. We likewise strictly enforced the Chatham House Rule to ensure a constant flow of conversation among CIDAWG participants.
- At all times, DHS also tried to be sensitive to the demands that the CIDAWG's work placed on its members. They were located all over the country across every time zone, and we recognized that their time was extremely valuable. To that end, we scheduled CIDAWG teleconferences for up to twice a month, for up to 2 hours at a time. While we scheduled 2 in-person meetings for the group in the Washington, DC, area during the year, we did so only with the participants' consent. We also provided them with several months of lead time so they could provide notice to their employers and budget and plan for the meetings accordingly.

The Value Proposition

The CIDAWG's first topic was the value proposition for a repository. How could it help advance the cause of cyber risk management and what kinds of analysis would be most useful to the cybersecurity industry, to CISOs and CSOs, and why? The brokers and underwriters responded that a repository could help facilitate the development of cybersecurity best practices that insurers should require within their policies as conditions for coverage. The CISOs and CSOs added that a repository could provide the data needed for more insightful peer-to-peer benchmarking that could help justify—or modify—existing cybersecurity investments. As they explained, knowing how a company's peers are faring on the cyber risk management front and how it compares to them goes a long way toward making the business case for needed funding. Both groups noted that repository-supported analysis likewise could help the cyber risk management community identify longer-term cyber risk trends, allowing for new kinds of cyber risk forecasting that could help further inform cybersecurity budgets.

In June of 2015, the CIDAWG completed its first white paper that captured the group's core findings. The paper detailed 6 major value proposition categories for the kind of repository that they were envisioning. Specifically, they believed that it could help by supporting analysis that:

- Identifies top cyber risks and the most effective controls to address them;
- Informs peer-to-peer benchmarking;
- Promotes sector differentiation;
- Supports cyber risk forecasting, trending, and modeling; and
- Advances cyber risk management culture.

The Data Categories

In September 2015, the CIDAWG released its second white paper about the cyber incident data categories that contributors should share into a repository to deliver on that value. Early on, the brokers and underwriters explained that they wanted to know more about the types of cyber incidents that are happening; their severity, impacts, and time lines; the apparent goals of attackers; effective response techniques; involved parties; and risk controls that are making a difference. During the course of our conversations, we asked the CIDAWG participants to flesh all this out by telling us what value each data category potentially brings to a better understanding of cyber incidents; what each one actually means and to whom; which data categories were the greatest priority, to which stakeholders, and why; and which of them are actually accessible,

What was particularly gratifying to see was how the CIDAWG members came to view each data category in relation to at least 1 of the 6 value proposition categories that they had previously identified. During their deliberations, they asked themselves, "How does this particular data category deliver on the value that we're all seeking together?" After 3 months of work, this resulted in a very compelling final list. While the brokers and underwriters were the first to offer up their ideas—they came up with 16 of their own data categories—the discussion did not stop there. The CISO and CSO participants identified their own set of 9 data categories that they believed were essential from a cybersecurity operations perspective. After sometimes intense debate and discussion, the CIDAWG completed a final list—coincidentally, of 16 consolidated data categories—that are a priority for both the insurance industry and cybersecurity professional community alike. They include:

- Type of Incident;
- Severity of Incident;

- Use of a Cyber Risk Management Framework;
- Incident Time Line;
- Apparent Goal(s) of Attackers;
- Contributing Causes;
- Specific Control Failures;
- Assets Compromised or Affected;
- Types of Impacts;
- Incident Detection Techniques;
- Incident Response Playbook;
- Internal Skills Sufficiency;
- Mitigation and Prevention Measures;
- Costs;
- Vendor Incident Report; and
- Related (Contextual) Events.

Overcoming Obstacles

As a next step, the CIDAWG addressed how private companies and other organizations could be encouraged to voluntarily share all this information into a repository. To prepare for this conversation, the CIDAWG hosted several experts who described already existing and on-going information-sharing efforts. Our hope was that the CIDAWG would use these models to propose similar approaches for an anonymized cyber incident data repository:

- Representatives from the Department of Defense (DoD) provided a very helpful overview of some of the information-sharing work that is being done by Defense Industrial Base or "DIB" companies. Specifically, DoD shared its insight into how DIB companies have created a trusted information-sharing environment by adopting a unique way of anonymizing data and using Non-Disclosure Agreements.
- The MITRE Corporation likewise detailed the progress of the Aviation Safety Information Analysis and Sharing System—the so-called "near-miss" database—that MITRE established and runs in partnership with the aviation sector. Specifically, the representative outlined the best practices MITRE had developed to promote the anonymized sharing of near-miss information by pilots, flight attendants, ground crews, and others to enhance flight safety.
- The Alliance for Telecommunications Industry Solutions (ATIS) also shared its experiences in creating a trusted environment for the confidential sharing of highly-sensitive network outage information.

