Insurance Industry Working Session Readout Report

Insurance for Cyber-Related Critical Infrastructure Loss: Key Issues

National Protection and Programs Directorate
Department of Homeland Security

July 2014

TABLE OF CONTENTS

BACKGROUND 1

EXECUTIVE SUMMARY 4

WORKING SESSION DISCUSSIONS 9

- **TOPIC 1: CYBER INCIDENT INFORMATION SHARING/DATA REPOSITORY** 9
  - Defining the Problem 9
  - Establishing the Value Proposition 11
  - Requirements for a Useful Cyber Incident Data Repository 12
    - Data Requirements 12
    - System Attributes 13
  - Challenges with Developing a Cyber Incident Data Repository 15
    - Scope of Repository 15
    - Adoption 15
    - Legal and Policy 17
    - Visibility 18
  - Creating a Cyber Incident Data Repository 18
    - Cyber Incident Data Repository Working Group 18
    - Data Template 19
    - Identifying Stakeholders with the "Best" Data 20
    - Government Catalysts 21
  - Characteristics of a Successful Cyber Incident Data Repository 21
  - Next Steps 22
- **TOPIC 2: CYBER INCIDENT CONSEQUENCE ANALYTICS** 22
  - Consequence Information Needs 23
  - Utility of Cyber Incident Consequence Analytics 25
  - Characteristics of Successful Tools and Platforms 27
  - Current Approaches 30
  - Barriers to Cyber Incident Consequence Analytics 32
  - Potential Action to Support Cyber Incident Consequence Analytics 33

TOPIC 3: CYBER RISK AND ENTERPRISE RISK MANAGEMENT 34

The Case for ERM in the Cyber Risk Space 35

Barriers to Implementing ERM in the Cyber Risk Space 37

Factors Supporting the Case for ERM in the Cyber Risk Space 39

The Limits of "ERM-Lite" 41

Final ERM Comments 42

CONCLUSION 44

APPENDIX 45

BACKGROUND

The Department of Homeland Security's (DHS) National Protection and Programs Directorate (NPPD) helps both private and public sector partners secure their cyber networks, assisting them collectively and individually and improving the Nation's overall cybersecurity posture in the process. Through these interactions, DHS has become aware of a growing interest in cybersecurity insurance. From October 2012 through November of 2013, NPPD held three public roundtables and workshops on this topic. Each examined the ability of insurance carriers to offer relevant cyber risk coverage at reasonable prices in return for an insured's adoption of cyber risk management controls and procedures that improve its cyber risk posture. NPPD focused the event discussions on the first-party cybersecurity insurance market – that is, on policies designed to transfer a company's own residual, direct costs from a cyber incident to carriers – rather than on the third-party market which typically provides coverage for data breach liability and related costs.[1] Readout reports from the events include a wide range of perspectives from carriers, risk managers, chief information security officers (CISOs) and other information technology (IT) professionals, critical infrastructure owners, and social scientists. They can be accessed on the DHS Cybersecurity Insurance webpage at: http://www.dhs.gov/publication/cybersecurity-insurance.

Among its initial findings, NPPD learned that the first-party cybersecurity insurance market is a nascent one, particularly when it comes to coverage for cyber-related critical infrastructure loss. Carriers cited several reasons for their limited offerings in this area, chief among them being: a lack of actuarial data; aggregation concerns; and the unknowable nature of all potential cyber threat vectors. Based on input from event participants and on its own research, however, NPPD identified three areas where it appeared progress could lead to more robust first-party coverage – not only for economic and intangible harms such as lost profits arising from "out of service" critical infrastructure but also tangible harms involving damage to and/or the destruction of that infrastructure:

- **Cyber incident information sharing/data repository**. Event participants reported that while insureds historically have shared information about cyber incidents and related losses with their carriers, most are afraid to report this data publicly given potentially negative regulatory or reputational consequences. They further advised that the limited sharing that has taken place has otherwise failed to spur the development of broadly accessible cyber risk actuarial data needed to advance the cybersecurity insurance market more comprehensively. To address this shortcoming, many participants cited the need for a secure method through which organizations could pool and share cyber incident information, on an anonymized basis, and make it

[1] First-party cybersecurity insurance policies typically cover a company's losses arising from events such as business interruption, destruction of data and property, and reputational harm. Third-party policies, by contrast, cover losses that a company causes to its customers and others, such as harms arising from the exposure of personally identifiable information (PII) through a data breach. *See* Office of the Under Secretary, *November 2012 Cybersecurity Insurance Event Readout Report*, Washington, D.C.: U.S. Department of Homeland Security, National Protection and Programs Directorate, November 2012, http://www.dhs.gov/publication/cybersecurity-insurance (May 30, 2014).

accessible to carriers and other risk management professionals. Some stated that a cyber incident data repository could be a helpful resource in this regard.

- **Cyber incident consequence analysis**. Event participants likewise noted that in the absence of more cyber risk actuarial data, carriers have struggled to estimate the probable first, second, and third-order effects of a cyber attack on critical infrastructure – key information they need in order to better determine the extent of first-party coverage they should offer and how to price it. Several participants suggested that developing and exercising new cyber incident models and simulations, with insurance industry input, would help carriers better understand the value of critical infrastructure and who might pay a premium to restore it. Specifically, they stated that such tools would help them understand: what cyber risks will implicate which infrastructure components; which components present the greatest concern from a business interruption perspective; what economic and other consequences might ensue without appropriate cyber risk controls in place; and which controls would likely have the greatest mitigation effect. While the participants stated that this information would be immediately helpful from an underwriting perspective, they emphasized that the development of parallel tools that help determine both the likelihood and the probable consequences of a cyber incident to a *particular organization* would resonate most with that organization's leadership. Such tools, they explained, would likely have the most success in driving more informed risk mitigation and risk transfer investments.

