Cybersecurity Insurance Workshop Readout Report

National Protection and Programs Directorate
U.S. Department of Homeland Security

November 2012

TABLE OF CONTENTS

INTRODUCTION

Cybersecurity insurance is designed to mitigate losses from a variety of cyber incidents, including data breaches, network damage, and cyber extortion. The Department of Commerce Internet Policy Task Force has described cybersecurity insurance as a potentially "effective, market-driven way of increasing cybersecurity" because it may help reduce the number of successful cyber attacks by promoting widespread adoption of preventative measures, encouraging the implementation of best practices by basing premiums on an insured's level of self-protection, and limiting the level of losses that companies face following a cyber attack.[1] Given this hope, many carriers and companies would like the cybersecurity insurance market to expand into new cyber risk areas to cover currently uninsurable risks such as cyber-related critical infrastructure failures, reputational damage, and the value of lost intellectual property and other proprietary data.

Despite the appeal of cybersecurity insurance in a world where news of cyber attacks is an almost daily occurrence, the cybersecurity insurance market today faces significant challenges. While a sizable third-party market exists to cover losses suffered by a company's customers, first-party policies that address direct harms to companies themselves remain expensive, rare, and largely unattractive. Observers blame several factors for this phenomenon, including: (1) a lack of actuarial data which results in high premiums for first-party policies that many can't afford; (2) the widespread, mistaken belief that standard corporate insurance policies and/or general liability policies already cover most cyber risks; and (3) fear that a so-called "cyber hurricane" will overwhelm carriers who might otherwise enter the market before they build up sufficient reserves to cover large losses. Traditional insurance coverage issues such as moral hazard and adverse selection likewise play a part in discouraging market entry by these carriers. Evolving the cybersecurity insurance market to one that offers more coverage to more insureds at lower prices therefore depends on two key factors: (1) the development of common cybersecurity standards and best practices; and (2) a clearer understanding of the kinds and amounts of loss that various cyber incidents can cause.

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

[1] DEPARTMENT OF COMMERCE INTERNET POLICY TASK FORCE, CYBERSECURITY, INNOVATION AND THE INTERNET ECONOMY (2011) at 23-24, *available at* http://www.nist.gov/itl/upload/Cybersecurity_Green-Paper_FinalVersion.pdf.

ABOUT THE WORKSHOP

During the summer of 2012, NPPD publicly announced its intent to convene the workshop through the Sector Outreach and Programs Division (SOPD) of NPPD's Office of Infrastructure Protection. On Monday, October 22, 2012, NPPD accordingly hosted a small number of participants, registered on a first-come, first-served basis, at the Intellectual Property Rights (IPR) Center in Arlington, Virginia. Participants hailed from the following stakeholder groups: (1) insurance carriers; (2) corporate risk managers; (3) information technology/cyber experts; (4) academics/social scientists; and (5) critical infrastructure owners and operators. Several federal agencies also sent representatives. As part of its planning, NPPD asked confirmed attendees to nominate breakout group topics in order to develop the workshop agenda, included in Appendix A, and to ensure that the agenda addressed matters of critical interest. Those topics included the following:

- Defining Insurable and Uninsurable Cyber Risks
- Cyber Insurance and the Human Element
- Cyber Liability: Who is Responsible for What Harm?
- Current Cyber Risk Management Strategies and Approaches
- Cyber Insurance: What Harms Should It Cover and What Should It Cost?
- Improving the Cyber Insurance Market: Stakeholder Roles and Responsibilities
- Sequencing Solutions: How Should the Market Move Forward?

Prior to the workshop, NPPD advised confirmed 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 key challenges facing the cybersecurity insurance market; and (2) to identify perspectives on how to begin overcoming those challenges. NPPD further explained that it hoped the report would help reinvigorate dialogue in this area and raise awareness. NPPD advised confirmed participants, however, that NPPD was not looking for, would not accept, and would not solicit group or consensus recommendations during the workshop. NPPD likewise clarified that neither DHS nor NPPD would make any decisions about agency positions or policy during the event. In addition to workshop leaders, organizers, and support personnel, NPPD hosted 60 participants from the following stakeholder groups:

- Insurance Carriers: 10
- Corporate Risk Managers: 9
- Information Technology/Cyber Experts: 9
- Academics/Social Scientists: 12
- Critical Infrastructure Owners/Operators: 9
- Government: 10

EXECUTIVE SUMMARY

KEY TAKEAWAYS

Companies purchase cybersecurity insurance and other classes of coverage in order to transfer risk to other parties – namely, insurance carriers. Risk transfer is just one of four risk management strategies, however, that also include risk acceptance (i.e., bearing a risk and budgeting for potential losses accordingly); risk mitigation (i.e., taking steps to contain and minimize anticipated risk losses); and risk avoidance (i.e., eliminating a risk entirely by removing the conditions that create it). Risk managers recommend that risk transfer be pursued as the last step of a comprehensive risk management strategy after risk acceptance, risk mitigation, and risk avoidance options have been exhausted. With this backdrop, workshop participants directed their discussions to two principal issue categories in the cybersecurity insurance context: (1) questions of risk assignment, including risk ownership, third party liability, and self-defense strategies; and (2) market information challenges such as cyber incident data development and cybersecurity information sharing, cybersecurity metrics, and cyber risk awareness.

ASSIGNMENT QUESTIONS

Participants initially addressed the question of who "owns" the risk for cyber-related critical infrastructure failures. Some would assign that role to the federal government because overwhelmed utilities will ultimately turn to government for assistance. Others responded that companies themselves are responsible and cited as proof the lawsuits filed against utilities impacted by the 9/11 attacks. Participants likewise discussed the many liability questions that arise with third party service providers, most notably cloud service providers that typically refuse liability for data losses even when they're responsible for them. Participants expressed specific concern about cloud computing given aggregation/dominant platform risk, a lack of transparency about service provider cybersecurity, and the unequal bargaining positions of parties contracting for this service. On the self-defense front, several participants observed that some firms, in the absence of adequate insurance, are considering going "on offense" with their cybersecurity risk management strategies – for example, by visiting the black market to ascertain the intent, motives, and capabilities of bad actors. Participants commented that companies would welcome a private-public dialogue about extending their right to self defense of property to the cyber domain. Finally, participants discussed possible options to incentivize private carriers to extend cybersecurity insurance coverage to "cyber hurricanes," including by:

- Establishing a federal reinsurance entity – like the entity established under the Terrorism Risk Insurance Act (TRIA) – to promote the development of actuarial data that carriers will need to create new insurance products; and
- Passing a "Cyber Safety Act" – modeled on the SAFETY Act – to promote the development of (1) new cybersecurity-enhancing technologies and services; (2) insurance requirements for purchasers of those offerings; and (3) corresponding liability caps.

Market Information Issues

Participants also turned their attention to the lack of shared data about cyber risks, their frequency, and their loss impacts. They noted that the cybersecurity insurance market has been most successful in the context of personal data breach where it covers company "cleanup" costs associated with credit monitoring, forensics, and customer notification. Ample and publicly available data about data breaches, they advised, has been at the root of that success. Participants expressed a desire for more government data and information sharing about other kinds of cyber incidents and risks. They also cited the need for a secure method to share incident information, on an anonymized basis, with carriers and other stakeholders. Such a method, they concluded, could help carriers and companies overcome the particularly vexing challenge of assigning value to data as an asset.

Participants likewise explained that no commonly agreed-to cybersecurity risk management standards, best practices, or metrics exist – a state of affairs that hinders the ability of carriers to conduct risk comparisons across companies. They added that broad agreement on such benchmarks, and federal government support for them, would go a long way toward helping carriers qualify companies for coverage and price policies appropriately. Participants next addressed the lack of benchmarks in terms of their impact on evolving risk management cultures. For many companies, they observed, cyber risks are converging with more traditional risks as a result of their adoption of enterprise risk management (ERM) strategies and their growing awareness about costly cyber incidents. Mid-size and small companies, however, lag their larger counterparts in this regard. Participants commented that given this environment, carriers don't rely solely on technical compliance with available standards when assessing a company's qualifications for insurance coverage. They instead examine a company's risk culture as well – specifically, the particular cybersecurity practices and procedures the company has adopted, implemented, and enforced for both corporate leaders and staff. This focus has led some carriers to draft custom policies for their clients rather than more generic template policies that could be marketed to others.

Participant Feedback

The workshop was a success. Participants provided both formal and informal feedback that included the following comments:

- "This was a great workshop with tremendous content. My staff is still digesting my notes. Look forward to the report. We received some very significant insights."
- "I think this is a very important effort, and in my opinion long overdue, if there is anything we can do to help let me know."
- "I enjoyed not only the presentations and breakout sessions, but the general networking with peers was extremely beneficial."
- "I enjoyed the sessions and have a number of takeaways. I look forward to the report."

SECTION ONE: PLENARY PANEL PRESENTATIONS

TOPIC 1: THEORY OF AND RESEARCH ON CYBERSECURITY INSURANCE

TYLER MOORE, PROFESSOR OF COMPUTER SCIENCE AND ENGINEERING
SOUTHERN METHODIST UNIVERSITY

PRESENTATION POINTS:

- Professor Moore defined "cybersecurity insurance" to mean a contract between an insurance carrier ("carrier") and a company that covers financial losses to the company resulting from damages caused by computer or network-based incidents. He described cybersecurity insurance as one potential component of a company's risk management strategy and identified three steps for effective cybersecurity risk management: (1) risk analysis, including identification and quantification of cyber risks; (2) risk management to reduce those risks, including risk acceptance, risk mitigation, risk avoidance, and risk transfer (i.e., cybersecurity insurance); and (3) risk monitoring to validate and document risks.

- Professor Moore stated that although effective cybersecurity risk management is an important component of a robust cybersecurity insurance market, computer science culture does not include an ingrained process for collecting data about cyber attacks and learning from them. Accordingly, more analysis of cyber risks must be done to fully inform step two (risk management) options and step three (risk monitoring) efforts. Professor Moore further explained that risk transfer in this context would involve the purchase of cybersecurity insurance, which falls into two categories: (1) first-party, which would cover direct losses to a company arising from things like business interruption and destruction of its data and property; and (2) third-party, which would cover losses that a company causes to its customers and others.

- Using the example of a phishing attack, Professor Moore illustrated how a company might exercise each of the step two (risk management) options to reduce losses from a cyber attack. If a company chooses to accept the risk of such an attack, it might budget for reimbursements of fraudulent transactions. If it chooses the risk mitigation option, by contrast, it might hire a security firm to shut down impersonating websites. If the company chooses risk avoidance, however, it might adopt a policy of refusing login attempts from overseas Internet Protocol (IP) addresses. Finally, if it chooses the risk transfer option, it might buy a cybersecurity insurance policy that would reimburse it for fraudulent transactions up to a certain amount of loss.

- Professor Moore cited several advantages of cybersecurity insurance that could accrue if the market were bigger. First, it might incentivize firms to implement good cybersecurity practices. Carriers, for example, might offer lower premiums to firms that adopt specific safeguards to mitigate their cyber risks. Second, cybersecurity insurance might incentivize carriers to identify effective cybersecurity measures, promoting the development of more accurate premiums that they can "reward" to companies that adopt those measures. Third, it also might help smooth financial outcomes by having companies make a small fixed payment upfront to help them avoid

the large and uncertain costs of a cyber-related loss. Finally, cybersecurity insurance might foster market-based security metrics that permit risk managers to trade off spending more to mitigate cyber risks with reductions in insurance premiums.

- Professor Moore also provided a brief history of cybersecurity insurance, which he advised has been commercially available since the late 1970s when one carrier became the first to offer information and communications technology (ICT) insurance after it had had engineers conduct ICT loss research. In the 1980s, the carrier made cybersecurity insurance policies available to banks and blue chip companies. In the 1990s, more carriers began offering such policies although few insureds made claims. All that changed, however, with Y2K and the 9/11 attacks when carriers became acutely aware of cyber vulnerabilities. After those events, premiums increased and carriers started excluding cyber risks from most general policies. As a result, Professor Moore explained, the cybersecurity insurance market today is small and has underperformed expectations. Policies are typically capped at $1 million to $50 million and contain unpopular exclusions.

- Professor Moore commented that the key barriers to a more robust cybersecurity insurance market aren't traditional issues like adverse selection or moral hazard. Carriers instead blame weak demand for policies on a lack of awareness about cyber risks. The biggest impediment on this front, he continued, is the lack of awareness about correlated risk arising from dominant (i.e., most popular) platforms. As more and more people use the same few platforms, he noted, the more vulnerable they all become to the same platform risks. Professor Moore cited three other challenges to the cybersecurity insurance market, including (1) ongoing difficulties with clarifying and quantifying covered cyber-related losses and assigning liability for those losses; (2) externalities, including situations where an initial victim doesn't endure the full brunt of a cyber attack because it's merely being used as a stepping stone to attack another target (and, accordingly, doesn't bear the full cost of the attack); and (3) a lack of information sharing about cyber incidents.