In December 2015, the CIDAWG released its third white paper that identified 8 perceived obstacles to repository sharing and potential ways to overcome them, many of which had been inspired by these outside group briefings. The obstacles included:

- Assuring Anonymization (prevent data from being traced back to a particular contributor);
- Ensuring Data Security (protect the repository itself from breaches);
- Cultural Challenges and Regional Differences (avoid potentially skewed data);
- Perceived Commercial Disadvantage to Participating in a Repository (address concern that participation could negatively impact business operations);
- Internal Process Hurdles to Participation (find ways to work through key reviewers);
- Perceived Value of Participation (evangelize the bottom-line benefits of participation);
- Assuring Appropriate, Adequate, and Equitable Participation (develop a series of benefits available only to repository contributors); and
- Technical Design Issues (make the repository easy to use).

Outcomes

DHS and the CIDAWG are currently planning a public workshop in April 2016 to obtain feedback on the CIDAWG's white papers. Specifically, they are planning to dive into the 16 cyber incident data categories in order to validate them. They also plan to assemble a panel of experts who will offer recommendations about how a repository should function during any future proof of concept stage.

While the CIDAWG will likely make a number of recommendations for next steps based on this input, one of them already is clear: The Federal Government should not actually own or operate the repository. While the CIDAWG members reported that they would welcome data from Federal agencies into a repository, they felt strongly that the private sector should find its own way during a future repository implementation stage. At the same time, however, they expressed great interest in

DHS continuing to convene the CIDAWG and any other working groups to take the work to the next level.

CYBERSECURITY FOR MID-SIZE AND SMALL BUSINESSES

As with the CIDAWG, DHS's convening power could provide tremendous benefit when it comes to helping mid-size and small businesses struggling with their cybersecurity efforts. By some estimates, the cybersecurity insurance market today is growing at 30% a year. Brokers and underwriters alike agree that mid-size and small businesses represent the next cohort of clients that they need to engage in order to sustain that growth. While the market already offers cybersecurity policies geared to these enterprises, they face the same challenge as their larger counterparts: Managing their cyber risk well over time in order to qualify for meaningful coverage. Unlike those counterparts, however, mid-size and small businesses tend to have weaker security that makes them much easier to attack successfully. It likewise makes them a prime launching point for attacks against others. As the "Target" data breach in 2013 starkly demonstrated, a cybersecurity failure by 1 small business—in that case, a heating, ventilation, and air conditioning (HVAC) vendor—can impose hundreds of millions of dollars in lost income and related litigation and settlement costs.

Mid-size and small businesses are falling behind for several reasons. As an initial matter, most lack the budgets, expertise, staff, and time to adequately and consistently address their cyber risks. Many have concluded—wrongly—that their relative anonymity protects them from breaches and cyber-related business interruption events. Given competing business concerns, moreover, still others have simply chosen not to prioritize cyber risk management very highly. Mid-size and small businesses accordingly often fail to comply with common cybersecurity standards that promise real protection through the deployment of appropriate security infrastructure. A growing number, for example, use the cloud as a cost-saving measure for their transactions, unfortunately without strong encryption technology in place. As a result, these businesses represent the weakest links in the global supply chain, making them less attractive business partners.

Large companies have awoken to this problem and are increasingly inquiring of their current and potential supply chain partners about the effectiveness of their cyber risk management programs. In many cases, the less-than-stellar answers they receive present a quandary that raises difficult questions:

- How should large companies define and measure "reasonable cybersecurity" for the mid-size and small companies with which they partner?
- Would imposing their own, potentially more costly cybersecurity requirements effectively put those enterprises out of business?
- Should large companies sever business ties with mid-size and small vendors and suppliers in favor of others that in reality may be no more "cyber secure"?
- How and how often should they verify whether a mid-size or small business is actually complying with cybersecurity requirements over time and "course adjusting" their cyber risk management investments in response as necessary?
- When does the risk of transacting business with a less-than-secure enterprise outweigh a large company's absolute need for a unique service or product that that enterprise provides?
- Does a cyber insecure organization provide products or services at such a competitive rate that a larger company should continue to take a chance through continued partnership?

Part of the answer to these questions is that cybersecurity in today's hyper-connected world is not like the television game shows "Weakest Link" or "Survivor" where mid-size and small businesses should somehow be eliminated or voted off the island automatically because they suffer a breach or other damaging cyber event. The fact of the matter is that all businesses—large, mid-size, and small—are linked through the supply chain. They all are on the same island. Accordingly, they need to work with each other to survive and thrive in today's fast-evolving cyber risk environment. Cybersecurity collaboration among these enterprises has never been more essential.

DHS should consider convening an on-going conversation focused on this topic. The CIDAWG provides an excellent model for how different cybersecurity stakeholders—brokers, underwriters, CISOs, CSOs, and other cybersecurity professionals—can be drawn together to confidentially discuss shared cyber incident data and analysis requirements. A similarly-structured dialogue could focus large, mid-size, and small business attention on the specific approaches and support structures needed to advance the cybersecurity performance of all partners across the supply chain.

Brokers and underwriters would have particularly insightful perspectives to share on this topic given their growing interest in encouraging better cybersecurity among the mid-size and small businesses that will comprise a sizable portion of their future client base. A new working group could assess, for example, how more effective cybersecurity collaboration among all supply chain partners—through initiatives like cybersecurity expert exchanges, best-practice knowledge sharing, compliance automation, and coordination of cybersecurity investments—might help establish mid-size and small businesses as more attractive insurance risks. As brokers and underwriters learn more about which cyber risk controls work for larger companies, they could become a powerful voice regarding which ones should be prioritized and adapted to the needs of the vendor and supplier community. Over time, the group's recommendations could be developed, shared, and updated through a standing private-public partnership effort dedicated to this issue.

