



MARCH 22, 2016

ROLE OF CYBER INSURANCE IN RISK MANAGEMENT

UNITED STATES HOUSE OF REPRESENTATIVES, COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION AND SECURITY
TECHNOLOGIES

ONE HUNDRED FOURTEENTH CONGRESS, SECOND SESSION

HEARING CONTENTS:

John Ratcliffe

Subcommittee Chairman, Subcommittee on Cybersecurity, Infrastructure Protection
and Security Technologies

[\[View pdf\]](#)

Matthew McCabe

Senior Vice President, Network Security and Data Privacy, Marsh FINPRO

[\[View pdf\]](#)

Adam W. Hamm

Commissioner, North Dakota Insurance Commissioner

[\[View pdf\]](#)

Daniel Nutkis

Chief Executive Officer, Health Information Trust Alliance

[\[View pdf\]](#)

Tom Finan

Chief Strategy Officer, Ark Network Security Solutions

[\[View pdf\]](#)

AVAILABLE WEBCAST(S)*:

[\[Watch Full Hearing\]](#)

COMPILED FROM:

- <https://homeland.house.gov/hearing/the-role-of-cyber-insurance-in-risk-management/>

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

*This hearing compilation was prepared by the Homeland Security Digital Library,
Naval Postgraduate School, Center for Homeland Defense and Security.*



**Statement of Subcommittee Chairman John Ratcliffe (R-TX)
Cybersecurity, Infrastructure Protection, and Security Technologies Subcommittee
House Homeland Security Committee**

*The Role of Cyber Insurance in Risk Management
March 22, 2016*

Remarks as Prepared

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 infrastructure 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 cyberspace.

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.

###

Testimony of
Matthew P. McCabe
Senior Vice President
Marsh, LLC

Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection and
Security Technologies
“The Role of Cyber Insurance in Risk Management”

March 22, 2016
Washington, DC

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 four 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 on 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.

¹See (accessible at http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf).

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 Enterprise. (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 systems that support critical infrastructure, the authors considered the challenge of how the private sector can develop greater resiliency.

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 standalone 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 healthcare 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 three 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.

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 on 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.

²See 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).

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.

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. 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.

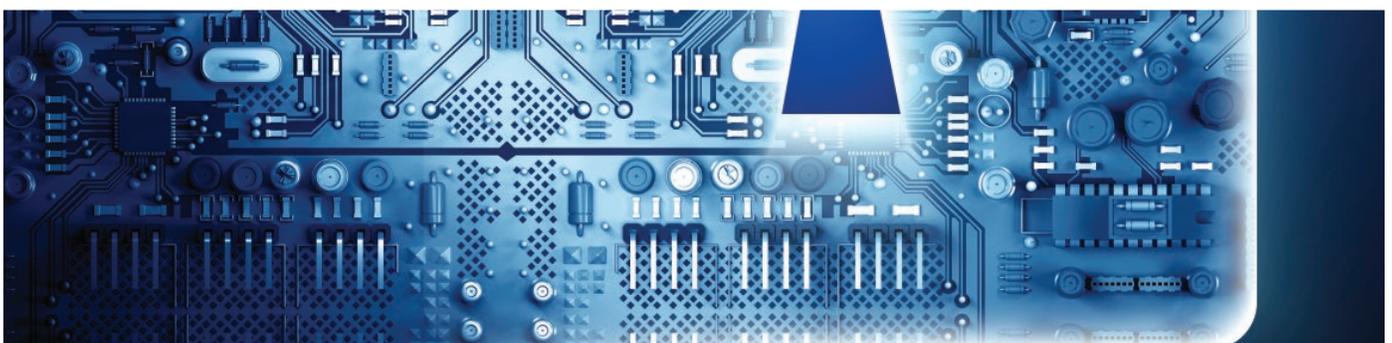
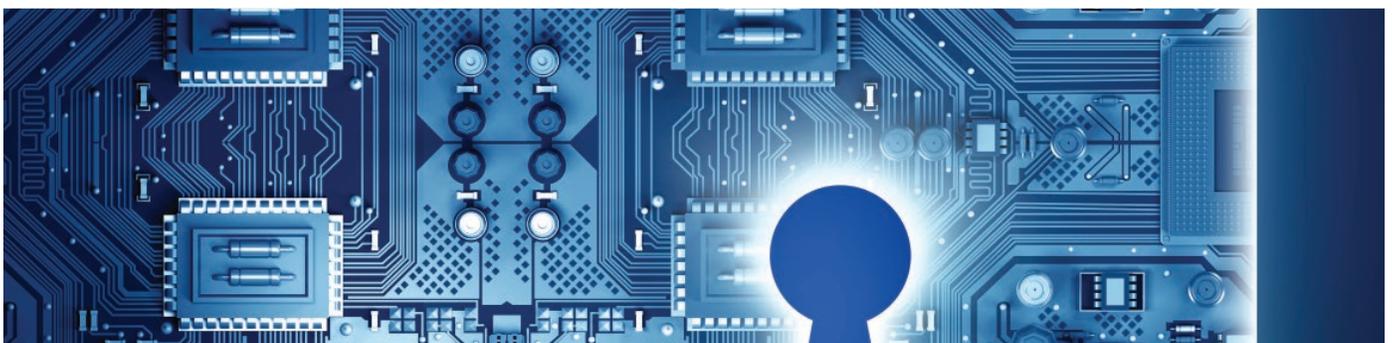
Thank you for allowing me to present this testimony. I am happy to take your questions.

Appendix to Marsh & McLennan Companies Testimony

A. Report: “Cyber Resiliency in the Fourth Industrial Revolution”

Cyber resiliency in the Fourth Industrial Revolution

A roadmap for global leaders facing emerging cyber threats



4th
4

Industrial Revolution—
complexity increases over time



1784

Steam engine



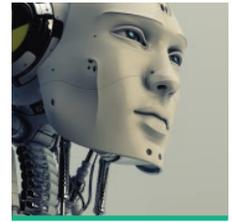
1870

Mass production



1969

Information technology



2020

Cyber-physical systems

**Fourth Industrial Revolution
cyber-physical systems**

- 100 billion connected devices
- Digital industrial control systems
- Machine-to-machine
- Mass customization
- Global sensor-net overlay
- Autonomous vehicles/homes
- Digital service avatars (iConcierge)

Breaches are inevitable; resilience is necessary

The First Industrial Revolution, in the late 18th century, was driven largely by steam engines. The second, in the late 19th century, introduced mass production and the division of labor. The third, in the late 20th century, involved digital automation and information technology.

Only decades later, the world is now on the cusp of a Fourth Industrial Revolution. This new world revolves around cyber-physical systems, the Internet of Things, and the Internet of Services. Our hyper-connectivity in this new digital world has been a boon for productivity—connecting and executing tasks with a speed that was inconceivable even five years ago.

With that hyper-connectivity, however, comes the risk of significant disruption through a cyberattack—the potential consequences of which have escalated dramatically. Until recently, cybersecurity largely meant defending against website defacements, denial of service attacks, and data breaches. The threat posed by them, however, is now morphing into the realm of physical assets and critical infrastructure.

While this risk intensifies, businesses, governments, customers, and individuals around the world demand even more from the new economy. Engaged in a repeating loop, the world is more dependent on technology, even as the risk posed by that dependence increases exponentially.

It's like running in a race without a finish line. As organizations bolster their defenses, adversaries adjust their strategies and methods of attack. New “zero day” attacks are conceived and launched. Organizations scramble to respond. This dynamic will continue—from our vantage point—for decades to come.

Our three companies—each a leader in its space—have come together to offer a roadmap for global leaders to respond to this threat. As it's become all too clear, there is no panacea or silver bullet. So, accepting the premise that breaches are inevitable, we set forth an approach for building cyber resilience. The critical objective is to enable organizations to withstand significant cyberattacks and continue core operations.

Mike Nefkens
Executive Vice President &
General Manager
Hewlett Packard Enterprise

Kevin Mandia
President
FireEye

Peter J. Beshar
Executive Vice President &
General Counsel
Marsh & McLennan Companies

The path to cyber resilience

Cyber breaches happen. That is the new reality. However, with cyber resilience, organizations can respond with agility to cyberattacks. So, despite an attack, the organization carries on—patients are treated, power is generated, commerce flows.

This new approach emphasizes five fundamental steps:

1. Identify your most critical assets—What do you have that is most valuable to others?
2. Gather intelligence on cyber threats—Who are the bad actors?
3. Understand your digital profile—What does your online activity signal to others?
4. Build a resilient system—What are the most critical elements of defense?
5. Plan for a breach—What can you do now to prepare for a crisis?

Building a moat around your organization has proven ineffective. In a dynamic threat environment, it is simply not possible to construct an impenetrable firewall. Instead, these five steps are designed to enhance your organization's ability to anticipate attacks, respond with agility, and maintain core operations.

Perfection is not the goal of this methodology, and not every organization will have equal need or resources to implement each step. Rather, this approach is intended to guide you on how to identify cyber priorities and develop a risk-based response.

1. Identify your most critical assets

All data is not created equal. Yet, the traditional approach to cyber defense is to construct a perimeter and treat all assets in a similar fashion. This method can lead to inefficiencies and misalignment of resources.

A better approach begins with a simple question: Why should my organization be concerned about cybersecurity? Answering this question with precision requires identifying which data, applications, and systems are essential for your organization to conduct operations, and then developing a cyber strategy that is driven by protecting core business functions—and not merely responding to threats.

So, what do you have to lose? What are your most critical assets? Intellectual property? Turbines? Customer data? Medical histories? Trade secrets? Proprietary financial data? Industrial control systems?

2. Gather intelligence on cyber threats

Evolution in the nature and sophistication of cyber threats has been stunning. And, it is only beginning.

In just the past few years, hackers have grown far more sophisticated, their attacks more complex, targets more encompassing, and the impact of those attacks more damaging. There is now a highly advanced underground online economy where hacker tools and illicitly obtained data are readily available. Companies must now confront the specter of data manipulation, extortion, and potential acts of terrorism. Understanding the ever-changing threat landscape plays an essential role in cyber resiliency.

