Cyber Risk Culture Roundtable Readout Report

National Protection and Programs Directorate
Department of Homeland Security

May 2013

TABLE OF CONTENTS

BACKGROUND

The Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD) helps both private and public sector partners secure their cyber networks – assisting them both collectively and individually and improving the nation's overall cybersecurity posture in the process. Through these interactions, DHS has become aware of a growing interest in cybersecurity insurance as well as limitations in the current market – especially the first-party market.[1] To better understand those limitations and how a more robust market could help encourage better cyber risk management, NPPD hosted its first-ever Cybersecurity Insurance Workshop during the fall of 2012. NPPD had two main goals for the event: (1) determine what obstacles prevent carriers from offering more attractive first-party policies to more customers at lower cost; and (2) promote stakeholder discussion about how to move the market forward.

On October 22, 2012, NPPD hosted a diverse group of participants, registered on a first-come, first-served basis, from five stakeholder groups that included insurance carriers, corporate risk managers, information technology/cyber experts, academics/social scientists, and critical infrastructure owners and operators. Several federal agencies also sent representatives. As part of its planning, NPPD asked participants to nominate breakout group topics in order to develop the workshop agenda and ensure that it addressed matters of critical interest. Participants nominated the following topics, which focused specifically on the first-party insurance market: (1) Defining Insurable and Uninsurable Cyber Risks; (2) Cyber Insurance and the Human Element; (3) Cyber Liability: Who is Responsible for What Harm; (4) Current Cyber Risk Management Strategies and Approaches; (5) Cyber Insurance: What Harms Should It Cover and What Should It Cost; (6) Improving the Cyber Insurance Market: Stakeholder Roles and Responsibilities; and (7) Sequencing Solutions: How Should the Market Move Forward? Participants shared a myriad of views on these topics, all of which were included in a workshop readout report available at http://www.dhs.gov/publication/cybersecurity-insurance.

Based on participant comments during the fall workshop and on feedback received after the publication of the readout report, NPPD decided to focus its next cybersecurity insurance discussion on a topic that had repeatedly arisen: how to build more effective cyber risk cultures as a prerequisite to a stronger and more responsive first-party insurance market. NPPD interviewed fall workshop participants and conducted other research in order to identify the key "pillars" of such cultures, each of which would help frame the agenda for a future roundtable discussion in this area. Specifically, NPPD planned to ask a diverse set of stakeholders to describe the importance of and challenges with implementing the identified pillars in three distinct but related contexts: within companies; between partnering companies; and nationally. NPPD likewise planned to solicit opinions about how large, mid-

[1] First-party cybersecurity insurance policies cover direct losses to companies arising from events such as business interruption, destruction of data and property, and reputational harm. Third party policies, by contrast, cover losses that a company causes to its customers and others, such as harms arising from the exposure of personally identifiable information (PII) through a data breach. *See* U.S. Department of Homeland Security. *Cybersecurity Insurance Workshop Readout Report*. ONLINE. 2012. National Protection and Programs Directorate. Available: http://www.dhs.gov/publication/cybersecurity-insurance [10 June 2013].

size, and small companies should go about meeting those challenges given their typically very different levels of expertise and risk management resources.

About the Roundtable

On April 11, 2013, NPPD publicly announced its intent to convene the cyber risk culture roundtable through the Sector Outreach and Programs Division (SOPD) of NPPD's Office of Infrastructure Protection. On May 13, 2013, NPPD hosted a small set of participants, registered on a first-come, first-served basis, at the National Intellectual Property Rights (IPR) Coordination Center in Arlington, Virginia, for this purpose. The participants, representing each of the aforementioned stakeholder groups, discussed four pillars of effective cyber risk cultures that NPPD had identified through its research. They included the following:

- Engaged executive leadership
- Targeted cyber risk management education and awareness
- Cost-effective technology investments tailored to organizational needs
- Relevant cyber risk information sharing

The goal for the roundtable was to discuss each of these pillars in greater detail and to identify potential approaches that companies of all sizes could adopt into their respective cyber risk management strategies.

Prior to the roundtable, NPPD advised participants that their input during the event would be included in a final readout report on a non-attribution basis. NPPD explained that the purpose of the readout report would be twofold: (1) to capture diverse ideas about the importance of each of the cyber risk culture pillars and the challenges that they entail; and (2) to record a wide range of stakeholder perspectives about how companies could best move forward with them. NPPD advised the confirmed participants that it was not looking for, would not accept, and would not solicit group or consensus recommendations during the roundtable. NPPD likewise clarified that neither DHS nor NPPD would make any decisions about agency policy or positions during the event. In addition to 11 roundtable leaders, organizers, and support personnel, NPPD hosted 39 participants from the following stakeholder groups:

• Insurance Carriers:	11
• Corporate Risk Managers:	6
• Information Technology/Cyber Experts:	8
• Academics/Social Scientists:	3
• Critical Infrastructure Owners/Operators:	10
• Government:	1

EXECUTIVE SUMMARY

KEY TAKEAWAYS

For an increasing number of companies that have adopted enterprise risk management (ERM) strategies, cyber risks are converging with more traditional business risks for purposes of prioritization and mitigation. Insurance carriers accordingly don't rely solely on technical compliance with existing information security standards when assessing a company's qualifications for cybersecurity insurance coverage. Many instead examine its risk culture – paying particular attention to internal cybersecurity practices and procedures that the company has adopted, implemented, and enforced in the areas of executive leadership; education and awareness; technology; and information sharing. Some carriers in fact focus primarily on a company's risk culture as part of the cybersecurity insurance underwriting process – a practice that leads to the drafting of custom policies for clients rather than more generic template policies that could be marketed more broadly to others. Given this environment, roundtable participants focused their roundtable discussions on three principal topics: (1) the business case for pursuing more effective cyber risk cultures; (2) the need for cost/benefit research into the effectiveness of various cyber risk controls; and (3) "right sizing" the role of cybersecurity insurance as a driver for better cybersecurity practice across industry.

THE BUSINESS CASE

Participants reported that the business case for first-party cybersecurity insurance has, in many respects, not been made. They cited an excessive and ongoing focus on cyber-related threats and vulnerabilities as a big part of the problem, noting that cyber risk analysts typically target their products to information technology (IT) professionals who focus tactically on technical matters rather than boards of directors that make strategic risk management investments. Several participants asserted that to get board attention, analysts should concentrate on translating cyber risk into business terms that highlight (1) the financial and reputational *consequences* of cyber incidents; and (2) the likelihood of those consequences happening from a *corporate* – i.e., not government – perspective. This approach, they stated, could have very positive implications for both the "packaging" of cyber risk information and how organizations prioritize their specific cybersecurity investments in response. Many participants cited the benefits of ERM in this regard, noting that the discipline is well-suited to helping companies identify not only the particular cyber risks they face but also appropriate mitigations for them. Several participants likewise described a similar need to make the "business case" for cybersecurity to the general public through longer-term education and awareness campaigns. They asserted that both the private and public sectors should recruit marketing experts and leverage relevant social research to develop a series of messages designed to instill a national "culture of cyber vigilance" – one that leads individuals to reflexively incorporate good cyber hygiene into both their personal and work lives.

COST/BENEFIT RESEARCH

Participants likewise called for more research when it comes to the costs and benefits of existing and future cybersecurity solutions. Once boards of directors engage on the topic of cyber risk, they asserted, they're going to want to know what to invest in to better manage it. Several participants observed that there's a general lack of objective proof that particular controls – policies, processes, technologies, and otherwise – have measurable and positive risk management impacts. A number of participants suggested that currently available cybersecurity solutions should be inventoried and tested in a way that tells companies what amount of cybersecurity they'd likely "get" from which combinations of controls so they can make more informed risk management decisions. The problem, several commented, is that there hasn't been a common call for this kind of research because most boards of directors don't yet know they need it.

The Insurance Incentive

Finally, many participants commented that expecting the insurance industry to spearhead the development of best cybersecurity practices that companies should adopt in return for lower first-party policy premiums is probably unrealistic. They advised that carriers typically don't spend weeks with potential insureds reviewing every aspect of an organization to see what's happening with its implementation of information security policies. Several participants explained that what many carriers do look for, however, is how well a company understands where it sits uniquely in the cyber risk landscape and how it's addressing its vulnerabilities beyond basic cyber hygiene. Those carriers therefore may ask:

- Does the company know what cyber incidents it's actually experienced and is likely to experience in the future based on both its own data and reports from outside sources;
- As part of that inquiry, does the company know what cyber incidents are happening and are likely to happen to similarly situated companies; and
- What cyber risk management investments is the company making in response to address its own, unique circumstances?

In short, if companies exhibit *engaged* cyber risk cultures – where informed boards of directors support targeted risk mitigations to address their most relevant cyber risks – then most carriers will consider them to have *effective* cyber risk cultures worth insuring. Cyber risk therefore does not have a "one size fits all" risk management solution that companies can simply purchase off the shelf. Carriers instead will reward those companies that maintain a sustained focus on their unique cyber risk profiles and wisely arrange their executive leadership, education and awareness, technology, and information sharing strategies to address them. To support companies striving for this level of engagement, all stakeholders – including carriers – should continue the conversation about best cybersecurity practices in order to identify a full range of action options that organizations can tailor to their particular cyber risk management needs.

SECTION ONE: OPENING REMARKS

THEME I: WELCOME

SPEAKER: BRUCE MCCONNELL, ACTING DEPUTY UNDER SECRETARY FOR CYBERSECURITY
NATIONAL PROTECTION AND PROGRAMS DIRECTORATE
U.S. DEPARTMENT OF HOMELAND SECURITY

KEY POINTS:

- Acting Deputy Under Secretary for Cybersecurity Bruce McConnell opened the roundtable by welcoming participants and observing that data breaches and other cyber-related losses continue to dominate the news. He specifically cited recent reporting about cyber-enabled bank thefts, intellectual property theft, and potentially destructive attacks against critical infrastructure. Mr. McConnell noted that, given this environment, it's not surprising that funding for the federal government's cybersecurity missions continues to be protected and increased in some cases. He referenced both Executive Order 13636 and Presidential Policy Directive 21 (PPD-21) as further evidence of the federal emphasis on cybersecurity, and discussed their general implications for cybersecurity policy and practice going forward.

- Acting Deputy Under Secretary McConnell then discussed Executive Order 13636's three core themes: (1) "building in" privacy as part of private and public sector cybersecurity efforts; (2) improving information sharing from the federal government to the private sector; and (3) protecting the nation's critical infrastructure. Regarding this third pillar, he noted that the Executive Order directs the National Institute of Standards and Technology (NIST) to develop, with extensive public input, a voluntary Cybersecurity Framework. That Framework, Mr. McConnell continued, will likely include not only technical controls but also other cybersecurity solutions such as alternate-provider agreements and personnel policies. The goal of both the Executive Order and the Framework, he explained, is to elevate the cyber risk management conversation in non-technical terms to senior executives in both the private and public sectors. He also mentioned that NIST would be hosting its next Framework workshop in Pittsburgh on May 29-30, 2013.

- Acting Deputy Under Secretary McConnell next noted that Executive Order 13636 directs the DHS and the Departments of Commerce and Treasury to prepare studies that examine market-based incentives that could encourage industry to adopt the Cybersecurity Framework. He stated that a wide range of potential incentives are under consideration – including good housekeeping seals of approval; changes to statutes to create safe harbors, and others. Mr. McConnell advised that the studies would be shared with the White House for review and publication.

- Acting Deputy Under Secretary McConnell also discussed PPD-21, commenting that it replaces Homeland Security Presidential Directive 7 (HSPD-7) that focused on counterterrorism. He explained that PPD-21 extends beyond standard protection activities to the promotion of a more holistic national resilience strategy, or "how we will operate under degraded conditions." He stated that PPD-21 takes an all-hazards approach to critical infrastructure security and resilience, including terrorism, extreme weather, and cybersecurity risks.