- Professor Moore noted that coverage for data breaches, where a wide range of third-party policies are plentiful, represents a cybersecurity insurance success story. He attributed that success to the large amount of actuarial data about data breaches that has accumulated as a result of state data breach disclosure laws. Professor Moore advised, however, that policies in this area nevertheless have important limitations. As an initial matter, they typically cover only direct losses from a breach such as the costs for sending out breach notification letters. Moreover, they don't extend to either a company's reputational damages or to harms suffered by individuals whose data has been exposed.

- Professor Moore then reviewed several kinds of losses that cybersecurity insurance might cover in the future:

- Industrial Espionage. Professor Moore stated that cybersecurity insurance for cyber-related industrial espionage might work because attacks typically target a particular company (i.e., incidents may not be globally correlated). However, firms have traditionally kept these types of incidents under wraps, fearing that reputational damages associated with disclosure will far outweigh the benefits of a cybersecurity insurance policy that requires incident reporting.

- Cybercrime. Professor Moore commented that cyber crimes that target individuals might also be insurable one day, particularly online banking and payment fraud crimes. He was less hopeful, however, about personal scams. While some individuals might purchase policies, the substantial risk of moral hazard in such situations – e.g., an individual may not use his or her best judgment to avoid such scams – will probably deter most carriers from covering this risk. He added that personal infrastructure crimes would also be unlikely candidates for cybersecurity insurance given externality concerns.

- Professor Moore noted that direct *losses* resulting from profit-motivated cyber crimes are actually very low – approximately $2-3 billion per year – while direct and indirect *costs* of such crimes are very high. He estimated, for example, that defense costs for such crimes total approximately $19 billion per year while indirect costs total an additional $40 billion per year.

- Finally, Professor Moore asserted that it's extremely unlikely that cybersecurity insurance will ever cover cyber catastrophes like a cyber "Pearl Harbor" given the large numbers of externalities that such events present. He concluded, however, that if externality issues could be addressed to the general satisfaction of carriers, cybersecurity insurance policies could help reduce vulnerabilities to such events by requiring insureds to comply with particular cybersecurity standards and related best practices.

TOPIC 2: CURRENT STATE OF CYBERSECURITY INSURANCE

EMILY FREEMAN, EXECUTIVE DIRECTOR FOR TECHNOLOGY AND MEDIA RISKS
LOCKTON

PRESENTATION POINTS:

- Ms. Freeman stated that because cybersecurity is a global issue, the cybersecurity insurance market is a global market – with carriers in London, New York, Zurich, Bermuda, Europe, the U.S. and elsewhere developing cybersecurity insurance products for their clients.

- Ms. Freeman presented a timeline that described how the cybersecurity insurance market has matured over the last two decades. She stated that the market for policies really got going with the dot-com revolution, noting that initial interest in this kind of coverage originated with errors and omissions (E&O) underwriters focused on personal liability. Ms. Freeman explained that starting around 1999, technology-focused insurers within the E&O space wanted to insure not only those companies that were creating new technologies but also users who depended on those technologies, including web developers and Internet-based providers. She added that the passage

of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which included rigorous information security and privacy standards for personally identifiable information (PII), subsequently led to huge growth in the market. In a similar way, Ms. Freeman continued, passage of California's data breach law in 2003 created another large pool of serious buyers in the credit card industry who wanted to transfer their liability risk for data fraud and theft. More recently, she concluded, data breaches suffered by retailers and ensuing court cases have transformed cybersecurity into a boardroom issue given the tremendous reputational damages and lost sales those breaches can cause.

- Ms. Freeman explained that there are significant challenges for cybersecurity insurance buyers and sellers. For buyers, she described tremendous confusion about cyber risks and their potential impacts on business. She stated that many companies don't know or understand what kinds of damages cyber risks entail, how large losses can be, or why they should care if they're not directly responsible for a loss (e.g., the externalities issue). Ms. Freeman added that some buyers fundamentally misunderstand the role of insurance versus spending money on enhancing cybersecurity. They're not mutually exclusive investments, she asserted, noting that both are essential to effective cybersecurity risk management. Ms. Freeman also mentioned that buyers historically had to undergo a burdensome checklisting process to apply for cybersecurity insurance, one that turned some buyers off to the market completely. An additional challenge for both buyer and sellers, she continued, is that there's no one simple "cure" for managing cyber risks that carriers can incentivize through insurance contracts. Effective risk management to prevent major cyber-related losses instead involves a holistic look at a company's people, processes, and technology. How a company addresses all three may be unique, Ms. Freeman added, sometimes requiring the crafting of custom insurance products for particular clients.

- Ms. Freeman also highlighted challenges posed by the outsourcing and offshoring of information technology (IT) and other business functions. A company can outsource a function, she stated, but it can't outsource the cybersecurity risk associated with that function. Underwriters accordingly must understand the environment within a company and the external environment in which it does business in order to scope the universe of cyber risks that it might encounter. Ms. Freeman cited company contracts with third party cloud service providers as one example of this phenomenon. She likewise mentioned that cross-border data breaches, which often implicate the laws and regulations of multiple countries, present another area of complicated and growing risk.

- Ms. Freeman estimated that there are over 50 carriers in the cybersecurity insurance market today that offer a wide variety of products. She mentioned that companies can purchase cybersecurity insurance as a standalone product or as part of special packages that address multiple areas of cyber risk. While Ms. Freeman reported that limits of insurance on the liability side now approach and sometimes exceed $100 million for large clients, she explained that a challenge lies with smaller clients. Carriers must ensure that policies are not only affordable but also accessible to these clients – i.e., carriers must educate them about security measures and require their implementation before qualifying them for coverage.

- Ms. Freeman stated that the market for third-party liability insurance, which covers harms to a company's customers arising out of a breach of its IT assets, continues to grow steadily. By contrast, the market for first-party policies, which covers direct losses to companies such as non-physical business interruption costs and reputational damages, lags considerably. Ms. Freeman observed that the relatively small market for first-party policies persists given (1) the limited amount and nature of coverage they offer; and (2) a lack of buyer understanding about how they could contribute to an overall cybersecurity risk management strategy.

- Ms. Freeman concluded her remarks by identifying several topics that she hoped the workshop would address, including: carrier exposure to aggregation losses; the lack of consistent cybersecurity standards available for adoption by companies; challenges to insuring data as an asset; private sector fears about the potential size of cyber-related losses; reputational harms; and cybersecurity crisis management issues.

TOPIC 3: CASE STUDY: FIRE INSURANCE – STANDARDS AND DATA

JASON AVERILL, LEADER, ENGINEERED FIRE SAFETY GROUP
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

PRESENTATION POINTS:

- Mr. Averill described how the number and frequency of fire deaths, injuries, and property losses have declined in the U.S. since 1980. He attributed the drop to a series of practices that fire prevention and protection professionals have developed over the last several decades – some of which might correlate to cybersecurity risk management practices and insurance.

- Mr. Averill explained that there are many ways to harden a building against fire problems, several of which factor into the assessments of fire insurance underwriters, including (1) identifying sources of fire (e.g., candles, electrical, heating devices, smoking); (2) identifying "targets" of fire (e.g., carpeting, clothing, drapes, furniture); and (3) using controls (e.g., compartmentalization, fire protection systems, notification systems such as alarms, public education about fire prevention and response). Those controls, he added, have multiplied over the years to include not only smoke alarms but also (1) stronger building codes and standards; (2) commercial and residential sprinkler systems; (3) reduced ignition propensity cigarettes; and (4) mattress flammability requirements.

- Mr. Averill advised that fire prevention efforts nationally have resulted in a wealth of statistics year after year including – perhaps most helpfully – the source of fires (i.e., the first item ignited). This data allows the National Fire Incident Reporting System (NFIRS) to gain insight into what causes fires and how they occur. Furthermore, Mr. Averill observed, the stable nature of this data helps fire prevention professionals make predictions about future fires and the likely magnitude of the losses they will cause. Such predictions, he noted, help fire prevention professionals to develop new fire mitigation controls and carriers to develop and price new fire insurance policies. Mr.

Averill noted that while much more money is spent nationally each year on fire prevention than on actual fire losses, statistics show that fire losses would increase significantly if fire prevention investments declined.

- Mr. Averill commented that the fire problem is largely an engineering and physics problem involving factors like chemistry, fluid dynamics, heat transfer, and materials. He likewise explained that the human element is a relatively limited factor when it comes to the fire problem with one exception: arson. Mr. Averill then examined how arson might be an analog to cyber attack.

- Mr. Averill first stated that arson represents just a small component of the overall incidence of fires in the U.S. every year – approximately seven percent – and that most arsonists are unsophisticated juveniles. Moreover, arson is a physical process with a more defined, identifiable scale (i.e., one or two buildings impacted by fire). Arson damages, he added, are straightforward. By contrast, Mr. Averill commented, computer hackers are usually sophisticated individuals who continuously move the bar/change the rules when planning cyber attacks. The inherently human aspect of a cyber attack, he added, makes it less predictable than the physical processes behind fire. Mr. Averill further noted that while a fire might impact a few buildings, cyber attacks could impact millions of computers and data worldwide. Potential damages from such attacks, moreover, lack the clarity common to the fire context.

- Mr. Averill concluded his remarks by noting several parallels between arson incidents and cyber attacks. Both arsonists and cyber attackers, he commented, are looking to make a profit. Moreover, consumer prevention behaviors, smoke alarms for fire and antivirus programs for cyber attack, can help mitigate risk in both situations.

SECTION TWO: BREAKOUT GROUP DISCUSSION TOPICS AND DISCUSSION POINTS

TOPIC 1: DEFINING INSURABLE AND UNINSURABLE CYBER RISKS

DESCRIPTION: Cyber risks vary widely in terms of threat, vulnerability and consequence. Accordingly, in today's cybersecurity insurance market, some risks are insurable, others are uninsurable, and still others – depending on the circumstances – are partially insurable. While many policies cover cyber-related incidents and losses to third-parties, for example, most don't cover first-party risks such as loss of company income resulting from downed networks; extraordinary expenses associated with restoring those networks; and reputational damages. More broadly, uncertainty about what cyber risks are covered and which are not, coupled with a general lack of awareness about cyber risks and their potential impacts, has kept many companies out of the market altogether. For those who do enter the market, moreover, some buy only token coverage that responds to the last cyber incident rather than more forward-looking, comprehensive policies. As a result, many companies deprive themselves of the full benefit that risk transfer could play in their cybersecurity risk management strategies. The purpose of this discussion was to capture current thinking about all these challenges.

DISCUSSION POINTS:

- The cybersecurity insurance market today is directly informed by its history. One insurer noted that 9/11 had a major impact on the development of the cybersecurity insurance market. Carriers deemed the massive computer network losses that day to be a widespread failure. They accordingly decided not to insure against computer viruses, wanting instead to contain losses from viruses and similar cyber hazards within a smaller limit of insurance. This narrower view of what would be covered in traditional insurance policies created a vacuum for those who wanted to insure these kinds of losses.

- One insurer noted that as technology has improved over the past decade – for example, patch management can now be implemented more quickly with fewer exceptions – cybersecurity events have generally become more insurable. Given this development, another insurer mentioned that the insurance industry is now trying to determine how it can help keep services and businesses online by encouraging the adoption of best practices that have broad acceptance across industry sectors. If stakeholders come to general agreement on what those practices should be, the insurer explained, carriers can require potential insureds to adopt them as a prerequisite to coverage.

- One insurer noted that the insurance industry is not monolithic and that various carriers are focusing on different approaches. Some carriers are working actively on enhancing reputational insurance products, which currently have low coverage limits in most cases, while others are not. Still others are creating policies on a customized basis for single clients, a trend that is leading to innovation across what is a very complex industry.

- An IT professional stated that there is both a first-party and third-party market for cybersecurity insurance. He explained that first-party cybersecurity insurance, where it exists, applies when a company's own systems are down and optimally would cover such things as restoring lost data, lost business, and reputational harms. Third-party cybersecurity insurance, he added, applies when companies face significant exposures because their systems have damaged a third party or lost their information (e.g., intellectual property (IP) or personally identifiable information (PII)).

Evolving Insurable Risks

- Participants commented that several cybersecurity risks are insurable: (1) liability arising out of data breach or loss (third-party); (2) notification and other costs related to data breach such as credit monitoring and forensic costs (third-party); (3) some first-party issues (e.g., network damage and cyber extortion); and (4) some regulatory issues (depending on the regulator and type of data involved). Other cybersecurity risks, such as insider threat, generally are covered under standard insurance for employee misconduct.

- One insurer noted that companies with large amounts of PII are increasingly adopting more and better data breach protections. A critical infrastructure representative concurred, adding that more and more companies are offering increasingly affordable data breach protection services. He added that the third-party cybersecurity insurance market is also growing because increasing amounts of available statistical data about data breaches have made it possible for carriers and companies to predict what related losses will look like in the future.

- Most participants agreed that every kind of cyber-related loss is potentially insurable – so long as there is a business case for offering insurance. That business case requires two conditions: a value that can be assigned to some tangible or intangible asset, and a party that is willing to pay premiums to restore that value should a loss occur.

- The value question, when it comes to insuring critical infrastructure, is a difficult one. One insurer stated that the federal government should not be worried about data breaches – which sometimes are malicious but many times happen by accident (e.g., lost laptops) – and should focus instead on bringing attention to major cyber/physical events and helping stakeholders determine who should foot the bill for them. Other participants likewise raised concerns about blended cyber/physical events and their implications for the insurance market generally.