A potential inventory of assets

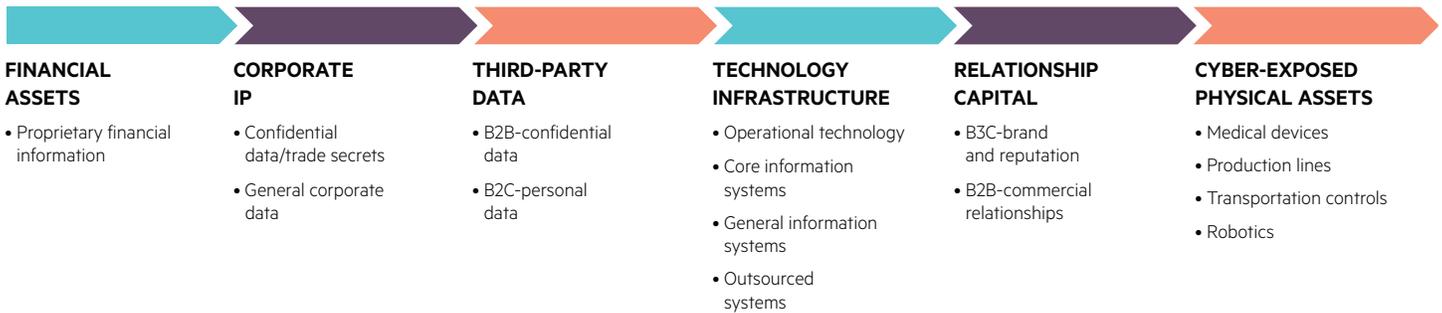


Figure 1: Sample inventory of assets¹

The cyber-threat landscape

Two other factors accentuate the threat posed by cyberattacks. First, on average, it takes an organization more than 200 days to realize that its systems have been breached.² Indeed, in multiple instances, breaches have been undetected for years. Second, in more than 65 percent of cyberattacks, it is a third party, and not the organization itself, which discovers that a breach occurred. For an organization to adopt cyber resilience, mature cyber threat intelligence is essential to identify threats and reduce the period of exposure.

Attacks on physical assets and critical infrastructure

Over the past several years, most publicly reported breaches have concerned data theft—such as credit cards, Social Security numbers, and patient records. Attacks are now morphing into the realm of physical assets that threaten the critical infrastructure—including electric grids, transportation systems, satellites, civilian nuclear facilities, and telecommunications networks. By exploiting industrial control systems and critical infrastructure, cyberattacks now pose a threat to public safety and economic security.

FireEye identified a series of advanced threat actors who possess a high-cyber capability to conduct network attacks and use a range of tactics and target critical industries worldwide. Recent threats to operational technology included:

- A new type of malware, discovered by FireEye in 2015, which creates a “loop” that sends instructions to hardware to alter its operations while appearing, on the surface, to be working properly.
- A malware discovered by Norwegian law enforcement in 2014 that compromised 50 Norwegian energy companies.
- The leaking of partial blueprints of a South Korean nuclear reactor by hackers linked to state actors.

¹ Source: Marsh

² M-Trends 2015: A View from the Front Lines, Feb. 2015, Madiant

	NUISANCE	DATA THEFT	CYBER CRIME	HACKTIVISM	NETWORK ATTACK	MALICIOUS INSIDER
Objective	Access and propagation	Economic, political advantage	Financial gain	Defamation, press and policy	Escalation, destruction	Financial gain, defamation, whistleblowing
Example	Botnets and spam	Advanced persistent threat	Credit card theft	Website defacements	Destroy critical infrastructure	Theft of IP
Targeted	No	Yes	Yes	Yes	Yes	Yes
Character	Automated	Persistent	Opportunistic	Conspicuous	Conflict driven	Informed and trusted

Figure 2: Actors on the cyber-threat landscape³

Within the energy sector in particular, potential targets include offshore drilling rigs, power generation plants, and pipelines exposed by direct connectivity to the Internet and enterprise IT networks.⁴

Compromise assessments and penetration testing—the “inside-out” approach

With increasing frequency, organizations rely on two tools to identify critical vulnerabilities: compromise assessments and penetration “pen” tests. Compromise assessments evaluate network end points for indicators of compromise or other anomalous activity. Experts use this tool, and pen tests, which analyze your internal security protocols, to assess your vulnerability.

Based on hundreds of tests carried out by FireEye, it is clear that the vast majority of systems are susceptible to attacks—despite traditional security controls in place. Consistently, indicators of compromise are discovered by forensic imaging, malware analysis, and review of incident log activity. Implementing a continuous state of testing, however, builds cyber resilience by finding and fixing critical weakness more quickly.

3. Understand your digital profile

Big Data approach to analyzing cyber risk—the “outside-in” perspective

Hackers look for opportunity and probe for weakness—a combination of the value of your assets and vulnerability of your systems. Big Data can now be harnessed to assess the likely motivation for and potential susceptibility to cyber events by relying exclusively on data points beyond an organization’s perimeter. This is the outside-in approach.

In the digital era, each organization creates a footprint through its online activity. Your business, just like an individual, leaves a trail of digital breadcrumbs behind.

For example, do your servers share web hosting platforms with others, or worse, with highly targeted companies? Can hackers spot instances of unpatched software by monitoring browsers used by employees to access the Internet? Is your organization subject to activity on the so-called “dark web?” What do your job postings for IT positions reveal about your operations? Will poor employee morale, as reflected in external surveys, correlate to insider attacks? What is your web presence and how strong is it?

Aggregating these and hundreds of other data points over time yields susceptibility and motivation scores that can be used to benchmark your organization against past performance and the performance of your peers. The susceptibility of an organization is defined by its technology, people, and processes; motivation describes why an outside actor would attack your organization. If a hacker probes two companies with similar networks and one has user credentials available on the dark web, which is the hacker more likely to attack?

³ Source: FireEye-Mandiant

⁴ In fiscal year 2014, the energy sector led all industries for the number of cyberattacks reported to the Industrial Control Systems Cyber Emergency Response Team at the U.S. Department of Homeland Security, with 79 reported attacks accounting for 32 percent of reported attacks. ICS-CERT Monitor, Sept. 2014 to Feb. 2015, https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf

As an example, Figure 3 is a scatter graph of 212 companies in the power industry ranked by susceptibility and motivation. This same analysis can be conducted on any sector or industry.

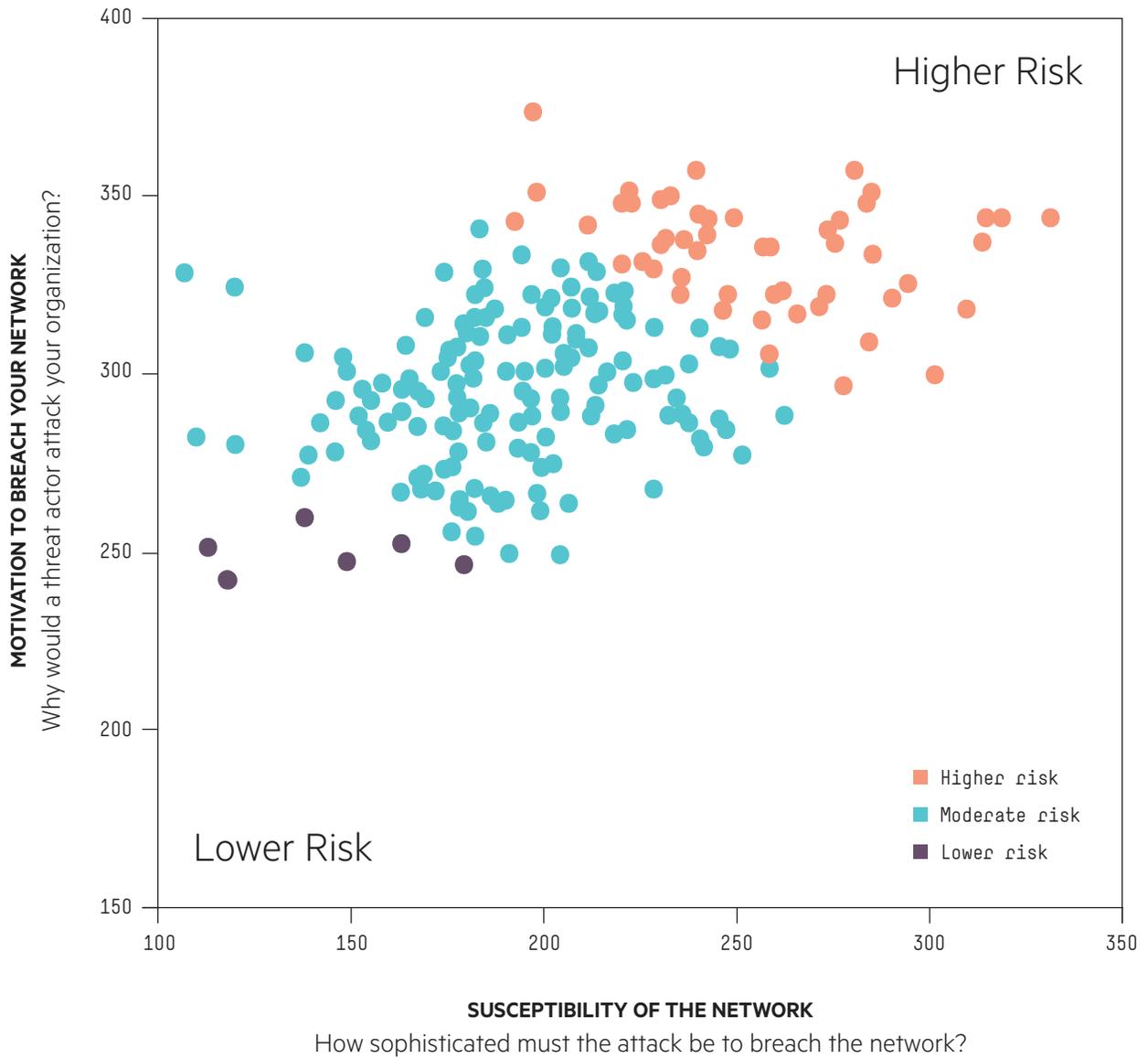


Figure 3: U.S. power, oil, and gas companies with \$1 billion or more in annual revenue⁵