- **Enterprise risk management (ERM)**. Event participants noted that while some large companies have adopted ERM programs,[2] few mid-size and small companies have followed their lead. Given the supply chain and other business interdependencies that exist among them, they continued, this dichotomy between ERM haves and have-nots presents a significant challenge. They asserted that broader adoption of ERM programs that incorporate cyber risk will help shore up cybersecurity "weak links." Several participants further observed that even among organizations that actively espouse and implement ERM practices, cyber risks often remain stubbornly outside the ERM fold. They attributed this shortcoming to a cultural divide that exists between CISOs on the one hand and chief financial officers, legal counsel, and risk managers on the other. The participants concluded that until new ERM-based approaches help

[2] The Risk and Insurance Management Society (RIMS) defines enterprise risk management (ERM) to mean "a strategic business discipline that supports the achievement of an organization's objectives by addressing the full spectrum of its risk and managing the combined impact of those risks as an interrelated risk portfolio." From the RIMS Web site, *What is ERM?*, www.rims.org/ERM/Pages/WhatisERM.aspx (May 29, 2014). RIMS further describes ERM as a "significant evolution beyond previous approaches to risk management" because it "(1) encompasses all areas of organizational exposure to risk (financial, operational, reporting, compliance, governance, strategic, reputational, etc.); (2) prioritizes and manages those exposures as an interrelated risk portfolio rather than as individual 'silos'; (3) evaluates the risk portfolio in the context of all significant internal and external environments, systems, circumstances, and stakeholders; (4) recognizes that individual risks across the organization are interrelated and can create combined exposure that differs from the sum of the individual risks; (5) provides a structured process for the management of all risks, whether those risks are primarily quantitative or qualitative in nature; (6) views the effective management of risk as a competitive advantage; and (7) seeks to embed risk management as a component in all critical decisions throughout the organization." *Id*.

these two camps work together to recast IT-based losses into terms of potential harm to investment, market cap, and reputation, most companies will have difficulty elevating responsibility for cyber risk management beyond their IT departments. They asserted that a new focus on evangelizing ERM and its benefits would help this situation.

NPPD publicly announced its intent to convene an insurance industry working session in March 2014 in order to flesh out all three potential progress areas in greater detail – a task that has become an increasing priority since Executive Order 13636 and the release of the Cybersecurity Framework.[3] NPPD hoped that a fuller understanding of insurance industry perspectives on each of them would lead to a sustained dialogue between carriers and potential insureds about how to best harness the incentivizing effect of private insurance contracts to promote more informed and effective cybersecurity practice. On April 7, 2014, NPPD accordingly hosted 30 participants, registered on a first-come, first-served basis in Washington, D.C., in an effort to obtain that understanding. In addition to 10 working session leaders, government guests, and support personnel, NPPD was joined by 10 insurance brokers,[4] 10 underwriters,[5] and 10 reinsurers.[6]

Prior to the insurance industry working session, NPPD advised the participants that their input during the event would be included in this readout report on a non-attribution basis. NPPD explained that the purpose of this report would be to capture diverse insurance industry ideas about each of the potential progress areas and how they could help move the first-party market forward. NPPD further advised that it was not looking for, would not accept, and would not solicit group or consensus recommendations during the working session. NPPD likewise clarified that neither DHS nor NPPD would make any decisions about agency policy or positions during the event. The comments, perspectives, and suggestions contained in this report consequently are those of the event participants only and do not necessarily reflect the views of DHS or NPPD.

---

[3] Both Executive Order 13636 and the Cybersecurity Framework seek to help both private and public sector owners and operators of critical infrastructure boost the cybersecurity of that infrastructure. Barack Obama. "Improving Critical Infrastructure Cybersecurity," Executive Order 13636, 19 February 2013, www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf (June 4, 2014); National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity*, Washington, D.C.: U.S. Department of Commerce, February 12, 2014, www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf (May 16, 2014) ("Cybersecurity Framework").

[4] An insurance broker is the agent of the insured in making contracts of insurance but sometimes is the agent of the carrier for some purposes (as payment of the premium) and of the insured for all other purposes. *Merriam-Webster Online Dictionary, s.v.,* "insurance broker," accessed May 16, 2014, http://www.merriam-webster.com/dictionary/insurancebroker.

[5] An insurance underwriter is a financial professional that evaluates the risks of insuring a particular person or asset and uses that information to set premium pricing for insurance policies. *Investopedia Financial Dictionary, s.v.*, "insurance underwriter," accessed May 16, 2014, http://www.investopedia.com/terms/i/insurance-underwriter.asp. Insurance underwriters are employed by insurance companies to help price life insurance, health insurance, property/casualty insurance and homeowners insurance, among others. *Id.*

[6] Reinsurance is insurance that is purchased by an insurance company (the "ceding" company) from one or more other insurance companies (the "reinsurer") directly or through a broker as a means of risk management. Wikipedia contributors, "Reinsurance," *Wikipedia, The Free Encyclopedia*, http://en.wikipedia.org/wiki/Reinsurance, accessed June 4, 2014. The ceding company and the reinsurer enter into a reinsurance agreement which details the conditions upon which the reinsurer would pay a share of the claims incurred by the ceding company. *Id*. The reinsurer is paid a "reinsurance premium" by the ceding company, which issues insurance policies to its own policyholders. *Id*.