- While some asserted that most policies would exclude physical damage from Supervisory Control and Data Acquisition (SCADA) system attacks, others responded that they actually *don't* exclude such cyber-caused events. A network security failure that allows a SCADA system attack to succeed, they explained, would fall within a standalone (i.e., cyber) market. For example, an IT professional noted that railroads, mass transit providers, and utilities already are insuring SCADA systems themselves under standalone cyber policies. Once physical damages occur as a result of a successful attack on a SCADA system, he continued, traditional property insurance would cover those resulting losses.

- One insurer described this phenomenon as "fire following" – that no matter what the underlying cause of a fire, the fire would be covered by fire insurance. Accordingly, whether a power plant caught fire because of a SCADA attack or some kinetic failure, the fire would be covered by fire insurance.

- A risk manager responded that the SCADA arena is nevertheless one where many issues are still in flux and that it remains an open question whether a general liability policy would cover physical losses resulting from a cyber incident. An insurer agreed, noting that carriers don't necessarily intend to cover cyber/physical events but will do so until the cyber component can be separated out of the equation more effectively. A second insurer predicted that cyber exclusions will begin to come from larger carriers that have separate cyber insurance units – similar to what happened when sexual harassment cases first began to be brought with great frequency. Those claims, the insurer explained, were gradually excluded from general coverage and offered under a separate policy. One social scientist noted that until a similar shift happens in the cybersecurity insurance market, there could be an insurance market failure if a damaging cyber/physical event occurs.

- Some participants believe that shift is already underway. An insurer noted that only about 25% of companies have cybersecurity insurance policies. Accordingly, those that lack explicit coverage often try to bring cyber incident claims in under other policies. This has led to an uptick in exclusions for cyber incidents in general liability policies, in an effort to push companies to purchase cyber-specific policies. One IT professional agreed, noting that every year, insurance policies are covering "less and less" as general liability coverage narrows and carriers create more and more stand alone cyber policies. A critical infrastructure representative concurred that such coverage exclusions are in flux. He asserted that the Stuxnet virus in particular has impacted the ongoing evolution of what losses are covered under general liability policies and what losses will be segregated out for separate coverage. Others noted that recent court decisions interpreting general liability policies in favor of insureds to include cyber-related criminal activity will lead to more explicit exclusions of cyber incidents.

- Throughout their discussion about cyber/physical risks, participants mentioned the power grid. A social scientist suggested that a better way to determine both the grid's value and who might pay a premium to restore it would be for stakeholders to disaggregate its many components and examine them individually. To do so, she asserted, there needs to be a clearer understanding of "what will happen" – namely, what grid components are of greatest concern; what likely harms might come to them; and what consequences might ensue? Answers to those questions will depend upon (1) continuing observation of actual conditions and events as they unfold in the real world; and (2) stepping up information sharing among relevant stakeholders. That information sharing, she said, could include analysis of risk-based models and scenarios that demonstrate possible impacts.

Currently Uninsurable Risks

- According to a plurality of the participants, several cyber risks are currently uninsurable: (1) catastrophic risks for which most believed the federal government should be responsible (e.g.,

war, terrorism, critical infrastructure failure, "in the wild" and state-sponsored computer viruses); (2) operational mistakes (e.g., true negligence); (3) reputational damage; (4) industrial espionage; and (5) data as an asset (e.g., intellectual property, trade secrets).

- One insurer explained that carriers are struggling with the dichotomy between physical and non-physical loss. For example, they're exploring how to insure the non-physical loss of a company's market operations (e.g., losses caused by a downed/unavailable network) as well as whether it's possible and appropriate to insure the risk of a simple operating mistake. Carriers are likewise trying to determine if hacktivism, cyber terrorism, and cyber attacks using weapons created by nation states could eventually become insurable risks. The insurer added that it's difficult to make these kinds of determinations now because there haven't been enough examples of catastrophic cyber events to use as benchmarks.

- Several critical infrastructure representatives asserted that there's no cybersecurity insurance for business interruption – for example, non-physical damage arising from a downed website, such as a loss of credit card sales. Others disagreed and explained that such policies, as imperfect as they may be, have been purchased by about 10% of companies. An insurer attributed their lack of popularity, however, to two main causes. First, most reinsurers don't offer full coverage for business interruption because it can be extremely expensive and may, in some cases, have a systemic cause that affects everyone. Accordingly, most reinsurers sell policies of this kind on a modular basis and cap coverage at a set limit. Second, business interruption coverage does not kick in immediately. Service typically must be down for some set period of time before a policy activates.

- Insurers doubted that business interruption insurance, even with its various caps and conditions, could serve as a model for insuring catastrophic cyber incidents. They mentioned that the potential loss from even one such incident, given risk aggregation concerns, would be too great.

- Some participants, however, stated that contracts for guaranteed service might be a promising area for expanded cybersecurity insurance coverage. A critical infrastructure representative explained that companies that "absolutely cannot lose power" can agree to pay a premium to get prioritized power both during and following a disaster. He asserted that cybersecurity insurance policies might be made to apply to this type of contract in order to address cyber-related power losses. An insurer agreed, noting that under existing insured guaranteed service contracts, insureds typically receive compensation for such technology loss claims against their errors and omissions (E&O) policies.

- Some participants noted that many cybersecurity insurance policies likewise exclude fines and other incurred penalties from coverage – either because applicable regulations expressly forbid such coverage or because carriers expressly exclude them within insurance contracts. To further advance the cybersecurity insurance market, however, participants agreed that this area should be explored in greater depth because fines and penalties associated with data breaches can be very expensive.

- Regarding data as an asset, participants asserted that companies have been unable to put a value on their IP and other information beyond valuations generated for mergers and acquisitions purposes. Trade secrets, one IT professional added, present a particular challenge because companies are unlikely to value their own trade secrets impartially. Most believed that this problem will be solvable in the longer-term.

Information Sharing Challenges

- Many participants identified a lack of information sharing about cyber risks and the frequency, magnitude and loss impact of actual and potential cybersecurity incidents as a major obstacle to preventing a more robust cybersecurity insurance market.

- One participant stated that top carriers don't want to share such information – among themselves or with government – because they ultimately "give more than they get." He added, however, that carriers would be more inclined to share if there was business value to doing so.

- Several others opined that lessons from the fire insurance industry would be of limited help in the cyber domain because most fires are observed by emergency services and law enforcement. Most cyber incidents, on the other hand, are not observed by anyone outside an organization. A social scientist mentioned that similar problems existed with fires until firefighting became professionalized. Once that happened, industry round tables (IRTs) were established to share fire incident information across industries. Along these lines, one insurer described the Financial Services Information Sharing and Analysis Center (FS-ISAC) as a potential model for cybersecurity information sharing. The FS-ISAC, she explained, is an existing tool that banks have used successfully to discuss their shared cybersecurity problems anonymously while minimizing any immediate reputational impact.

- Many participants stated and/or agreed that the federal government should step up its own information sharing efforts about cyber threats, especially regarding "in the wild" and state-sponsored viruses.

- One insurer drew a distinction between a "cyber 9/11," an overwhelmingly catastrophic situation in which he believes the federal government must act as the insurer of last resort, and a "cyber hurricane," a situation where thousands of policy holders are impacted by a single but potentially more manageable event. He advised that carriers won't cover terrorism and war-related cyber attacks but are developing ways to handle cyber hurricanes. The insurer opined, however, that discussing and thinking about these categories separately will help foster a spirit of partnership between the federal government and the insurance industry that will promote better information sharing and similar progress. Toward that end, he recommended the creation of a private-public partnership to encourage the insurance industry to play its part in protecting the nation's critical infrastructure. Among other things, such a partnership could promote the following initiatives:

- Cybersecurity legislation modeled on the Terrorism Risk Insurance Act (TRIA),[2] creating a U.S. government reinsurance facility to provide reinsurance coverage to insurers following "declared" cyber hurricane events. Such a facility would create a temporary federal back stop for large scale cyber incidents until carriers have had sufficient time to review accrued data about them in order to develop policies to insure against related losses.

- The establishment of a cyber underwriting and loss information sharing organization which would require members to provide insurance for certain catastrophes, including cyber-related critical infrastructure failures, in consideration for the availability of both federal reinsurance and cyber incident loss data.

- Other participants raised concerns with categorizing the realm of potential cybersecurity events as "cyber 9/11s" or "cyber hurricanes." One social scientist asserted that doing so would create distinctions without meaning because the same technologies would be involved in both scenarios. Others questioned whether carriers could even define a particular attack – e.g., a distributed denial of service (DDOS) attack on the banking industry – as either a 9/11 or cyber hurricane situation. An insurer warned, moreover, that drawing such distinctions could lead to unintended effects. He opined that attribution during a cyber 9/11 – for example, a cyber war – is very challenging and might lead some carriers to automatically categorize a particular incident as an excluded event.

CORPORATE CULTURE CONSIDERATIONS

- A risk manager advised that while corporate boards of directors now talk about cybersecurity issues, they're still not asking if they're insured against cybersecurity risks. Instead, they're differentiating between how resilient their organizations are on the one hand and what cyber risks are too big for them to manage on the other. For example, if boards determine that a particular cyber risk is systemic, they usually leave it unaddressed.

- Another participant agreed with this assessment and asserted that the federal government bears responsibility for "overblowing" the cybersecurity threat. He stated that cyber risks instead need to be defined and described in a way that makes companies understand (1) that they're responsible for addressing them; and (2) that there are ways to effectively do so. An insurer responded that this is happening in some companies already, without government prodding, because corporate lines of responsibility for personnel, physical, and cybersecurity are increasingly blurring. The same security person at the top of an organization, he added, is now often responsible for all three areas.

- Several participants opined that stakeholders nevertheless need to figure out how to incentivize companies to engage in cyber risk mitigation by linking cybersecurity and cybersecurity insurance directly to the boardroom. One risk manager noted that market resilience – i.e., maintaining a company's stock price – is essential when a company suffers reputational damage and that cybersecurity insurance can be a signal that a company is competently managing its risk. Several

[2] *See* Terrorism Risk Insurance Act of 2002, P.L. 107-297, available at http://www.treasury.gov/resource-center/fin-mkts/Documents/hr3210.pdf.

other participants agreed, noting that the idea of "reputation insurance" is making a comeback given large drops in the stock prices of some companies following publicized breaches. They added that tools to measure reputational damage are being developed. Given this environment, participants suggested that already ongoing discussions on this topic should be merged with conversations about cybersecurity insurance.

- One participant expressed confidence that reputational risk provisions that protect corporate boards of directors will likely be built into many cybersecurity insurance policies within the next year. Those provisions, he explained, would most likely be designed to reward companies that adopt standards, practices, and controls that restore their operations (and reputations) quickly.

- Participants noted that the SEC's guidance from October 2011 – which effectively requires publicly-traded companies to disclose not only their material cybersecurity risks and cyber incidents but also their insurance policies to address them – has had some impact on corporate boards of directors. An IT professional stated, however, that it's too early to tell whether the guidance will change corporate behavior because (1) it's not law; and (2) companies assessing whether they have a "material" risk are still trying to determine how to balance disclosing too much information versus too little. The concern is that by disclosing too much information, a company might educate bad actors about how and where to attack them. An insurer concurred, noting that the SEC's emphasis on material risk means that many companies will self-insure and assess even large cyber risks as immaterial. Accordingly, many companies today are taking the position that their existing insurance policies cover cyber incidents and that they don't need special cyber coverage.

- Other participants mentioned that education about what cyber risks industry should address and how, as well as what role cybersecurity insurance can play, are essential to "fixing" corporate attitudes toward cyber risk. A critical infrastructure representative agreed and expressed concern that some companies are at a disadvantage vis-à-vis carriers because they don't know what losses policies actually cover. He asserted that potential insureds, especially mid-size and small companies, need a much clearer understanding of what protections they're purchasing and for what risks. A social scientist commented that this mismatch of knowledge hurts carriers as well. Without fully understanding what cyber risks threaten them, and how cybersecurity insurance addresses those risks, some companies might conclude that policies are overpriced and accordingly choose not to make a purchase. An insurer responded that cybersecurity insurance policies nevertheless are available to large, mid-size, and small companies at a range of prices and that companies can obtain such policies even after they suffer a breach or other damaging cyber incident.

- Participants likewise emphasized that any educational initiative regarding cybersecurity insurance must be a two-way street. One critical infrastructure representative explained that his large company obtained the cybersecurity insurance coverage it needed after having its top IT professionals communicate the company's risk management strengths to some 30 insurance carriers. As a well-educated consumer, his company now has 15 of those carriers covering all aspects of its risk profile.

- One participant noted that a challenge going forward will be motivating mid-size and small companies, which often lag when it comes to cybersecurity, to improve their cybersecurity. Given network and service interdependencies among large, mid-size, and small companies, getting all parties to make better cybersecurity investments will be critical for protecting everyone in the economic chain.