⁵ Source: Marsh Global Analytics

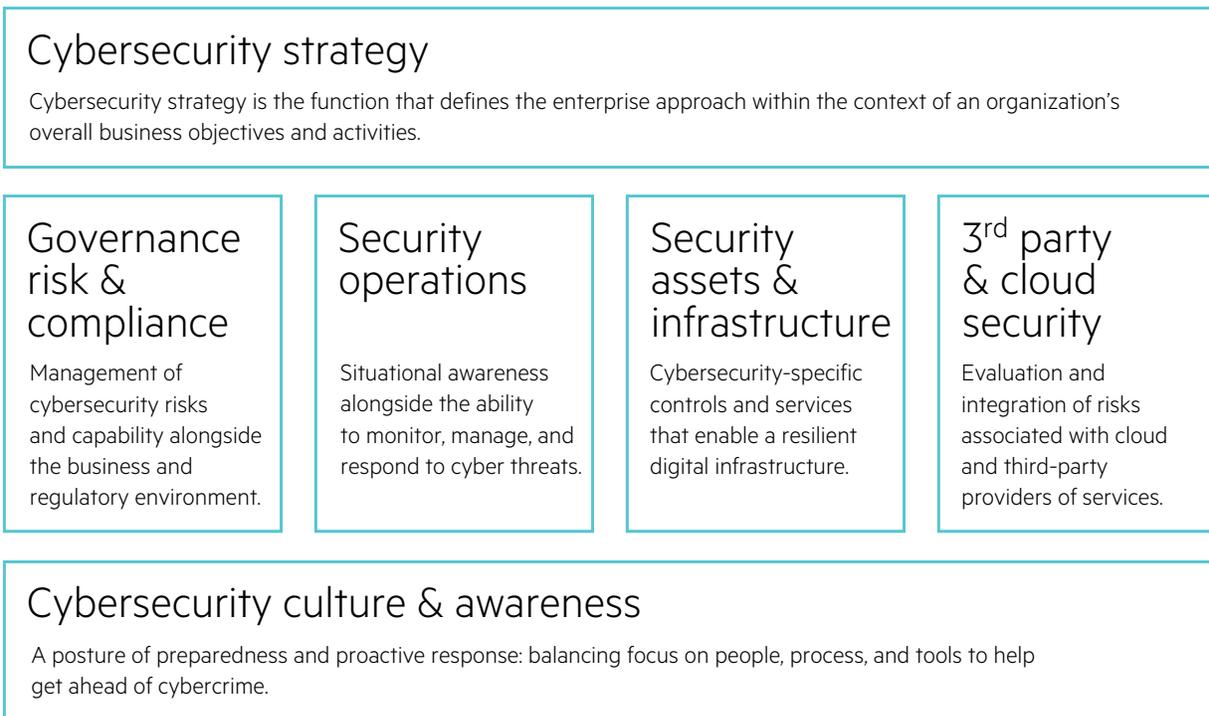


Figure 4: Six core elements of cybersecurity⁶

4. Build a resilient system

With a deeper understanding of your critical assets and overall threat environment, the next step is to develop a strategic framework for deploying your resources. This process should address six core elements:

- Cybersecurity strategy
- Governance, risk, and compliance
- Security operations
- Security assets and infrastructure
- Third party and cloud security
- Cybersecurity culture and awareness

⁶ Source: HPE

- **Cybersecurity strategy**

An organization's overarching strategy determines its risk management goals. Objectives may be as basic as safeguarding data and ensuring confidentiality, integrity, and availability or improving security by reducing vulnerabilities. More complex priorities include benchmarking progress against an established industry standard.

Challenge: Stove-piping

Poor communication, lack of management engagement, and an absence of board oversight are barriers to effective development of a cyber strategy. Cyber-risk management is an enterprise concern, not simply a technology issue. However, even organizations that accept this notion can struggle to embrace sound enterprise risk management practices unless senior management takes ownership of this issue, and the board provides necessary oversight.

- **Governance, risk, and compliance**

Almost more than any other risk a company faces, are the myriad of stakeholders involved in building cyber resilience. The board of directors. Multiple members of the senior management team, including the CEO, CFO, general counsel, CIO, head of HR, and chief information security officer (CISO). Your employees. Your vendors. The role of the board and each member of senior management, in particular, should be clearly articulated in order to enhance your organization's agility to respond to a dynamic threat and avoid conflict.

Challenge: An avalanche of new laws

Cybersecurity laws, regulations, and policies are fragmented and in a constant state of flux. It is estimated that more than 140 new pieces of security or privacy legislation will be passed globally in the next two years. There is almost no commonly accepted framework that an enterprise can use across industry, and national and regional environments. Organizations must strive to adopt enterprise standards and protocols to guide the appropriate allocation of resources.

- **Security operations**

A company's security operations identify threats to the organization and direct real-time responses to mitigate damage and business disruption. A key responsibility of security operations is to implement tactical controls that keep pace with evolving threats. For example, as social engineering attacks like spear phishing prove to be distressingly effective, detonation or "sandbox" software may mitigate this risk. As organizations struggle to protect personally identifiable information, data loss prevention (DLP) software is an important component of an organization's security toolkit.

A security operations center (SOC) forms the core of the security operations function, providing situational awareness alongside the ability to monitor, manage, and respond to cyber threats. In its 2015 Enterprise Report on the State of Security Operations, Hewlett Packard Enterprise (HPE) found that 20 percent of SOCs were not providing minimum security monitoring capabilities, while 87 percent were not meeting recommended levels of security.

Challenge: Attribution

The inability of companies to identify the sources of attacks provides hackers with a significant advantage. Advanced attackers acting with impunity rapidly change tactics to bypass traditional defenses. Industry and government leaders must accelerate their commitment to gathering and sharing threat intelligence to improve attribution.

- **Security assets and infrastructure**

These include data centers, servers, software, and personal devices, which should employ controls that protect data, users, applications, and networks from threats. Legacy systems create inherent vulnerabilities for many reasons, including the challenge of patching known software vulnerabilities.

A multi-layered defense protects all forms of infrastructure, from conventional networks to emerging cloud and mobile platforms. The first line begins with firewalls at the perimeter. Next, systems are segmented to isolate and protect critical operations. Within a system, applications are protected through tight controls around access privileges, including two-factor authentication. At the most granular level, data at rest or in transit is protected through encryption.

Challenge: Shrinking the attack surface

The rapid development of the Internet of Things and proliferation of mobile devices create an ever-expanding set of entry points for hackers. For many organizations, data sprawl is the top cyber vulnerability. To shrink your attack surface, your organization should review its network architectures to eliminate unneeded Internet connections and avoid accumulating data for no reason. Limiting your attackers' opportunities is as important as any investment in technology.

- **Third party and cloud security**

A key lesson of prominent data breaches over the past two years is that any organization is only as cyber resilient as the weakest of its third-party vendors. Regulators, focused on third-party vulnerabilities, are introducing cybersecurity mandates related to vendors. An organization must now actively manage its network supply chain ecosystem, and align controls with the vendor's network activities. At the same time, moving data and applications to the cloud—with the right safeguards—can *increase* security and resilience.

Challenge: Assessment of cloud performance

While outsourcing offers great advantages and, at times, improved security, it also adds complexity. Organizations should establish controls that:

- Limit vendor access within your network.
- Avoid overreliance on any specific outsourced vendor.
- Impose an obligation on vendors to provide notice before transferring your data to other jurisdictions.

- **Cybersecurity culture and awareness**

Evolving culture to meet threats—Technology solutions, including end-to-end encryption, cannot eliminate cyber risk. More than 90 percent of successful cyberattacks are launched via spear phishing campaigns. Accordingly, creating a cyber-aware culture and providing training for employees are critical elements of cyber resilience. Many, if not most, cyber breaches trace back to human error. Accordingly, organizations must focus on their people and processes for addressing cyber risk. Cyber resilience must reside in the organization's DNA, so it becomes an organizational imperative to protect and enable digital interactions.

Challenge: Lack of focus on the user

Training should never grow stale or formulaic. Employees can be an organization's greatest vulnerability. A key challenge is to convert this vulnerability into an asset by training employees to become the first responders—who recognize incidents and protect the organization.

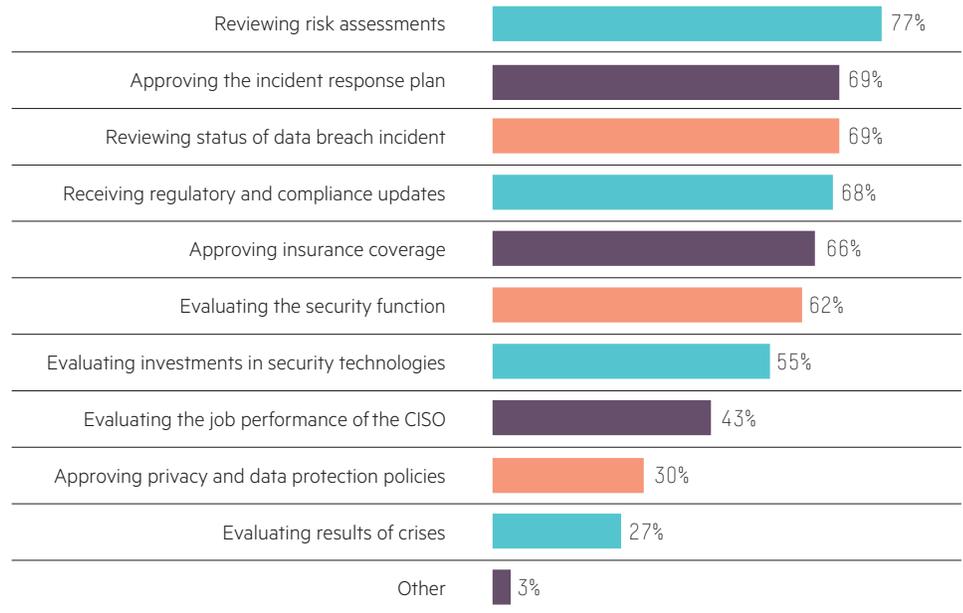


Figure 5: Role of senior executives in incident response⁷

5. Plan for a breach

Cyber resilience through response and recovery

Almost inevitably, an organization’s efforts to prevent attacks will eventually fail. Cyber resilience depends on an organization’s ability to respond to a significant breach and continue operating effectively. In this regard, there are two important steps to consider: contingency planning and the mitigation and transfer of financial risk.