- Acting Deputy Under Secretary McConnell concluded his remarks by describing the roundtable as an opportunity to focus on an important and long-term matter: how to enhance the cybersecurity insurance market by developing a better understanding of the elements of an effective cyber risk culture. He stated that the roundtable would be a good opportunity to engage a cross-section of DHS partners and to share information that is often stovepiped within organizations. By so doing, participants can help identify common cyber risk management best practices that should be adopted by large, mid-size, and small companies alike.

THEME II: IMPORTANCE OF EFFECTIVE CYBER RISK CULTURES TO CYBERSECURITY INSURANCE MARKET

SPEAKER 1: LAURIE CHAMPION
MANAGING DIRECTOR, ENTERPRISE RISK MANAGEMENT
AON RISK SOLUTIONS, GLOBAL RISK CONSULTING

KEY POINTS:

- Ms. Champion described the October 2012 DHS Cybersecurity Insurance Workshop as both "very engaged" and an important opportunity for people from different backgrounds to discuss current challenges to the cybersecurity insurance market. She added that many conversations that began at the session – during formal sessions and informal sidebars – have continued to this day. Ms. Champion then made three general observations about the conversations:

    - Responsibility for Cyber Risk. Participants did not agree about who "owns" cyber risk – not only within companies but also externally at the "macro" level. For example, Ms. Champion noted that participants debated whether cyber risk should be owned by the private sector, the public sector, or shared by both. The answer to this question, she noted, will have implications for other factors including proactive cyber risk management activities, including threat information sharing, cost sharing, and the development and implementation of solution sets.

    - Enterprise Approach to Cyber Risk Management. Participants mentioned but did not flesh out ideas regarding enterprise approaches to identifying cyber risks and prioritizing action and investments to address them. Going forward, Ms. Champion commented, representatives from corporate management, the IT community, and multiple enterprises should consider convening a "what are we dealing with" conversation that defines the problem in business terms. Once the problem is better understood, she continued, those same representatives should consider hosting a similar "what should the solution be" discussion.

- Nature of Cybersecurity Insurance. Participants agreed that cyber risk involves not only third-party data breach but also first-party financial, reputational and other harms. Ms. Champion commented that although the participants cited cybersecurity insurance as a potential "solution" to these potential losses, a core issue remained unresolved: should cybersecurity insurance be seen as a solution in its own right or only as a backstop when other risk management strategies have failed? Ms. Champion explained that the first approach might encourage business leaders to see cybersecurity insurance carriers as a source of identifying and understanding cybersecurity best practices that they would incentivize companies to adopt by offering them lower premiums in return for demonstrated compliance. The second approach, she added, would encourage management to first understand and mitigate their known cyber risks before seeking to transfer any residual risk through the purchase of an appropriate policy. In practical terms, she concluded, both insurers and insured (companies or other organizations) have a role to play in understanding and mitigating cyber risk.

- Ms. Champion then stated that participants had spent considerable time during the workshop discussing the role of leadership in promoting organizational resiliency. She noted that the remaining challenges in this area include identifying best practices for translating technical cyber risk information into business terms that senior executives can better understand, developing cyber risk solution sets, and driving industry toward implementation of practical solutions.

SPEAKER 2: OLIVER BREW
VP, SPECIALTY CASUALTY DIVISION
LIBERTY INTERNATIONAL UNDERWRITERS

KEY POINTS:

- Mr. Brew commented that it's taken quite a while for the cybersecurity insurance market to reach critical mass despite the fact that many of the risks that arise in cyberspace are not new (e.g., intellectual property theft, lost profits, privacy, and reputational damages). Rather, he stated it is simply that there are new methodologies within the networked economy within which these traditional risks can arise. Mr. Brew then quoted Facebook COO Sheryl Sandberg who stated in reference to the high growth technology industry, "If you are offered a seat on a rocket ship, don't ask which seat; just get on." In contrast, Mr. Brew noted, the insurance industry hasn't been known for its dynamism when addressing cyber risk but is gradually finding its feet and becoming more innovative regarding the cybersecurity insurance market.

- Mr. Brew observed that there's no single answer to the question of why the first-party market has not developed more rapidly, a confounding phenomenon given growing awareness in most quarters about the cyber risk environment. He cited the ubiquity of network computing and

Moore's Law[2] before observing that (1) cyber threats continue to grow; (2) media coverage about cyber incidents is increasing; (3) related legislative efforts have been and continue to be highly publicized; and (4) cyber-related litigation has become more common. Mr. Brew offered several reasons why more customers, despite these trends, may not be seeking coverage:

  - Cost and Revenue Concerns. Companies always review new money spent. The insurance market is itself cyclical, and some potential customers see cybersecurity insurance as a luxury purchase rather than a core portfolio item.

  - Uncertainty. Some potential customers question whether cybersecurity insurance carriers will actually "pay out" after a cyber event. As a result, they are reluctant to dive into what they consider to be an untested market.

  - High Risk Appetites. Entrepreneurs, especially in the technology field, are inherent risk takers. Some consequently forego cybersecurity insurance coverage because they don't see it as a necessary investment.

  - Maturity. Awareness and incentives structures that address cyber risk exposure have not fully matured, and most companies remain unaware of the availability of cybersecurity insurance.

- Mr. Brew asserted that, over time, the insurance industry can help change cyber risk management behavior for the better. A more mature cyber risk culture, he explained, could benefit society in much the same way that automobile and fire insurance already benefit individual consumers. For example, Mr. Brew continued, careful drivers and homeowners who install smoke alarms qualify for premium discounts and other benefits under their policies. He advised that the unmet challenge to the cybersecurity insurance market – especially the first-party market – is that carriers and other stakeholders have yet to identify consistent cyber risk trends and the safeguards that organizations can implement in order to best manage them.

- Mr. Brew then cited Verizon's 2013 Data Breach Investigations Report and noted its finding that 90 percent of cyber attacks over the previous year were preventable with simple or intermediate systems in place.[3] Under the circumstances, he asserted, there's clearly room for improvement in most organizations when it comes to cyber risk management.

[2] A simplified version of Moore's Law, a computing term which originated around 1970, states that processor speeds, or overall processing power for computers, will double every two years. *See Moore's Law*. ONLINE. N.D. Moore's Law. Available: http://www.mooreslaw.org/ [11 June 2013]. More precisely, Moore's Law states that the number of transistors on an affordable central processing unit (CPU) will double every two years. *Id.*

[3] This statistic refers only to the number of cyber attacks in 2012 and not to any measure of consequences. *See* Verizon. *2013 Data Breach Investigations Report*. ONLINE. 2013. Verizon RISK Team. Available: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf [18 June 2013].

- Mr. Brew concluded that while private and public sector organizations likely can't stop all attacks, they could do more to prevent and/or mitigate them by addressing the four pillars of an effective cyber risk culture as outlined in the roundtable agenda: leadership (responsible for setting an example and enterprise-wide cyber risk management expectations); education and awareness (required to instill an understanding of basic cyber hygiene); technology (designed to promote security and to protect privacy); and information sharing (essential to inform cyber risk management activities within organizations, among them, and between the private sector and government). The critical factor, he added, is that all pillars are symbiotic and rely on each other to be effective.

SPEAKER 3: JAKE KOUNS
CEO
OPEN SECURITY FOUNDATION

KEY POINTS:

- Mr. Kouns opened his remarks by citing both a Gartner report estimating that worldwide security spending would hit $85 billion by 2016,[4] and Director of National Intelligence James Clapper's recent comments describing cyber attacks by non-state actors as a leading worldwide threat to U.S. security.[5] He stated that experts at Risk Based Security had assessed 2012 to be the worst year on record for data breaches and that they expected more such breaches, involving ever-increasing amounts of personally identifiable information (PII), in 2013.[6]

- Mr. Kouns commented that the IT vulnerabilities that have led to this state of affairs have shown almost no signs of improvement over time and cited both cross site scripting (CSS or XSS) and structured query language (SQL) injection as just two examples of well-known and as yet unresolved cyber attack methods.[7] He added that the Open Sourced Vulnerability Database, a

[4] *Global Security Spending to Hit $86B in 2016*. ONLINE. Sept. 12, 2013. Associated Press. Available: http://www.infosecurity-magazine.com/view/28219/global-security-spending-to-hit-86b-in-2016 [11 June 2013].

[5] Dozier, Kimberly. *U.S. Intel Chief: Cyberterror Leading Threat*. ONLINE. April 11, 2013. Associated Press. Available: http://bigstory.ap.org/article/us-intelligence-chief-cyberterror-leading-threat [11 June 2013].

[6] *See* Risk Based Security/Cyber Risk Analytics at https://cyberriskanalytics.com.

[7] Cross-site scripting is a vulnerability in web applications which attackers may exploit to steal a user's information. The National Institute of Standards and Technology (NIST) defines cross site scripting (CSS or XSS) as "[a] vulnerability that allows attackers to inject malicious code into an otherwise benign website. These scripts acquire the permissions of scripts generated by the target website and can therefore compromise the confidentiality and integrity of data transfers between the website and client. Websites are vulnerable if they display user supplied data from requests or forms without sanitizing the data so that it is not executable." *See* U.S. Department of Commerce. *NIST IR 7298 Revision 2, Glossary of Key Information Security Terms*. ONLINE. May 31, 2013 [sic]. National Institute of Standards and Technology. Available: http://csrc.nist.gov/publications/drafts/ir-7298-rev2/nistir7298_r2_draft.pdf [18 June 2013]. By contrast, structured query language injection is a code injection technique that exploits a security vulnerability occurring in the database layer of an application. The Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) defines structured query language (SQL) injection as "an attack technique that attempts to subvert the relationship between a webpage and its supporting database, typically in order to trick the database into executing malicious code. SQL injection usually

project that provides unbiased technical information about security vulnerabilities, identifies anywhere from 7,600 to 9,000 new vulnerabilities each year that enable such attacks.[8]

- Mr. Kouns next discussed Metasploit, which he described as a successful open source penetration testing platform created by HD Moore that has helped turn once complicated cyber attacks into more of a "point and click" exercise for even unsophisticated actors. He then referenced HD Moore's Law for the proposition that "casual attacker power grows at the rate of Metasploit."[9] In other words, better and better cybersecurity is needed in order to protect against even inexperienced attackers who are becoming increasingly capable of exploiting known IT vulnerabilities.

- Mr. Kouns also raised a philosophical question to help frame the roundtable agenda: should companies focus their cyber risk management efforts on patching vulnerable IT products, or should IT manufacturers and suppliers instead focus on poorly written code before bringing their products to market? He observed that shifting more attention to poorly written code might be appropriate given the fact that the number of IT vulnerabilities – and the corresponding security costs to address them – continue to rise.

- Mr. Kouns likewise noted that effectively leveraging technology to manage cyber risks remains an ongoing challenge. He cited Wendy Nather for the proposition that many organizations are "living below the security poverty line," explaining that the cybersecurity budgets for many mid-size and small companies are practically nonexistent.[10] As a result, he continued, those companies often have little or no IT expertise, are unable to follow through on IT consultant recommendations, and accordingly focus only on "putting out fires" rather than managing long-term cyber risk issues. Mr. Kouns observed that companies that seek to adopt layered cybersecurity approaches typically find themselves in need of numerous cybersecurity products and stated that each such system costs $2000 or more – making fully implemented, layered cybersecurity far more the industry exception than the industry rule.

- Mr. Kouns then described today's cybersecurity reality in stark terms. He asserted that limited technology solutions exist for addressing cyber risks. Most vendor options typically fall short of

involves a combination of over-elevated permissions, unsanitized/untyped user input, and/or true software (database) vulnerabilities. Since SQL injection is possible even when no traditional software vulnerabilities exist, mitigation is often much more complicated than simply applying a security patch." *See* U.S. Department of Homeland Security. Structured Query Language Injection. ONLINE. 2009. United States Computer Emergency Readiness Team. Available: http://www.us-cert.gov/sites/default/files/publications/sql200901.pdf [11 June 2013].

[8] *See* Open Sourced Vulnerability Database at http://www.osvdb.org.

[9] Corman, Joshua. *Intro to HDMoore's Law*. ONLINE. Nov. 1, 2011. Cognitive Dissidents Blog. Available: http://blog.cognitivedissidents.com/2011/11/01/intro-to-hdmoores-law/ [27 June 2013].