Thank you. I am happy to answer any questions you may have.

Mr. RATCLIFFE. Thank you, Mr. Finan. I now recognize myself for 5 minutes of questions.

Mr. McCabe, I want to start with you. You know, in having this hearing and looking at the cyber insurance market more broadly, as I've talked about, I want to get to a point where we see a permeation of the market where cyber insurance becomes commonplace. I'm hopeful that, in the future, we get to the point that Mr. Finan was just making, where any small business who sells their products on-line through a public-basing website would be able to buy appropriate and effective cyber insurance.

From your perspective, where you are at Marsh, can you see that happening, and if so, what factors or changes have to take place for us to get there?

Mr. MCCABE. So as I said in my testimony, the takeup rate increases over the last 3 years have been very healthy double-digit takeup rates. So I think that what we have here is a very strong growing market. I absolutely believe that this is going to become a common coverage for each company to carry.

I think probably one of the limitations right now is that security dollars are always finite. You have companies that are assessing, well, do I spend another dollar on a technical solution, or do I put that dollar towards insurance? Quite frankly, I think we often face a culture where companies would prefer technical solutions. But over time we discovered that there is no silver bullet and that there is always going to be some residual risk, despite how strong your practices are.

So I think that is what is really driving insurance as a product today, and I think it is going to continue to grow.

Mr. RATCLIFFE. Thank you.

Commissioner Hamm, in your testimony, you talked about the lack of actuarial data. What that led to, I believe you said, was that in cyber we see more customized policies, and because they're more customized, they're more costly. Can you speak to how additional cyber incident data could be leveraged by insurance commissioners like you? I mean, does that lead to more diverse cyber products?

Mr. HAMM. So to begin, to me, where that actuarial data is primarily going to be used is by the industry itself to get more of a comfort level in coming up with products, developing those products. Then as they do that, those products would then be submitted to State insurance departments to review the rates and forms. So if those are based on better actuarial data, there is more of a likeli-

hood that once they reach State departments of insurance, that those products will then be approved and then hit the market. So that would probably be my answer to your question there.

I would say, though, I want to make sure and highlight, what you said in your opening statement was spot on. This market is in its infancy, and it is going to take decades before you get predictably to a fully mature and developed market. So what this market really needs is time, patience, and support, and support from folks like you, folks like me as a regulator, to help with that actuarial data piece so that the market can grow organically over time. Thank you.

Mr. RATCLIFFE. Thank you. I appreciate the comments.

To that point, about aggregating data, I want to shift to you, Mr. Nutkis, and ask you, with respect to the ISAO model, when it comes to aggregating cyber incident data, what are the aspects of it from your perspective that can facilitate this process, if it can?

Mr. NUTKIS. Sure. So we see the ISAO model having a lot of potential to support both the aggregation of data, but then also the ability to link the cyber threats that are coming in through the ISAO through threat catalogues to the bolstering of the controls framework itself. So it is another feed, as the actual data is, into strengthening the controls, which therefore the organizations then have a better security posture and, hopefully, less residual risk.

Mr. RATCLIFFE. Okay. Thank you. Have your members found that applying for cyber insurance, has it caused them to bolster their cybersecurity standards? Is that an assumption we can state?

Mr. NUTKIS. So I think what our members have found is that cyber insurance has become very, very expensive, a lot more expensive than it was in the past, and that they are, as I think was mentioned, they are looking at ways to figure out where they should invest the dollars they have. They have a pool of dollars. I think what we have demonstrated is, is that if, in fact, you make good decisions on your cyber controls, you can reduce your cyber premiums, and therefore you have better cyber resilience, and you still get cyber insurance. That's the behavior I think we're trying to drive to, which is getting people to focus on really minimizing residual risk and finding ways to more cost effectively do that.

Mr. RATCLIFFE. Thank you. My time has expired. I'm hoping maybe we will do another round of questions. But I will now recognize the Ranking Member for his questions.

Mr. RICHMOND. Thank you, Mr. Chairman. I will just pick up where you left off. Mr. Finan, I think in your testimony you talked about comparing it to a building fire and fire suppression devices. But I will tell you, as a person who went through Katrina and Rita, the two big hurricanes in Louisiana, after those hurricanes, we as a legislature went in and said, you know what, maybe we need to reexamine our building codes. We need to make sure that we require people to build homes that can withstand winds of X, and da, da, da.

So part of it, I guess, seeps into what we would consider risk culture. So I guess that, you know, as we talk about you all identifying companies as they examine their enterprise-wide risk, the risk of a cyber attack is low on their priority analysis. How do we

or does the insurance change not only behavior but standards across the whole potential clientele for cyber insurance?