Contingency planning

Operating on the premise that every institution will ultimately be breached, contingency planning is critical. For example:

- Does your organization have a written incident response plan?
- Which executive will lead your incident response?
- Have you engaged in a simulated exercise to test your plan?
- Which outside advisors will you depend on? Have you engaged them on retainer?
- Have you developed relationships with key government officials?

To the extent that an organization has taken these steps, many will have limited their preparations to a data breach. With the looming threat posed to critical infrastructure, it is important that organizations conduct contingency planning against threats to physical assets as well.

Bottom line—in the absence of adequate preparation, organizations that are victimized by a cyberattack rapidly become, in the eyes of regulators, customers, and consumers, the perpetrator of the offense.

⁷ The Importance of Senior Executive Involvement in Breach Response, Ponemon Institute LLC, sponsored by HPE Security Service, October 2014

Mitigation and transfer of financial risk

Cyber insurance can bolster cyber resilience by creating important incentives that drive behavioral change. As a threshold matter, the simple act of applying for insurance forces insureds to assess the strength of their cyber defenses. And, do so against a rapidly changing platform. Organizations are increasingly embedding technology and developing software and applications for their consumers in order to stay competitive. Oftentimes, however, there are inadequate tollgates for security or privacy. While risk transfer cannot substitute for proper preparation, it remains a component of cybersecurity strategy.

Whether prodded by a board of directors or desire to obtain coverage as inexpensively as possible, prospective cyber insurance buyers conduct gap analyses against industry benchmarks. Underwriters scrutinize whether these companies have disciplined procedures for patching software, monitoring their vendor networks, and preparing for breaches. Cyber insurance also prompts an evaluation of potential consequences by using statistical modeling to assess different damage scenarios.

Once a cyber insurance policy is purchased, the insurer has the incentive to help its policyholder avoid or mitigate cyberattacks. As a result, many insurers now offer monitoring and rapid response services to policyholders. Ultimately, in the event of a disabling attack, cyber insurance can limit an institution's economic damage and help accelerate its recovery.

This combination of economic incentives has driven significant increases in the purchase of cyber insurance. Figure 6 shows the 2015 cyber insurance take-up rates by industry sector. The number of Marsh U.S.-based clients purchasing standalone cyber insurance increased 27 percent in 2015 compared with 2014.

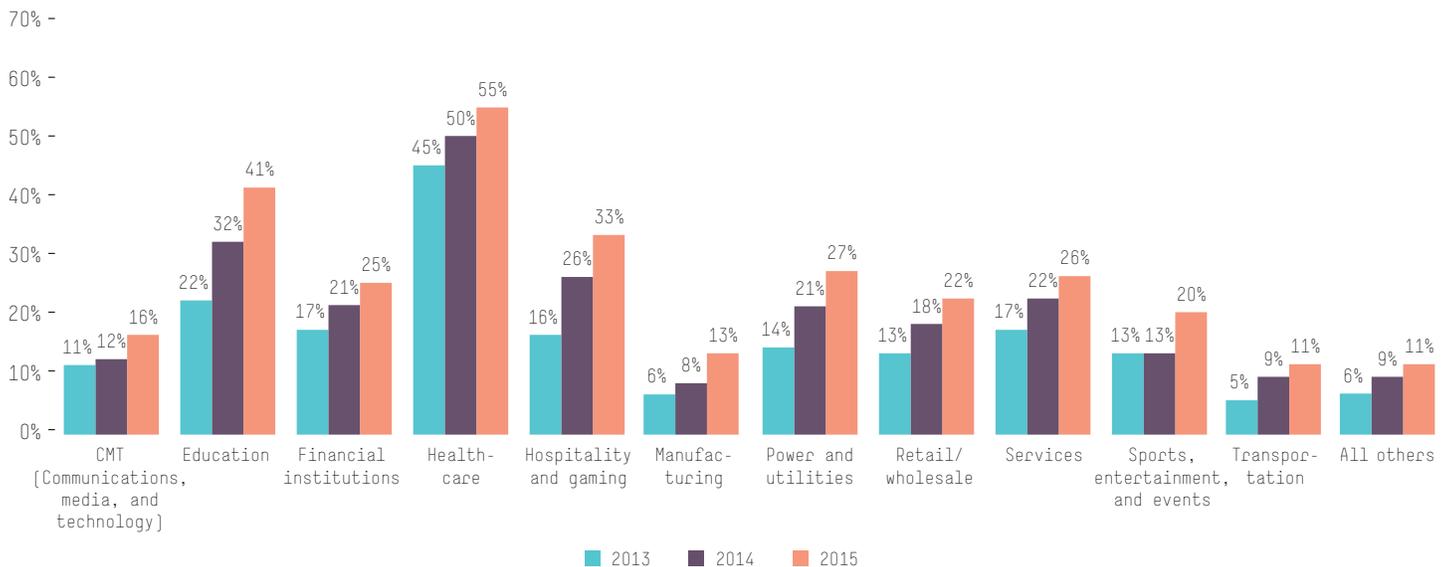


Figure 6: Cyber insurance take-up rate by industry⁸

⁸ Source: Marsh Global Analytics

A call to action

Hewlett Packard Enterprise, FireEye, and Marsh & McLennan Companies joined together to offer this roadmap for cyber resilience. Our intent is to provoke thought and action—not fear and paralysis.

Look at your organization through a different lens. Perfection is not the goal. As in the previous industrial revolutions, organizations that exhibit the greatest agility in responding to changing circumstances will be able to achieve all that the Fourth Industrial Revolution has to offer.

About the authoring organizations

Hewlett Packard Enterprise

Creating a technology platform that helps your business thrive in a disruptive marketplace takes experience and an understanding of how IT systems interact with each other—and the people who use them. Let Hewlett Packard Enterprise be your transformation partner of choice—benefit from our unparalleled global reach, portfolio of world-class security service offerings, expertise, products, and technologies. hpe.com/services/security

For more information, please contact Andrzej Kawalec, HPE Security Services Chief Technologist at andrzej.kawalec@hpe.com

FireEye

FireEye is changing the way organizations worldwide prepare for and respond to advanced cyberattacks. Combining industry-leading security technology, threat intelligence, and incidence response expertise, FireEye provides a complete global threat management platform that stops attacks that bypass traditional security tools. FireEye detects and resolves these cyber breaches in minutes, limiting the loss of data and the damage to intellectual property and brand reputation. FireEye.com

For more information, please contact info@fireeye.com

Marsh & McLennan Companies

Marsh & McLennan Companies provide advice and solutions to mitigate cyber risk. As the world's most trusted cyber insurance broker, Marsh, Inc. advises over 1000 clients regarding network security and privacy issues and has won Advisen's award for Cyber Broker of the Year—2014 and 2015. www.marsh.com/us/services/cyber-risk.html

For more information, please contact Thomas Reagan, Cyber Practice Leader at thomas.reagan@marsh.com or Robert Parisi, Cyber Product Leader at robert.parsi@marsh.com



Sign up for updates

★ Rate this document

© Copyright 2016 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein. All third-party trademarks are the property of their respective owner.

4AA6-3809ENW, January 2016

Testimony of
Adam W. Hamm
Commissioner
North Dakota Department of Insurance
On Behalf of the National Association of Insurance
Commissioners

Before the
Subcommittee on Cybersecurity, Infrastructure Protection, and
Security Technologies
Committee on Homeland Security
United States House of Representatives

Regarding:
The Role of Cyber Insurance in Risk Management

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,

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 five 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 U.S.

² Attachment A – NAIC Cybersecurity (EX) Task Force Membership List

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 contracts between two or more parties, subject to a certain amount of customization, so if you’ve seen one cybersecurity policy, you’ve seen exactly one 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 policyholder 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 U.S. – “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 policyholders 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 policyholders, 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, policyholders 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 policyholders 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 U.S., 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 policyholders.” 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 policyholders by taking enforcement measures against bad actors.

Insurance regulation involves front-end, ongoing, and back-end monitoring of insurers, products, and insurance agents (or producers). The system’s fundamental tenet is to protect policyholders 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 ongoing 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 ongoing 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 policyholder. 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 six 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 cyber security 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 U.S. 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 policyholder 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 two to three billion dollars. 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 nationwide.

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 standalone 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 received 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.

³ Attachment B.

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 twelve *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 ongoing efforts in developing formal regulatory guidance for insurance sector participants.⁵

Most recently, on March 3rd, the Cybersecurity Task Force exposed its new *Insurance Data Security Model Law* for public comment – written comments should be submitted by Wednesday, March 23rd, and feedback will be discussed at the open meeting of the task force on April 4th 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/HR 2205, the Data Security Act, would lessen existing consumer

⁴ Attachment C.

⁵ Attachment D.

⁶ Attachment E.

protections in the insurance sector and could undermine our ongoing 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 cyber security posture across our sectors.

Current State of Play

I recently met with a group of insurance CEO's to discuss the NAIC's ongoing 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 leadoff 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 policyholder 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 policyholders 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 policyholders. Thank you again for the opportunity to be here on behalf of the NAIC, and I look forward to your questions.