- Related to this discussion, one critical infrastructure representative asserted that when insureds attempt to collect on a cybersecurity insurance policy for a breach or other loss, they often experience issues with "minimal acceptable standards" clauses. He asserted that carriers sometimes look at the forensics of a breach and claim, after the insured has been paying premiums, that the insured has not followed minimal acceptable standards. They accordingly seek rescission of the policy and refuse to pay. An insurer responded that "minimal acceptable standards" language is no longer included on standard policies. Instead, carriers now insist that potential insureds comply with standards (e.g., Payment Card Industry Data Security Standard (PCI-DSS)) before the insurer even starts coverage.

Cloud Computing Concerns

- Participants also discussed cloud computing, a cost-saving service offered by third party providers that involves storing, managing, and processing data on remote servers hosted on the Internet rather than on local servers. Companies contracting for this service typically seek cybersecurity insurance to cover losses caused by the third party provider – for example, lost business that results from a cloud security breach or outage. An IT professional noted that there hasn't been significant movement to negotiate cloud contracts or to standardize security provisions within them, although steps in this direction are underway. While people often take security within the cloud for granted, he added, systemic risk in the cloud is a real concern.

- Several insurers warned about risk aggregation with the cloud, explaining that many insureds subscribe to the same cloud computing service/platform. If that service were to come under cyber attack or experience some other cyber-related failure, they continued, all of those insureds would be impacted simultaneously and would likely make similar loss claims against their shared carrier. Such an event could wipe out the carrier's entire book of business. One carrier stated that the federal government should play a larger information sharing role when it comes to this and other kinds of cyber risk aggregation.

- Other participants described the cloud in terms of IP loss. While a company's own IP is typically not covered by a cybersecurity insurance policy, a cloud service provider that loses the company's customer data could be protected from third party claims if appropriate arrangements have been made. Specifically, an insurer explained, the company and the cloud service provider would need to define both the value of the data to be protected, with the assistance of an unbiased third party professional, and each party's liability for protecting the data *before* entering a service contract. With those conditions in place, a carrier would have what it needs to assess, develop, and price an appropriate policy.

- An IT professional observed, however, that a company contracting with a cloud service provider can never really transfer liability for a data breach to that provider. Customers will still hold the company that they interact with directly responsible for the breach, not the unknown (and unseen) service provider. Put simply, it's the company's brand that will suffer even if the provider is at fault. The IT professional concluded that, under these circumstances, the best a company can do is negotiate indemnification provisions with a cloud service provider that require it to compensate the company if the provider is responsible for a loss.

- Another IT professional noted that cloud computing is fraught with other issues that make it a challenging area for cybersecurity insurance coverage. He asserted that cloud service providers do not report data breaches to carriers for primarily three reasons: (1) some willfully fail to report because if they're seen as unreliable and unsecure, they'll no longer be in business; (2) others don't know what data their customers are storing in the cloud; therefore, even if they're required under law and/or regulation to disclose breaches of certain types of information, they don't realize that their obligation has been triggered; and (3) under some contracts, providers actually own the data once it's in the cloud; accordingly, they don't believe they have an obligation to disclose a breach of what they consider to be their own data. For these reasons, a social scientist noted, cloud service providers are unlikely to allow carriers to audit them. She added that they've been able to keep prices for their services low, in part, by not disclosing breaches and by successfully pushing back against audits that might reveal cybersecurity vulnerabilities.

TOPIC 2: CYBER INSURANCE AND THE HUMAN ELEMENT

DESCRIPTION: In some respects, cybersecurity insurance is different from other kinds of insurance because of what drives its purchase: damaging cyber incidents that are almost always accidentally or intentionally caused by people. This human element is never static. A company's risk culture – including the priority corporate boards of directors place on cybersecurity, how well employees implement cybersecurity best practices in their workplaces, and how often those practices are updated – varies from organization to organization. Complicating matters is the fact that the motivations of a wide range of bad actors who want to corrupt or steal data; cripple critical infrastructure; or cause other forms of mayhem can change from minute to minute. The constant evolution of information technologies and their exploitable vulnerabilities, moreover, only compounds these challenges. The purpose of this discussion accordingly was to share various stakeholder perspectives on how the human element can be effectively managed, despite this complexity, in order to encourage a more robust cybersecurity insurance market.

DISCUSSION POINTS:

DEFINING THE HUMAN ELEMENT

- An IT professional stated that although companies want to be cyber secure, the single biggest vulnerability to their security is the individual. He accordingly defined the "human element" to

mean the insider threat of a human actor undermining an organization's cybersecurity either through ignorance or intention.

- During the group discussion, participants expanded this definition to include the full gamut of potential human actors involved in the causation, prevention, mitigation of and recovery from a cyber incident. For example, those actors might include:
    - Company insiders, including not only rank and file employees who through ignorance or malicious intent cause a cyber incident but also information technology (IT) managers, risk managers, and personnel from the finance, human resources, and legal departments who have roles in addressing cyber risks and incidents;
    - Third party contractors who provide companies with business support – including cloud, IT, and other services – who must themselves exercise good cybersecurity to protect their corporate clients; and
    - External attackers – including nation states, criminals, terrorists, hacktivists, and others who seek to alter, steal, damage, or render inaccessible corporate assets through cyber means.
- One participant asserted that "insider threats" include well-meaning company personnel who strive to get new products out the door before the company's competitors. In some cases, they do so by deliberately circumventing their company's security processes. The participant stated that corporate leaders should develop executive committees to develop strategies for keeping their companies competitive without sacrificing security in the process.
- Other participants cited examples of the uninformed human actor in action, emphasizing that people, policies, and security processes – not technologies – are the crucial factors for getting cybersecurity right. Participants cited several examples of bad cyber practices by employees, including: (1) working from home on unsecure systems; (2) leaving laptops in public places (e.g., buses); (3) using iPhones for sensitive work matters; (4) using thumb drives to transfer files; and (5) using their personal devices, as part of the growing bring your own device (BYOD) trend, to do their work. One participant advised that the failure of senior executives to follow cyber policies and processes while on foreign travel is "one of the worst breaches that we have."

Corporate Culture Considerations

- Several participants commented that broader and more consistent adoption of better cybersecurity practices by rank and file employees ultimately depends upon a corporate ethos that makes those practices a clear senior management priority. Put simply, changed behaviors must start with and be practiced by individuals at the top of an organization.
- An IT professional referenced a recent study that found that 87% of companies lack an enterprise risk management approach – a missed opportunity that, if pursued, would allow corporate leaders to prioritize cyber and other risks holistically across their entire organizations. He noted, however, that the trend in large companies has been to elevate responsibility for cyber risk beyond IT

departments to "higher levels" – including chief financial officers and risk managers in positions to influence corporate policy. By contrast, the IT professional concluded, most mid-size and small companies remain segmented and tend to silo cybersecurity risk management duties exclusively within their IT departments.

- An insurer observed that such segmented companies are hindered in their ability to develop and share consistent messages about cyber risks, policies, and processes. In only two situations, he commented, will corporate leaders engage their rank and file employees in a cross-cutting way on cybersecurity matters: (1) when companies are working with carriers to assess their cybersecurity risk management and related insurance needs – an exercise that requires an enterprise-wide examination; and (2) after a cyber incident has caused some kind of loss and the company is accordingly incentivized to fix the problem.

- A critical infrastructure representative stated that collaboration on cybersecurity risk management happens more consistently in the nuclear sector, in large part because the Nuclear Regulatory Commission requires that both physical and cybersecurity experts coordinate their efforts using an enterprise risk management approach. As a result, he explained, a committee structure has developed to support this work both within companies and in partnership with other companies. The critical infrastructure representative likewise noted that the Department of Homeland Security (DHS) has advocated that a similar cybersecurity risk management approach be adopted by all critical infrastructure sectors.

- A risk manager stated that in his experience, more and more companies are moving toward an enterprise risk management approach that will help address cyber risks. He asserted that in the minds of corporate boards of directors and others along the leadership chain, IT and network security issues are now converging with more traditional risk issues. This is now happening to such a degree, he added, that cyber risk is seen as a threat not only to individual companies but also to personal and even national security. A representative from local government recommended that cybersecurity should be cast as a "duty of care issue" to continue incentivizing corporate leaders moving in this direction.

- A number of participants asserted that little education about good cybersecurity practices is happening for rank and file employees. More is needed to break from past thinking, they asserted, which encouraged employees to view cyber risk an "IT Team" issue and not their problem. One insurer agreed, adding that day-to-day cybersecurity practices need to be human-friendly so they don't hinder employees from doing their work. If they're not human-friendly, he warned, employees will engage in workarounds that will put their companies at risk. He then stated that employees get turned off by terms like "IT" and "network" and accordingly advocated for changing the verbiage.

- Another insurer concurred, noting that cybersecurity discussions cause the eyes of even senior risk managers to "kind of glaze over." Although younger generations of risk managers have a keener appreciation of the problem, he observed, a change of verbiage would be helpful for these

audiences as well. Along these same lines, an IT professional asserted that even more progress would be made if cyber risks could be monetized. Once that happens, he stated, it will be easier to discuss these risks in understandable terms with chief financial officers and other high ranking executives.

- Several social scientists addressed cognitive and motivational biases within organizations as obstacles to better cybersecurity risk management and, by extension, a more robust market for cybersecurity insurance. Cognitive biases, they explained, involve situations where individuals are unaware of the risks of their behavior. By contrast, motivational biases involve other factors, such as the high costs of a risk management investment, that deter people from taking action. The social scientists advised that cognitive biases should be addressed through education, while motivational biases should be handled through regulation.

- Participants also asserted that corporate culture challenges do not begin and end with potential insureds. An insurer noted that many insurance underwriters do not have IT backgrounds and may not themselves fully appreciate the intangible aspects of cyber risk. A risk manager concurred, noting that many carriers make a decision to insure based upon one measure: corporate revenue. Carriers instead should look at a company's data policy and security processes to get an understanding of how the company is addressing the human element. In short, she concluded, the human element should be considered by carriers from a liability and loss perspective when assessing a company for cybersecurity insurance coverage.

Cybersecurity Metrics, Requirements and Standards

- Several participants commented that the federal government should be involved in defining metrics and setting data security requirements that carriers can use to qualify companies for cybersecurity insurance policies. Others stated that what's needed is general guidance about cybersecurity "must haves" – even if at only a low baseline – to inform cybersecurity insurance discussions between carriers and potential insureds. Still others stated that the insurance industry itself should set minimum cybersecurity standards so it can send the message that if companies don't meet certain conditions, they'll be ineligible for coverage. Some participants countered, however, that it's very difficult to define meaningful minimum standards because they're out of date as soon as they're published.

- A social scientist suggested that the federal government could help drive the development of metrics, requirements and standards by gathering data from carriers about the kinds of cybersecurity insurance policies available, companies purchasing them, and claims filed. An analysis of this data, he asserted, could help answer questions regarding what characteristics of a company will make it more likely to file a claim. An insurer responded that carriers will likely not want to share this information because it would reveal proprietary and/or sensitive company information. The social scientist countered that given the stakes, carriers nevertheless should be incentivized to provide this data through appropriate grants, liability protections, and shield laws.

- An insurer noted that many companies outsource their IT services to third party providers, and that carriers often assess a company's eligibility for cybersecurity insurance with an eye toward those providers. Underscoring the need for metrics, requirements, and standards, the insurer asserted that companies often expect more cybersecurity from these providers than they can actually deliver. If companies want cybersecurity insurance, he concluded, they should obtain specific security assurances from providers before they trap themselves in long-term service contracts.

TOPIC 3: CYBER LIABILITY: WHO IS RESPONSIBLE FOR WHAT HARM?

DESCRIPTION: The critical infrastructure of the modern world undergirds every aspect of our daily lives and is interconnected in many ways. The energy, communications, and water sectors, for example, are all interdependent and dependent on each other. Electrical energy is essential for all telecommunications and cyber activity. Electrical energy likewise is necessary to transport water which, in turn, is necessary for cooling electronics and to produce power (i.e., steam turbines). Internet-enabled information technologies, moreover, are critical for operating Supervisory Control and Data Acquisition (SCADA) and other control systems that regulate water and wastewater plants and electrical transmission. Cyber attacks and other incidents that impact these and other sectors accordingly represent a serious risk to society. Likewise, much of the public's personal data is stored in widely dispersed private sector databases. Banks, credit card companies, online retailers, and their service providers often maintain vast amounts of personally identifiable information as part of their operations. All this data is an attractive target for cyber criminals. When a cyber attack or incident takes multiple critical infrastructures offline or causes a data breach or other harm, the question of who is responsible for what resulting harm is a complicated one. The purpose of this discussion accordingly was to share opinions on how to start answering that question.

DISCUSSION POINTS:

CLOUD COMPUTING CONCERNS

- An insurer identified cloud computing as a major liability concern and noted that there's a lack of clarity about who's responsible for what losses in the cloud. He cited aggregation risk as a specific worry, stating that the small number of dominant platforms supporting cloud services sets the stage for potentially large losses. If one such platform goes down, he explained, thousands of users could be impacted simultaneously. This could bankrupt a single carrier who insures a significant percentage of those users overnight. The insurer likewise emphasized that cloud service providers will not accept liability for data losses. Another insurer agreed that aggregation risk could give rise to "many, many" claims and that most companies do not understand that platforms supporting cloud services must be cyber secure as well.