Mr. FINAN. Thank you, Congressman. I think it does. One of the discoveries that we made during the CIDAWG conversations, and even in the prior workshops that we held, is that a lot of this is a cultural problem. You have boards of directors and senior leaders that are very comfortable with traditional business risks. They can range from workplace violence to competition. Cyber risk unfortunately, even in some very large companies today, have been relegated to sort of the IT department. Frankly, those aren't people that often talk with one another.

The CISOs and other cybersecurity professionals that we were engaging were having a very hard time breaking through. How did they express what they knew in business terms, chiefly, the financial impact of a cyber event, and the reputational damage to a company that could result if a breach or a vulnerability leading to a breach wasn't properly addressed beforehand?

I think insurance, though, plays an incredibly valuable bridging role in that the boards of directors and chief risk officers and CFOs understand what insurance is about, and they see the business benefit to it. CISOs are increasingly seeing it as an avenue to express what they know. One of the great things about the CIDAWG was that we were able to bring the insurance industry together with a lot of cybersecurity professionals who wouldn't again normally speak to one another, but they started to understand what each other's concerns were, the underwriters and brokers certainly wanting to sell an insurance product but also not wanting to take on too much risk by overextending the policies that they were offering. The technical expertise of a CISO, once you combine those, you're really addressing both sides of the same coin.

So I think one of the outputs of the CIDAWG effort is that you have the insurance industry and the cybersecurity professional community more in sync and speaking together, using the same vocabulary to express that business risk that is cyber risk. So I see insurance as a vehicle to really make cyber risk more of an enterprise risk management problem, and it is something that I think should be strongly encouraged.

Mr. RICHMOND. I guess another part of what I heard today was the cost and whether, you know, we can—I guess in my world, I would say actuarially sound. If the actuarially sound part is something that we focus on, I guess my question would be, for companies that have not invested in their cybersecurity, their information technology, and all those things to make their company stronger to fend off a cyber attack, is the insurance affordable? For companies who do that and invest in it, is the insurance affordable?

So I guess my question is: Is this something that small businesses would be able to afford, and is it something that our large businesses can afford? Probably Mr. McCabe or Mr. Hamm.

Mr. MCCABE. So cyber insurance is made available to every size of business. We segment our brokerage depending on the revenues of the clients, and we have a specific group that are specifically concentrating on small and mid-size business. You know, I would estimate that the takeup for small and mid-size businesses on cyber insurance is somewhere around 20 percent. That lags behind

larger organizations that have more than a billion dollars in revenue, but still, a very healthy takeup and still growing rapidly.

As far as the moral hazard issue, I mean, if a company is not investing in their basic security, I would imagine that they are most likely not going to invest in the cyber insurance aspect of it either. I don't think that in the cyber insurance industry, I don't think that the moral hazard problem is really applicable. I mean, and that would be in comparison to, well, I have fire insurance so I am going to leave greasy rags around the house and I am going to leave highly flammable foods next to them because, you know, I have my house secured with insurance now.

I mean, nobody knows how big the breach is going to be, and nobody knows what the outcome of a cyber breach might be. Executives could lose their job. You could lose the entire shop. You know, potentially an entire company could go down from a cyber breach. That is why it really does need, as has been spoken on this panel previously, enterprise risk management, because this is one of those risks that can take an evenly sailing ship and knock it right off course. I think that cyber insurance is a piece of the puzzle that supports the other aspects of risk management.

Mr. RICHMOND. Thank you. I yield back.

Mr. RATCLIFFE. I thank the gentleman.

The Chairman now recognizes the gentleman from Pennsylvania, General Perry.

Mr. PERRY. Thank you, Mr. Chairman.

Mr. McCabe, I am sorry I had missed the opening part of your testimony, so I don't want to rehash stuff that has already been gone over, but your last comments kind of piqued my curiosity. I am a guy that started a business in my mom's garage. Right. That was a long time ago, and we weren't so concerned about this at the time. But did you say that there are policies for every level of business, and at the smaller level they are based almost solely on the business's income? I just want to kind of make sure I understand what you said there.

Mr. MCCABE. So premiums are always going to be tied to the sector of the business——

Mr. PERRY. Right.

Mr. MCCABE [continuing]. The revenues of the business, and the security practices. Those are probably the largest 3 determinatives of what a premium is going to be. Yes, I mean for me, you know, probably if I am involved with putting a program in place, the limit of a policy is typically going to be for $10 million for the first primary sold. Right? That is not going to be true for every company. Smaller companies can get million-dollar, much smaller policies.

Mr. PERRY. Can you give me an idea? You want a million-dollar policy, as a guy that ran a business, in the scope of everything else, plant and equipment and employees, and all the other products that you got. What are we talking about? Is it a 6-month premium? Is it an annual deal?

Mr. MCCABE. It is an annual deal.

Mr. PERRY. Give me some idea.

Mr. MCCABE. To tell you the truth, I am going to be more solid on premiums for much larger businesses because that is the class that I handle. But you do have to remember, even from your ques-

tion, it is a wide-open question because for the business that you are running, well, how big is your digital footprint? How on-line are you? How much do you rely on on-line presence to conduct your business? What is the manner of your business? Are you collecting health data? Are you collecting——

Mr. PERRY. I understand the risk exposure, and I am kind of asking you how long is the string. But if you could, at some point after the fact——

Mr. MCCABE. Absolutely.