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 Rothman	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
Ángela 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 Nordman/Sara Robben/Tony Cotto/Cody Steinwand

.....
Affix Bar Code Above

New Page

CYBERSECURITY AND IDENTITY THEFT INSURANCE COVERAGE SUPPLEMENT

For The Year Ended December 31, 20__
(To Be Filed by April 1)

NAIC Group Code

NAIC Company Code

Company Name

If the reporting entity writes any stand-alone cybersecurity insurance coverage, please provide the following:

1. Stand-Alone Cybersecurity Insurance Policies

Number of Claims Reported		Direct Premiums		Direct Losses		Adjusting and Other Expenses		Direct Defense and Cost Containment		Number of Policies in Force	
1 First Party	2 Third Party	3 Written	4 Earned	5 Paid	6 Incurred	7 Paid	8 Incurred	9 Paid	10 Incurred	11 Claims-Made	12 Occurrence
		\$	\$	\$	\$	\$	\$	\$	\$		

If the reporting entity writes any stand-alone identity theft insurance coverage, please provide the following:

2. Stand-Alone Identity Theft Insurance Policies

1 Number of Claims Reported	Direct Premiums		Direct Losses		Adjusting and Other Expenses		Direct Defense and Cost Containment		10 Number of Policies in Force
	2 Written	3 Earned	4 Paid	5 Incurred	6 Paid	7 Incurred	8 Paid	9 Incurred	
	\$	\$	\$	\$	\$	\$	\$	\$	

If the reporting entity writes any cybersecurity insurance coverage that is part of a package policy, please provide the following:

3. Cybersecurity insurance that is part of a package policy

Number of Claims Reported		Direct Losses		Adjusting and Other Expenses		Direct Defense and Cost Containment		Number of Policies in Force	
1 First Party	2 Third Party	3 Paid	4 Case Reserves	5 Paid	6 Case Reserves	7 Paid	8 Case Reserves	9 Claims-Made	10 Occurrence
		\$	\$	\$	\$	\$	\$		

3.1 Can the direct premium earned for the cybersecurity coverage provided as part of a package policy be quantified or estimated? Yes [] No []

3.11 If the response to 3.1 is no, please fully explain why the insurer cannot quantify or estimate direct premiums earned:

.....
.....

New Page

CYBERSECURITY AND IDENTITY THEFT INSURANCE COVERAGE SUPPLEMENT (Continued)

For The Year Ended December 31, 20__
(To Be Filed by April 1)

3.2 If the response to question 3.1 is yes, provide the quantified or estimated direct premiums written and direct premium earned amount for cybersecurity insurance included in package policies:

	Cybersecurity Insurance Direct Premiums Written	Cybersecurity Insurance Direct Premiums Earned
3.21 Amount quantified:	\$ _____	\$ _____
3.22 Amount estimated using reasonable assumptions:	\$ _____	\$ _____

3.3 If the liability portion of a cybersecurity policy is a claims-made policy, is an extended reporting endorsement (tail coverage) offered? Yes [] No []

If the reporting entity writes any identity theft insurance coverage that is part of a package policy, please provide the following:

4. Identity theft insurance that is part of a package policy

1 Number of Claims Reported	Direct Losses		Adjusting and Other Expenses		Direct Defense and Cost Containment		8 Number of Policies in Force
	2 Paid	3 Case Reserves	4 Paid	5 Case Reserves	6 Paid	7 Case Reserves	
	\$	\$	\$	\$	\$	\$	

4.1 Can the direct premium earned for the identity theft coverage provided as part of a package policy be quantified or estimated? Yes [] No []

4.11 If the response to 4.1 is no, please fully explain why the insurer cannot quantify or estimate direct premiums earned:

.....
.....

4.2 If the response to question 4.1 is yes, provide the quantified or estimated direct premiums written and direct premium earned amount for identity theft insurance included in package policies:

	Identity Theft Insurance Direct Premiums Written	Identity Theft Insurance Direct Premiums Earned
4.21 Amount quantified:	\$ _____	\$ _____
4.22 Amount estimated using reasonable assumptions:	\$ _____	\$ _____

Principles for Effective Cybersecurity: Insurance Regulatory Guidance¹

Due to ever-increasing cybersecurity issues, it has become clear that it is vital for state insurance regulators to provide effective cybersecurity guidance regarding the protection of the insurance sector's data security and infrastructure. The insurance industry looks to state insurance regulators to aid in the identification of uniform standards, to promote accountability across the entire insurance sector, and to provide access to essential information. State insurance regulators look to the insurance industry to join forces in identifying risks and offering practical solutions. The guiding principles stated below are intended to establish insurance regulatory guidance that promotes these relationships and protects consumers.

Principle 1: State insurance regulators have a responsibility to ensure that personally identifiable consumer information held by insurers, producers and other regulated entities is protected from cybersecurity risks. Additionally, state insurance regulators should mandate that these entities have systems in place to alert consumers in a timely manner in the event of a cybersecurity breach. State insurance regulators should collaborate with insurers, insurance producers and the federal government to achieve a consistent, coordinated approach.

Principle 2: Confidential and/or personally identifiable consumer information data that is collected, stored and transferred inside or outside of an insurer's, insurance producer's or other regulated entity's network should be appropriately safeguarded.

Principle 3: State insurance regulators have a responsibility to protect information that is collected, stored and transferred inside or outside of an insurance department or at the NAIC. This information includes insurers' or insurance producers' confidential information, as well as personally identifiable consumer information. In the event of a breach, those affected should be alerted in a timely manner.

Principle 4: Cybersecurity regulatory guidance for insurers and insurance producers must be flexible, scalable, practical and consistent with nationally recognized efforts such as those embodied in the National Institute of Standards and Technology (NIST) framework.

Principle 5: Regulatory guidance must be risk-based and must consider the resources of the insurer or insurance producer, with the caveat that a minimum set of cybersecurity standards must be in place for all insurers and insurance producers that are physically connected to the Internet and/or other public data networks, regardless of size and scope of operations.

Principle 6: State insurance regulators should provide appropriate regulatory oversight, which includes, but is not limited to, conducting risk-based financial examinations and/or market conduct examinations regarding cybersecurity.

Principle 7: Planning for incident response by insurers, insurance producers, other regulated entities and state insurance regulators is an essential component to an effective cybersecurity program.

Principle 8: Insurers, insurance producers, other regulated entities and state insurance regulators should take appropriate steps to ensure that third parties and service providers have controls in place to protect personally identifiable information.

¹ These principles have been derived from the Securities Industry and Financial Markets Association's (SIFMA) "Principles for Effective Cybersecurity Regulatory Guidance."

Principle 9: Cybersecurity risks should be incorporated and addressed as part of an insurer's or an insurance producer's enterprise risk management (ERM) process. Cybersecurity transcends the information technology department and must include all facets of an organization.

Principle 10: Information technology internal audit findings that present a material risk to an insurer should be reviewed with the insurer's board of directors or appropriate committee thereof.

Principle 11: It is essential for insurers and insurance producers to use an information-sharing and analysis organization (ISAO) to share information and stay informed regarding emerging threats or vulnerabilities, as well as physical threat intelligence analysis and sharing.

Principle 12: Periodic and timely training, paired with an assessment, for employees of insurers and insurance producers, as well as other regulated entities and other third parties, regarding cybersecurity issues is essential.

W:\National Meetings\2015\Summer\TF\Cybersecurity\Guiding Principle Documents\Final Guiding Principles 4 16 15.docx



NAIC Roadmap for Cybersecurity Consumer Protections

This document describes the protections the NAIC believes consumers are entitled to from insurance companies, agents and other businesses when they collect, maintain and use your personal information, including what should happen in connection with a notice that your personal information has been involved in a data breach. Not all of these consumer protections are currently provided for under state law. This document functions as a Consumer Bill of Rights and will be incorporated into NAIC model laws and regulations. If you have questions about data security, a notice you receive about a data breach or other issues concerning your personal information in an insurance transaction, you should contact your state insurance department to determine your existing rights.

As an insurance consumer, you have the right to:

1. Know the types of personal information collected and stored by your insurance company, agent or any business it contracts with (such as marketers and data warehouses).
2. Expect insurance companies/agencies to have a privacy policy posted on their websites and available in hard copy, if you ask. The privacy policy should explain what personal information they collect, what choices consumers have about their data, how consumers can see and change/correct their data if needed, how the data is stored/protected, and what consumers can do if the company/agency does not follow its privacy policy.
3. Expect your insurance company, agent or any business it contracts with to take reasonable steps to keep unauthorized persons from seeing, stealing or using your personal information.
4. Get a notice from your insurance company, agent or any business it contracts with if an unauthorized person has (or it seems likely he or she has) seen, stolen or used your personal information. This is called a *data breach*. This notice should:
 - Be sent in writing by first-class mail or by e-mail if you have agreed to that.
 - Be sent soon after a data breach and never more than 60 days after a data breach is discovered.
 - Describe the type of information involved in a data breach and the steps you can take to protect yourself from identity theft or fraud.
 - Describe the action(s) the insurance company, agent or business it contracts with has taken to keep your personal information safe.
 - Include contact information for the three nationwide credit bureaus.
 - Include contact information for the company or agent involved in a data breach.
5. Get at least one year of identity theft protection paid for by the company or agent involved in a data breach.
6. If someone steals your identity, you have a right to:
 - Put a 90-day initial fraud alert on your credit reports. (The first credit bureau you contact will alert the other two.)
 - Put a seven-year extended fraud alert on your credit reports.
 - Put a credit freeze on your credit report.
 - Get a free copy of your credit report from each credit bureau.
 - Get fraudulent information related to the data breach removed (or “blocked”) from your credit reports.
 - Dispute fraudulent or wrong information on your credit reports.
 - Stop creditors and debt collectors from reporting fraudulent accounts related to the data breach.
 - Get copies of documents related to the identity theft.
 - Stop a debt collector from contacting you.

To learn more about the protections in your state or territory, contact your consumer protection office at <https://www.usa.gov/state-consumer> or your state or territory’s insurance department at www.naic.org/state_web_map.htm.

Standard Definitions Under This Bill of Rights

Data Breach: When an unauthorized individual or organization sees, steals or uses sensitive, protected or confidential information—usually personal, financial and/or health information.

Credit Bureau (Consumer Reporting Agency): A business that prepares credit reports for a fee and provides those reports to consumers and businesses; its information sources are primarily other businesses.