[10] Nather, Wendy. *Living Below the Security Poverty Line*. ONLINE. May 26, 2011. 451 Research. Available: https://451research.com/report-short?entityId=67682 [11 June 2013].

needed protection, he continued, and they don't seem to be improving. Technical controls, he added, are often too complicated and/or costly for businesses to implement. He noted that the lack of available information about which cyber risks are most likely to materialize only compounds these problems. Without more security intelligence, he concluded, most organizations cannot make informed decisions about where to best spend their limited cybersecurity budgets.

- Mr. Kouns commented that given this landscape, some companies may be inclined to buy cybersecurity insurance rather than spend on technology solutions and other cybersecurity controls. In short, he stated, they may opt to transfer risk entirely rather than invest in expensive and largely unproven cyber risk mitigation efforts. He concluded that without minimum underwriting requirements by carriers, this phenomenon could give rise to a moral hazard situation that encourages companies to take further risks rather than improve their cyber risk cultures.

SECTION TWO: EFFECTIVE CYBER RISK CULTURE PILLAR DISCUSSIONS

PILLAR I: THE ROLE OF EXECUTIVE LEADERSHIP

DESCRIPTION: Getting boards of directors and other corporate executives engaged on the subject of cyber risk management presents a major obstacle to promoting a more robust cybersecurity insurance market. In many companies, especially mid-size and small firms, cybersecurity is too often thought of as an operational IT problem rather than a longer-term, enterprise risk management issue. The purpose of this pillar discussion accordingly was to explore stakeholder viewpoints on how to break through barriers that prevent companies from addressing cyber risk more effectively through comprehensive risk management approaches.

DISCUSSION POINTS:

RISK MANAGEMENT RESEARCH

- A risk manager commented that most corporate leaders, especially at the board level, don't actively engage on cybersecurity issues – a situation that presents a major obstacle to better cyber risk management across the business world. She then discussed this point in relation to research she had conducted with the Wharton School that focused on how corporate leaders impact the development of effective risk cultures generally. Part of that research, she explained, involved comparing companies that exhibit both "above average" and "below average" risk management maturity/capability as determined by a five-point scale. That scale, she advised, included 120 questions that measured indicators such as governance; process/methodology; integration of risk information; and organizational culture/leadership. Certain behaviors, the risk manager explained, correlated with better risk management. For example:

  - 92 percent of above average organizations reported that they communicate risk management information throughout their enterprises and act upon it. Among below average companies, by contrast, 63 percent reported that they don't communicate or act upon such information.

  - 89 percent of above average organizations reported that they actively decide how much risk to take in any given business situation. Among below average companies, by contrast, 60 percent reported that they don't actively engage in such decision-making.

  - 88 percent of above average organizations reported that they incorporate risk management plans into their resource allocation processes, budgets, performance plans, and execution plans. Among below average companies, by contrast, 66 percent reported that they don't incorporate risk management plans into these areas.

- The risk manager noted that while this research wasn't directly tied to cybersecurity, she expected that companies with more mature risk management processes would likely be the companies that managed cyber risk best.

ENGAGING EXECUTIVES

- A critical infrastructure representative commented that money and fear of loss are the biggest factors that get board of director attention. To focus boards on cyber risk management, she continued, risk managers and IT professionals must make cyber risk understandable in terms of both financial and reputational impact. The representative explained that such impacts are often easily understood; for example, the costs associated with a PII breach in the health care industry – including fines and penalties, credit monitoring services for affected parties, and "active imaging" (public relations/reputation response) – are as significant as they are concrete. Experience is the greatest educator in this regard. Put simply, she stated, executives will be highly motivated to address cyber risk after their company incurs sizable cyber-related losses even just one time. The representative illustrated her point by observing that while health care companies today use both cybersecurity and personal information liability insurance, they began doing so only after senior executives came to understand the enormous costs that could arise if a cyber attacker accessed and changed patient medical records.

- A second critical infrastructure representative noted that if IT professionals, risk managers, and others can explain the financial and reputational impacts of cyber risks to corporate leaders, those leaders will be less likely to look at cyber risk as just a technical problem in need of a technological solution. Instead, he asserted, they will look more holistically at cyber risk and will seek a broader risk solution that includes an examination of the human element and other factors. An IT professional concurred and noted, "Being able to show a board of directors or senior leadership that a given potential threat impacts the risk state of a company in a particular way has much more meaning to those individuals than simply providing them a detailed technical analysis of the threat."

- A third critical infrastructure representative agreed that whether or not boards of directors accurately perceive and prioritize cyber risk depends upon their company's actual, real-life exposure. He stated that every company is its own best intelligence source in this regard, explaining that the best way to engage boards is to give them a "what do I look like" understanding of what's happening within their own companies. That picture, he continued, emerges from the volumes of breach and other incident data stored within a company's own audit logs. The representative concluded that most boards don't have a way to meaningfully access that information and, in some cases, don't want to know. A fourth critical infrastructure representative concurred, adding that only when leaders see themselves in the risk – e.g., in terms of personal financial or criminal liability – does it change their perception and motivation to engage the risk. A fifth critical infrastructure representative countered, however, that most board members do understand the stakes because they typically serve on the boards of multiple companies, at least some of which have experienced a major cyber incident.

Cyber Risk as Enterprise Risk

- A critical infrastructure representative commented that an enterprise risk management (ERM) approach is essential for getting cyber risk discussions "out of the technology stovepipe and into an organization's broader risk management process."[11] The common vernacular, priorities, and solutions that come with ERM, he explained, make all the difference in the world. The representative added that incorporating cyber risk into a broader ERM strategy will help promote discussion beyond its technical/technological aspects to its impact on a company's other business concerns – including customer satisfaction, reputation, sales, and supply chain resilience. Those discussions, he continued, must engage both corporate leadership and legal counsel. The representative emphasized that a mature ERM program involves not only the identification and prioritization of cyber risks in relation to a company's other risks but also potential solution sets designed to address those cyber risks. An insurer concurred, noting that those solution sets might include communications, compliance, insurance, public relations, technology, and other options. Too often, he observed, companies fail to extend ERM prioritization to the solution set side of the equation.

- An insurer commented that ERM is critical for building a culture that actively searches for problems versus a culture that is fearful of discovering them. Actively searching for problems, he asserted, gets to the heart of what companies should be striving toward in order to build effective cyber risk cultures. A critical infrastructure representative agreed, noting that ERM approaches applied in this space will help senior executives both better relate to cyber risk and more fully understand their company's level of cyber risk management maturity.

- An insurer stated that a key factor for assessing this maturity includes the extent and quality of a company's internal information sharing about cyber risk – including, especially, the degree to which it's examined as a cross-cutting, inter-departmental matter. This one factor, he asserted,

[11] The Risk and Insurance Management Society (RIMS) defines enterprise risk management (ERM) as "a strategic business discipline that supports the achievement of an organization's objectives by addressing the full spectrum of its risk and managing the combined impact of those risks as an interrelated risk portfolio." Risk and Insurance Management Society. *What is ERM?* ONLINE. N.D. Available: http://www.rims.org/ERM/Pages/WhatisERM.aspx [10 June 2013]. RIMS further described ERM as a "significant evolution beyond previous approaches to risk management" because it "(1) encompasses all areas of organizational exposure to risk (financial, operational, reporting, compliance, governance, strategic, reputational, etc.); (2) prioritizes and manages those exposures as an interrelated risk portfolio rather than as individual 'silos'; (3) evaluates the risk portfolio in the context of all significant internal and external environments, systems, circumstances, and stakeholders; (4) recognizes that individual risks across the organization are interrelated and can create combined exposure that differs from the sum of the individual risks; (5) provides a structured process for the management of all risks, whether those risks are primarily quantitative or qualitative in nature; (6) views the effective management of risk as a competitive advantage; and (7) seeks to embed risk management as a component in all critical decisions throughout the organization." *Id*.

represents the critical difference between organizations that "get it or don't get it." The insurer observed that in most companies, internal information sharing about cyber risk significantly lags information sharing about other risks – a major blind spot within otherwise comprehensive risk management strategies. He noted that companies that have overcome this deficiency tend to be regulated companies. As an example, he cited the uptick in the number of reported data breaches involving personal health information (PHI) following the passage of state data breach notification laws.

- An IT professional noted that the IT community needs to step up in this regard. One tactic used by security folks for years, he explained, was that of fear, uncertainty and doubt – or "FUD" for short. The IT professional commented that whether they used FUD to procure more funding, or simply to show corporate leadership how difficult IT problems actually were, they did themselves a disservice by not casting cyber risk in business terms. He added that he still sees IT professionals in some immature organizations using FUD to emphasize the importance of cyber incidents reported in the news. In a similar fashion, he reported, certain cybersecurity providers use FUD in their messaging to corporate leaders in order to market their products. Whatever the motivation, the IT professional concluded, FUD has little place in the cybersecurity decision-making process because it does little to address the full spectrum of cyber risk.

Applying ERM to Cyber Risk

- An IT professional stated that in his company, which has an active ERM program, he has direct access to the board of directors and educates them about cyber risk. He noted that he had worked in other organizations where the Chief Information Officer (CIO) was buried several levels below the board, a situation where alternate routes to senior leadership became essential. Specifically, the IT professional explained, the best option under those circumstances involved establishing an effective chain of command populated with people who understood not only the risk but also his need to (eventually) engage senior leadership. Without the ability to communicate with the board, he concluded, CIOs often find themselves in a "red light running" situation where it becomes the norm to run red lights because the board takes notice only when a cyber "accident" happens.

- A risk manager stated that the board of directors in his company began prioritizing cyber risk management only after the General Counsel explained various liability issues associated with data breaches and other potential cyber events. With this input, he continued, the board directed senior management to develop policies and procedures for mitigating his company's cyber risk. The IT professional added that to generate and hold this kind of board attention going forward, the CIO and/or his or her deputy must have direct access to the board. To do so, he recommended that an executive risk committee be established to brief the board at least annually about the organization's cyber risk exposure. The IT professional asserted that the executive risk committee should be comprised of both senior risk managers and a diverse set of "risk owners" – a feature that will allow people with less corporate stature to be heard by the board. He then commented that the executive risk committee must present cyber risks from an enterprise perspective, using business language, in order to cross-pollinate relevant risk information, raise awareness, and engage others to develop enterprise-wide solution sets. Finally, the IT professional stated that the composition of the board itself is critical for addressing cyber risk. He observed that board members must not only be sufficiently aware of how a company's cyber risk profile is evolving but also have the "backbone" to confidently direct that risk management action be taken.

- A risk manager agreed and commented that an ERM program that assesses all of a company's risks horizontally across the organization avoids situations where risk owners focus myopically on their own domains. ERM, he added, helps boards of directors and senior executives overcome the all too easy approach of turning to the CIO to address all cyber risks. Instead, ERM frames the risk in an "entire enterprise" context.

- A critical infrastructure representative commented that in order to firmly incorporate cyber risk as part of an effective ERM strategy, IT professionals, risk managers, and others must use appropriate buzzwords that boards of directors and senior executives will understand. He added that in his company, cyber risks are therefore cast in terms of potential harm to reputation, market cap, and investment.

- An insurer emphasized the importance of building an effective cyber risk culture on a firm ERM foundation. He commented that asking "who is the risk owner" is the wrong question. Instead, an ERM practitioner should properly ask: who are the multiple risk *owners*? The insurer then provided an example. When a corporate CIO and/or CSO submits a report to the board about the potential consequences of a cyber risk, he advised, he or she should also solicit General Counsel input on related legal liability issues. Given the tremendous weight that corporate executives give to their legal departments, he added, the CIO and/or CSO should then have counsel actually co-sign the document. The insurer asserted that a successful ERM-based approach should not stop there. On the contrary, he continued, the heads of all internal departments affected by a cyber risk should also contribute to the report in order to explain how it implicates their equities. Those department heads, he concluded, should likewise co-sign the report.