Mr. PERRY [continuing]. Give us some kind of idea, based on some of that criteria, what businesses are looking at just, you know, so we can kind of be in the game on that.

I want to move on a little bit. Mr. Hamm, how do we ensure these policies keep up with something as evolving as this? I mean, you know, I think about upgrades. I used to do P and C limits, right. So when you upgrade, when you put airbags in, or you do all these safety systems of an industry moving towards a certain direction, or sprinklers or whatever, this industry involves bad actors that are moving in a nonlinear fashion. They don't announce their intention, and so you don't know what your risk is day-to-day. How do we keep up?

Do you have any—that almost sounds like an unanswerable question, too, but you're in the position to have to answer.

Mr. HAMM. I'll do the best I can to answer it. To begin with, because this line of insurance is still in its infancy, we are basically at a point where if you have seen one cybersecurity policy, you have seen one cybersecurity policy. Right? So my colleagues and I, and there are 11,500 of us in State insurance departments across the country, we are busy reviewing the rates and forms that are coming in from companies looking to sell these sorts of products, and you have about 4 or 5 dozen of those companies out there selling these.

So we are making sure that from a standpoint of a regulator, that the products that are actually hitting the market are complying with State laws in the 50 States. In addition to that, we are reviewing those companies to make sure that they are financially sound so that they will be there to pay claims when they come due. Because the only way this market is going to go from infancy to fully developed is if there is a comfort level by individuals and businesses and Governmental entities that what is actually growing and developing in this country, in terms of a cyber insurance market, is actually going to be there for the long haul.

Mr. PERRY. So that speaks to the lawfulness or, you know, complying and comporting with what you said the rules and requirements——

Mr. HAMM. Right.

Mr. PERRY [continuing]. And I guess to soundness of the institution. But it doesn't necessarily get to the issue of an ever-changing landscape from an actuarial standpoint, from a risk assessment standpoint.

Mr. HAMM. Which is a big part of why this market is developing. Even though it is developing quickly, in some ways it is developing slowly, because they need more and more data in order to answer the question you are asking.

Mr. PERRY. So Mr. Nutkis talked about this a little bit, and maybe the question should be for him, but I want to stay on you a little bit. So who should determine the standards? I am not a big Federal Government guy. I know I am sitting in the place, but who is determining the standard? If it is the insurance industry, is the fox guarding the henhouse? Am I going to be required to report? Is the insurance company going to—you know, the insurance company that has my policy is going to want to know my risk exposure. How do we determine, and should we be determining, the greater risk exposure? I mean, one thing begets another.

I know there is a whole lot of questions there, but——

Mr. HAMM. Right.

Mr. PERRY. Where is the repository of all this information, and how do you safeguard it? I mean, it is different than accident crash data or something like that. Right? So how do we do this for this?

Mr. HAMM. So I am going to do the best I can to answer that question. From my perch as a regulator, I don't really much care where the repository of that data is. Okay? I don't care if it is some arm of the Federal Government, if it is some private entity. That doesn't matter to me. What matters is that that data that is actually being gathered is useful, okay, and it is being shared with me as a regulator so I can do my job.

Mr. PERRY. But as a regulator, and it is a guy that this is your business, this is your livelihood, your passion, your expertise, what is your recommendation? Do you want another Federal program?

Mr. HAMM. No.

Mr. PERRY. Okay. All right. That's all I needed to do hear. Thank you.

Mr. Chairman, I yield back.

Mr. HAMM. Thank you for the lifeline.

Mr. RATCLIFFE. I thank the gentleman.

The Chair now recognizes the gentleman from Rhode Island, the Chairman of the House Cyber Caucus, Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman. I want to thank you for holding this hearing. I want to thank our witnesses for being here today and deeply appreciate your work with DHS and on this issue, in general.

So we have come a long way since I first started on the cybersecurity issue back in 2007. We have certainly raised awareness. We have come a long way in getting everybody, for example, in the National security apparatus from the President on down, to understand how challenging and difficult cybersecurity is, how important it is to the country, how vulnerable we are in many ways, and very dependent on cyber-related issues.

Now, of course, what do we do about it? There is a variety of tasks that we need to take, that we are taking. Some of it will come through legislation. Others are going to come through regulation. Others are going to come from this public-private partnership certainly, which is going to be vital because Government nor private sector can do this independently on its own.

Also a role for the FCC. I have met with FCC commissioners and have written several times to the chair of the FCC, and they are moving in the direction doing more in this space as well. The insurance industry also, I believe, has a critical role to play here. I have

met with some of the largest insurers in the country, both to encourage them to move more into this space, but also to hear from them and clearly see what they are doing in this space. They are now writing policies that are more reflective of the risks that companies face in this area.

Clearly, if you have 2 companies, and 1 is investing heavily in cybersecurity protections and doing everything they can to protect customer data and prevent the consequences of a cyber attack, the policy should be written to reflect that. Those that are doing very minimal amount, then the policy should be written and priced accordingly as well. So I think this is an important discussion.

So, Mr. Finan, I found your testimony very insightful. I deeply appreciate your work with DHS and thank you for your commitment to public service. I am wondering if you can clarify a few things for me. I am certainly very fond of the NIST cybersecurity framework, and I fully understand the importance of having a risk-based approach to handling cybersecurity risks.