Credit Freeze (Security Freeze): A way you can restrict access to your credit report and prevent anyone other than you from using your credit information.

Personal Information (Personally Identifiable Information): Any information about a consumer that an insurance company, its agents or any business it contracts with maintains that can be used to identify a consumer. Examples include:

- Full name.
- Social Security number.
- Date and place of birth.
- Mother’s maiden name.
- Biometric records.
- Driver’s license number.

Helpful Links:

“Credit Freeze FAQs” (Federal Trade Commission—FTC) – www.consumer.ftc.gov/articles/0497-credit-freeze-faqs

“Disputing Errors on Credit Reports” (FTC) – www.consumer.ftc.gov/articles/0151-disputing-errors-credit-reports

“Taking Charge: What to Do If Your Identity Is Stolen” (FTC, May 2012). Tri-fold brochure; online PDF; can order bulk copies at no cost – <https://bulkorder.ftc.gov/system/files/publications/pdf-0009-taking-charge.pdf>

“Know Your Rights” (FTC) – <https://www.identitytheft.gov/know-your-rights.html>

“What Is Identity Theft?” (video; FTC) – www.consumer.ftc.gov/media/video-0023-what-identity-theft

“When Information Is Lost or Exposed” (FTC) – <https://www.identitytheft.gov/info-lost-or-stolen.html>

State Consumer Protection Offices (USA.gov) – www.usa.gov/directory/stateconsumer/index.shtml

Directory of State Insurance Regulators (NAIC) www.naic.org/state_web_map.htm

World’s Biggest Data Breaches (information is beautiful) – www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

PRELIMINARY WORKING AND DISCUSSION DRAFT

Draft: 3/2/2016
 Draft of New Cybersecurity Model Law
 Cybersecurity (EX) Task Force

INSURANCE DATA SECURITY MODEL LAW

Table of Contents

Section 1.	Purpose and Intent
Section 2.	Applicability and Scope
Section 3.	Definitions
Section 4.	Information Security Program
Section 5.	Consumer Rights Before a Breach of Data Security
Section 6.	Investigation of a Breach of Data Security
Section 7.	Notification of a Breach of Data Security
Section 8.	Consumer Protections Following a Breach of Data Security
Section 9.	Power of Commissioner
Section 10.	Hearings, Witnesses, Appearances, Production of Books and Service of Process
Section 11.	Confidentiality
Section 12.	Cease and Desist Orders and Reports
Section 13.	Penalties
Section 14.	Judicial Review of Orders and Reports
Section 15.	Individual Remedies
Section 16.	Immunity
Section 17.	Obtaining Information Under False Pretenses
Section 18.	Rules and Regulations
Section 19.	Severability
Section 20.	Effective Date

Section 1. Purpose and Intent

The purpose and intent of this Act is to establish the exclusive standards for data security and investigation and notification of a breach of data security applicable to licensees in this state.

Section 2. Applicability and Scope

Consistent with authority to regulate the business of insurance pursuant to the McCarran-Ferguson Act, 15 U.S.C. § 1011 et seq. and the laws of this state, this Act is intended to regulate the business of insurance. No other provision of state or federal law or regulation regarding data security or investigation or notification of a breach of data security shall apply to licensees subject to the provisions of this Act.

Section 3. Definitions

As used in this Act, the following terms shall have these meanings:

- A. “Breach of data security,” “breach,” “data breach,” or “security breach” means the unauthorized acquisition of personal information.

The term “breach of data security” does not include the unauthorized acquisition of personal information that is encrypted, redacted, or otherwise protected by another method that renders the information unreadable and unusable if the encryption, redaction, or protection process or key is not also acquired without authorization.

- B. “Consumer” means an individual or entity, including but not limited to policyholders and their family members.

PRELIMINARY WORKING AND DISCUSSION DRAFT

- C. “Consumer reporting agency” has the same meaning as “consumer reporting agency that compiles and maintains files on consumers on a nationwide basis” in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)).
- D. “Encrypted” means rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.
- E. “Information security program” means the administrative, technical, or physical safeguards that a licensee uses to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personal information.
- F. “Licensee” means all licensed insurers, producers and other persons licensed or required to be licensed, or authorized or required to be authorized, or registered or required to be registered pursuant to the Insurance Law of this state.
- G. “Personal Information” means
- (1) A financial account number relating to a consumer, including a credit card number or debit card number, in combination with any security code, access code, password, or other personal identification information required to access the financial account; or
 - (2) Information including:

The first name or first initial and last name of a consumer in combination with:

 - (a) The consumer’s non-truncated social security number;
 - (b) The consumer’s driver’s license number, passport number, military identification number, or other similar number issued on a government document used to verify identity;
 - (c) A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online or financial account of the consumer;
 - (d) Biometric data of the consumer used to gain access to financial accounts of the consumer;
 - (e) Health information of the consumer;
 - (f) Information that the consumer provides to a licensee to obtain an insurance product or service used primarily for personal, family, or household purposes from the licensee;
 - (g) Information about the consumer resulting from a transaction involving an insurance product or service used primarily for personal, family, or household purposes between a licensee and the consumer;
 - (h) Information the licensee obtains about the consumer in connection with providing an insurance product or service used primarily for personal, family, or household purposes to the consumer; or
 - (i) A list, description, or other grouping of consumers (and publicly available information pertaining to them), that is derived using the information described in [Subparagraphs (f) through (h), information provided to licensees] that is not publicly available.
 - (3) Any information or data except age or gender, that relates to:
 - (a) The past, present or future physical, mental or behavioral health or condition of a consumer;

PRELIMINARY WORKING AND DISCUSSION DRAFT

- (b) The provision of health care to a consumer; or
- (c) Payment for the provision of health care to a consumer.

The term “personal information” does not include publicly available information that is lawfully made available to the general public and obtained from federal, state, or local government records; or widely distributed media.

- H. “Substantial harm or inconvenience” means
 - (1) Identity theft; or
 - (2) Fraudulent transactions on financial accounts.
- I. “Third-party service provider” or “service provider” means a person or entity that maintains, processes or otherwise is permitted access to personal information through its provision of services directly to the licensee.

Section 4. Information Security Program

- A. Implementation of an Information Security Program

Each licensee shall develop, implement, and maintain a comprehensive written information security program that contains administrative, technical, and physical safeguards for the protection of personal information.
- B. Objectives of Information Security Program

A licensee’s information security program shall be designed to:

 - (1) Ensure the security and confidentiality of personal information;
 - (2) Protect against any anticipated threats or hazards to the security or integrity of the information; and
 - (3) Protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to any customer.
- C. Appropriateness of Information Security Program

The scale and scope of a licensee’s information security program shall be appropriate to:

 - (1) The size and complexity of the licensee;
 - (2) The nature and scope of the activities of the licensee; and
 - (3) The sensitivity of the consumer information to be protected.
- D. Risk Assessment

The licensee shall:

 - (1) Designate an employee or employees to coordinate the information security program;
 - (2) Identify reasonably foreseeable internal or external threats that could result in unauthorized disclosure, misuse, alteration or destruction of personal information or personal information systems;

PRELIMINARY WORKING AND DISCUSSION DRAFT

- (3) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information;
- (4) Assess the sufficiency of policies, procedures, personal information systems and other safeguards in place to control these risks, including consideration of risks in each relevant area of the licensee's operations, including:
 - (a) Employee training and management;
 - (b) Information systems, including network and software design, as well as information processing, storage, transmission, and disposal; and
 - (c) Detecting, preventing, and responding to attacks, intrusions, or other systems failures; and
- (5) Design and implement information safeguards to control the risks identified in its risk assessment, and regularly assess the effectiveness of the safeguards' key controls, systems, and procedures.

E. Risk Management

The licensee shall:

- (1) Design its information security program to control the identified risks, commensurate with the sensitivity of the information, as well as the complexity and scope of the licensee's activities, using as a guide, the *Framework for Improving Critical Infrastructure Cybersecurity* developed by the National Institute of Standards and Technology (NIST), including adopting the following security measures:
 - (a) Place access controls on information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing personal information to unauthorized individuals who may seek to obtain this information through fraudulent means;
 - (b) Restrict access at physical locations containing personal information, such as buildings, computer facilities, and records storage facilities, to permit access only to authorized individuals;
 - (c) Encrypt electronic personal information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;
 - (d) Design procedures to ensure that information system modifications are consistent with the licensee's information security program;
 - (e) Utilize multi-factor authentication procedures, segregation of duties, and employee background checks for employees with responsibilities for, or access to, personal information;
 - (f) Regularly test or monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems;
 - (g) Implement response programs that specify actions to be taken when the licensee suspects or detects that unauthorized individuals have gained access to information systems;
 - (h) Implement measures to protect against destruction, loss, or damage of personal information due to potential environmental hazards, such as fire and water damage or technological failures; and

PRELIMINARY WORKING AND DISCUSSION DRAFT

- (i) Develop, implement, and maintain appropriate measures to properly dispose of personal information;
 - (2) Address cybersecurity risks into the licensee's enterprise risk management process; and
 - (3) Use an Information Sharing and Analysis Organization (ISAO) to share information and stay informed regarding emerging threats or vulnerabilities.
- F. Oversight by Board of Directors
- (1) If the licensee has a board of directors, the board or an appropriate committee of the board shall:
 - (a) Approve the licensee's written information security program; and
 - (b) Oversee the development, implementation, and maintenance of the licensee's information security program, including assigning specific responsibility for its implementation and reviewing reports from management.
 - (2) If the licensee has a board of directors, the licensee shall report to its board or an appropriate committee of the board at least annually, the following information:
 - (a) The overall status of the information security program and the licensee's compliance with this Act; and
 - (b) Material matters related to its program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security breaches or violations and management's responses, and recommendations for changes in the information security program.
- G. Oversight of Third-Party Service Provider Arrangements
- The licensee shall:
- (1) Select and retain third-party service providers that are capable of maintaining appropriate safeguards for the personal information at issue;
 - (2) Require the third-party service providers to do the following, by contract:
 - (a) Implement and maintain appropriate safeguards for the personal information at issue, including those security measures listed in [Section 4E(1), Risk Management].
 - (b) Notify licensee within three (3) calendar days of a discovery of a breach of data security in a system maintained by the third-party service provider that has been contracted to maintain, store, or process data containing personal information on behalf of a licensee;
 - (c) Indemnify licensee in the event of a cybersecurity incident that results in loss;
 - (d) Allow licensee or its agents to perform cybersecurity audits of the third-party service provider; and
 - (e) Represent and warrant its compliance with all requirements; and
 - (3) Oversee or obtain an assessment of the third-party service provider's compliance with contractual obligations, where appropriate in light of the licensee's risk assessment.