- Another insurer agreed with this ERM implementation approach and stated that companies should originate their questions about technology from *outside* their IT departments. "Let the non-techies ask the basic questions and let IT respond," he asserted. The insurer commented that companies should adopt this approach because no department should lead a risk inquiry into itself.

- A third insurer added that to increase the amount of information available about cyber risk, the Securities and Exchange Commission (SEC) should start investigating companies that have blatantly not disclosed material cyber risks.

ERM Challenges

- Several participants commented that ERM programs have not always delivered on their promise given a variety of implementation and interpretation issues.

- A critical infrastructure representative stated that the initial wave of ERM in her organization didn't feel very effective and that people found themselves following multiple documenting processes that never led to actual risk management activity. "It turned people off," she commented, "and didn't translate into their everyday jobs." The representative added that ERM done right should flesh out high-level cyber risk solution sets into actionable business decisions that everyone within an organization can understand and implement.

- In a similar vein, an IT professional warned that ERM for some companies results in nothing more than a "massive risk register" in which everything under the sun becomes a risk. He encouraged ERM experts to "right size" ERM in a way that not only identifies cyber and other risks but also prioritizes them against each other and otherwise makes the business case for action. A critical infrastructure representative agreed with this concern, stating that his company's ERM efforts initially resulted in the development of a lengthy risk register that initially went nowhere. He explained, however, that his company subsequently prioritized key risks on the register and has now developed prescribed actions for employees to take in order to address them. The representative described this change as a "cultural shift."

- An IT professional responded that there's still no good way of quantifying and prioritizing cyber risk. Until an effective methodology for determining the consequences of a cyber event and the likelihood of their happening exists, he commented, both the credibility of cyber risk warnings and the case for making related cyber risk management investments will remain in doubt. The IT professional explained that, at the end of the day, boards of directors want reliable data about cyber risk – not "Chicken Little" warnings. If cyber becomes a credible, existential threat to businesses, he concluded, they'll become much better at managing these risks.

- A risk manager asked the participants if they thought small companies could effectively manage cyber risk without a large ERM program in place. One critical infrastructure representative responded affirmatively – so long as they have effective cyber risk cultures. Another critical infrastructure representative disagreed, arguing that a company's size and resources have a big impact. He asserted that many mid-size and small companies struggle with implementing ERM because they don't enjoy economies of scale that would otherwise allow them to fund robust ERM programs; they typically don't understand ERM language; and they haven't received formal training to maintain ERM over the long term. A third critical infrastructure representative agreed, commenting that a “strong dichotomy” is emerging between ERM and cybersecurity haves and have nots – those who have the capability and resources to address cyber risk as part of a larger risk management paradigm and those who are lost and at risk. He added that mid-size and small companies nevertheless can be secure – to a point – but would benefit from some kind of over-arching support structure that pools know-how, skills, and other resources about both ERM and IT security.

ERM Versus Strict Criteria Approaches

- One critical infrastructure representative whose organization advises and represents a number of companies in the same sector stated that his organization chose to develop baseline cybersecurity standards rather than rely exclusively on ERM approaches. He explained that early ERM implementation efforts among companies in his sector allowed them to remain “sovereign” and to accordingly assess very similar risks very differently. The representative stated that given the resulting disparities, the companies ultimately agreed that some fundamental risks within the sector – e.g., Supervisory Control and Data Acquisition (SCADA) system risks – should be addressed uniformly through “bright line” criteria that automatically characterize certain conditions as requiring mitigation.[12] He advised that the criteria, which have been in place for approximately five years, establish a security floor that companies are free to exceed using ERM and other risk management approaches. The representative added that companies undergo regular compliance audits on the criteria.

- A social scientist expressed reservations about this approach. He asked the critical infrastructure representative if compliance with the bright line criteria actually improves cybersecurity and, if so, how the sector measures those improvements. “If no one is measuring the outcomes,” he asked, “what is the purpose?” The representative responded that, as a general matter, compliance with common criteria fosters a certain level of security within an industry if they’re well written and are directed to commonly shared risks. He described the criteria in his specific sector as effective. A second critical infrastructure representative responded that measuring the success of any risk management approach – criteria-based or otherwise – ultimately depends on the desired outcome. It’s difficult to find objective measures, he observed, because we can’t agree on what outcomes we want. An IT professional agreed and cautioned that the sector under discussion might not be an exemplar for other sectors because of its unique attributes.

[12] DHS defines a supervisory control and data acquisition (SCADA) system as “a generic name for a computerized system that is capable of gathering and processing data and applying operational controls to geographically dispersed assets over long distances.” U.S. Department of Homeland Security. *Explore Terms: A Glossary of Common Cybersecurity Terminology*. ONLINE. N.D. United States Computer Emergency Readiness Team. Available: http://niccs.us-cert.gov/glossary#letter_s [17 June 2013].

- A risk manger asked if it might make sense for all sectors to (1) establish minimum cybersecurity requirements that companies should meet based on their size and scope; and (2) create frameworks and roadmaps that companies should use to fulfill those requirements. An insurer responded that regulations and standards exist for a reason, and that some are better than others. He concurred that companies should focus on (1) getting their organizations into compliance with at least some minimum cybersecurity standard; and (2) figuring out how to improve on such a standard on their own. A critical infrastructure representative doubted the efficacy of this approach, however, citing both the general lack of available cybersecurity standards as well as the lack of maturity of most organizations to comply with even those that do exist. He recommended that companies instead focus on building knowledge bases within their organizations about cyber risk and incentivizing good and specific behavior by employees to address them.

ERM, Information Sharing, and Insurance

- An insurer explained that a company's purchase of cybersecurity insurance doesn't always go hand in hand with risk management. On the contrary, he asserted, many companies – including well-funded organizations – initially believe that they won't be the victims of a cyber attack or that they can forego coverage until something actually happens. For example, the insurer continued, his company has many clients who first explore insurance, choose not to buy, experience a data breach, and only then return to purchase a policy. He noted that while the value of the lost data and the response costs are often the prime motivators for a purchase in these circumstances, the true costs go far beyond those narrow categories and include lost business/profits, damaged reputations, and other first-party damages as well. The insurer observed that the real differentiator between those who purchase before an incident and those who don't is whether a company maintains a centralized ERM structure for risk management and cyber risk information sharing. He concluded that more facts about cyber risk, coupled with greater awareness within companies and across society about their costs, are necessary to encourage greater adoption of ERM strategies and the incorporation of cyber risk within them.

- A critical infrastructure representative concurred, emphasizing that building an effective cyber risk culture is about more than education. He advised that in addition to giving employees information about cyber risk, companies must also create conditions that make them want to act on that information. The representative stated that a risk culture that clarifies why certain cyber risk management activities, practices, and protocols are required is an important first step toward incentivizing employees to do the right thing. A second critical infrastructure representative agreed with the cultural aspect of the cybersecurity challenge and commented that enhancing a company's risk management practices in this area goes directly to an organization's DNA: its identity and what it stands for as an enterprise.

- A third infrastructure representative agreed that information sharing about cyber risk is the key to building more effective cyber risk cultures that, in turn, will promote the development of a more robust cybersecurity insurance industry. The more public cyber incidents become, he noted, the more cyber "norms" become apparent. The representative added that once that happens, companies can better assess how much cyber risk they're willing to tolerate. He then commented that that awareness will help carriers determine what kinds of cybersecurity insurance policies they should write. The representative concluded that large enterprises need to figure out how to protect other companies that don't have the resources to insure and protect themselves.

- Another critical infrastructure representative stated that cybersecurity insurance doesn't cover mid-size and small companies because they typically can't comply with even the basic standards that policies require. He asserted that this presents a "double whammy" for those companies when competing for business: they can't keep up with large companies that *can* afford to meet standards (and differentiate themselves from mid-size and small companies accordingly) and they consequently don't have the coverage they need when cyber attackers strike. An insurer challenged this assessment, asserting that carriers are eliminating "maintain reasonable practices" language from policies so they can provide coverage to mid-size and small companies. He added that carriers have gotten better with underwriting over the last several years, resulting today in an insurance market that not only better matches needs but also removes the most onerous barriers to market entry.

- An insurer concluded that boards of directors and corporate leaders need to approach cybersecurity as a carrot, stick and culture challenge. Carrot and stick incentives modify behavior in the short term, he noted, but only lay the groundwork for an enduring and effective cyber risk culture. The insurer commented that although ERM approaches often take a long time to bring such cultures about, they're well worth it. Once instilled, he observed, they'll never go away. The insurer noted, for example, that if a company believes it has a moral obligation to protect the PII it maintains, it will make cybersecurity a priority for everyone at all levels of the enterprise.

Unique Challenges for Unique Cultures

- An IT professional asserted that while ERM principles work for most companies within most sectors, how and to what extent large, mid-size, and small companies implement them will vary considerably. He added that corporate executives need to assess not only the consequences a particular cyber risk might have on their companies but also the likelihood that those consequences will actually occur. The goal of an effective ERM program, he continued, should be to minimize not only legal risk and associated liability costs but also – and more fundamentally – to drive better cybersecurity. The IT professional observed that compliance with just a strict set of standards doesn't mean security; on the contrary, he added, in some cases it can mean "anti-security." The IT professional concluded that ERM, done right, offers companies sufficient flexibility to avoid such negative outcomes.

- A critical infrastructure representative agreed with this assessment, noting that the probability that a company will be breached often depends on who the company is – for example, how well-known and/or how popular or unpopular it is with the public. These factors, he continued, need to be considered individually by each company during its ERM risk and solution set identification and prioritization process.

PILLAR II: THE ROLE OF EDUCATION AND AWARENESS

DESCRIPTION: In order to build more effective cyber risk cultures as a foundation for a more robust cybersecurity insurance market, education and awareness campaigns about cyber risk and the roles and responsibilities of individuals and organizations in addressing it should occur at multiple levels. To this end, many observers assert that companies should not only take action within their own organizations on this front but also encourage their business partners to do the same. More broadly, and longer-term, they note that education and awareness campaigns should also happen at a societal level in order to establish a national "ethos" of cybersecurity. The purpose of this pillar discussion accordingly was to obtain participant viewpoints on this topic and how such campaigns should proceed.

DISCUSSION POINTS:

RAISING THE PROFILE

- An insurer asked participants for their opinions about what approaches might be most effective for building better cyber risk education and awareness programs and suggested several potential themes for discussion. Citing the success of the Smokey the Bear forest fire awareness campaign, he first asked if some kind of "Sam the Safety Robot" equivalent could be used to message the importance of more effective cyber risk cultures. The insurer next mentioned that a secondary motive behind state data breach disclosure laws had been to raise the profile of risk management cultures surrounding data protection. He observed that those laws have encouraged companies to prioritize the development of best practices in this area, even in the absence of national data breach management legislation. Finally, the insurer brought up the issue of proportionality: the idea that mid-size and small companies, given budget and other constraints, don't have the same cybersecurity capabilities as their larger counterparts. On the other hand, he noted, the likelihood of those companies coming under cyber attack in the first place might be proportionally less given their relative anonymity.

CYBERSECURITY CAMPAIGNS

- An IT professional responded that Smokey the Bear, "Duck and Cover" drills during the Cold War, and the "Buckle Up" car safety campaign all had something in common: a known enemy with known consequences. He observed that cyber risk is far more systemic, and that potential enemies and consequences are legion. The IT professional asserted that planners behind future cybersecurity education and awareness campaigns therefore must determine early in their work who they want to target with their messages and what bad results they want to prevent.

- An insurer commented that, depending on its sponsor, a cybersecurity education and awareness campaign should target one of three potential audiences: employees internal to a company; the company's potentially insecure third party suppliers/vendors; and society generally.

- A second insurer added that in our society, campaigns work well for changing negative behavior like smoking and would likely work well for developing a strong cyber risk culture nationally. The message of such a campaign, he asserted, should be simple – addressing basic themes such as "privacy by design" and "security by design." He added that companies should consider including these messages within their mission statements. The insurer likewise recommended that such messages be shared as part of both school curriculums across all grade levels and regularly occurring workplace education and training programs.