That said, as you indicated in your testimony, current insurance offerings are not typically tailored to liabilities we tend to focus on in this committee, such as third-party harm due to an attack on an industrial control system. So, again, I fully recognize the value of raising the cybersecurity floor, but I just wanted to make sure I understood your testimony. Did I get that about right?

Mr. FINAN. Yes, I think so. Specifically, to the NIST cybersecurity framework, Congressman, the underwriting community especially has been very supportive of it because it gave a vocabulary and an approach for brokers and underwriters to discuss cyber risk in a way that everyone was comfortable. You didn't have to be a technical expert. I think the jury is still out on what the ultimate impact might be of the framework because they want to see how usage translates to fewer losses or less severe losses. So I think that there is a tremendous potential, but they are taking a wait-and-see approach. I think NIST is working and engaging with the insurance industry to see where it may head next.

Mr. LANGEVIN. Okay. Thank you for that. In that case, is it possible that the floor we are raising is focused on business risk, for example, to a financial system, rather than on a risk relating to operational technology, since they are unlikely to be insured against?

Mr. FINAN. Yes. I think insurance can have that floor-raising impact. The C-suite understands the benefit of cybersecurity insurance and insurance base, generally. They see it through business terms, and they see it as an opportunity to really make that hard decision between, what Mr. McCabe was talking about, do you spend the last dollar on a technical solution, or do you transfer the risk through insurance? I think it is engendering some very healthy conversation between and among chief risk officers and other senior officials within companies with their cybersecurity teams. It is bridging that cultural divide that still remains, for most companies, but it is a vehicle to finally have that conversation, and I think that is healthy.

I think they are figuring it out, about what controls actually deliver value. That is going to be a long-term and on-going discussion. But insurance is a good umbrella under which to have it.

Mr. LANGEVIN. One other follow-up on this line of questioning. Is there a widely-accepted definition of cybersecurity incident that you found, at least among critical manufacturers?

Mr. FINAN. Not that we came across, and I think it is because of the newness. People in the industrial control system space are very concerned about business interruption, obviously the physical damage that could result to critical infrastructure, if a hacker were to get in and have that intent. But because it is new to the insurance industry, as a concept and a potential area of coverage, they haven't really defined it too specifically yet. But I think that is why the kind of collaboration that a group like the CIDAWG was encouraging is something that DHS should continue, because you start to move toward those common definitions and vocabulary.

Mr. LANGEVIN. I think that would be helpful, and I am hoping that we are going to see us move in that kind of a direction and have that common understanding. I know my time has expired.

Mr. Chairman, I don't know if you are going to do a second round, but if you are, I am going to stay. All right. I yield back.

Mr. RATCLIFFE. I thank the gentleman.

The Chair now recognizes my friend, the gentleman from Florida, Mr. Clawson. By the way, is it too late to offer condolences on your Boilermakers?

Mr. CLAWSON. You know, it is a yearly thing, so don't worry about it. When I see you dunk a breakaway, then you and I can talk. To be a tough guy, you have to have hit somebody at some point, right? Thanks for coming. If I knew it would have been a conversation about basketball, I would have checked your own credentials.

I am okay with voluntary cyber risk information being shared by companies. I am all right with that. My own observation was that most CEOs and boards are all over this. They are all over this. They know that disaster is right around the corner, and it is not just financial interruption of business. It is embarrassment, and customers have a hard time getting over it. Moreover, a lot of us are business-to-business suppliers, and we don't have a lot of choice in the matter, to begin with. So we are part of a larger supply chain that makes this more complicated, and, moreover, it is an international supply chain.

The final point I guess I would make is that every ERP implementation that I have done is unique. I wonder about an insurance market, I hear actuarial data, and I say, wait a minute, every time I did an SAP it was a little different. Sometimes we touched a base code; sometimes we didn't. Sometimes we integrated with the financials and with the customers; sometimes we didn't.

So to set up data that is somewhat standardized so that an insurance industry can make decisions when there is no standardized data, I will just tell you, from my desk, I don't know. I don't know. I don't know if that is even practical, because these things are very, very customized and very, very unique. That is what they are, because every business is different. You know, I operated in 20 countries or so, you know, and all of them had governing bodies. Therefore, all of my instincts tell me, let the market catch up to itself.

I know if I was going to buy insurance, the only person I would buy it from is the consultant doing my SAP or whatever it was, the

ERP implementation. To have a third party that is not involved in my system, that is therefore going to decide whether he is going to pay me and everybody, not knowing who messed up on keeping, you know, everything secure, seems like a very difficult thing to do. So I know what I would do if I was going to buy insurance from one of these things, and I am spending 3 to 5 percent of my top line on IT every year, I would buy it from the guy that helps me put in the system.

Given all that—2 minutes of talking about that—it just seems to me that we have to let the market catch up here. The less the Government is involved, the better. You just slow it down. The data that we collect, in order to have a standardized kind of approach to this, is not going to be worth a lot because every implementation of an IT system is unique. So I am worried about the whole thing that we will try to help, but we will actually make things different. Do you all agree with that? I mean, we will try to help, but we will make things more difficult. Do you all agree with that, or am I missing on that?