PRELIMINARY WORKING AND DISCUSSION DRAFT

H. Program Adjustments

The licensee shall monitor, evaluate and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its personal information, internal or external threats to information, and the licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to personal information systems.

Section 5. Consumer Rights Before a Breach of Data Security

- A. The licensee shall provide consumers with information regarding the types of personal information collected and stored by licensee or any third-party service providers it contracts with.
- B. The licensee shall post its privacy policy on its websites and make it available to consumers in hard copy, upon request. The privacy policy shall explain what type of personal information licensee collects, what options consumers have about their data, how consumers can review and change or correct their data if needed, how the data is stored and protected, and what consumers can do if the licensee does not follow its privacy policy.

Section 6. Investigation of a Breach of Data Security

- A. If a licensee believes that a breach of data security has or may have occurred in relation to personal information that is maintained, communicated, or otherwise handled by, or on behalf of, the licensee, the licensee shall conduct an investigation.
- B. During the investigation, the licensee shall:
 - (1) Assess the nature and scope of the incident;
 - (2) Identify any personal information that may have been involved in the incident;
 - (3) Determine if the personal information has been acquired without authorization; and
 - (4) Take reasonable measures to restore the security and confidentiality of the systems compromised in the breach.

Section 7. Notification of a Breach of Data Security

- A. If the licensee determines under [Section 6, Investigation of a Breach of Data Security] that the unauthorized acquisition of personal information involved in a breach of data security is reasonably likely to cause substantial harm or inconvenience to the consumers to whom the information relates, the licensee, or a third party acting on behalf of the licensee, shall notify, without unreasonable delay:
 - (1) An appropriate Federal and state law enforcement agency;
 - (2) The insurance commissioner;
 - (3) Any relevant payment card network, if the breach involves a breach of payment card numbers;
 - (4) Each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, if the breach involves personal information relating to 1,000 or more consumers; and
 - (5) All consumers to whom the personal information relates.
- B. Providing Notice to the Commissioner

No later than five (5) calendar days of identifying a data breach, the licensee shall notify the commissioner, providing as much of the following information as is known to the licensee:

PRELIMINARY WORKING AND DISCUSSION DRAFT

- (1) Date of the breach;
 - (2) Description of the breach, including how the information was lost, stolen, or breached;
 - (3) How the breach was discovered;
 - (4) Whether any lost, stolen, or breached information has been recovered and if so, how this was done;
 - (5) Whether any individuals involved in the incident (both internal and external) have been identified;
 - (6) Whether a police report has been filed;
 - (7) Description of the type of information lost, stolen, or breached (equipment, paper, electronic, claims, applications, underwriting forms, medical records etc.);
 - (8) Whether the information was encrypted;
 - (9) The time period covered by the information that was lost, stolen or breached;
 - (10) Number of residents of the state affected by the breach;
 - (11) Results of any internal review identifying either a lapse in internal procedures or confirmation that all procedures were followed;
 - (12) Identification of remedial efforts being undertaken to cure the situation which permitted the information security incident to occur;
 - (13) Copies of the licensee's privacy policies and data breach policy;
 - (14) Name of a contact person who is both familiar with the details and able to authorize actions for the licensee; and
 - (15) Other regulatory or law enforcement agencies that have been notified and when notification was provided.
- C. Providing Notice to Consumer Reporting Agencies

No later than sixty (60) calendar days of identifying a data breach, the licensee shall notify each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis, if the breach involves personal information relating to [1000] or more consumers.

D. Providing Notice to Consumers

- (1) No later than sixty (60) calendar days of identifying a data breach, the licensee shall notify all affected consumers.
- (2) Licensee will provide the notification in writing by first-class mail, unless the consumer has agreed to be contacted through e-mail.
- (3) No later than forty-five (45) calendar days of identifying a data breach, the licensee shall provide to the commissioner, a draft of the proposed written communication to consumers. The commissioner shall have the right to edit the proposed communication before the licensee sends it to consumers. This proposed notification shall be written in plain English and include the following information:

PRELIMINARY WORKING AND DISCUSSION DRAFT

- (a) A description of the type of information involved in the data breach;
- (b) A description of the action that the licensee or business it contracts with has taken to safeguard the information;
- (c) A summary of rights of victims of identity theft prepared under § 609(d) of the Fair Credit Reporting Act (15 U.S.C. 1681g(d));
- (d) The steps consumers can take to protect themselves from identity theft or fraud, which shall include an explanation that consumers shall have a right to do the following:
 - (i) Put a 90-day initial fraud alert on their credit reports;
 - (ii) Put a seven-year extended fraud alert on their credit reports;
 - (iii) Put a credit freeze on their credit report;
 - (iv) Get a free copy of their credit report from each credit bureau;
 - (v) Get fraudulent information related to the data breach removed (or “blocked”) from their credit reports;
 - (vi) Dispute fraudulent or wrong information on their credit reports;
 - (vii) Stop creditors and debt collectors from reporting fraudulent accounts related to the data breach;
 - (viii) Get copies of documents related to the identity theft; and
 - (ix) Stop a debt collector from contacting them;
- (e) Contact information for the three nationwide consumer reporting agencies;
- (f) Contact information for the licensee or its designated call center; and
- (g) An offer from the licensee to the consumer to provide appropriate identity theft protection services free of cost to the consumer for a period of not less than twelve (12) months.

E. Providing Notice Regarding Breaches of Third-Party Service Providers

Licensee shall comply with [Subsections B and D] by notifying the commissioner and consumers in the event of a breach of data security in a system maintained by a third-party service provider. The computation of licensee’s deadlines shall begin on the day the third-party service provider provides notice to licensee.

- F. Notwithstanding the requirements of [Subsections C, D, and E], notice may be delayed where requested by an appropriate state or federal law enforcement agency. The commissioner shall be notified of any such request.

Section 8. Consumer Protections Following a Breach of Data Security

After reviewing the licensee’s data breach notification, the commissioner shall prescribe the appropriate level of consumer protection required following the data breach and for what period of time that protection will be provided. At a minimum, the licensee will offer to pay for at least twelve (12) months of identity theft protection for affected consumers.

PRELIMINARY WORKING AND DISCUSSION DRAFT

Section 9. Power of Commissioner

The commissioner shall have power to examine and investigate into the affairs of any licensee to determine whether the licensee has been or is engaged in any conduct in violation of this Act. This power is in addition to the powers which the commissioner has under [insert applicable statutes governing the examination of insurers]. Any such examination shall be conducted pursuant to [insert applicable statutes governing the examination of insurers].

Section 10. Hearings, Witnesses, Appearances, Production of Books and Service of Process

- A. Whenever the commissioner has reason to believe that a licensee has been or is engaged in conduct in this state which violates this Act, the commissioner shall issue and serve upon such licensee a statement of charges and notice of hearing to be held at a time and place fixed in the notice. The date for such hearing shall be not less than [insert number] days after the date of service.
- B. At the time and place fixed for such hearing the licensee charged shall have an opportunity to answer the charges against it and present evidence on its behalf. Upon good cause shown, the commissioner shall permit any adversely affected person to intervene, appear and be heard at such hearing by counsel or in person.
- C. At any hearing conducted pursuant to this section, the commissioner may administer oaths, examine and cross-examine witnesses and receive oral and documentary evidence. The commissioner shall have the power to subpoena witnesses, compel their attendance and require the production of books, papers, records, correspondence and other documents which are relevant to the hearing. A stenographic record of the hearing shall be made upon the request of any party or at the discretion of the commissioner. If no stenographic record is made and if judicial review is sought, the commissioner shall prepare a statement of the evidence for use on the review. Hearings conducted under this section shall be governed by the same rules of evidence and procedure applicable to administrative proceedings conducted under the laws of this state.
- D. Statements of charges, notices, orders and other processes of the commissioner under this Act may be served by anyone duly authorized to act on behalf of the commissioner. Service of process may be completed in the manner provided by law for service of process in civil actions or by registered mail. A copy of the statement of charges, notice, order or other process shall be provided to the person or persons whose rights under this Act have been allegedly violated. A verified return setting forth the manner of service, or return postcard receipt in the case of registered mail, shall be sufficient proof of service.

Section 11. Confidentiality

- A. Any documents, materials or other information in the control or possession of the department of insurance that is furnished by a licensee or an employee or agent thereof acting on behalf of licensee, or obtained by the insurance commissioner in an investigation pursuant to this Act shall be confidential by law and privileged, shall not be subject to [insert open records, freedom of information, sunshine or other appropriate phrase], shall not be subject to subpoena, and shall not be subject to discovery or admissible in evidence in any private civil action. However, the insurance commissioner is authorized to use the documents, materials or other information in the furtherance of any regulatory or legal action brought as a part of the insurance commissioner's duties.
- B. Neither the insurance commissioner nor any person who received documents, materials or other information while acting under the authority of the insurance commissioner shall be permitted or required to testify in any private civil action concerning any confidential documents, materials, or information subject to [Subsection A].
- C. In order to assist in the performance of the insurance commissioner's duties under this Act, the insurance commissioner:

PRELIMINARY WORKING AND DISCUSSION DRAFT

- (1) May share documents, materials or other information, including the confidential and privileged documents, materials or information subject to [Subsection A], with other state, federal, and international regulatory agencies, with the National Association of Insurance Commissioners, its affiliates or subsidiaries, and with state, federal, and international law enforcement authorities, provided that the recipient agrees to maintain the confidentiality and privileged status of the document, material or other information;
 - (2) May receive documents, materials or information, including otherwise confidential and privileged documents, materials or information, from the National Association of Insurance Commissioners, its affiliates or subsidiaries and from regulatory and law enforcement officials of other foreign or domestic jurisdictions, and shall maintain as confidential or privileged any document, material or information received with notice or the understanding that it is confidential or privileged under the laws of the jurisdiction that is the source of the document, material or information; and
 - (3) **[OPTIONAL]** May enter into agreements governing sharing and use of information consistent with this subsection.
- D. No waiver of any applicable privilege or claim of confidentiality in the documents, materials, or information shall occur as a result of disclosure to the commissioner under this section or as a result of sharing as authorized in [Subsection C].
- E. Nothing in this Act shall prohibit the insurance commissioner from releasing final, adjudicated actions including for cause terminations that are open to public inspection pursuant to [insert appropriate reference to state law] to a database or other clearinghouse service maintained by the National Association of Insurance Commissioners, its affiliates or subsidiaries of the National Association of Insurance Commissioners.