- An IT professional noted that as part of an annual claims trend study that his company conducts, cloud service providers and other third parties are responsible for cybersecurity vulnerabilities and resulting cyber incidents approximately one-third of the time – a fraction that's on the increase. He observed that it's only been in the last year that most companies (and people) have been putting

sensitive information into clouds, and that some cloud service providers are now outsourcing that data to still other cloud service providers. The IT professional asserted that this trend will create a "spider web" of liability in the event of a breach.

- An insurer commented that unless a company has "a lot of weight to throw around," most customers have little power to negotiate responsibility for losses with cloud service providers. Another insurer added that when they can, companies need to negotiate and specify in cloud contracts what losses are covered, by whom, and at what levels. A critical infrastructure representative advised that the only time his company was able to get their cloud service provider to assess their own cybersecurity was to make it a condition for doing business. Another critical infrastructure representative advised, however, that cloud service providers are catching on to the need to "do" due diligence when it comes to cybersecurity. Accordingly, he concluded, there's a growing market incentive for better cybersecurity in the cloud going forward.

- Several participants noted that when cloud service providers have accepted liability for cloud-related losses, they usually limit it to only the service they've agreed to provide. Some cloud service providers nevertheless recognize that they might be sued for losses regardless of such limits and therefore purchase errors and omissions (E&O) insurance to transfer additional liability risk. Participants recommended that carriers offering E&O coverage in this scenario specifically identify the perils they'll cover and those they'll exclude, depending on the cybersecurity capabilities of the cloud service provider in question. Providers who offer superior cybersecurity, they added, should pay a lower premium for coverage.

- A social scientist asked about existing standards that apply to cloud services that might inform a customer's purchase of those services. An IT professional advised that the International Organization for Standardization (ISO) has released standards that can be customized into frameworks in this area; that the Cloud Security Alliance is also trying to develop standards; and that International Computer Security Association (ICSA) Labs is developing a cloud certification program. He advised, however, that large cloud service providers are unlikely either to tell potential customers what security measures they use or to permit an outside security audit of their platforms.

- Participants also discussed the federal government as a consumer of cloud computing services. A government participant advised that her agency is required to scan its networks for cybersecurity purposes, but that cloud service providers won't allow her agency to do the same with their platforms. She noted that her agency will likely not purchase cybersecurity insurance but is still interested in outsourcing for cloud services. Another government participant advised that the newly initiated Federal Risk and Authorization Management Program (FedRAMP) includes a process for approving cloud service providers for federal agencies at a "medium-risk level." He advised that he's counting on FedRAMP's pre-certification process as assurance that a cloud services provider has met a minimum level of security. At the same time, he added, his agency will continue its due its diligence because, "we cannot outsource responsibility for our security."

Cyber Terrorism And Cyber War

- A government participant noted that the Department of Homeland Security (DHS) and other federal agencies sponsor a variety of anti-terrorism safety programs geared to kinetic threats, but that they don't offer many equivalent programs for terrorist cyber threats. He added that critical infrastructure owners and operators have done a very good job on the kinetic side of the equation; typically, they hire experts to recommend companies that can provide them with robust command and control (e.g., guards, sensors) capabilities. When it comes to cybersecurity, however, companies are still looking for ground truth when it comes to metrics, requirements, and standards that will help them bolster their internal processes and quality assurance.

- Another participant noted that the government can attribute kinetic attacks to nation states and that – depending on the vector of the attack – the government, not owners and operators, will be liable for addressing such attacks. A critical infrastructure representative agreed, noting that his company does not have an army to protect it from a physical attack by a nation state. With regard to cyber attacks, however, he stated that it's unclear who "owns" the risk. He advised that given the prevailing confusion, his company currently self-insures against most types of cyber incidents.

- An IT professional noted that acts of terrorism are not covered by insurance. He also mentioned the issue of nation state attacks on companies that result in intellectual property (IP) losses and stated that such losses aren't covered under cybersecurity insurance. The IT professional described this situation as a "huge hole" and a "huge risk." An insurer responded that although most insurance policies have terrorism and war exclusions, most carriers won't be able to deny a cyber-related claim on these grounds unless (1) it's clear that an act of terrorism or war has occurred; or (2) a more specific exclusion addressing cyber terrorism or war is included in the policy.

- This comment led to a specific discussion about Stuxnet and recent attacks on the financial services sector that some have linked to various nation states. Some participants categorized these attacks as acts of cyber terrorism or cyber war. An insurer asserted that even if the attacks could be attributed to a specific nation state, it will be impossible to make a claim against that state. Instead, financial institutions, carriers and ultimately consumers will end up paying for the loss.

Critical Infrastructure Considerations

- While some participants asserted that the federal government should take responsibility for cyber attacks from nation states, not everyone agreed. One participant mentioned that after 9/11, claims were filed against companies – not the government. A federal government representative added that companies should not assume that the federal government will take responsibility unless it requires them to adopt a particular security solution prior to a successful attack. Even then, she commented, it's unclear that the government would own the liability.

- Building on this theme, an IT professional noted that while consumers live in a competitive environment, critical infrastructure companies really don't have competition (e.g., consumers are typically locked into one electricity supplier, water company, etc.). The IT professional asserted

that the federal government should accept liability for the cyber risk under these circumstances. If a critical infrastructure company can't handle the loss, he reasoned, it will ask the government to step in to address it. To do so, the IT professional suggested that the federal government set up a revolving fund to address cyber-related critical infrastructure losses like the fund it has established to address flood losses.

- Critical infrastructure representatives had different reactions to this proposal. One disagreed, asserting that when critical infrastructure owners and operators have been overwhelmed by losses in the past, other companies have stepped in to help – not the federal government. Another noted, however, that if the critical infrastructure in question is regulated and owners and operators have met applicable standards, it would be hard to hold them accountable. Under those circumstances, he concluded, the government *should* step forward and accept liability.

- A federal government participant asserted, however, that regulations and standards don't make the federal government responsible for loss. Instead, she stated, the only obligation the government might have would be to provide additional information to owners and operators about any increased threats. That information, she commented, would empower auditors and insurance companies to demand critical infrastructure companies to increase their security in order to maintain their coverage.

THE COURTS, LIABILITY AND THE MARKET

- Participants also discussed the role of the courts in assigning liability. They highlighted a recent case in the First Circuit Court of Appeals that involved a bank that had transferred money outside of the U.S. after authenticating what turned out to be stolen credentials. The district court had ruled that because the end user was responsible for keeping its credentials secure, the bank was not liable for the loss. The First Circuit overturned the ruling on the ground that the end user was not sophisticated enough to know that its credentials had been misused. As a result, an IT professional noted, end users are now suing banks for not having "reasonable security measures" in place.

- An insurer observed that it's difficult to assign liability in electronic injury cases and that, historically, the bar has been set at "gross negligence" – a very high standard that's made it difficult for harmed parties to hold *anyone* responsible for their losses. This same situation, he added, is likely to play out with cloud service providers. If a harmed party could successfully sue a cloud service provider for a data breach, then the utility of the service would disappear and the provider's continued existence would be in jeopardy.

- The participants subsequently turned their attention to how the market might help sort out these issues. A critical infrastructure representative asserted that whoever has the brand equity will have the ultimate responsibility for a loss even if a supplier, vendor, or service provider is to blame. Stated another way, the company whose name is in front of the consumer – regardless of fault – will own the liability because its reputation will be on the line. That company accordingly

will have to insist on superior cybersecurity by its suppliers, vendors and service providers in order to protect both its customers and itself from harm. The critical infrastructure representative concluded that the market, not the government, should work toward best solutions in this regard.

- A social scientist stated that the whole point of cybersecurity insurance is to try to transfer risk to someone else and questioned why a company with brand equity should have to keep tabs on the cybersecurity of its contractors as well. The critical infrastructure representative responded that the amount of loss to a company's customers from a breach will be immaterial compared to the loss of the company's reputation and an ensuing loss of customers and sales. He added that, over time, these high stakes will drive cybersecurity solutions through business contracts and related transactions most efficiently.

- Participants noted that this situation will likely lead every company to do for itself in a fairly chaotic environment, although some allocations of liability – as informed by the market – will work better than others.

- A federal government participant asserted that distinctions need to be drawn among guilt, liability, and responsibility. Some guilty parties (e.g., third parties) might never pay for losses in some cases. Instead, a company that collects data is ultimately liable for its security given reputational concerns. At the same time, he added, no system will ever be completely secure so everyone must accept some responsibility for some risk. The question for companies thus becomes, "Do we accept the risk we face or do we transfer it somewhere else?" A critical infrastructure representative agreed, asserting that companies must take extra steps to protect the data they've collected – at least until more standards, best practices, and metrics, and more cybersecurity insurance options, can assign liability more precisely.

- As part of this conversation, an IT professional noted that "big data" is the buzzword of the day, and that companies that have massive amounts of data, like banks, are increasingly focusing on cybersecurity to protect it. Another IT professional advised that when data breaches first occurred in the retail business, the consequences "scared" the whole industry into ramping up security – a phenomenon that is now taking place on a smaller scale in the medical industry.

TOPIC 4: CURRENT CYBER RISK MANAGEMENT STRATEGIES AND APPROACHES

DESCRIPTION: Many organizations have both centralized and distributed resources for managing their cybersecurity needs – including full-time professional staff and third party service providers who provide essential compliance, legal, policy, privacy, and technical support. Approaches to managing cybersecurity risk vary, however, across and within sectors. For example, cybersecurity risk management strategies are often informed by different regulations and standards such as ISO 27001, NERC-CIP, PCI-DSS and the NIST 800 series publications. These authorities and others offer organizations a patchwork of options for meeting their cybersecurity risk management requirements. To date, however, there are no consensus cybersecurity best practices or controls upon which all organizations can rely. A more mature cybersecurity insurance market might encourage the adoption of such

practices and controls. The purpose of this discussion accordingly was to explore how the different stakeholder groups view current obstacles and opportunities in cybersecurity risk management and how they might influence the development of cybersecurity insurance policies going forward.

DISCUSSION POINTS:

- A critical infrastructure representative asserted that corporate risk managers have moved away from the concept of cybersecurity risk prevention and toward the concept of cybersecurity risk management – the goal being to complicate an adversary's malicious activity by making a company a less attractive target. He added that response time when cyber attacks occur is critical; in most cases, companies have only minutes to address threats to networks. The critical infrastructure representative noted that, as a result, corporate risk managers are increasingly looking to predictive analytics about cyber risks that they hope will inform their cyber risk preparedness.

- A social scientist asked how companies currently identify the likelihood of a cyber attack and quantify its associated risks. Several participants responded based on their individual experiences:

    - An IT professional described the frequency and severity of events as the "Holy Grail" of cybersecurity risk management. He added that while companies can analyze the frequency of cyber incidents based on some available data, it's harder to determine their severity. The problem, he explained, is that different industries are held to different standards. He cited the medical industry as an example, noting that it has more cyber-related claims than most because of the Health Insurance Portability and Accountability Act's (HIPAA) rigorous information security and privacy standards.

    - An insurer stated that carriers assess companies on a geographical and sector basis, noting that common sense often helps identify which companies are most likely to be attacked.

    - A critical infrastructure representative commented that the best thing that companies can do to assess the frequency and severity of a cyber attack is to build relationships with all stakeholders – inside and outside government – who have actionable and trustworthy threat intelligence about the risk. Even if a company has the best threat information available, he added, it will provide only a partial picture for risk prioritization purposes.

- A critical infrastructure representative commented that the Department of Homeland Security (DHS) has done a good job of identifying cyber threat actors. She stated that companies can't insure themselves against everyone and everything, however, and asked how they should decide what cyber risks to address through insurance. Another critical infrastructure representative responded that even if a company follows available standards and best practices to a tee, it will not be immune to cyber attacks and intrusions. A government participant noted that while that's true, the real issue isn't being protected against the biggest and most complex cyber threats; instead, it's worthwhile for companies to immunize and protect themselves against basic threats. An IT

professional agreed, stating that the market dictates the proper level of response to cyber risks and cost. He added that large companies generally have solved the problem of virus-based attacks and that sophisticated cyber attacks are now their major problem.

Corporate Culture Considerations

- An insurer noted that when it comes to cyber risk, a number of risk management benchmarks based on company size, data type, and other factors exist. There is no single, unified benchmark, however, for all risk scenarios. Another insurer asserted that while benchmarks are good in theory, they're not good in practice because rank and file employees tend to subvert information technology (IT) practices to suit their needs. He added that risk managers can never "build out" the human element from the equation, so IT professionals and risk managers alike must account for it within their cybersecurity strategies.

- A third insurer stated that companies would be well-served by developing standard operating procedures (SOPs) for cybersecurity risk management that can serve as a foundation for engaged corporate risk cultures. Those cultures, he added, should include incentives for corporate leadership as well as rank and file employees to know and consistently implement the SOPs. A fourth insurer commented that those incentives work best when both leadership and staff are held accountable for SOP compliance. He added that a corporate culture that promotes this accountability filters positively throughout the company – creating the conditions necessary for even the least knowledgeable employee to improve their cybersecurity performance. A critical infrastructure representative noted, however, that corporate leadership must do more than just send emails back and forth with staff. Instead, leaders must hold many conversations across their organizations to initiate and enforce each and every SOP's implementation.