- An IT professional took issue with the federal government's broad-based "let's train grandma about cyber" campaign approach. Such Smokey the Bear-type awareness campaigns, he asserted, are useless. A second IT professional disagreed, noting that Smokey the Bear is still out there and is well-loved by children. He argued that the country needs similar public service announcements to help create a broad baseline of understanding about cyber risk.

- A social scientist stated that the challenge of developing a successful cybersecurity education and awareness campaign involves figuring out how to best reach and appeal to sometimes very different audiences. Even better than Smokey the Bear, she observed, was a Center for Disease Control and Prevention (CDC) campaign to inform people about emergency preparedness kits. That campaign included a zombie apocalypse-themed public service announcement on YouTube that got 50 million hits from the public.

- In the absence of a clear cyber adversary, a critical infrastructure representative suggested that companies should focus their internal campaigns on good cyber hygiene in order to have at least an incremental impact on employee behavior.[13] He cautioned, however, that getting hundreds of thousands of employees across an enterprise on the same cyber hygiene page is not a cheap or easy task, especially when one considers the costs associated with repeating and updating the campaign over time. Setting up processes to promote accountability for compliance with cyber hygiene requirements, he added, is equally expensive. The representative noted that his own company budgets for education and awareness campaigns by prioritizing the particular

[13] Good cyber hygiene includes: (1) setting strong passwords and keeping them confidential; (2) optimizing operating systems, browsers, and other critical software by installing updates; (3) maintaining an open dialogue with family, friends, and the community about Internet safety; (4) limiting the amount of personal information posted online and using privacy settings to avoid sharing information widely; and (5) exercising caution about receiving and reading online material. *See* U.S. Department of Homeland Security. *National Cybersecurity Awareness Month: Do Your Part*. ONLINE. N.D. Available: http://www.dhs.gov/national-cyber-security-awareness-month [11 June 2013].

cyber risks it wants to address and then measuring the impact of targeted risk management messages against those risks. For example, he stated, his company briefed employees about phishing attacks and then tested employee awareness and behavior in the days and weeks thereafter in order to track progress in preventing them.

- An insurer agreed that cybersecurity education and awareness campaigns should not be directed just to senior executives. Especially within companies, he stated, management should regularly solicit insights about existing and emerging cyber risks from the company's IT professionals in order to help inform both future iterations of internal campaigns and related employee training programs. The insurer concluded that if employees know that privacy and security are high-level priorities for senior leadership, and that their input into those priorities matters, that sense of inclusion can help drive organizational change.

- Finally, a social scientist commented that he sees an "obvious" opportunity for insurance carriers – as part of or in the wake of cybersecurity awareness and education campaigns – to supply cyber risk management strategies and technologies to their clients. Lower risk clients are more profitable, he explained, so carriers should have a natural incentive to improve the cybersecurity postures of the customers they serve.

Education and Training

- An IT professional commented that he thinks about cyber risk education and training as falling into either a business bucket or a government bucket:

    - With regard to the business bucket, he commented that most people learn about cyber risk in their workplaces. He warned, however, that simply sharing information about cyber risk and steps to address it isn't enough because employees already are inundated with information. He asserted that a better approach instead is for companies to involve human resource departments from the start in the development of cyber risk education and training. Those departments, he explained, are uniquely positioned to incorporate economic incentives into the mix that could encourage employees to apply what they've learned – for example, structuring annual evaluations and conditioning promotions and salary increases upon demonstrated compliance with cyber hygiene requirements.

    - With regard to the government bucket, he recommended that the government focus its efforts on developing solid education and training programs for boards of directors and senior executives about the economics of cybersecurity. He observed that while most corporate leaders today understand that the Bring Your Own Device (BYOD) trend and cloud computing will save them money on a quarter by quarter basis, they don't understand the long-term financial risk of these developments – most especially when it comes intellectual property loss.

- Another IT professional disagreed, asserting that if society focuses cyber risk education and training only on boards of directors, then the nation will be 15 to 20 years too late in the culture to effectively manage cyber risk. The nation also needs to start cybersecurity education with children when they're very young, he added, noting that this type of long-term investment will help ensure that cybersecurity becomes ingrained in children long before they enter the business world. The IT professional acknowledged that a serious information gap exists now with current corporate leaders and therefore urged the government to take action directed at that population. He did not, however, have high hopes. The challenge in getting boards of directors to take the time to learn about cyber risk, he explained, is that a commitment of this nature competes with the board's main concern: making money for the company. The IT professional concluded that until boards do so, it will be impossible to even begin discussing how to prioritize cyber risk against other business risks, make the investment case, and change the culture.

- A critical infrastructure representative emphasized the need for integrating cyber risk training into the daily work of employees. His company, he explained, starts every meeting with a short safety briefing – for example, about CPR, steps for operating Automated External Defibrillators (AEDs), how to evacuate a building, and the location of first aid kits. This repetition, he explained, reinforces the culture of safety that his senior leadership wants to foster at all levels of the enterprise. The representative commented that the nation is not there yet with cybersecurity and it won't get there without similar repeated briefings and other activities.

- A risk manager emphasized that all employees of a company should receive some kind of basic cybersecurity awareness instruction. When appropriate, he continued, certain employees should receive roles-based training tailored to their particular responsibilities. For example, employees who handle very sensitive Health Insurance Portability and Accountability (HIPAA) and PII should receive more focused training on those topics. Tying such training to their everyday duties, the risk manager observed, makes it more meaningful and effective.

- A social scientist commented that no matter what training a company pursues, the actual experience of a cyber incident is the best teacher. Companies that hack themselves with their own red teams, he asserted, are likely in a much better place when it comes to understanding and acting appropriately upon cyber risk. He likewise recounted a story about cyber-trained West Point cadets, 80% of whom clicked a phishing email related to their semester grades. He then cited his personal experience, noting that his 18-year-old daughter is much smarter today about cybersecurity after he hacked her computer five years ago. An insurer relayed a similar story, describing how one of his colleagues – to prove the point – moved and hid all the unsecured laptops in his office after business hours.

Near Misses

- A social scientist observed that an effective cyber risk culture must be a culture of vigilance – not only against known cyber risks with knowable consequences but also against "near misses." She described such near misses as hazards that realistically might have happened if conditions had been only slightly different. The social scientist recommended that organizations identify, study, and invest against those "almost" hazards as part of a truly proactive – i.e., vigilant – cyber risk management strategy, including related education and awareness programs. Such vigilance, she asserted, is especially necessary given the problem of cognitive bias. She explained that people often take chances and attribute successful outcomes to skill rather than luck. For example, with regard to hospital hand-washing, doctors still tend to believe that they wash their hands much more frequently than they actually do. Likewise, NASA scientists in the 1980s knew about the foam insulation problem with its space shuttle fleet but took no action to address it until the Columbia disaster. The social scientist concluded by describing an effective cyber risk culture as one that doesn't leave similar cyber near misses to chance.

The Power of Data

- A critical infrastructure representative noted that education and awareness investments to bolster effective risk cultures must be justified by the data. The improvement in hand-washing in hospitals, she stated, happened because of a critical event in the 1990s that changed awareness across the industry. In short, data gathered at that time about deaths resulting from unnecessary infections showed the value of hand-washing to saving lives. Public health advocates constantly publicized the study results through messaging and public awareness campaigns. Hospitals accordingly began enforcing hand-washing policies, she explained, by tracking their patient infection data. The representative concluded that this constant messaging, monitoring, and data flow facilitated a profound shift in health care culture.

- Another critical infrastructure representative argued that this same kind of change could happen with cyber, but only if boards of directors and senior executives are first provided with data about how cyber risks are actually manifesting themselves within their companies and the value of available risk management options to address them. Until companies know what cyber hazards are happening to them and what they cost, he added, leaders won't even get to the question of what kinds of cyber risk management actions they should take. The representative noted that tracking a company's own cyber incident data, comparing it to the experiences of similar companies, and packaging analysis for senior executive review is a relatively new phenomenon that only now is coming into its own.

- An IT professional agreed with this assessment, noting that IT professionals have known about SQL injection attacks for about 10 years but that companies are still vulnerable to them. He explained that little progress has been made because most corporate leaders don't know if SQL injection attacks have actually harmed their companies. If the data answers this question in the affirmative, he commented, the culture may shift quickly – especially if harm has been significant in terms of financial and/or reputational loss. Such a shift, the IT professional concluded, might encourage companies to demand that colleges and universities teach their computer science graduates about how to code more securely.

Incentives and Personalization

- An insurer commented that "people will do what they're paid to do" when it comes to building an effective cyber risk culture. He described a company that had experienced a non-cyber event that resulted in a $3 million loss of revenue. Thereafter, the insurer stated, senior executives engaged with middle-level managers to develop ways they could protect against similar kinds of events in the future. He explained that they developed together a performance metrics program through which the mid-level managers would be held accountable. The program likewise incentivized the managers to comply with the program's requirements through salary increases and bonuses. The insurer observed that involving the managers in both the development and execution of the solution sets for which they'd be responsible was key to the program's success. He added that a similar program could be developed to promote better understanding about and action against cyber risk. Among other things, it could clarify:

    - What business functions are supported by specific IT in the workplace and why those functions are important to the company;

    - What bad things could happen to or through the IT in the event of a cyber attack or other incident;

    - Each employee's role in helping to prevent those bad things from happening; and

    - How each employee will be held accountable, through both positive and negative incentives, for doing so.

- A critical infrastructure representative approved of this approach, emphasizing that unless organizations give their people knowledge about *why* they're being asked to do something, they won't comply and will instead find a work around. He stated that providing this explanation, as part of a broader change management process, will help make employees true believers and gradually shift the culture in the process.

- Another insurer agreed that building an effective cyber risk culture first requires incentivizing employees through a variety of carrots and sticks. So-called "carrots," he continued, might include awards, seals, and other recognition for being the most cyber secure department within a company. So-called "sticks," he added, are the easiest to develop and might include denied bonuses and salary increases. The insurer noted that a top-down focus on building an effective cyber risk culture – using these incentives – will take a long time but will be the most sustaining. For example, he stated, when a janitor working at NASA in the 1960s was asked what he did for a living, he said, "My job is to put a man on the moon." Likewise, the insurer concluded, if everyone in a hospital environment felt the need to ensure the confidentiality and integrity of patient data, it would yield tremendous dividends in terms of cultural change and patient privacy.

- A risk manager asserted that one way to initiate this kind of top-down focus might include tracking cyber-related security breaches and other incidents over time as well as the hours, money, and other resources spent recovering from them. She stated that she initiated such a process within her own company, directing her team to use a special code to track expenses related to training, computer cleanup, and overall burden on the business. That information, the risk manager explained, established an analytical understanding of cyber-related costs and has helped her advocate more effectively for IT resources to target the most troublesome problems with the most responsive solutions. In the long run, she advised, this knowledge-based approach saves the company money.

- An IT professional suggested that companies wanting to build more effective cyber risk cultures should look to organizational risk management, a mature field that offers good insights into fostering better risk awareness through education, training, and reinforcement. For purposes of cyber risk, he asserted that senior IT managers don't have all the answers for how well a given technology works. Organizational risk management strategies, he continued, would encourage constant dialogue among all levels of an organization in order to assess its effectiveness.

Budget Considerations

- In order to advocate effectively for cyber risk education and awareness budgets, a risk manager stated that boards of directors and corporate executives should hear a consistent message along these lines: "Cyber risk is not going away, there's a cost to not dealing with it well, and you need to participate in the solution." She added that repetition of this theme is essential. While many companies are certainly aware of cyber risk, she concluded, it's not an omnipresent concern for them.

- A critical infrastructure representative countered that some organizations – large, mid-size, and small – will nevertheless resist such cyber risk messaging because of the potentially negative financial impacts that awareness could entail. For example, he noted, the discovery of various IT vulnerabilities resulting from a more proactive approach to cybersecurity could result in a company's having to disclose them publicly and accordingly subject them to a corresponding increase in insurance premiums. As a further example, the representative noted that only 20% of payment card industries patch their automation systems, both before and after a breach. If the message doesn't get through to them even after they've suffered a loss, he observed, nothing will.