Section 12. Cease and Desist Orders and Reports

- A. If, after a hearing pursuant to Section [section on hearings], the commissioner determines that the licensee charged has engaged in conduct or practices in violation of this Act, the commissioner shall reduce his or her findings to writing and shall issue and cause to be served upon such licensee a copy of such findings and an order requiring such licensee to cease and desist from the conduct or practices constituting a violation of this Act.
- B. If, after a hearing pursuant to Section [section on hearings], the commissioner determines that the licensee charged has not engaged in conduct or practices in violation of this Act, the commissioner shall prepare a written report which sets forth findings of fact and conclusions of law. Such report shall be served upon the licensee charged and upon the person or persons, if any, whose rights under this Act were allegedly violated.
- C. Until the expiration of the time allowed under Section [section on judicial review] of this Act for filing a petition for review or until such petition is actually filed, whichever occurs first, the commissioner may modify or set aside any order or report issued under this section. After the expiration of the time allowed under Section [section on judicial review] of this Act for filing a petition for review, if no such petition has been duly filed, the commissioner may, after notice and opportunity for hearing, alter, modify or set aside, in whole or in part, any order or report issued under this section whenever conditions of fact or law warrant such action or if the public interest so requires.

Section 13. Penalties

- A. In any case where a hearing pursuant to Section [section on hearings] results in the finding of a knowing violation of this Act, the commissioner may, in addition to the issuance of a cease and desist order as prescribed in Section [section on cease and desist orders], order payment of a monetary penalty of not more than [\$500] for each violation but not to exceed [\$10,000] in the aggregate for multiple violations.

PRELIMINARY WORKING AND DISCUSSION DRAFT

- B. Any person who violates a cease and desist order of the commissioner under Section [section on cease and desist orders] of this Act may, after notice and hearing and upon order of the commissioner, be subject to one or more of the following penalties, at the discretion of the commissioner:
- (1) A monetary fine of not more than [\$10,000] for each violation;
 - (2) A monetary fine of not more than [\$50,000] if the commissioner finds that violations have occurred with such frequency as to constitute a general business practice; or
 - (3) Suspension or revocation of an insurance institution's or agent's license.
- C. Notwithstanding the foregoing, nothing in this Act shall be construed to limit the commissioner's authority under [insert citation to Unfair Trade Practices Act].

Section 14. Judicial Review of Orders and Reports

- A. Any licensee subject to an order of the commissioner under Section [section on cease and desist orders] or Section [section on penalties] or any licensee whose rights under this Act were allegedly violated may obtain a review of any order or report of the commissioner by filing in the [insert title] Court of [insert county] County, within [insert number] days from the date of the service of such order or report, a written petition requesting that the order or report of the commissioner be set aside. A copy of such petition shall be simultaneously served upon the commissioner, who shall forthwith certify and file in such court a transcript of the entire record of the proceeding giving rise to the order or report which is the subject of the petition. Upon filing of the petition and transcript the [insert title] Court shall have jurisdiction to make and enter a decree modifying, affirming or reversing any order or report of the commissioner, in whole or in part. The findings of the commissioner as to the facts supporting any order or report, if supported by clear and convincing evidence, shall be conclusive.
- B. To the extent an order or report of the commissioner is affirmed, the court shall issue its own order commanding obedience to the terms of the order or report of the commissioner. If any party affected by an order or report of the commissioner shall apply to the court for leave to produce additional evidence and shall show to the satisfaction of the court that such additional evidence is material and that there are reasonable grounds for the failure to produce such evidence in prior proceedings, the court may order such additional evidence to be taken before the commissioner in such manner and upon such terms and conditions as the court may deem proper. The commissioner may modify his or her findings of fact or make new findings by reason of the additional evidence so taken and shall file such modified or new findings along with any recommendation, if any, for the modification or revocation of a previous order or report. If supported by clear and convincing evidence, the modified or new findings shall be conclusive as to the matters contained therein.
- C. An order or report issued by the commissioner under Section [section on cease and desist orders] or [section on penalties] shall become final:
- (1) Upon the expiration of the time allowed for the filing of a petition for review, if no such petition has been duly filed; except that the commissioner may modify or set aside an order or report to the extent provided in Section [section on cease and desist orders]; or
 - (2) Upon a final decision of the [insert title] Court if the court directs that the order or report of the commissioner be affirmed or the petition for review dismissed.
- D. No order or report of the commissioner under this Act or order of a court to enforce the same shall in any way relieve or absolve any licensee affected by such order or report from any liability under any law of this state.

PRELIMINARY WORKING AND DISCUSSION DRAFT

Section 15. Individual Remedies

- A. If any licensee fails to comply with Section [insert section(s) addressing consumer rights] of this Act with respect to the rights granted under those sections, any person whose rights are violated may apply to the [insert title] Court of this state, or any other court of competent jurisdiction, for appropriate equitable relief.
- B. In any action brought pursuant to this section, the court may award the cost of the action and reasonable attorney's fees to the prevailing party.
- C. An action under this section must be brought within two (2) years from the date the alleged violation is or should have been discovered.
- D. Except as specifically provided in this Act, there shall be no remedy or recovery available to consumers, in law or in equity, for occurrences constituting a violation of any provisions of this Act.

Section 16. Immunity

No cause of action in the nature of defamation, invasion of privacy or negligence shall arise against any person for disclosing personal or privileged information in accordance with this Act, nor shall such a cause of action arise against any person for furnishing personal or privileged information to a licensee; provided, however, this section shall provide no immunity for disclosing or furnishing false information with malice or willful intent to injure any person.

Section 17. Obtaining Information Under False Pretenses

Any person who knowingly and willfully obtains information about a consumer from a licensee under false pretenses shall be fined not more than [\$10,000] or imprisoned for not more than one year, or both.

Section 18. Rules and Regulations

The commissioner may, upon notice and opportunity for all interested persons to be heard, issue such rules, regulations and orders as shall be necessary to carry out the provisions of this Act.

Section 19. Severability

If any provisions of this Act or the application thereof to any person or circumstance is for any reason held to be invalid, the remainder of the Act and the application of such provision to other persons or circumstances shall not be affected thereby.

Section 20. Effective Date

This Act shall take effect on [insert a date which allows at least a one year interval between the date of enactment and the effective date].

**Testimony of Daniel Nutkis
CEO of HITRUST Alliance
Before the Homeland Security Committee,
Subcommittee on Cybersecurity, Infrastructure Protection, and Security
Technologies
Hearing entitled: “The Role of Cyber Insurance in Risk Management”
March 22, 2016**

Prepared for Submission

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 healthcare 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 healthcare 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 healthcare 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 healthcare 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 healthcare.

Healthcare 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 healthcare organizations and business associates, have adopted the HITRUST CSF, making it the most widely adopted privacy and security framework in healthcare.

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 healthcare industry, the HITRUST CSF Assurance Program provides healthcare 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 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 healthcare 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,

¹ Healthcare 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.

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).

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 healthcare industry. This program facilitates the early identification of cyber-attacks and the creation of best practices specific to the healthcare 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 healthcare 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 healthcare 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 healthcare 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 healthcare organizations and evaluate the industry’s preparedness against attempts to disrupt U.S. healthcare 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 healthcare organizations, HITRUST, and government agencies.

I only share this information to provide context on our engagement, experience, knowledge, and commitment in supporting the healthcare 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

³ See <https://www.dhs.gov/healthcare-and-public-health-sector>

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 dependent 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 healthcare 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 healthcare 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 healthcare organizations over the past few years, it is clear that healthcare 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, healthcare 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 healthcare 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 three 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 healthcare 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 healthcare 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 five 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 five other cyber underwriters regarding leveraging this approach, with an expectation that two more will be participating by midyear. It is clear that this approach is a win-win for the healthcare industry, underwriters, and of course, the members and patients whose information they are responsible for safeguarding.

For healthcare 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 cyber security and risk management challenges facing the healthcare 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 healthcare 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 healthcare 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 healthcare 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 policyholders while allowing organizations to grow and mature their information security programs.

HITRUST, through its many tools and programs, remains committed to ensure that the healthcare 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.



STATEMENT OF

THOMAS MICHAEL FINAN
CHIEF STRATEGY OFFICER
ARK NETWORK SECURITY SOLUTIONS

BEFORE THE

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMELAND SECURITY

Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

“The Role of Cyber Insurance in Risk Management”

Tuesday, March 22, 2016
311 Cannon House Office Building

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' 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' 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 three to five minutes, hours, or days ahead but – like its external partners – three to five years ahead.

Insurance, we learned, is a key part of that process. When we began DHS' 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 ongoing 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 worldwide. 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 ongoing 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 ongoing 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 two 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 four “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' 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 three 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 hand-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 four 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:

- During DHS' 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 two hours at a time. While we scheduled two in-person meetings for the group in the Washington, D.C., 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

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

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 six 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 timelines; 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 one of the six 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 three 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 nine 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 Timeline;

- 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 ongoing 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 eight 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’ 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 one 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 ongoing 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.