Mr. HAMM. Yes.

Mr. CLAWSON. Anybody disagree with what I just said?

Mr. MCCABE. So, of course, not disagree.

Mr. CLAWSON. If you do, that is okay.

Mr. MCCABE. I would want to try and put some bones around what we are doing going forward. So I know for the data repository, I mean, there is no "there" there yet. It is just a conversation. I think it is a question of how they reach the ultimate solution. So to add another layer of complexity for everything you are talking about, I mean, this peril has been compared several times to fire; but, of course, we are not facing a fire here. We are facing an adversarial relationship that changes tactics and technique. So that can call into question just how valuable is actuarial data, if the threat is going to change every time you change your security.

But, you know, one of the things that I did not mention, but I do want to mention, is this committee, the subcommittee and the committee and Chairman and this entire Congress, has done a lot of great work on cyber information-sharing legislation getting passed this year. We are going to see a lot more information sharing among many different ISAOs. Right?

So if we are starting to get into this culture where we are doing much more information sharing, then maybe there is a way we can glean from that financial impact data that can lead to trends. That does not have to be a Federal Government solution. Maybe that can represent value to several different industries, including the insurance industry.

Mr. CLAWSON. I am okay with that, if it is voluntary. But I do want to say to the Chairman, thank you for this. I just want to make sure people up here that sometimes don't understand the complexity of what you all are talking about, it is easy to come to a conclusion that we can make some sort of standardized impact on a moving target that is beyond complex and that we in Government don't understand. I just want to make sure you all get that point. I mean, that is my point to the group. Be careful on what we try to do here, or we will make a very difficult situation even worse because the threats are, you know, so difficult.

Thank you. I yield back.

Mr. RATCLIFFE. I thank the gentleman. I'm going to open a second round of questions for anyone that is interested. I had a couple of follow-ups that I wanted to make sure we got to today.

I want to come back to you, Mr. McCabe. Technical questions. But do insurers generally mandate certain prerequisites or cybersecurity efforts at all before anyone could be issued coverage in this space?

Mr. MCCABE. I mean, certainly it depends how we define efforts. But I think the question is—absolutely. You know, if you find out that you have an applicant who simply isn't using firewalls because they don't believe in them, then the insurance market is just simply going to walk away from them. From a far more practical example, take for instance retailers. So if you have a retailer who simply is choosing not to be compliant with PCI standards, it is going to be very, very difficult to get that particular applicant coverage.

Take that a step further. If you have a retailer who is not keeping up with the technical standards, the practices that would have prevented breaches like Target and Home Depot back in 2014, and that is using end-to-end encryption, that is tokenizing your data so it is just transaction numbers; it is not the actual card numbers—if you don't have those state-of-the-art practices, then it is going to be very, very difficult, if not impossible, to get that retailer coverage.

So I think, while for most industries there is not a hard-and-fast rule, because there isn't regulation, because it is very hard to regulate in this space because things change so quickly, but there certainly are practices that are required. Now, there are, of course, certain industries where there is heavy regulation. There is HIPAA compliance. There is FERC, NERC standards, CIP standards. I mean, those, of course, you have to comply with.

Mr. RATCLIFFE. So as a follow-up to that, and maybe, Mr. Hamm, you can weigh in on this as well. Are there certain common conditions in cyber insurance policies, or in limitations or exclusions to those policies, that essentially would undermine the effectiveness of that coverage?

Mr. HAMM. Nothing that I have seen yet. Again, the market is in such an infancy stage that my colleagues and I haven't got to a point where we are reviewing so many different rates and forms that I can give you, you know, an informed answer to that question.

Mr. RATCLIFFE. So when we talk about assessing the solvency of insurance policies that cover cyber, is there a point, or at what point do we need to be concerned about U.S. companies becoming insolvent because of their inability to cover one-off cyber events of a great magnitude?

Mr. HAMM. So thankfully, we are not there yet, obviously. That is one of the reasons why the NAIC is so interested in gathering very granular level data on what this market is looking like, not just to give us a snapshot of claims, premiums, losses, et cetera, but to start to tell us if there are any of these companies that are selling these sorts of products that may not fully understand the

risks they are taking on and may not be able to pay claims when they come due.

So that is a big part of why we are gathering that data. We are going to get the first batch of that here within the next few weeks. We would be happy to provide that to this committee, once we have it in a form that we can release publicly.

Mr. RATCLIFFE. So, Mr. Finan, I want to ask you a question, because of your experience in setting up the CIDAWG. We have had this conversation about standing up a data repository of some type. In your mind, who would be the ideal entity to house that?

Mr. FINAN. I am going to do it in my basement. No. It is a great question, Congressman. Truly, I think the CIDAWG members themselves are probably the best equipped to answer that. The CIPAC meetings that we were holding, the Critical Infrastructure Protection Advisory Council, we really had not pushed toward who should own and operate. They were very clear, however, that the ghost of Edward Snowden still lives, and they were not overly keen on the Federal Government owning and operating.