Higher Education

- A critical infrastructure representative reported that only one university in the nation requires its computer science graduates to take a computer security course. He commented that IT companies and others are consequently forced to hire from a pipeline of talent that "doesn't have an iota of understanding about the impact of poorly written code and associated vulnerabilities." The representative added that schools erroneously think that cybersecurity will automatically be taught to graduates in the workplace, a mistaken notion that should be dispelled.

- A risk manager agreed and stated that to address this problem, he provides new employees with secondary training about how to write appropriate code prior to involving them in customer projects. He explained that he currently directs much of this training to Generation Y personnel because, "The stuff they are posting on places like Facebook shows the concept of protecting data is somewhat foreign to them."

Reaching Mid-Size and Small Companies

- An insurer asked participants for their thoughts about what responsibility large companies have for helping their mid-size and small vendors meet basic cybersecurity requirements. An IT professional stated that defense contractors often face this question. Such companies, he observed, will never join an information sharing and analysis center (ISAC),[14] so cybersecurity must be made easy for them. The IT professional commented that mid-size and small businesses instead want to purchase off-the-shelf antivirus or other products in order to market themselves as "cyber secure." He added that if those products are not passive and/or cost-effective, they will simply pursue workarounds. The IT professional likewise doubted that large companies would change the behavior of their vendors by insisting that they comply with contractual cybersecurity requirements. "This is whistling past the graveyard," he noted, because large companies don't have the resources to police their many suppliers. He asserted

[14] DHS defines Information Sharing and Analysis Centers (ISACs) as "private sector-specific entities that advance physical and cyber critical infrastructure and key resource (CIKR) protection by establishing and maintaining collaborative frameworks for operational interaction between and among members and external partners. ISACs, as identified by [a critical infrastructure] sector's Sector Coordinating Council (SCC), typically serve as the tactical and operational arms for sector information-sharing efforts. ISAC functions include, but are not limited to: supporting sector-specific information/intelligence requirements for incidents, threats, and vulnerabilities; providing secure capability for members to exchange and share information on cyber, physical, or other threats; establishing and maintaining operational-level dialogue with the appropriate governmental agencies; identifying and disseminating knowledge and best practices; and promoting education and awareness. ISACs vary greatly in composition (i.e., membership), scope (e.g., focus and coverage within a sector), and capabilities (e.g., 24/7 staffing and analytical capacity), as do the sectors they serve." U.S. Department of Homeland Security. National Infrastructure Protection Plan. ONLINE. 2009. Available: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf [10 June 2013].

that even if they did, mid-size and small vendors would simply walk away from contracts rather than come into compliance.

- A social scientist responded that no product or service exists that mid-size and small businesses can buy to comprehensively address their cybersecurity needs. The answer, he continued, really is more about making the necessary investments to build an effective cyber risk culture nationally – within which cybersecurity products and services are features, not the centerpiece. An IT professional agreed that mid-size and small businesses that don't "get" cybersecurity today aren't going to get it tomorrow unless the culture changes.

- A critical infrastructure representative likewise remarked that to help mid-size and small businesses, security should be built "into the infrastructure" from the outset – e.g., the IT manufacturing process upon which everyone relies. He cited the example of adding fluoride to public drinking water in order to protect everyone's teeth. The representative acknowledged that it's difficult to monetize this kind of investment and asserted that, as an alternative, mid-size and small companies should consider pursuing cybersecurity awareness training, basic content filters, application security, and other measures that are widely available.

- A risk manager commented that unless a company has a good cyber risk culture, supported by senior leadership, all the technology in the world will not protect it from attack. At a minimum, he stated, mid-size and small businesses should have access to a set of cybersecurity guidelines to help them navigate the basics, such as how to properly handle PII, proprietary data, and other sensitive information. The risk manager suggested that such guidelines should be developed and taught to business owners in the very same way that the federal government teaches the private sector about the handling and protection of classified information, including the potential criminal sanctions for failing to do so. Adding technology into the mix to enable employees to more easily comply with the guidelines, he concluded, would be helpful.

- Some participants questioned why mid-size and small businesses – Joe's Pizza, for example – should be of particular "risk culture" concern. A critical infrastructure representative responded that if Joe's Pizza goes under because of a Distributed Denial of Service (DDoS) attack, then customers have one less pizza option. An IT professional agreed, noting that Joe's Pizza becomes very important at the macro level because every small business like Joe's Pizza represents an individual, a family, and a company of employees that have lost their income because of an IT failure. An insurer commented that a multi-layered and tailored approach to cyber risk education and training therefore appears necessary in order to avoid leaving anyone, including Joe's Pizza, behind.

PILLAR III: THE ROLE OF TECHNOLOGY

DESCRIPTION: Technology can help build, enforce, and sustain effective cyber risk cultures – through up-to-the minute notifications of security breaches that inform the work of both IT professionals and risk managers; automated oversight of information security policies to track compliance and to identify areas for improvement; opportunities to engage the "human element" appropriately to minimize malicious activity and innocent errors; and best practices when it comes to layered defenses. The purpose of this pillar discussion accordingly was to explore these and other options for leveraging technology in support of enhanced cyber risk management efforts that could help encourage the development of a more robust cybersecurity insurance market.

DISCUSSION POINTS:

EVIDENCE-BASED RISK MANAGEMENT

- An IT professional stated that he supports leveraging education and awareness to help promote more effective cyber risk cultures but emphasized that technology plays a critical role as well. He added that he's a firm believer in "evidence-based" risk management, and that companies need data in order to make actionable risk management decisions. To that end, the IT professional cited the Data Loss Database which he said shows that 90.8 percent of all breaches in 2012 were cyber-related. Given that alarming statistic, he asked, how can security technology actively promote better cyber risk management?

COST/BENEFIT CONSIDERATIONS

- An insurer observed that translating the benefits of a particular security technology into quantifiable cost/benefit terms – an approach that would go a long way toward getting business managers on the same page as IT professionals – is very difficult. Given the fact that cyber risk evolves constantly, he observed, companies need help in determining their return on investment in this area.

- A social scientist responded that the question of what kinds of security controls are best at reducing risk should not be left to speculation. On the contrary, he continued, data collected through cybersecurity self-assessment forms should make the question "very answerable." The social scientist then described how such forms could help populate a security control spreadsheet, which in turn would include rows listing various security controls with corresponding columns representing capability characteristics, costs, policies, related claims data, and other appropriate information. If one could correlate self-assessed security controls with claims data, he asserted, it would be possible to show the effectiveness of a particular control. He added that researchers need more claims data in order to conduct this work.

- A risk manager stated that she has partnered with a company that is a leader in assessing the impact of security technology investments. Among other things, she explained, the company analyzes and explains IT vulnerabilities in a way that is understandable to non-technical corporate leaders and identifies who within a company needs to be alerted in the event of a breach.

- A critical infrastructure representative asked how insurers go about assessing a company's network for its level of cybersecurity and for which related risk management investments they typically check. An insurer replied that it's impossible to identify every exposure of an organization's network by "looking under every hood and turning over every stone." Instead, he explained, insurance is a trust-based industry and that the best that carriers can do is look for certain indicators as litmus tests. The insurer provided the following examples:

    - Encryption. A company's use of encryption demonstrates a certain level of maturity – e.g., the company is also likely to have standard anti-virus firewall configurations in place.

    - Chief Performance Officer (CPO). A company that employs a CPO or a functional equivalent – someone with individual accountability for measuring, managing, and improving a company's performance – suggests that it's more likely to implement an information security program and put resources behind it.

    - Industry Standards. A company's demonstrated compliance with applicable industry standards – such as Payment Card Industry (PCI) and HIPAA standards – indicates that it has a certain level of sophistication when it comes to compliance/security functions.

    - Standard Standards. A "distributed" company that has a presence in multiple locations exhibits a high degree of maturity when it applies the same cybersecurity standards (i.e., reporting triggers for cyber incidents) in every office.

- The insurer emphasized that the questionnaires that carriers use to identify these and other indicators are surveys, not technical audits. Even so, he concluded, the questionnaires often ask more questions than companies can answer.

- A critical infrastructure representative replied that a company can pretty much figure out how insurers underwrite against cyber risk by looking at their application questions – each of which gets to key risk factors. She asserted that if a company's IT professionals don't see these applications, and if they aren't involved in completing them, then the company opens itself up to real cyber risk exposure. In short, she concluded, IT professionals should be involved in the process in order to bridge the all-too-common business/IT divide.

- A social scientist questioned the value of lengthy insurer questionnaires, asserting that no carrier can tell a company what marginal reduction of risk a particular security technology investment will provide. For example, he asked, what's the value of encryption?

- An insurer responded that lengthy questionnaires getting at a company's technology were now the exception rather than the rule because cybersecurity underwriting has changed. "The majority of cyber incidents that we see today indicate human error," he explained, "so our application has changed based on the reality that most losses don't result from technology per se." He added that most insurers therefore no longer conduct lengthy technology assessments as part of the cybersecurity insurance underwriting process.

- A second insurer stated that technologists assume that technology is the holy grail of underwriting, but it isn't. We don't look at technology as a stand-alone factor very much, he explained, noting that no single technology exists that will prevent a cyber attack. The insurer added that carriers instead view technology through the prism of a company's risk culture. When carriers do ask about it, he continued, they do so with very basic questions aimed at how technology supports a company's business processes and people. "If companies can't answer those questions," he explained, "we don't underwrite them." The insurer then stated that cybersecurity insurance underwriting essentially tries to weed out the 20 percent of companies "who have no clue about cybersecurity from the pool of potential insureds." He noted that carriers also look at a company's mission, size, and industry to inform their underwriting decisions.

- A third insurer added that while his company examines a potential insured's loss prevention technologies as part of its underwriting process, it also focuses on a company's cybersecurity training for employees. He noted, however, that there's little data available about how many employees within companies have received such training – making comparisons across companies difficult. The insurer likewise observed that the competitiveness of the market prevents carriers from developing a comprehensive repository of this and other kinds of data about actual and potential insureds.

- A fourth insurer commented that the move away from detailed surveys about security technology and other controls resulted from the increasingly competitive nature of the cybersecurity insurance market. "My form might ask 50 questions, but another insurer might ask only ten questions," he explained. "Companies won't want to fill out our 50-question application form."

- An IT professional asserted that technology is nevertheless important with regard to insider threats. If someone downloads four gigabytes of a company's data every day, he noted, tools exist to detect this behavior to protect a company's assets in jeopardy. More broadly, he concluded, more actuarial data about what security technology works in the hands of a company's IT workforce would help them better leverage existing technology investments. An insurer responded that having the right technology is just part of the solution. Actually using it – and using it effectively – is much more important. For example, he continued, while technology exists to keep logs of all of a company's network activity, a person must actually analyze logs to detect problems and report them up the chain for action. "Nobody is doing this," the insurer commented. The IT professional agreed that companies spend a lot of time, money, and effort to monitor their networks but that nobody is looking at how to get the "big picture" from all the discrete data points available to them.

Lag Time Concerns

- An IT professional observed that security technology is obviously important to building an effective cyber risk culture, but that there's an unavoidable lag between the onset of new threats and the development of new technology. He asserted that security technology therefore is "always" reactive, even if it's essential, and cited anti-virus software that protects against known malware as just one example. The IT professional recommended efforts to promote awareness of new security technologies as they become available and to accelerate their implementation by organizations before a cyber incident happens. In so doing, he concluded, the lag between new threats and applied solutions can be reduced.

The Human Element

- Another IT professional responded that companies typically host several different layers of technology, some for the back office and some for the end user. For purposes of building an effective cyber risk culture, he asserted, companies should focus on the technology that impacts the end user. The IT professional advised that the end user represents not only the greatest technology risk but also the greatest technology challenge.

- An insurer commented that a big part of that challenge results from a perception by companies that when it comes to technology, they must choose between security and performance. He noted that encryption, for example, is a valuable security technology that nevertheless has a significant performance cost in terms of expense and operational impact (e.g., slowing down employee work flows). The insurer stated that to make security technology a more meaningful part of effective cyber risk cultures, companies should invite IT professionals and end users to a common table to discuss why particular security technologies are necessary; how those technologies work; how employees actually use them; and how they should be improved to support business operations.