EXECUTIVE SUMMARY

During the insurance industry working session, participants addressed the cyber incident information sharing, cyber incident consequence analysis, and ERM agenda topics in that order:

REPOSITORY REMARKS

Many participants voiced strong support for the creation of a cyber incident data repository where private and public sector organizations – and the Federal government – could submit appropriate cyber incident information on an anonymized basis. Over time, they explained, such data could help populate cyber risk actuarial tables that are essential for providing insurance but which nevertheless remain largely undeveloped. Additionally, such data could inform related cyber incident trend analysis by leveraging insights gained from previous cyber attacks, vulnerability exploitations, and other events, and help companies frame their responses accordingly. In the immediate term, this data could enable CISOs and other IT professionals to better benchmark their organizations' current cyber risk management performance against their peers. The participants asserted that the promise of access to data supporting such peer-to-peer comparisons could incentivize a wide variety of organizations to participate in any future repository effort. They likewise addressed the value proposition of a repository more broadly, describing how it could help inform cybersecurity best practices through the identification and implementation of better cyber risk control investments in a variety of cyber risk circumstances. Many participants specifically cited the particular usefulness of a repository that informs a better understanding of critical infrastructure "interconnectedness." While enthusiastic about the repository concept, they nevertheless encouraged NPPD to engage non-insurance professionals about it in order to assess a repository's value to the wider cyber risk management community.

To this end, the participants shared their ideas about which data points should be captured on a template that all repository contributors could use when nominating cyber incident information for inclusion. They likewise discussed the need to clearly define thresholds for the kinds of "cyber incidents" a repository should capture and the kinds of critical infrastructure loss analysis it consequently should support. The participants also described the optimal qualities of a repository, including efficient data aggregation; easy searchability; automatic updating; and strong security. They then offered their perspectives on the kinds of entities that would be good candidates to host a beta test for the repository; which stakeholders – including third-party vendors[7] – should be invited to engage in its design and execution; and which specific sectors would be good candidates for initial participation. The participants further offered their opinions about which sources of data would provide a beta test, and a future repository, with a firm foundation for success. While generally not supportive of the Federal government owning and operating it, several participants still urged the Federal government to populate a future repository with relevant information that it may possess.

Finally, the participants highlighted several potential obstacles that a cyber incident data repository would likely encounter, such as scoping and design issues; challenges with incentivizing

[7] For purposes of this readout report, the terms "third-party vendors" and "vendors" shall include both cybersecurity and IT service providers.

participation; and carrier limitations when it comes to understanding the mechanics of cyber-related critical infrastructure loss and what categories of such loss warrant coverage. They also shared their opinions about how repository effort leaders could work through those obstacles.

Analytics Approaches

Several participants explained that current cyber incident consequence analysis efforts often fall short because they suffer from a dearth of publicly available information about critical infrastructure vulnerabilities and how cyber attackers could exploit them. They accordingly described the kinds of information that they hoped the Federal government could provide to help them build out the models, simulations, and exercises they need to more confidently expand first-party coverage for cyber-related critical infrastructure loss. The participants noted, moreover, that by helping to identify priority cyber risks in this area, a mature cyber incident data repository one day could directly support these analytics-based approaches. Ultimately, they explained, an organization's risk leaders need a better sense of the likelihood and probable consequences of cyber risks to critical infrastructure before they can make a convincing business case to address them. They emphasized that clearer insights into critical infrastructure interconnectedness would be particularly helpful in this regard, especially when it comes to highlighting cyber risk accumulation areas that do not fall neatly within a particular industry sector.

Many participants anticipated that significant challenges could hinder initial progress on any enhanced cyber incident consequence analytics initiative. Participants recognized that the Federal government may possess highly relevant data for modeling critical infrastructure dependencies, interdependencies and vulnerabilities but may not be able to share it. They nevertheless emphasized that even generic models and cyber risk scenarios would be helpful tools for carriers. To the extent they spur deeper conversations about an organization's unique cyber risk circumstances, they explained, such models and scenarios could identify underwriting questions that carriers should ask both potential insureds and their vendors about their cyber risk exposures and the steps they have taken to address them. The participants clarified, however, that not just any generic model or scenario will do. They advised that to provide maximum benefit, they should:

- Capture how critical infrastructure exists, functions, and interconnects in the real world;
- Provide CISOs and other IT professionals with greater insight into the "systemic risk" arising from that interconnectedness in order to inform peer-to-peer benchmarking activity;[8]
- Improve visibility into not only the drivers of specific cyber incident costs but also the risk controls that would most effectively mitigate those drivers; and
- Address core insurance industry needs, including the need to estimate probable maximum loss.[9]

---

[8] The World Economic Forum defines the term "systemic risk" to mean "the potential loss or damage to an entire system as contrasted with the loss to a single unit of that system. Systemic risks are exacerbated by interdependencies among the units often because of weak links in the system. These risks can be triggered by sudden events or built up over time with the impact often being large and possibly catastrophic." World Economic Forum. *Global Risk 2010: A Global Risk Network Report* (Geneva, Switzerland: World Economic Forum, 2010), 10, http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2010.pdf (June 17, 2014). For purposes of this readout report, the term "systemic risk" means the potential for a cyber incident to cause cascading effects across different critical infrastructures given the dependencies and interdependencies that exist among those infrastructures.