- The ongoing problem, one risk manager advised, is that rank and file employees in most companies don't know that what they're doing or not doing may have an adverse impact. Most SOPs, moreover, are not user-friendly. When asked if user education would help improve the situation, an insurer responded that it might be part of a solution but likely would not go deep enough. At the end of the day, even with the best cybersecurity risk management training, users will still find workarounds. A second risk manager agreed, adding that good cybersecurity comes down to people who are dedicated and enthusiastic about security, aware of threats, and incentivized to do the right thing.

- A government participant asserted that, given the human element, cybersecurity risk management decisions should be moved away from end users whenever possible. He stated that risk management technologies should be adopted to automatically protect company information in the same way that car manufacturers install safety technology to minimize human error.

- A social scientist asked how companies measure how well they're doing when it comes to executing their SOPs and broader cybersecurity risk management strategies. A critical infrastructure representative suggested that a good set of metrics would be helpful – including, for example, a

measure of how many pieces of malware actually make it into the corporate environment. He added that penetration testing is another important way to assess the effectiveness of a company's cybersecurity measures.

Data Compartmentalization

- Participants reported that in order to enhance the security of their data from cyber attackers, many companies are starting to compartmentalize. Instead of protecting all of their data across their entire enterprise, IT professionals and risk managers are increasingly identifying – through intensive discussions and examination – the "crown jewels" that merit special protection. Once that data has been identified, IT professionals isolate it from corporate intranets and the World Wide Web. Participants advised that such data typically comprises no more than two to three percent of a company's total data. A similar trend is apparently underway with cyber risks to the global supply chain. According to one critical infrastructure representative, companies have realized that they can't protect every aspect of that chain and therefore have started prioritizing key functions, nodes and systems.

- A critical infrastructure representative recommended that companies *not* model their compartmentalization approaches on the federal government's classification system, which he described as being plagued with over-classification problems. Another critical infrastructure representative emphasized, however, that the private sector has the opposite challenge: companies tend to "under-classify" their most valuable information. In his view, the federal government's classification system and a private sector system for isolating data crown jewels could share many of the same attributes. The success of both, however, will depend upon accountable, well-trained people who are incentivized to implement them properly.

Risk Management on Offense

- A social scientist asked whether companies should incorporate "attacks" as part of their cybersecurity risk management strategies. Specifically, he mentioned infiltrating the black market to ascertain the motives, intent, and capabilities of cyber attackers in order to thwart them before they act. A critical infrastructure representative responded that, in a certain sense, obtaining a better understanding of cyber attackers from the federal government and other sources is an example of cybersecurity risk management on "offense." He added that if it were legal to attack cyber attackers before they strike, and if unintended consequences could be minimized, owners and operators might consider more such offense options.

- An insurer reported that new technologies are emerging to identify and track cyber criminals – a major advance toward fixing the long-standing cyber attack attribution problem. Other participants noted that companies have a right to self defense of their property in the physical world and that a dialogue should be initiated between the private sector and the federal government, particularly law enforcement, about what companies should be permitted to do with that authority in cyberspace. Participants expressed particular interest in a company's right to eliminate bad actors from their systems and to recover their stolen data.

Risk-Based Cybersecurity Insurance

- An insurer noted that most cyber-related losses today result from data breaches and that practically "everyone" wants breach notification insurance as a result. He commented that many carriers need to learn more about cyber risks and the consequences cyber-related data breaches before they can develop truly attractive policies. The insurer asserted that only 17 carriers actually provide cybersecurity insurance policies today. Only five or six of those carriers, he added, are willing to develop "manuscripted" policies – custom-drafted from scratch – to cover cyber-related losses excluded by template policies. They do so, he added, by analyzing data on non-public cyber incidents shared by their clients.

- A critical infrastructure representative asked if carriers offer to lower premiums if companies take steps to better manage cybersecurity risk. An insurer responded that potential clients often know more about their cyber risks than anyone else. Carriers therefore engage clients heavily during the underwriting process. Historically, the insurer explained, they used extensive questionnaires to obtain client input about risks but today speak directly with clients in order to understand their vulnerabilities and risk management controls. Based on these interactions, he concluded, carriers over time have (1) determined on a percentage basis where companies will most likely experience cyber-related data breaches; (2) analyzed the likely financial consequences of those breaches; and (3) developed premium pricing frameworks accordingly.

- An insurer asserted that many companies don't want to pay for cybersecurity insurance and would rather pay for lawyers when losses happen – a mindset that results from corporate leadership not paying sufficient attention to cyber risks. He asserted that this situation should be addressed through better education of corporate boards of directors and more consistent risk messaging from the insurance industry and business leaders generally about the stakes. The insurer added that if cyber criminals know that executives are actively communicating about and addressing cyber risks to their companies, that knowledge alone can deter them from attacking.

Cybersecurity Standards

Effects of Standards on Cyber Risk Management Strategies

- When asked if any standards exist that can be used to inform corporate cybersecurity risk management strategies, an insurer responded that companies in Europe and across the Asia/Pacific region use ISO 27000 information security management standards as the basis for their internal cyber risk assessments. He also mentioned that organizations that handle cardholder information for major credit, debit, and other cards use the Payment Card Industry (PCI) information security standard.

- An IT professional commented that although different companies interpret these and other standards differently, they serve the very useful purpose of "ruling out burning plank issues." Stated another way, carriers use standards to identify companies that manage cyber risks in a

completely different way from their peers and decide whether those different approaches should qualify or disqualify them from coverage. Good cyber risk managers, he added, also seek the most current "best practice" information to help them address existing gaps and emerging issues.

- A critical infrastructure representative stated that standards become outdated quickly and, consequently, are often updated quickly. He noted that unless there is significant flexibility within the standard itself, it can become an unsustainable burden for companies to keep up with changes. Another participant added, however, that very flexible standards that give companies too much leeway undermine the rationale for having a "standard" in the first place.

- An insurer noted that we live in a world of outsourcing, and that it's virtually impossible for companies to ensure that their third party service providers are complying with available standards. A second insurer stated, however, that there are commercial drivers for adopting such standards. While good cybersecurity used to be considered a business advantage, it's now becoming the norm. In order to get business, he explained, it's good business to be "up to standard". One participant noted that companies who outsource for services are increasingly requiring third party providers to meet certain standards. A critical infrastructure representative cited the privacy and information security rules included in HIPPA as an example. Companies that don't comply with HIPPA, she stated, have no chance of winning a bid for a contract that requires such compliance.

- Other participants cited fear of regulation as another driver for the adoption of available standards. They explained that companies believe they can manage cyber risk better by coming up with solutions themselves and consequently adopt ISO 27000, PCI, and other information security standards to avoid government action. An information technology professional reported that some private sector companies are planning discussions about developing new, more rigorous cybersecurity standards. Those discussions will likely take place within the next year.

- A critical infrastructure representative added that in addition to such discussions, there's already a fair amount of informal conversation underway among companies about cybersecurity benchmarks and best practices. He reported that he regularly meets with his colleagues at other companies to share information about their cyber-related risk management experiences and how they're securing their environments. Many of them, he added, are faced with the same challenges. An insurer commented that such information sharing is not universal, however, especially when it comes to third party service providers. In that context, he asserted, many companies simply find it easier to write a liability paragraph into a services contract rather than do an in-depth analysis of, and information sharing about, a third party's security protocols.

- A second insurer commented that handling cybersecurity through contractual liability provisions is unlikely to encourage better security practices. She stated that the "right" contract negotiators are rarely at the table when such provisions are drafted; in most cases, she added, IT professionals responsible for a third party's cybersecurity never see the contract. The second insurer suggested that a better approach would be for companies to assess supplier cybersecurity before signing deals and to then periodically reassess during the life of the contract. A critical infrastructure

representative raised practicality concerns with this approach. Some companies have thousands of service providers, he noted, and doing assessments for all of them – on even a rudimentary basis – would be logistically difficult and prohibitively expensive.

Standards and Cybersecurity Insurance Assessments

- An insurer stated that discussions focused solely on a company's technical compliance with available standards are of limited utility when setting rates for policy premiums. Instead, he continued, carriers should have long discussions with companies about their risk cultures. The potential size of a loss, as informed by those risk culture discussions, is a best indicator for pricing cybersecurity insurance contracts.

- An infrastructure owner commented that actuarial models for setting rates for policy premiums already exist. In response, an IT professional remarked that carriers actually are "making it up as they go along." An insurer responded that the problem with using actuarial data to develop rates is that there's too much variability in the data. He concurred that carriers are "making it up as they go along" but that they have no other choice. Without definitive standards for what acceptable cybersecurity looks like that can be applied to companies across the board, carriers must assess companies and their risk cultures on a company-by-company basis. Moreover, he concluded, as long as the federal government doesn't take an active role, the market is left to its own devices to determine what standards and best practices should apply.

- Another insurer concurred that carriers apply a variety of overlapping principles to assess whether a company should qualify for cybersecurity insurance and at what price. He noted, however, that we live in a commercial reality where a company applying for insurance will likely choose a carrier with a less stringent assessment than a carrier with a more stringent one.

Cyber Incident Impacts on Insurance Policies

- An insurer asserted that if a company covered by a cybersecurity insurance policy files a claim and the carrier pays it, it doesn't necessarily mean that the carrier will cancel the contract. The carrier may, however, impose additional cybersecurity requirements on the company as a condition for continued coverage. He added that after a breach, some companies actually become more secure on their own because they are determined not to be successfully attacked again.

- Another insurer stated that a carrier's avoiding particular companies following a breach might make sense if the resulting losses are systemic, but only if there's evidence of demonstrable negligence. He added that companies should expect their policy premiums to change after a loss and should take action to clean up their security. An IT professional agreed, noting that he works for a government entity that started looking at its IT security and budgeting for it only after a major cyber incident occurred. He added that following some breaches, an overreaction sometimes occurs which leads to a less-than-optimal allocation of risk management resources. The IT professional concluded that risk-based analysis of cyber incidents should drive security and not just recent experience.

- An insurer commented that a change that will likely have a big impact on the U.S. cybersecurity insurance market is coming soon. In 2014, the European Union (EU) will begin imposing fines for significant breaches of personal information, totaling up to two percent of a company's global revenue. The insurer mentioned that this represents a potentially huge penalty that will focus companies' interest on cybersecurity insurance. Specifically, the EU hopes to incentivize corporate leaders to prioritize cybersecurity risk management within their companies by elevating cyber issues out of their traditional IT silos. The insurer advised that the EU fines will apply to American companies that do business in the EU.

TOPIC 5: CYBER INSURANCE: WHAT HARMS SHOULD IT COVER AND WHAT SHOULD IT COST?

DESCRIPTION: While the headlines are full of stories about data breaches, online identity theft, and cyber warfare, there is uncertainty about what cyber risks are of greatest concern to stakeholders, what best practices should be adopted to mitigate those risks, and which ones carriers are ultimately able and willing to cover. Carriers likewise need appropriate ways to quantify those risks and to measure the effectiveness of cybersecurity risk management strategies and security improvements over time that avoid "stab in the dark" approaches. Although mature risk models based on probabilistic risk analysis exist for physical risks to the nuclear power and other industries, it's unclear where the equivalent "state of the art" stands for cyber risks. Enhancing the cybersecurity insurance market accordingly will remain a difficult proposition until stakeholders begin exploring and answering these questions. The purpose of this discussion accordingly was to initiate conversation on these critical issues.

DISCUSSION POINTS:

PRICING CONSIDERATIONS

- A social scientist commented that no exact science exists to determine the best price for an insurance policy but noted that to do so, carriers tend to convert everything to corporate revenue. Pricing therefore becomes a question of determining how much a company can lose rather than the likelihood of risk to a company or the company's compliance with available standards. Instead of corporate revenue, she asserted, a better metric for insurers to consider is the number of recorded cyber incidents that a company has experienced. One insurer agreed, but emphasized that such records aren't publicly available – a situation that makes it impossible for carriers to develop the actuarial information they need for application to a broader set of potential insureds. A second insurer, however, disagreed with the social scientist's position and said that pricing determinations should depend on the type of coverage to be provided. For hacking protection, he noted, corporate revenue is the most relevant metric.

- A critical infrastructure representative stated that insurance policy pricing should be directly informed by an assessment of a company's risk culture. How long that company has complied with available standards and best practices can be an indicator of how "defensible" it is against cyber attack. By the same token, he added, the larger the company, the more likely it is to be the target of a cyber attack – another key consideration that should factor into pricing.

- Following this discussion, an insurer commented that how carriers price cyber risk is just one aspect of a broader inquiry about the proper role and scope of cybersecurity insurance that should examine: (1) cyber risks that carriers don't cover; (2) cyber risks that carriers should cover and at what cost; (3) cyber risks that carriers are comfortable covering on their own; and (4) other cyber risks that threaten the public good (e.g., catastrophes) that lend themselves to discussion through a private-public partnership.