- A second insurer commented that many corporate leaders don't want to talk about their technology investments with their IT departments because they're non-technical professionals, feel out of their depth, and therefore don't know what to say. He stated that companies nevertheless purchase technology to try to quickly fill security gaps but that it's ultimately people who must make the technology work. The insurer added that some companies don't understand the centrality of the human element to all this and instead persist in trying to fix bad technology with more technology. He then noted that the root of the problem goes back to education and awareness – in this case, for corporate leaders who don't understand the security technologies that they're purchasing, how they should be implemented, or how their workforce actually uses them. Without that understanding, the insurer concluded, companies can't accurately assess the costs and benefits of investing in one technology over another.

- An IT professional agreed and asserted that the effectiveness of security technology depends in large part on a company's particular mission. Too often, he observed, corporate leaders see a particular technology as "the solution" to cyber risk without taking the end users into account. For example, the IT professional continued, encryption might be easy to implement in a healthcare organization at first, but it can become very expensive to manage and maintain over time as it becomes more pervasive throughout the enterprise. Depending upon their business model and size, he added, other companies might have a completely different experience. The IT professional concluded that, regardless of the environment, even the most well-integrated security technology will never protect a company against the "weakest link" in the security chain: the human element.

What Kind of Technology?

- A social scientist observed that technology's role in promoting a more effective cyber risk culture is not so much about the adoption of technology as it is about the adoption of good technology. The goal, he added, should be to prevent security technology from getting in the way of the "good guy" doing his or her work. The problem, he continued, is that most security technology today cannot differentiate between "good guys" and "bad guys." The social scientist concluded that the challenge involves more of a design/usability question than a "use the technology yes/no" question.

- A critical infrastructure representative commented that when his organization engages companies to assess why people violate cybersecurity risk management policies and processes, it typically sees a significant decrease in violations after employees become more aware of them. He noted, however, that violations will continue to trend upward – even despite better education and awareness – in situations where employees lack a fundamental understanding of the technologies they're using (e.g., SCADA systems). Accordingly, the representative concluded, companies should be careful not to oversell cybersecurity risk management policies and processes as complete cyber risk solutions. People instead need basic knowledge about the technologies they're operating as well.

- A risk manager observed that IT departments often deploy security technology into corporate network architectures in a helter-skelter way that doesn't work with existing business processes. Much of the problem, she asserted, results from a lack of interaction between IT and non-IT professionals. "IT people just want to solve problems," the risk manager observed, "while business people don't want to be bothered." She concluded that there needs to be much better communication between both groups in order to ensure that security technologies support rather than hinder business operations.

- An IT professional commented that security technology has most value "where humans are inherently bad at doing something." He explained that he started his career in the intelligence field, and that the email tool that his organization had deployed forced him to tag classification labels on every email before he sent it. Private and public sector organizations, the IT professional continued, should consider purchasing technology that requires similar "forced tagging" in order to "have the immune systems of business networks protect information."

- An insurer stated that from a reinsurer point of view, better technology reduces cyber risk. If everyone is better protected through technology, he added, then society receives a net benefit. The insurer cautioned, however, that if all companies are protected by the same technology, risk aggregation concerns arise. "Whereas good tech helps secure systems," he explained, "a monoculture of a single good technology aggregates risk such that if a vulnerability does emerge, it has large, cascading losses." The insurer added that if one "bad guy" can exploit a single vulnerability in the technology to attack one company, he or she can do the same to attack all other companies using the same technology.

- A critical infrastructure representative noted that certain security technologies already are available that can help companies maintain their business work flows in the face of cyber risk. An IT professional responded, however, that there's no magic bullet or one-size-fits-all solution that all companies should adopt. On the contrary, he noted, many companies often don't have the same security technology deployed internally from office to office given varying business needs at different business locations. The IT professional concluded that companies instead should look at current modes of attack – specifically, the cyber incidents that they're actually experiencing – and then invest in security technology and other controls that address related vulnerabilities. He emphasized that each company needs to do its own cost/benefit analysis of those investments that's tailored to its unique cyber incident history.

- A second IT professional likewise commented that there are architectural aspects of security and that it's difficult to separate security as a practice from overall business process. He noted that prescriptive security controls that focus on generic best practices, absent the broader context of how the business operates and how that is reflected in the IT landscape, can easily become inefficient or even counterproductive. The IT professional stated that depending on the situation, it may make more sense to invest in architecture simplification versus more security. For example, he explained, a company that has weak information architecture governance might have databases that are designed and deployed without consideration of master data management concepts. Therefore, data may be replicated to address specific business functions absent an enterprise information model, leading to a proliferation of databases. Security in this situation, the IT professional noted, might best be improved by strengthening information architecture controls in the form of improved architecture governance. He concluded that with a better architecture, database proliferation can be reduced – allowing for better control of information versus focusing on traditional security controls across numerous (unnecessary) databases.

Technology Tools

- An insurer asked what burden the government has to help industry develop advanced technologies to improve security. An IT professional responded that DHS has developed the Cyber Security Evaluation Tool (CSET) for this purpose and added that while it's not perfect, it may be a good tool for companies to explore.[15] He added that the commercial world has not leveraged military resources particularly well despite their similar availability. The IT professional cited Security Technical Implementation Guides (STIGs) in this regard.[16] Finally, he mentioned Sandia National Laboratories as a potential solutions source.

- A critical infrastructure representative commented that the private sector has generated similar tools, including Verizon Incident Sharing (VERIS), a publicly available, open-source framework. The representative explained that VERIS provides a common taxonomy and allows companies to assess the effectiveness of their cyber risk mitigations over time while simultaneously comparing themselves to other companies within their sector. A social scientist asked how companies using VERIS could compare their performance with other companies. The critical infrastructure representative advised that companies could use a VERIS portal for this purpose.

Self-Awareness Through Big Data

- A critical infrastructure representative stated that companies should not focus so much on the "best" technology as they should on data analytics. Specifically, he asserted, the more critical inquiry for corporate leaders is what cyber incidents are actually happening to their companies; how their experience compares to similar companies within the same industry; and whether their existing risk mitigation controls adequately address their exploited vulnerabilities. In short, the representative commented, companies should prepare their cybersecurity budget spend on real data about how they're being attacked.

- An IT professional noted that there aren't enough people being trained to do this kind of analysis and asked if government and/or the private sector would be stepping into the breach. A second critical infrastructure representative responded affirmatively, stating that "something

[15] *See* U.S. Department of Homeland Security. *Assessments. Cyber Security Evaluation Tool (CSET)*. ONLINE. N.D. Industrial Control Systems Computer Emergency Response Team (ICS-CERT). Available: http://ics-cert.us-cert.gov/Assessments [18 June 2013].

[16] *See* U.S. Department of Defense. *Security Technical Implementation Guides*. ONLINE. June 21, 2013. Defense Information Systems Agency (DISA). Available: http://iase.disa.mil/stigs/index.html [24 June 2013].

will scale eventually" and that there will likely be intense competition for data analysts in this area going forward.

- An insurer cautioned that carriers are very wary of big data analytics. He asserted that big data may have a lot of value when it comes to building models that help to assess a particular company's unique place on the cyber risk landscape for underwriting purposes. Carrier experience with big data, however, is limited. The insurer observed that significant and as yet unexperienced cyber events – on the scale of a financial crisis or hurricane – could "trash" even the best of models.

PILLAR IV: THE ROLE OF INFORMATION SHARING

DESCRIPTION: Boards of directors and other corporate executives can't manage cyber risk effectively if they don't understand what cyber risks their companies face. In order to bridge the divide between these leaders and their IT departments, companies should consider focusing their attention on the kinds of cyber risk information that senior decision-makers need and want, from what sources, in what formats, and for what risk management purposes. The goal of this pillar discussion accordingly was to identify key ideas about how to approach and address these questions in support of more effective cyber risk cultures and, in the process, a more responsive cybersecurity insurance market.

DISCUSSION POINTS:

DEFINING THE CHALLENGE

- A risk manager asked the participants to describe communications obstacles that they've experienced between corporate leaders who need to make cyber and other risk management decisions and IT professionals most knowledgeable about the cyber incidents impacting their companies. He specifically asked the participants to describe how those obstacles have been overcome and what steps, if any, might be applicable beyond their own environments.

INFORMATION SHARING FOUNDATIONS

- An IT professional commented that his company adopted an intelligence-driven cyber risk management model several years ago. He noted that his company generates an overwhelming amount of information as part of its daily business operations, all of which his team funnels through filters to determine what data is most relevant and actionable. He explained that his team then converts that subset of data into readable formats that non-technical professionals can understand. The IT professional noted that the move to an intelligence-driven risk management model, although the right thing to do, has required considerable investments of time and other resources.

- A risk manager responded that intelligence-driven risk management models nevertheless help overcome stove-piping problems that too often lead to ignorance and competing goals within both commercial and government enterprises. For example, he cited ignorance among people within the federal Intelligence Community (IC) regarding the authorities, missions and capabilities of agencies outside their own and the kinds of information that those agencies need to conduct their work. When someone in U.S. Customs and Border Protection (CBP) doesn't think to share information with the FBI, he commented, there's a real problem. The risk manager also cited similar challenges between law enforcement and the IC. "Law enforcement wants credit for an arrest," he observed, "while the IC wants to avoid arrests that would shut down potential sources of information." The risk manager then stated that the same phenomenon extends to individual companies, where internal business units and IT units often find themselves at odds. The tremendous distrust that results, he concluded, can only be overcome with procedures that define roles and responsibilities for cyber risk information sharing and hold relevant parties accountable.

- A risk manager commented that in the cyber context, industry is trying to work with government to share information but doesn't know what information to share or with whom. He observed that no procedures for sharing exist and that industry lacks understanding about what can be done with information it might have to help cybersecurity efforts more broadly. Another risk manager asserted that if companies adopt enterprise security programs – for which internationally-accepted standards and practices exist – then they will inevitably do the right security activities, including the right kinds of cyber risk information sharing.

- An IT professional and risk manager from the same company described how they've worked together to overcome some of these challenges:

    - The IT professional explained that he brings cyber risks and related technical information to the risk manager so they can translate it into financial and reputational terms that the board of directors can understand. The IT professional advised that, in so doing, they not only help inform high-level risk management decisions but also develop business relevant metrics that they use to gauge progress in implementing approved solutions.

    - The risk manager commented that before he brings these "translated" cyber risk issues to the board, usually on a quarterly basis, he shares them with human resources, finance, and security personnel so they travel not only up but also across the company for input and feedback. He stated that to support this approach, he's found it effective to have security personnel sit down with business units so business units can better understand the risks and security personnel can better understand business needs.

    - The IT professional added that, in addition to this more formal quarterly sharing, he regularly discusses cyber risks with board members on an ad hoc basis "without getting so granular that they can't see [business] value." To support those discussions, he explained, he prepares a technical briefing as a backup in case board members want more details.

- The IT professional further noted that he's observed an increasing number of IT professionals getting business degrees so they can "talk the business talk" about security with business units and then translate business talk back into technical terms for IT department action.

External Source Information Sharing

- A critical infrastructure representative expressed his hope that both EO 13636 and PPD-21 – released in February of 2013 – would help address many of the aforementioned information sharing challenges. He noted that under the EO, the Central Intelligence Agency (CIA), DHS, FBI, and National Security Agency (NSA) have been directed by the President to provide enhanced cyber threat data to the private sector. The representative stated that several federal agencies had recently released a cyber threat-related joint intelligence bulletin (JIB) and that his company expects to see more of them in the future. He noted, however, that the JIB was not a "machine readable" product that would have made it easier to access and use. The representative said that he hoped intelligence sharing about cyber threats will improve over the next several months.