Several participants described the limited success they have already had in attaining these objectives during their own scenario-based cyber risk modeling work. They likewise identified a variety of private and public sources of relevant expertise that could be leveraged to enhance similar modeling and simulation efforts going forward. One particularly useful avenue, they asserted, would be for the Federal government to design, develop, and execute a cyber incident table top exercise in partnership with not only the first responders and other stakeholders that already participate in hurricane and other natural disaster exercises but also insurance industry representatives and vendors who would bring unique cyber risk perspectives to the exercise. Participants identified several categories of "missing data" to support such an exercise that, if obtained, would increase its value considerably. To boost the exercise's chance of success, moreover, participants underscored the need to effectively market the exercise to critical infrastructure owners and operators as: a substantive effort supported by defensible data; inclusive of a broad range of subject matter experts; and designed to address relevant cyber risks in a way that generally promotes awareness about cyber vulnerabilities and specifically educates individual participants about their own exposures. Finally, the participants shared their ideas about how the exercise and any future generic models and cyber risk scenarios that it informs could contribute to company-level modeling efforts. Those "closer to home" efforts, they advised, often get the most attention from corporate leaders and therefore have the most success in driving dedicated cyber risk management investments.

ERM Evangelization

Participants discussed the tremendous value that ERM brings to organizations seeking to assess their business risks more holistically and to prioritize their risk management investments more effectively against areas of greatest perceived peril. They observed that many companies nevertheless exclude cyber risk from established ERM programs, thus depriving themselves of the full range of cybersecurity insurance coverage options that might otherwise be available to them. Put simply, carriers view companies with strong, cyber risk-inclusive ERM programs as a safer bet when it comes to providing coverage. Several participants added that such companies are also more likely to understand their need to manage their cyber and other business risks beyond the four walls of their organizations to include their critical infrastructure, supply chain, and other outside partners. This focus on interconnectedness, they continued, will help lay the groundwork for extending first-party coverage to at least some of the physical damages that might arise from a cyber incident. With this end goal in mind, the participants shared their ideas about the elements of an effective ERM program that most cybersecurity insurance underwriters would likely find attractive.

---

[9] Probable maximum loss is generally defined as the value of the largest loss that could result from a disaster, assuming the normal functioning of passive protective features (e.g., firewalls, nonflammable materials, etc.) and proper functioning of most (perhaps not all) active suppression systems (e.g., sprinklers). Wikipedia contributors, "Probable Maximum Loss," *Wikipedia, The Free Encyclopedia*, http://en.wikipedia.org/wiki/Probable_maximum_loss, accessed May 15, 2014. It [probable maximum loss] is neither *foreseeable* nor *possible* loss – rather, it is the maximum loss which *probably* will happen when, and if, the peril insured against usually occurs. Edward B. Black. "Discussion by Edward B. Black," In *Proceedings of the Casualty Actuarial Society* (Boston: Sperry Rand Corporation, 1970), LVI: 46, http://www.casact.org/pubs/proceed/proceed69/1969.pdf (June 17, 2014).

Despite their hope for ERM in the cyber risk space, the participants acknowledged various persistent obstacles to more successful ERM evangelization. At the outset, they observed that many mid-size and small companies simply lack the resources to implement *any* ERM program, let alone one that fully integrates cyber risk. Even among companies with ample resources, they added, some are reluctant to initiate ERM programs because they fear having to address expensive cyber vulnerabilities that those programs might reveal. Other participants cited communications breakdowns between IT and non-IT security professionals as another major obstacle to ERM adoption. These groups use very different language to express basic risk concepts, they explained, and too often find themselves talking past each other. The participants advised that while ERM can help overcome these barriers, doing so often requires ERM leads and CISOs to collaborate closely in order to identify key cyber risks and to develop corresponding (and comprehensible) risk messages to senior management. Furthermore, participants described difficulties associated with extending in-house ERM programs to vendors. They cited as examples mid-size and small companies that outsource their cybersecurity services as a cheaper, more efficient way of doing business. Such companies, they noted, typically have no control over how or if those third parties manage their cyber risk well.

Notwithstanding these difficulties, the participants identified several factors that could directly advance the case for ERM in the cyber risk space and, by extension, the case for cybersecurity insurance:

- Several participants noted that many companies have become increasingly aware of cyber risk as a result of highly-publicized data breaches and the costs they impose on impacted organizations. Boards of directors and CISOs accordingly have become much more open to exploring ERM and insurance options to address this residual risk as part of their overall risk management strategies. One participant asserted that recent events have blown new wind into the ERM sails that the insurance industry raised only a few years ago. That wind, she stated, will likely help brokers and underwriters make the case for including cyber risk within ERM programs in the future.

- Other participants shared their views about how regulators could help advance ERM and the cybersecurity insurance market by requiring the adoption of ERM as a standard cyber risk management practice. They explained that regulatory agencies could help define and refine a common ERM standard by identifying the most effective ERM approaches and then encouraging their use. Several participants commented that if such a common standard should emerge, carriers might require compliance with it as a condition for cybersecurity insurance coverage.

- Still other participants suggested that mid-size and small companies might be more inclined to adopt a scaled-down version of ERM that might be cheaper and easier to implement. Several countered, however, that such an “ERM-lite” approach would likely lead to companies addressing some but not all of their risks, thereby undermining the value of ERM itself. They likewise expressed concern that ERM-lite programs, while well-intentioned, might amount to nothing more than rote check-the-box exercises that fail to effectively address an organization’s actual risk profile.