INFORMATION SHARING ISSUES

- Expanding on this point, an insurer stated that there are certain risks with potentially very large losses (e.g., crop failures and floods) that the federal government must assume as the "insurer of last resort." There are other significant risks, however, that the insurance industry might be able to cover in the future that would serve the public good. To insure against cyber-related critical infrastructure failures and losses, he continued, a private-public partnership would be necessary to establish the conditions for market entry by private carriers. Specifically, he asserted, the federal government would need to provide reinsurance for a five to 10-year period during which cyber risk and incident information can be shared – and relevant actuarial data developed – to support the business case.

- Another insurer agreed that the federal government serves as the "back stop" when catastrophe strikes and cited a lack of actuarial data and information sharing as significant obstacles to developing new cybersecurity insurance products for even more discrete cyber risks. For example, if a cyber attack on a major cloud service provider were to impact multiple industries, and if carriers subsequently "tapped out" because they were required to pay on thousands of loss claims, the federal government would have to step in to help prevent a market failure. What's needed to address this less-than-optimal situation, he continued, is a robust reinsurance market that would allow the private sector to assume this back stop role. The insurer explained that while reinsurers normally would use statistical analysis to decide whether to invest against this kind of risk, there simply isn't enough quantifiable data about cloud-related losses – yet – to do so.

- A third insurer added that while there's historically been some information sharing about cyber-related incidents and losses, most companies are afraid to report this data given potential regulatory, reputational, and other impacts. The limited sharing that has taken place, moreover, has occurred only with people who absolutely need to know. This lack of sharing has kept carriers in the dark and the cybersecurity insurance market in check.

- Participants agreed that if society wants the insurance industry to start expanding coverage to currently uninsurable losses, carriers will need to know more about what kinds of incidents are actually happening, how they should be valued, and how to measure the effectiveness of cybersecurity risk management strategies designed to address them. Several participants recommended that an independent reporting mechanism be created by carriers, companies, and other interested stakeholders so they can begin sharing relevant data on these topics. An insurer cited the Terrorism Risk Insurance Act (TRIA) as a model for this arrangement, noting that it

establishes the federal government as the insurer of last resort in terrorism cases until enough data exists to encourage private carriers to enter the reinsurance market.[3] A similar framework, he argued, could be established for cyber incidents.

- The same insurer added that to succeed, however, there must be demand for the new cybersecurity insurance products that this arrangement could help foster. He stated that buyers would be motivated to purchase the policies if they could limit their liability for losses to a set amount of required and available insurance. The insurer accordingly recommended passage of a "Cyber Safety Act," modeled on the Support Anti-Terrorism by Fostering Effective Technologies Act (SAFETY Act),[4] to spur the development of cybersecurity enhancing technologies. Like the SAFETY Act, he asserted, a Cyber Safety Act could require buyers of those technologies to purchase cybersecurity insurance in an amount set by the federal government and could likewise cap buyer liability at that same amount. In his view, buyers would flood the market to avail themselves of both the insurance protection and corresponding liability limits.

OPEN PERILS

- An insurer expressed concern for mid-size and small companies that increasingly outsource their IT and other services to third party providers to save on costs. He asserted that many of them believe, at face value, provider representations that they practice good cybersecurity. Rather than purchase the full package of insurance they might need in the event of a provider-caused loss, many mid-size and small companies accordingly buy only a limited amount of coverage (e.g., baseline coverage required by law or regulation). The insurer warned that if mid-size and small companies don't get a firmer handle on their risks and those of their third party providers – and insure against them appropriately – they may find themselves in a world of hurt down the road. If more and more companies continue on this path, he added, aggregation concerns will cause carriers to avoid insuring companies affiliated with the same provider.

- A social scientist stated that he was concerned that the group had not addressed anything other than cyber attacks on IT systems. He described a scenario where a cyber attack on a website results in various malfunctions in a car's operation, causing a crash. If car insurance doesn't explicitly cover the loss, he asked, what happens? An insurer responded that while a policy is not infinite regarding what it covers, carriers do cover losses that aren't specifically intended at the

[3] *See* Terrorism Risk Insurance Act, *supra* note 2.

[4] The SAFETY Act provides liability protection to sellers of anti-terrorism technologies and services that are designed to prevent, detect, deter, or respond to a terrorist attack. Liability for a seller whose technology or service receives SAFETY Act designation is capped at the level of insurance coverage that the Department of Homeland Security requires it to carry. SAFETY Act protections may also extent to users. *See* Homeland Security Act of 2002, P.L. 107-296, Subtitle G, available at https://www.safetyact.gov/pages/homepages/SamsStaticPages.do?insideIframe=Y&contentType=application/pdf&path=sams\refdoc\Safety_Act_Legislation.pdf.

time a policy activates. A second social scientist replied that such instances are known as "open perils" and that if a policy doesn't mention a potential loss as not being covered, it's covered.

TOPIC 6: IMPROVING THE CYBER INSURANCE MARKET: STAKEHOLDER ROLES AND RESPONSIBILITIES

DESCRIPTION: Cybersecurity insurance stakeholders include insurance providers, risk management professionals, social scientists, information technology (IT) experts, and critical infrastructure owners and operators. All of the groups have a shared interest in a more robust cybersecurity insurance market as well as their own unique interests that depend upon their particular areas of expertise, their varied roles and responsibilities, and their perceptions about how those roles and responsibilities will evolve going forward. This forum accordingly offered a space for participants to build awareness about what roles are, could, and should be played by different stakeholders in enhancing the cybersecurity insurance market, what specific responsibilities those roles should entail, and obstacles and opportunities for fulfilling them.

DISCUSSION POINTS:

STAKEHOLDER SPECIFICS

- A social scientist commented that as a researcher, his role in advancing the cybersecurity insurance market is to help quantify cyber risks better. He stated that researchers should work toward "putting a number" on different information technology (IT) systems in order to help companies and consumers compare their respective cybersecurity strengths and weaknesses.

- Another social scientist reflected on what he'd heard earlier in the day – specifically, that carriers are good at providing coverage for risks that they understand and can quantify. He shared his perspective that carriers don't know how to quantify cyber risk well enough to feel confident when they underwrite cybersecurity insurance policies. Companies accordingly need to explain the cyber incidents that they've experienced better, in terms of the actual impact, so carriers can make more informed assessments about policy coverage. A critical infrastructure representative agreed, noting that companies themselves also need to understand the cyber incidents that they've experienced better in order to be informed consumers.

- Regarding the role of carriers and the federal government, an insurer stated that carriers will provide cybersecurity insurance products when they understand the risks and the government will "cover" citizens against harms when it's not appropriate for carriers to do so – typically, when catastrophic and/or systemic risks are involved (e.g., cyber-related critical infrastructure failures, terrorist attacks, and war). He added that carriers in theory should be responsible for cyber hurricanes (i.e., widespread cyber losses not caused by nation states) but that they don't yet know how to underwrite such losses. To address this shortcoming, the insurer continued, carriers and the federal government should form a private-public partnership to help foster the development of

actuarial data and information sharing not only between carriers and the government but also among carriers as well. He advised that the only place where this kind of cybersecurity information sharing occurs today is within sector Information Sharing Analysis Centers (ISACs).

- A social scientist stated that the role of the National Institute of Standards and Technology (NIST) is to provide and improve IT security and other standards. Better data about cyber risks and losses, he added, will result in more complete and improved NIST standards. The social scientist also referenced a draft document that describes the Department of Homeland Security (DHS) as the lead agency/clearinghouse for sharing unclassified information about cybersecurity (e.g., intelligence, data attacks, malware identification) with both private sector and public organizations. He recommended that such information be sent to both carriers and sector ISACs, including the Financial Services ISAC (FS-ISAC). He likewise recommended that DHS and the Treasury Department encourage the FS-ISAC to share this information directly with carriers to inform their policy development efforts.

- Several participants referenced group discussions that took place earlier in the day regarding the roles and responsibilities of corporate boards of directors in improving the cybersecurity insurance market. Among other things, they asserted, they must foster risk cultures that hold both corporate leaders and rank and file employees accountable for complying with the available standards and cybersecurity standard operating procedures (SOPs) that they've adopted within their organizations.

- An insurer commented that the federal government should play the role of "market driver" by exercising its procurement power to help set common cybersecurity standards. He noted that in the private sector, contractual requirements can be a very effective tool for encouraging the adoption of better cybersecurity by business partners. The federal government, he asserted, could likewise set a tone via its own contract requirements by requiring third party service providers to meet specific standards. Once those standards are published, he continued, carriers could use them in future insurance products as well. Another participant commented that while every federal government contract has insurance requirements, none of them require cybersecurity insurance. Having the federal government set the tone through procurement would "raise the game in all aspects of risk management, including cybersecurity insurance." The impact of this approach on changing risk behaviors, a third participant added, would be "profoundly effective."

INFORMATION SHARING BODY

- An insurer commented that companies produce a lot of useful information about cyber attacks. If there was an independent body that could share that data anonymously, he added, it could significantly improve the ability of the insurance industry to offer more relevant products and price them appropriately.

- A second insurer remarked that if the federal government legislated an independent body of this kind, it could incentivize companies to share their cyber incident information in return for their being able to remove critical infrastructure exclusions from their current cybersecurity insurance

policies. A third insurer responded, however, that this approach would put the cart before the horse. A first order of business, he asserted, would be to identify stakeholders who need to be incentivized to participate as well as a funding mechanism for the independent body that stakeholders would be willing to support. One participant suggested that future members could pay a premium to the federal government – assuming it initiated its operations – until the private sector was in a position to take over responsibility.

- Another insurer emphasized that it would be important to manage expectations about what the independent body could accomplish regarding cyber-related information sharing. He emphasized that there are key cyber incidents that the insurance industry does not cover. When it does provide coverage, he added, it does so because an extensive accumulation of risk data exists. Cyber risk is one area where that data is still largely absent. While the independent body could promote the kind of information sharing that carriers need to develop new policies, the insurer concluded, progress on collecting and analyzing that data – and translating it into new product offerings – will likely be slow.

- In response, an insurer recommended that the insurance industry ask its customers about the kinds of cyber risks they want covered in order to avoid spending years creating products customers don't want. Another insurer replied that this approach actually leads to another information sharing problem. In his experience, he stated, when carriers go to mid-size and small companies that don't have good cybersecurity or significant assets to protect, they'll turn down insurance. If carriers nevertheless point out that large companies depend on the security of the mid-size and small companies with which they do business, the mid-size and small companies will still wonder why they should care about insurance. Accordingly, if carriers were to ask them what kind of cybersecurity insurance they need, they'll think of their bottom line – not the public good – when answering the question. The disconnect is so significant, he concluded, that cybersecurity insurance might have to be free just to pique the interest of mid-size and small companies.

- One participant suggested that an organization like the American Council for Technology – Industry Advisory Council (ACT-IAC) might be a good forum for conversations about how to transition the federal government's reinsurance role in the cyber hurricane context to private sector carriers.

Culture and Responsibility For Losses

- Another participant mentioned the responsibility of individuals for cybersecurity outside the workplace, noting that the general need for cybersecurity education discussed earlier in the day underscored the need for cybersecurity insurance products for the "home user." An insurer responded that cybersecurity insurance for individuals is unlikely to be cost effective. He added, however, that individual policies geared toward identity protection already are available, typically for high net worth individuals.

- Another participant asked about where the education "piece" might fit within cybersecurity insurance policies for individuals. He expressed concern that if a person had such a policy, they might foolishly think that they're totally protected and won't bother with cybersecurity best

practices. Another participant responded that cybersecurity insurance policies for individuals could be crafted in a way to drive better cybersecurity risk management behavior by companies and individuals.

- An insurer observed that if society can create a national risk culture that prioritizes the protection of personal information, we'll be in a much better position to discuss not only individual responsibility for cybersecurity but also the responsibility of other stakeholders – including technology providers. The insurer observed that people adopt new technologies into their worlds faster than they can understand them. When things go wrong with a geospatial technology, he asked, is it the responsibility of the smart phone producer that tracks your location; the social media site that posts your location with a photograph; the internet service provider (ISP); or is it just the consumer?

- A participant commented that in order to develop a savvy risk culture when it comes to technology, transparency will be key. The participant noted that most people don't know all the functions of their smart devices and asked whether people should be liable for what they don't know. Another participant responded that people don't take the initiative to understand because they don't perceive risk. For the same reasons many people don't know much about how their cars work, he observed, many people don't know much about how their mobile computing and communications devices operate.

- An insurer stated that Europeans have fewer issues of this kind. With regard to the private sector, he explained, responsibility for cyber incidents in Europe belongs to the technology provider (e.g., the business or website that collects and processes data). With regard to government, he added, there are many agencies at all levels of government in the U.S. with a wide variety of uncoordinated opinions and voices. Europe, by contrast, has a much more straightforward structure that simplifies which agency is responsible for what aspect(s) of cybersecurity and what information they must share with whom.

TOPIC 7: SEQUENCING SOLUTIONS: HOW SHOULD THE MARKET MOVE FORWARD?