However, they did feel that the Federal Government had an enormous role to play in terms of convening the conversation so they themselves could figure it out. They are also very interested in the Federal Government providing data about cyber incidents so they could start to get their underwriting bearings. However, there are a couple of models that are out there. I know the working group has talked about ISAOs as a potential model, ISACs as well. I know a number have been interested in potentially looking at FFRDCs and universities and similar communities.

But the truth of the matter is, is that this is a needs and requirements discussion about what is the value of a repository? What data do you need? Ultimately, what is it going to get you in terms of better understanding about how to invest more wisely against the risk? Really, anyone could take these public documents and decide to build a repository. We really wanted to lay out the roadmap for them to do that, and I think the group next month will have some recommendations that are more specific. But it is really for anyone to read and review and, hopefully, engage.

Mr. RATCLIFFE. All right. Thank you very much. My time has expired again.

The Chair now recognizes the gentleman from Rhode Island, Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman. Mr. Finan, if I could return to you. I was intrigued by your description of the aviation industry's near-miss database and its possible application to a cybersecurity context. So I imagine that a better understanding of the interconnectedness of critical infrastructure would be essential to be able to grasp the consequences if an incident had been a miss in the cyber world—I should say had not been a miss in the cyber world.

Does that comport with your thinking, and can you suggest what additional research would need to be done to adopt this model?

Mr. FINAN. So the near-miss repository was something that really captured the imagination of the working group because at the outset, the commercial aviation sector didn't believe that they could actually share very sensitive information among themselves to find

common, you know, safety solutions. But lo and behold, they did. They were able to create that environment largely through the development of nondisclosure agreements. They encrypt data. They had an anonymization protocol. So we brought them in to come and talk to us about how they did it. Really, we needed to dispel the notion that a repository would somehow be impossible to develop.

There were other examples as well. DOD came in and talked about some of their experiences with creating an anonymization protocol. There were other groups that, you know, sort-of talked about how they worked it. None was perfect, but it did convince folks that, hey, this is potentially doable.

I think the main goal is that when you have a group of individuals that are facing a shared business problem, and cyber risk is certainly that, that the people who say no, and the fear, ultimately has to relent to some kind of sharing. So the recommendation was, gee, if we could do something like the near-miss database for the aviation sector, that would get us closer.

So we had a very in-depth conversation with the organizers from MITRE who put that together. They, I think, will be participants in the workshop that DHS is hosting next month, really to generate ideas. Because some of this information, some of it is sensitive certainly, but if you can share it at a generic enough level, the insurance industry and the CISOs that joined us really felt strongly that that would be enough for them to get a fix on what needs to be done, and how to direct their budgets against cyber risk, accordingly. So I am happy to report that there are these models that can be adopted.

Mr. LANGEVIN. Very good. That is very helpful. Thank you.

Mr. McCabe, and I certainly welcome any of the other panelists to chime in. Can you describe the claims investigation, if any, that you conduct following a cybersecurity incident?

Mr. MCCABE. So the broker is usually not responsible for claims investigation. That will be by the carrier into their claims or by the company itself by retaining their own counsel. I mean, typically what happens is there is a cyber breach, and the first move by the insured would be to reach out to their attorneys, who will coordinate with the forensics company to find out exactly what happened and what is the impact. Then based on that impact, you might have different responsibilities.

If it has been a breach of personally identifiable information, then State law requires certain efforts, such as notifying, credit monitoring, and fraud restoration. Perhaps, you know, there is an extortion demand in which there is an entire different set of services that have to go in. Perhaps there is a business outage in which it is more a forensics investigation of, well, what has this company actually lost and what are the expenses that you have suffered as a result of that business outage?

I think that that is typically how the incident response comes. But from an investigation into what actually happens during the claim, that is usually headed up by the carrier.

Mr. LANGEVIN. So in the part of the investigation, as the carrier is doing this, do they go back and look at, did the insured do what they said they had done in terms of complying, say, with NIST standards and such that, you know, obviously that the policy was

written in such a way that the company, the firm, made certain representations that they raised their level of cybersecurity protection to X level. Is there a part of that investigation that does forensics to see if they actually did what they said they were doing?

Mr. MCCABE. Sure. Of course. Ranking Member Richmond brought this up in his opening statement as well, that during the application process, you can make representations upon which the underwriter will rely, and that actually becomes part of your application. Now, if it turns out what you represented is not true, that could be grounds for denying the claim. That is really one of the things that incentivizes the better practices. You have to let the rubber meet the road on how you are practicing security. You can't just get the insurance based on a bad-faith application.

Mr. LANGEVIN. Very good. Okay. Thank you all very much. Unless there is anything else from the panel on that particular topic?

Okay. I yield back.

Thank you, Mr. Chairman.

Mr. RATCLIFFE. I thank the gentleman. We will let that be the last word. I thank all the witnesses for your testimony today and the Members for all of their questions. The Members of the committee may have some additional questions for any of you witnesses and, if so, we will ask you to respond to those in writing. Pursuant to Committee Rule VII(e), the hearing record will be held open for a period of 10 days.

Without objection, the subcommittee stands adjourned.

[Whereupon, at 11:30 a.m., the subcommittee was adjourned.]