Whatever their individual point of view, most participants agreed that the case for ERM in the cyber risk space and for cybersecurity insurance generally would benefit from greater public awareness and education about cyber risk. Such education and awareness, they concluded, would provide a much needed foundation for longer-term cybersecurity gains within companies, among partnering companies, and across society.

WORKING SESSION DISCUSSIONS

TOPIC 1: CYBER INCIDENT INFORMATION SHARING/DATA REPOSITORY

DESCRIPTION: During NPPD's prior events, carriers and other participants described the importance of better cyber incident information sharing as a prerequisite to establishing the kind of robust actuarial tables needed to advance both the first- and third-party cybersecurity insurance markets. They stated that greater knowledge about real-world cyber incidents – including data on their types and frequency, parties affected, and impacts – would help carriers craft policies more attuned to the cyber risk management needs of potential insureds. They advised that this data also would help identify the kinds of cyber risk controls that organizations should put in place as a prerequisite for coverage. One idea that surfaced repeatedly was the creation of a cyber incident data repository where this information could be stored and analyzed. This working session discussion therefore sought to identify specific insurance industry ideas on how such a repository should be structured in order to provide maximum value from an actuarial perspective. Among other topics, the participants discussed the value proposition of a cyber incident data repository not only to carriers but also to other cyber risk management professionals.

DISCUSSION POINTS:

DEFINING THE PROBLEM

- Participants focused their initial discussions on defining key terms. An underwriter highlighted the difficulties associated with articulating what is meant by a "cyber incident." He stated that the term is often used in a generic sense to describe a broad range of cyber events with negative implications, both malicious and unintentional. The underwriter added that some cyber incidents have obvious physical consequences, such as cyber-enabled attacks that lead to damaged critical infrastructure. Others, he noted, occur solely within virtual space and result in lost or stolen data, incapacitated networks, and resulting business interruption. He added that while the latter cyber incidents do not cause actual physical damage, they still inflict significant financial and reputational harm on affected entities. The underwriter asserted that for repository purposes, the term "cyber incident" accordingly should be defined to specifically include or exclude particular cyber events. To avoid information overload, moreover, he suggested that appropriate thresholds be established to exclude low or no impact cyber events from repository consideration.[10]

[10] The underwriter further commented that physical damages to critical infrastructure resulting from a cyber event are likely already insured under existing insurance mechanisms. A second underwriter disagreed, asserting that cyber-related critical infrastructure damages probably are *not* covered by existing property policies or other categories of coverage. The second underwriter advised that even when such coverage appears to exist – for example, in a property insurance contract that is silent on the matter – it is highly doubtful that such coverage was affirmatively intended by the carrier. Without that intention, he added, it is safe to assume that the risk has not been priced or underwritten accordingly. The second underwriter concluded that as different carriers have come to recognize areas of possible cover that they had not contemplated, they have increasingly introduced new cyber risk exclusions in policies in order to reduce any ambiguity or silence that could be interpreted in an insured's favor. He added that the trend toward a stand-alone cybersecurity insurance market – for both first-party and third-party coverage, will likely continue.

- Other participants noted that determining how to classify cyber incidents is a live issue within the insurance industry. A broker commented that carriers already classify cyber incidents based on the nature of the event – for example, as data breaches, mishandling of information, or failures of technology – and stated that existing taxonomies such as these could provide a conceptual basis for describing how the failure of underlying critical infrastructure might affect the provision of technical services. An underwriter countered that what constitutes a cyber incident should instead be determined from an industry point of view – i.e., as a privacy incident or as a business interruption incident. He observed that carriers currently offer good coverage for the former but not the latter. A second broker agreed with the underwriter's characterization of cyber incidents, describing them alternatively as privacy/data security type risks and outage risks which, in turn, can be further "binned" into physical and non-physical damage events.

- Several underwriters also highlighted the challenges associated with the use of the term "critical infrastructure." Two underwriters noted that the insurance industry typically identifies critical infrastructure in terms of risk accumulation.[11] In some instances, they explained, such infrastructure corresponds closely to infrastructure identified by the Federal government through its sector-based approach (e.g., the Energy, Transportation Systems, and Water and Wastewater Systems Sectors).[12] In others, however, it involves pockets of risk accumulation associated with business support functions – such as cloud computing – that depend upon multiple infrastructure components "not bound to certain sectors or industries." In short, the underwriters explained, the insurance industry employs data-driven approaches to identify pockets of high risk within the cyber ecosystem writ large, without regard to neatly defined categories. They asserted that repository planners consequently will need to define the term "critical infrastructure" in a way that captures this reality.

---

[11] For purposes of this readout report, the term "risk accumulation," sometimes known as "risk aggregation," refers to an insurance concept where a limited risk could impact multiple policy holders. The most obvious examples or risk accumulation involve natural disasters, such as earthquakes and hurricanes concentrated in a specific geographic area, and terrorist attacks. In the cyber risk context, concerns about risk accumulation often involve cyber risk becoming concentrated in an outsourced third-party vendor– such as a cloud or other services provider – so much so that the provider becomes a source of multiple loss claims following a single cyber incident (e.g., a cyber attack that results in a service outage). The challenge for carriers is that unlike the situation with earthquake and hurricane models, carriers in the cyber risk context do not have data to measure the likelihood and/or consequences of a cyber-related service outage involving a major cloud or other service provider.