DESCRIPTION: Last summer, the European Network and Information Security Agency (ENISA) developed four recommendations for enhancing the cybersecurity insurance market in Europe: (1) scoping challenges to that market by surveying private sector companies in order to determine their knowledge of the cyber insurance market; types of cyber risks and losses insured; premiums, pay-outs and other issues; (2) exploring whether harmed parties should be able to initiate "collective action" against service providers that do not adopt sufficient cybersecurity protocols – and whether the right to such collective action would encourage better risk management practices by providers, a more robust cybersecurity insurance market, or both; (3) adoption of frameworks to help firms determine the value of their information in order to better inform a decision to purchase cybersecurity insurance; and (4) exploring the role of government as the insurer of last resort. Whether any or all of these ideas would work in the American cybersecurity insurance market, and in what sequence, is uncertain. The purpose of this discussion accordingly was to obtain current thinking by the various stakeholder groups about what

steps should be taken and in what priority order to help develop a more robust cybersecurity insurance market in the U.S.

DISCUSSION POINTS:

CYBERSECURITY VOCABULARY

- An insurer stated that when it comes to insurance, the word "cyber" should be banned because it's confusing. If we in the insurance industry don't understand what we mean by "cyber," he asked, how can we expect users to understand? The insurer explained that the term encompasses so many things – such as network security, data breach, and loss of intellectual property – that it's hard for customers to figure out what a particular policy actually covers. A risk manager agreed and suggested that insurers should instead discuss cyber as a "class of coverage" under which different categories of loss fall. An IT professional recommended that the Department of Homeland Security (DHS) come up with standard taxonomies that insurers and other stakeholders could use to engage more productively. Toward that end, he mentioned that the federal government's National Initiative for Cybersecurity Education (NICE) could be a useful mechanism for educating chief executive officers and other corporate leaders about cyber risks and cybersecurity insurance.

FIRE AND CYBER

- A critical infrastructure representative stated that the analogy between sprinkler systems for commercial buildings and cybersecurity best practices for companies is a good one. Sprinkler systems lower the likelihood and extent of damage from fire and, accordingly, the cost to insure a commercial building. Cybersecurity best practices, he added, could do the same thing. The critical infrastructure representative further asserted that companies already think about risk this way as part of their risk models. He then suggested that to encourage companies to identify and implement cybersecurity best practices, carriers should do a better job of communicating (1) the types of cyber incidents their policies cover; (2) the number of companies purchasing such policies; and (3) the premium savings available to companies who implement best practices.

- A social scientist expressed his discomfort with correlating insurance with better social outcomes. Good data ensures good outcomes, he explained, and what carriers currently face is a data problem about cyber risk – not a problem with motivating companies to adopt cybersecurity best practices. The social scientist emphasized that carriers that provide fire insurance are agnostic about whether people have safe homes. Instead, they want the certainty that data can provide to properly price insurance premiums.

- A risk manager commented that the different agendas and missions of federal government agencies might spur very different reactions to a cyber "arson" situation. On the one hand, he stated, DHS wants to promote better cybersecurity and will try to help a company put out a fire. On the other hand, the Federal Trade Commission (FTC) and state attorneys general will want to punish perceived negligent behavior, will assume you've been negligent, and will sue you.

- An insurer responded that he was uncomfortable with the fire and cyber analogy. In a cyber arson situation, he explained, it's not about just one bad actor trying to burn down your house. It's about everyone trying to burn down your house. He stated that, for that reason, the fire and cyber domains don't really parallel each other. Another social scientist agreed, commenting that cyber arson is also about a bad actor lighting your house on fire so he or she can light all houses on fire.

- While an IT professional concurred that the fire and cyber analogy falls short, he stated that the same data problems that once challenged the fire insurance market now face the cybersecurity insurance market. He noted that carriers can insure many things so long as they know what the risks are and what the economics surrounding them look like. As more data has become available, especially in the data breach area, more insurance policies have become available. The lack of data surrounding cyber-related catastrophe, intellectual property, and reputational losses, he observed, makes those losses much harder to insure.

THE DATA OPTION

- One participant responded that the "data option" for improving cybersecurity insurance products already exists. He noted that companies have lots of data in their systems that they could use to understand what kinds of cyber incidents they've experienced and what risks they face. The problem, however, is that few have interpreted that data to clarify their potential losses and corresponding insurance needs. A critical infrastructure representative explained that companies haven't done that work, in part, because they don't know that affordable and otherwise attractive cybersecurity insurance policies exist. A government representative observed that they instead choose to self-insure – a situation that prevents carriers from obtaining and analyzing the data they need to enhance their product offerings. An insurer added that this problem is compounded by the reluctance of individual carriers to share, for proprietary reasons, the cyber incident data that they do possess with other carriers. He estimated that only about five percent of cyber incidents have been made public – too low a figure to support the development of new cybersecurity insurance policies much beyond the third-party market.

- Another insurer cautioned that self-insurance should not be discounted as a reasonable risk management strategy. When a company decides to self-insure, he stated, it typically knows about its cyber risks, however inexactly, and sets aside funding in the event of a loss. That approach, he emphasized, is not the same thing as ignoring risk.

- Several participants discussed potential avenues out of the data logjam. A critical infrastructure representative stated that while companies may not understand the overall cyber risk they face, they usually do have a good understanding of their business and, accordingly, the potential consequences of a data breach, infrastructure failure, or other loss. A social scientist opined that it's the responsibility of the federal government to provide the "big picture" view of cyber risks – especially when such risks have not been previously experienced as actual hazards. As an example, an insurer cited cyber risks involving the loss of highly sensitive intellectual property (IP), which could jeopardize up to 95 percent of a company's total revenue, as risks the government

should particularly highlight. Greater awareness about these and the full spectrum of cyber risks, he added, could lead to a greater appetite for cybersecurity insurance products.

- Several participants drew a distinction between large, mid-size and small companies when it comes to exercising the data option. A social scientist commented that while big companies may have a good handle on their data and interpreting what it means for purposes of risk transfer, that's not necessarily the case for mid-size and small companies that often don't have chief information security officers on staff. Without that expertise, he asserted, it may be difficult for them to make informed decisions about cybersecurity insurance. The social scientist described this situation as a serious problem because mid-size and small companies are often less resilient to cyber incidents than their larger counterparts. On a final note, he observed that mid-size and small companies also face a significant "lemon" problem when it comes to cybersecurity insurance. Without the benefit of a chief information security officer's input, it's difficult for most of them to discern which carriers offer quality policies and which do not.

- An IT professional agreed with this assessment and stated that mid-size and small companies need education about the many insurance options available to them and which make the most sense for their organizations. For starters, a government participant suggested, they could retain the services of a chief information security officer for help. Participants noted that such services and others are increasingly common in the marketplace. An insurer acknowledged that carriers have traditionally ignored mid-size and small companies because they've instead gotten top dollar from large companies. He advised, however, that carriers are now desperate for revenue and that their success going forward will depend on their ability to educate all companies about available policies.

- Several participants commented that companies that researched cybersecurity insurance three to five years ago and concluded that it was too expensive were correct. They asserted, however, that there are many more carriers today that are offering policies at affordable prices. Moreover, those companies are doing a better job educating companies about what they're selling. There are actually lots of options, an IT professional stated, and if a company looks hard for a policy that meets their needs, they'll find it. An insurer added that not every company – large, mid-size, or small – requires cybersecurity insurance to cover losses beyond the "fundamentals." Some, however, do need first-party coverage for intellectual property and reputation protection.

Information Sharing and Reinsurance: The Government Role

- Participants also discussed the federal government's role in helping to solve cybersecurity insurance market challenges in two key areas: information sharing and reinsurance.

- Regarding improved information sharing, a risk manager commented that having multiple federal agencies with different agendas and missions working the problem would be untenable. While DHS may want to promote two-way information sharing with companies in order to promote better awareness of cyber risks and cybersecurity practices, its sister agencies with law enforcement and/or regulatory missions will likely hold against them any information they share. Accordingly, most companies may resist a federal role in any independent body the private sector decides to

establish for cybersecurity information sharing unless that role is clearly defined and structured. A critical infrastructure representative agreed that the punitive attitude of some in government would be a hindrance to government participation, especially when companies go to tremendous expense to find problems in their networks. He concluded by saying that sharing information about cyber incidents and having it come back at companies in the form of a lawsuit or new regulatory requirements makes little business sense.

- In response, a social scientist mentioned that, at least in the medical industry, liability and shield laws have been successful in promoting better information sharing about risks – even when government has been part of the conversation. Participants concluded that these and other data issues should be part of a sustained conversation going forward.

- Regarding reinsurance, participants discussed the limitations of the federal government's role as insurer of last resort. While most agreed that the federal government should play this role, some stated that it would likely not have much practical effect in terms of keeping mid-size and small companies solvent after a cyber incident – especially if those companies aren't part of the "critical infrastructure environment." Moreover, most participants agreed that the federal government would only take on the reinsurer role if there was a true "cyber tsunami" or if intensive public pressure came into play. This led to discussions about what cyber incidents would quality as a cyber tsunami.

CONCLUSION

Participants stated that they enjoyed the workshop and expressed great interest in continuing the discussion about the future of cybersecurity insurance through similar, increasingly focused, DHS-catalyzed events. Several insurers reported that they were happy to learn that models for partnering with the federal government on cybersecurity information sharing already exist and could be leveraged going forward. They also said that they appreciated the perspectives of critical infrastructure representatives and other stakeholders about why they are reluctant to share information about cyber incidents and what might help incentivize them to do so. Another participant stated that aggregated risk should be further defined and discussed given the potentially very negative consequences to carriers and customers alike. A social scientist likewise expressed surprise that these workshop conversations, with a broader group of stakeholders, were so different from discussions he typically has with his colleagues about cybersecurity risk management. The scientist particularly noted the workshop participants' emphasis on available standards, compliance and certification as essential building blocks for enhancing cybersecurity – areas he advised meet with skepticism in academia.

Regarding next steps, an IT professional suggested that future cybersecurity insurance workshops should focus on specific issues that had an initial hearing at this workshop. An insurer added that future workshops should examine in greater depth cyber-related critical infrastructure losses and their implications for the insurance industry. Another insurer reported that future sessions should assess how the insurance industry is addressing cyber-related losses of intellectual property (IP) and the industry's progress in valuing IP as an asset. A risk manager concurred, suggesting that such a review should also look at how data analysis of scenarios and other methodologies are helping or could help in this regard. A critical infrastructure representative supported continuing the conversation on the precise roles that the federal government could play to help make the cybersecurity insurance market a better functioning one. Toward this end, a social scientist recommended discussing the kinds of research topics that academics both inside and outside government should pursue in order to help advance the cybersecurity insurance market. An IT professional proposed that greater attention be paid to the true economics of cybersecurity – specifically, how companies come to their decisions about what network systems to buy, develop and deploy; what cyber risks to manage and how; and what services to outsource for business support and under what circumstances. Finally, a social scientist recommended that future workshops also focus on "bridging the cost divide" between carriers and customers.

To keep the momentum going, several other participants suggested that there be clearly defined end goals for future workshops, along with pre-read materials regarding cybersecurity trends, analysis and use cases. Workshop 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 Workshop

Defining Challenges to Today's Cybersecurity Insurance Market

Monday, October 22, 2012

Agenda

8:30 – 9:15 Breakfast/Networking

9:15 – 9:30 Introduction/Overview (Bruce McConnell) – Suite 150, Auditorium

9:30 – 10:30 Plenary Panel

Theory of and Research on Cyber Insurance – Suite 150, Auditorium

- Tyler Moore – Professor of Computer Science and Engineering at Southern Methodist University

Current State of Cyber Insurance

- Emily Freeman – Executive Director for Technology and Media Risks, Lockton

Case Study: Fire Insurance – Standards and Data

- Jason Averill – Leader, Engineered Fire Safety Group at NIST

10:30 – 10:40 Plenary Panel Q&A

10:40 – 10:45 Break / Move to Rooms

10:45 – 11:45 Break Out Session 1

- Defining Insurable and Uninsurable Cyber Risks
  - Suite 200A
- Cyber Insurance and the Human Element
  - Suite 150, Auditorium
- Cyber Liability: Who is Responsible for What Harm?
  - Suite 200B

11:45 – 12:45 Lunch/Networking

12:45 – 1:45 Break Out Session 2

- Defining Insurable and Uninsurable Cyber Risks
  - Suite 200A
- Current Cyber Risk Management Strategies and Approaches
  - Group 1 – Suite 150, Auditorium
  - Group 2 – Suite 200B
- Cyber Insurance: What Harms Should It Cover and What Should It Cost?
  - Suite 150, Auditorium

1:45 – 2:00 Break / Move to Rooms

2:00 – 3:00 Break Out Session 3

- Defining Insurable and Uninsurable Cyber Risks
  - Suite 200A
- Improving the Cyber Insurance Market: Stakeholder Roles and Responsibilities
  - Suite 150, Auditorium
- Sequencing Solutions: How Should the Market Move Forward?
  - Suite 200B

3:00 – 3:30 Break / Facilitators Prepare for Final Presentations

3:30 – 4:00 Presentation of Discussion Topic Key Themes – Suite 150, Auditorium

4:00 – 4:30 Discussion by Attendees (Tom Finan) – Suite 150, Auditorium

- Comments/Reactions to Discussion Topic Key Themes
- Next Steps
- Q&A