- An IT professional commented that the lack of machine readable products presents a particular problem for mid-size and small companies. He commented that while he sees more and more technologists trying to talk with each other about cyber risk and how to best address incidents, no combined effort to pull everything together exists. Until that occurs, the IT professional concluded, there won't be a full picture of what's happening. Another IT professional stated, however, that a variety of publications exist that streamline cyber risk/cyber incident information to make it accessible to smaller firms.

Internal Source Information Sharing

- Participants next turned to the topic of information products that companies generate internally to inform board of directors risk management and investment decisions. A critical infrastructure representative stated that his company hosts a 16-member corporate risk council that convenes regularly to share information about cyber and other risks with implications across the enterprise. He explained that individual member input, which the council presents to the board every six months through the company's business intelligence function, provides a good picture of the company's risk profile.

- A second critical infrastructure representative responded that his company has a similar council that presents its findings to the board of directors in summary fashion. He attributed the success of his company's council to the board holding it accountable for not only identifying cyber and other risks but also reducing them, and measuring their progress in doing so, over time.

- A third critical infrastructure representative observed that this approach doesn't work everywhere. Cyber-related "near miss" events in the health care industry, she explained, don't typically rise to the level of mandatory reporting and consequently don't make it into board presentations within her organization. The representative added that a reporting gap similarly exists regarding IT professionals who see suspicious activity, are concerned that something bad may be happening on a network, but aren't compelled to report their concerns via mandatory reporting. This gap, she asserted, needs bridging.

- An insurer cautioned that enhancing cyber risk information sharing should not focus exclusively on corporate IT departments and how IT professionals communicate cyber risk to boards of directors and other corporate executives, rank and file employees, and others. Information sharing instead is about *sharing*, he emphasized, and not about one-way communication. The insurer asserted that not all facets of cyber risk information sharing are technical and that senior executives like the General Counsel accordingly should be expected to contribute to company-wide conversations on the topic as well. He added that companies should identify and engage not only internal partners and audiences for cyber risk information sharing but also outside companies.

Near Misses II

- An IT professional revisited the issue of near misses and risk management, commenting that if a company looking for near misses observes that bad people are scanning its systems all day long, it may "freak people out." What, he asked, is a near miss in cybersecurity and how should companies incorporate them as part of their broader risk management strategies?

- A social scientist responded that companies should be looking for slight deviations that could turn a benign event like a scan into something catastrophic. She explained that this requires close reviews of after action reports (AARs) of non-events to determine how things could have gone off the rails. The social scientist added that the focus in the described scenario, for example, should be on identifying what could be different tomorrow – about the adversary, the company's security configuration, or otherwise – that could let an adversary into a company's network and wreak havoc. This kind of heads up, she continued, would help companies figure out what they need to do today to mitigate the risk tomorrow. The social scientist then emphasized that the point is for companies to instill a culture of awareness rather than a culture that assumes security skill rather than luck. She explained that it's like counting the number of times a doctor washes his hands: we want to have a culture that keeps searching for problems (i.e., a lack of hand washing) and not a culture that that's afraid to search for and admit them.

- An IT professional responded that companies are at a point with cyber risk where they're "getting lucky every day" and accordingly should focus on taking near misses into account. Unless a company has zero-day vulnerabilities all figured out,[17] he observed, it's constantly vulnerable to attack. The IT professional concluded that if an adversary dedicates the time to getting into a company's assets, the adversary will succeed – a fact of life that supports the argument that companies should adopt risk mitigation rather than risk avoidance strategies.

- The social scientist concurred, noting that companies should instill "cultures of vigilance." She commented that the movie company Pixar has been very successful, but that it doesn't content itself with those successes. On the contrary, the social scientist stated, the company conducts sophisticated post-release assessments of their films to identify what could have gone better. She emphasized that Pixar does so with all of its films, even its most successful releases.

Cross-Sector Information Sharing

- An insurer commented that although critical infrastructure sectors are vertically oriented, IT touches everything across sectors. He added that replicating a legal structure that supports the exchange of real-time data that keeps everyone, across all sectors, aware, would be helpful.

- An IT professional replied that his company has looked at existing sector communication and stated that when it happens, such as with the Financial Services ISAC (FS-ISAC), it works very well. He asserted that other ISACs, however, have not been as successful with information sharing and that some ISACs exist – for all intents and purposes – in name only.

- A second IT professional questioned whether now might be a good time to rethink how cross-sector information sharing is currently structured. He asserted that big banks probably have more in common with big defense industrial base companies than with community banks. These kinds of highly sophisticated companies, he continued, should be permitted to share cyber risk information among themselves, across sectors, and then more broadly with others. The IT professional stated that such exchanges help develop trust among the players, without having to join an ISAC. He added, however, that he's not seen anything from government that truly helps bring companies together.

Cross-Carrier Information Sharing

- An insurer noted that every carrier is different when it comes to assessing information sharing and other aspects of a company's cyber risk culture for underwriting purposes. While most carriers consider information sharing by a potential insured to be a positive sign, he added, every company shares information differently. The insurer explained that carriers therefore

[17] A zero-day (or zero-hour or day zero) attack or threat is an attack that exploits a previously unknown vulnerability in a computer application, meaning that the attack occurs on "day zero" of awareness of the vulnerability. *See* Zero-day attack. (n.d.). In *Wikipedia*. Retrieved June 26, 2013, from https://en.wikipedia.org/wiki/Zero-day_attack.

weigh “information sharing” efforts differently from company to company depending on their particular circumstances.

- A critical infrastructure representative recommended that carriers look to federal mandates about patient safety information sharing as a potential source of lessons for how to pool and share cyber-related claims data. He specifically cited the Department of Health and Human Services’ Agency for Healthcare Research and Quality (AHRQ), a patient safety organization that uses a standardized tool to collect information about patient harm. Cyber incidents are a subset of the information submitted to AHRQ, the representative noted, and it consequently could be a good source of actuarial data – at least insofar as healthcare organizations are concerned. A second critical infrastructure representative agreed, noting that the AHRQ system is protected from legal discovery, a prior barrier to patient safety information sharing. She added that a series of AHRQ-like organizations with similar protections could be established for other sectors and serve as additional sources of actuarial data.

- An IT professional asked if the insurance industry wanted to establish its own ISAC. An insurer responded that the insurance industry technically is part of the Financial Services Sector which already has an ISAC, the FS-ISAC. He added that carriers should consider using the FS-ISAC as a platform to share relevant data but asserted that they will also need new constructs to share cyber-related claims information.

- An IT professional asked the other participants what carriers would do with cyber-related claims data if they decided to establish a shared database. Several participants responded:

    - An insurer stated that companies adopting best practices would benefit if more actuarial data about the size, scope, and frequency of cyber incidents becomes better known. Put simply, such information would help carriers offer better coverage at lower prices. He added that costs also will come down when carriers become more comfortable with the concept of sharing this kind of data and are otherwise incentivized to do so. The insurer concluded, however, that such sharing will likely undermine some of the competition across the industry.

    - A second insurer replied that incentivized information sharing among carriers nevertheless has a proven track record of informing and enhancing effective risk management. With more data on the size, scope, and frequency of cyber incidents – and the precise mechanisms involved in those incidents – carriers would be in a better position to develop policies that require potential insureds to adopt certain risk management controls as a prerequisite to coverage.

    - A third insurer commented that while there’s a tremendous need for carriers to share cyber-related claims data in order to enhance their cybersecurity insurance offerings, it's unlikely to happen. He explained that carriers are simply unwilling to share this kind of proprietary information. A fourth insurer agreed that because carriers compete with each other, they won't put "all of our secrets" into a big data pool. He added that the Cyber Intelligence Sharing and Protection Act (CISPA) was designed to address this problem, but that privacy advocates had concerns about potential governmental use of the data.

- An IT professional observed that without legislation, current anti-trust barriers that prevent unlawful industry collusion would likewise stymie the effort to create a carrier database for claims data.

- An insurer asserted that carriers should nevertheless share claims data through ISO, the Insurance Services Office, but lack incentives to do so. Alternatively, he stated, the federal government could establish a cyber data sharing clearinghouse and encourage carriers to participate through tax and other incentives. The insurer stated that in such an organization, the federal government would serve as the insurer of last resort and membership would be voluntary. Once sufficient actuarial data has been generated, he added, the industry would be able to kick the federal government out and move the market forward on its own.

CONCLUSION

Participants reported that the roundtable's focus on building effective cyber risk cultures – and, specifically, the challenges involved in tailoring such cultures to a company's particular circumstances – was both relevant and useful. At the conclusion of the roundtable, the participants offered several comments regarding potential next steps.

Exploring ERM. An insurer asserted that ERM could be better leveraged to help corporate leaders understand that cyber risk is just one subset of broader discussions about business risk. A risk manager agreed, stating that future ERM discussions should examine how it could be used not only by large but also by mid-size and small companies to (1) translate technical cyber risk information into actionable business terms; and (2) assess cyber risk across internal corporate silos. A second insurer noted that those conversations should likewise emphasize the utility of ERM in identifying and defining potential solution sets to key cyber risks as a predicate to a comprehensive "carrot, stick, culture" incentives strategy. A third insurer added that more Generation X and Y participants should join future roundtable given their very different ideas about privacy risk than those of other generations.

Understanding Costs and Benefits. An IT professional stated that the roundtable had convinced him that a more robust cybersecurity insurance market could be a powerful force in establishing and "enforcing" cybersecurity best practices. He concluded, however, that one size does not fit all and suggested that companies first focus on understanding their unique place within the cyber risk landscape before investing in particular cyber risk controls. Several other participants agreed and expressed their interest in exploring the costs and benefits of such controls – whether policy, process, or technology in nature. They explained that if companies come to understand both the cyber incidents that they've actually experienced and those that they'll likely face in the future, they'll want to know how to go about determining which investments provide the most "bang for the cybersecurity buck." They suggested that future events should start the process of answering that question.

Incentivizing Better Risk Management. Participants expressed interest in pursuing additional incentives-oriented discussions. A risk manager and social scientist agreed that liability issues surrounding "going on offense" against cyber adversaries would likely be an interesting topic to many. The risk manager added that a number of companies do data analytics, forensics, and penetration testing for large, mid-size, and small companies and may – as part of their legitimate operations – incur legal liability if they come across PII. He recommended that these issues also be included as part of future agendas. An insurer and a second risk manager, in turn, recommended that stakeholders turn their attention to the overall economics of cybersecurity insurance rather than legal immunity issues only. Other participants agreed that they'd welcome a pros and cons conversation about cybersecurity incentives generally.

Roundtable leaders and organizers agreed to share this feedback with DHS and NPPD senior leadership and to communicate with participants about next steps.

APPENDIX: FULL AGENDA

Cybersecurity Insurance Roundtable
Defining the Pillars of an Effective Cyber Risk Culture

Monday, May 13, 2013
National Intellectual Property Rights Coordination Center
2451 Crystal Drive – Suite 200
Arlington, VA 20598-5105

AGENDA

8:00 – 8:30 Arrival/Registration

8:30 – 8:45 Opening Remarks from DHS/NPPD

- *Deputy Under Secretary for Cybersecurity (Acting) Bruce McConnell*
- *Tom Finan, Senior Cybersecurity Strategist and Counsel*

8:45 – 9:15 Remarks from Cybersecurity Insurance Workshop (October 2012) Attendees: "The Importance of an Effective Cyber Risk Culture as a Foundation for Cybersecurity Insurance"

- *Laurie Champion, Managing Director – Enterprise Risk Management, Aon Risk Solutions, Global Risk Consulting*
- *Oliver Brew, Vice President, Specialty Casualty Division, Liberty International Underwriters*
- *Jake Kouns, Director, Cyber Security and Technology Underwriting Risks, Markel Corporation*

9:15 – 10:15 Pillar I Discussion: The Role of Executive Leadership (Champion)

10:15 – 10:30 Break

10:30 – 11:30 Pillar II Discussion: The Role of Education and Awareness (Brew)

11:30 – 12:30 Pillar III Discussion: The Role of Technology (Kouns)

12:30 – 1:30 Lunch (On Your Own)

1:30 – 2:30 Pillar IV Discussion: The Role of Information Sharing (Finan)

2:30 – 3:00 Summary Discussion/Q&A/Close