[12] Presidential Policy Directive 21 (PPD-21) – Critical Infrastructure Security and Resilience – "describes a national effort to share threat information, reduce vulnerabilities, manage consequences, and hasten response and recovery efforts related to critical infrastructure." Office of Infrastructure Protection, National Infrastructure Protection Plan, Washington, D.C.: U.S. Department of Homeland Security, National Protection and Programs Directorate, 2013, www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience (June 7, 2014) ("NIPP"). It also identifies 16 critical infrastructure sectors: Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Health, Information Technology, Nuclear Reactors, Materials, and Waste, Transportation Systems, and Water and Wastewater Systems. *Id*.

- Many participants commented that this definition diversity underscores one of the primary challenges associated with establishing a cyber incident data repository: robust participation by a wide range of organizations will depend upon the ability of government and other participating stakeholders to provide a clear answer to the question of what problems a repository will help solve. Clearly defining the terms "cyber incident" and "critical infrastructure" will be an important first step in this regard.

Establishing the Value Proposition

- Despite some uncertainty about definitions and the specific intended use of a cyber incident data repository, participants agreed that a well-crafted repository could be very helpful to the insurance industry. An underwriter explained that much insurance work revolves around predicting loss – specifically, the frequency of actual events, their likelihood, and their associated damages. Cyber incidents are difficult to quantify according to these measures, he added, because there is not yet a significant history from which to draw data. He concluded that a repository therefore would be the place to build a much needed loss "library." A broker agreed, contrasting cybersecurity insurance policies with traditional fire insurance policies. He noted that the insurance industry has nearly a century of data regarding fires and can use that body of knowledge to make predictions on which to base policy coverage limits and pricing. A cyber incident data repository, he stated, could begin to do the same for cybersecurity insurance. The underwriter responded that although some cyber risks will likely remain uninsurable (e.g., truly catastrophic cyber-related loss), a repository still would be valuable to the extent it could "ballpark" the financial and other costs of less severe cyber incidents. In so doing, it could help organizations better direct and prioritize their cyber risk mitigation efforts.

- Another underwriter commented that a second benefit of a repository could be its potential contribution to the development of cybersecurity best practices. Historical data, he explained, allowed carriers to investigate and promulgate fire safety best practices such as sprinkler systems, alarms, and outward opening doors – all of which carriers typically require today as a condition for commercial fire insurance coverage. The underwriter asserted that knowing how often certain cyber incidents occur and which vulnerabilities are being exploited by bad actors – data a repository could record over time – will help carriers identify similar patterns and trends that will help them develop and advertise similar best practices. "If 70% of attacks look like 'X' against a utility," he noted, "that information will provide carriers and their customers with a helpful frame of reference for managing the risk."

- Along these lines, several participants noted that a repository could be especially helpful when it comes to promoting a better understanding of the interconnectedness of many critical infrastructures and what impacts a cyber-caused disruption will likely have on multiple organizations as a result. Specifically, they noted that a repository could provide significant value to CISOs and other IT professionals by helping them better identify this kind of systemic risk to their boards of directors and other senior leaders. Other participants noted that a

repository likewise could be used to emphasize the notion of cyber risk interconnectedness more broadly. For example, they commented that repository data could help underscore an important central message to members of the private sector: that recently publicized data breaches in the retail sector could have happened in *any* sector, and that no industry in the cyber ecosystem is immune from similar cyber incidents.

- Other participants commented that a repository would have utility from day one, with usefulness increasing over time as participants learn more about past cyber incidents and gather more data about new ones. Good primary source data in a repository, they added, will help develop truly helpful cyber incident models and simulations that reduce uncertainty about catastrophic events and in the process clarify which events along the severity continuum, involving which critical infrastructure nodes, merit particular risk management attention.

Requirements for a Useful Cyber Incident Data Repository

Data Requirements

- Participants next discussed the data requirements and system attributes that should characterize a useful cyber incident data repository. Many agreed that, at a minimum, it should help carriers understand the causes, effects, and context of current and emerging cyber incidents. Many also agreed that repository data should be structured around the following categories that address the specific information needs of the insurance industry:

    - Attack and/or incident payloads (e.g., Distributed Denial of Service (DDoS) attack);
    - Attack and/or incident causes (e.g., misconfigured firewall, poor training);
    - Attack and/or incident goals/targets;
    - Attack and/or incident frequency;
    - Attack and/or incident severity/intensity;
    - Impacts to systems (including cascading effects) and response capabilities of impacted organizations;
    - Compromised areas (i.e., what vulnerabilities were exploited, what systems were affected);
    - Financial and other costs incurred in preventing and recovering from attacks and/or incidents (i.e., to return to pre-attack/incident states);
    - Timelines of attacks and/or incidents (dates of actual occurrence, discovery, and reports);
    - Timeframes for attack successes and for discovering and stopping attacks;
    - Third-party vendor involvement in attacks and/or incidents;
    - Impacted third-party vendors (e.g., to identify risk accumulation situations);
    - Dates of first entry of attacks and/or incidents into repository and dates/details of entry updates;

- Success and failure rates regarding the discovery of common attacks and/or incidents;[13]
- Related activities that provide attack and/or incident context (e.g., upcoming merger discussions); and
- Preventative actions undertaken to block future attacks and/or incidents.

- Several advised that this information, if appropriately analyzed, could help accomplish the following cyber risk management objectives and enhance cyber risk mitigation and cyber risk transfer strategies accordingly:

  - Identify, track, and assess patterns and trends based on attack/incident descriptions;
  - Develop models and simulations based on those patterns and trends to assess costs associated with attacks and/or incidents – including losses stemming from infrastructure interconnectedness – and to identify responsive cyber risk controls;
  - Develop dynamic pictures of cyber threats as they evolve, along with dynamic pictures of anticipated costs associated with events; and
  - Develop best practices based on patterns and trends identified from cyber incident and attack histories and improve understanding of the costs associated with incidents and attacks.

- Many participants emphasized the twin imperatives of anonymizing the data submitted into a cyber incident data repository and ensuring the "paramount" security of the repository itself. Two underwriters likewise noted the need to have strong access controls in place, with different levels of permission to access data granted to cleared individuals depending upon their defined roles and identities. One broker, however, expressed reservations about anonymizing repository data. He asserted that disclosing the identities of contributing companies might be a crucial component of building confidence in the representativeness of the data and therefore incentivizing others to contribute. Alternatively, he added, other companies might be concerned that anonymized information about a data breach could be reverse engineered if specific details about the breach were to be subsequently publicized. In short, he concluded, those companies might fear that repository participation would expose them to liability. Several participants responded that should the broker's concerns bear out, new protections for repository contributors may be necessary.

System Attributes

- Participants largely agreed that a cyber incident data repository should be developed by the stakeholders that would find it most useful. Several noted the inherent trade-off between the breadth of data in a repository on the one hand and the accessibility of that data on the other. A repository should be easily searchable, they explained, and therefore should not contain "too

[13] Several participants stated that success and failure rate information of this nature could help carriers "tease out" the fact that one sector was able to stop a DDoS attack while another sector remained vulnerable. By extension, such information could help carriers determine how well particular cyber risk mitigation techniques work in different industries.

much or too detailed" information. The participants accordingly recommended that a working group of potential repository users be established to develop: (1) a defined set of cyber incident categories of priority concern; and (2) corresponding standardized templates for submitting data about actual cyber incidents that fall within those categories. They stated that developing the categories and templates as an initial order of business would help guide and inform the specifics of the repository's design. For example, several commented that they would like the categories and templates to appear as part of a drop-down menu that repository users could use to classify the cyber incidents that they nominate for inclusion.

- An underwriter highlighted the importance of aggregating existing cyber incident data sets, gathered within individual sectors, in ways that are beneficial to users. He stated that integrating those data sets into a unified repository would promote not only that aggregation but also the enhanced analysis that it naturally supports. The underwriter noted that this development would mark a significant improvement over current sector practice, which typically limits access to sector cyber incident data sets to sector members only. A broker concurred, adding that aggregated cyber incident data from vendors would be a particularly helpful repository contribution given its potential to clarify which cyber threats and vulnerabilities present the greatest danger. While some vendors publicize generic information about cyber incidents that they've experienced, she continued, anonymized *but specific* details about their impacts – made available to a repository through a standardized template – would be invaluable. The broker advised that Information Sharing and Analysis Centers (ISACs) would benefit from a similar approach.[14] She cited the Industrial Control System Information Sharing and Analysis Center (ICS-ISAC) as one example of such a potential beneficiary and stated that it currently provides only generic information about approximately 200 utility-related cyber incidents. "Until we know more information about what losses those cyber incidents entailed," she concluded, "it's hard for carriers to determine policy prices."

- Many participants agreed that a repository and the data included within it should be dynamic and updated over time – perhaps through "blind" automatic follow up messages that ping cyber incident contributors for additional cost/impact information on a periodic basis. Unlike a fire where damage is done and payments are made, an underwriter explained, cyber losses can continue and evolve after the initial event. She advised that a static snapshot of a cyber incident is consequently of only limited utility. Other participants agreed and suggested that the repository also could prompt contributors for information about new cyber incidents they experience in order to ensure fuller data capture.

[14] DHS defines Information Sharing and Analysis Centers (ISACs) as, "Operational entities formed by critical infrastructure owners and operators to gather, analyze, appropriately sanitize, and disseminate intelligence and information related to critical infrastructure. ISACs provide 24/7 threat warning and incident reporting capabilities and have the ability to reach and share information within their sectors, between sectors, and among government and private sector stakeholders." *See* NIPP, *supra* note 12.

Challenges with Developing a Cyber Incident Data Repository

Many participants agreed that a cyber incident data repository, if it combines information in ways that benefit carriers, would improve the status quo and enhance the insurance industry's ability to provide meaningful cybersecurity insurance coverage. They noted a wide range of challenges, however, that if not addressed early in the planning process could diminish the utility of a repository or otherwise inhibit its use.

Scope of Repository

- Throughout the working session, many participants stated that a primary goal when structuring repository data should be to make it broadly useful – not only to a large number of carriers but also to other cyber risk management professionals. An underwriter countered, however, that a repository would have more success if it instead provided meaningful focus on the "segments" of the cyber ecosystem where cybersecurity insurance could be most useful. For example, he explained, while commonplace "workaday" cyber attacks are of no particular interest to the Federal government, cyber attacks on utilities certainly are of heightened importance. The underwriter advised that a threshold on data significance accordingly should be established in order to prevent the repository from becoming overwhelmed by data that distracts from more consequential cybersecurity problems that require more comprehensive risk mitigation and risk transfer solutions.

- Several participants concurred and suggested that it might make sense to initially scope a cyber incident data repository to address only cyber incidents with potentially catastrophic consequences. A second underwriter disagreed, asserting that catastrophic cyber loss "spooks" the insurance industry, will likely not be covered in any event, and therefore should not be the focus of a repository development effort. A third underwriter added that a wide spectrum of cyber incidents that fall far short of a catastrophe exists – including cyber incidents that may cause significant physical damages. He commented that a repository therefore would be better served by bifurcating received cyber incident data in a way similar to how the property insurance market divides potential property losses into both catastrophic and non-catastrophic loss. The underwriter concluded that repository planners should similarly identify where that line should fall in the cyber loss context.

- A reinsurer concurred with this recommended approach, noting that more data on non-catastrophic but systemic cyber incidents would be especially useful for the reinsurance community.

Adoption

- Participants also discussed the likely challenges involved in incentivizing "adoption" of the repository by potential users. Several brokers and underwriters noted that concerns about potential liability, unwillingness to apply scarce resources to information sharing, and simple

apathy all might combine to diminish the urgency of corporate leaders to participate. Under the circumstances, one broker stated, it may be necessary to require mandatory reporting of cyber incidents in order to make the repository work. An underwriter disagreed strongly, asserting that a mandatory reporting regime would "shut this data sharing effort down." Others agreed, noting that it would be not only contradictory but also very difficult to require "mandatory anonymous" reporting. In the end, they concluded, repository advocates instead will need a strong value proposition to persuade organizations to contribute voluntarily.

- A second underwriter stated that the mere fact that multiple industry players contribute to a repository is unlikely to serve as such a value proposition. On the contrary, he noted, organizations in many sectors already exchange ideas and information at a high level through ISACs and other mechanisms. He emphasized, however, that if stakeholders outside the insurance industry could also access repository data and find it helpful, its perceived utility could increase considerably. Specifically, the underwriter explained that CISOs value information about how their organization compares to their peer organizations. A reinsurer concurred with this assertion, noting that one of the biggest problems CISOs have is with properly allocating investments against their respective organizations' cyber risks. The opportunity to better understand what cyber risk management investments their peers are making – even at an anonymized, aggregate level – and what success those peers are having with those investments would likely incentivize their participation. A broker agreed, noting that information that helps a CISO either defend his or her cybersecurity program and/or justify enhancing it would likely be of significant interest. "If we're looking for CISOs to contribute cyber incident data," he continued, "then we also need to provide them with this valuable benchmarking information in return." The underwriter concluded that CISOs would give such information special weight if carriers tied it to explicit financial incentives – i.e., attaining a specific level of cybersecurity through the adoption of particular cyber risk controls and/or metrics in return for more extensive insurance coverage at lower prices.

- Despite this hope, several underwriters observed that many organizations don't have the budgets to employ full-time CISOs much less the ability to devote significant resources to monitoring their networks and cataloguing discovered cyber incidents for inclusion in a repository. Nevertheless, they continued, data from those organizations is particularly important for improving existing cyber risk analysis and advancing insurance industry knowledge in the process – precisely because those organizations *haven't* shared data in the past. The underwriters commented that making the repository's "value case" to these organizations therefore will be essential for ensuring both their participation and the improved cyber risk awareness that that participation will provide.

- Given these concerns, many participants agreed that a major part of a repository's value proposition is its potential to help individual organizations identify their most significant cyber risks. An underwriter stated that analysis of repository data over time would enhance the ability of carriers to identify and put a dollar figure on high consequence cyber risks of most relevance

to different critical infrastructure sectors. To the extent individual organizations within a particular sector are aware of and (hopefully) reporting their own cyber incidents, he added, carriers will be able to advise them about which incidents merit risk management action from a bottom line, peer-to-peer comparison perspective. A second underwriter added that while not all organizations need cybersecurity insurance, some sectors likely need it more than others. He concluded that a repository that clarifies which sectors would benefit most from coverage – again, as informed by the data – will likely encourage mid-size and small organizations within those sectors to participate so they can assess their specific circumstances and arrange their cyber risk management investments accordingly. Those investments, he noted, might include an investment in cybersecurity insurance.

Legal and Policy

- Several participants highlighted precedents that likely would affect the development of a cyber incident data repository. A broker cited so-called "CL 380" coverage exemption clauses, which she described as increasingly commonplace in property insurance policies written for energy sector companies. She explained that those clauses allow carriers to deny claims for physical damage and/or loss that stem from both accidental and malicious cyber incidents. The broker asserted that the adoption of these clauses indicates that, like terrorism risk, carriers are beginning to exclude cyber risk from more traditional lines of coverage in favor of stand-alone cybersecurity insurance lines of coverage. She commented that the insurance industry accordingly needs an improved focus on linking its information requirements in both the cyber and terrorism risk markets given their similar stand-alone status and similar focus on covering business interruption loss. In practice, the broker observed, achieving such a linkage requires an improved understanding of the root causes of business interruption experienced by companies. One way to attain that understanding, she concluded, is to include cyber risk in the root cause analyses that carriers currently perform. What impact the repository data informing those analyses might have remains an open question.

- Other participants responded by describing the special position that U.S. critical infrastructure occupies in the realm of terrorism protection. They explained that if electric companies, for example, temporarily lose the ability to provide their services to customers as a result of a terrorist attack, U.S. law and regulatory policy allow them to recover their costs through rate base adjustments. They pointed out that this ability to pass recovery costs forward to consumers – i.e., to make everyone share responsibility for the loss – is unique to some sectors of U.S. critical infrastructure. They then advised that because regulated entities in other countries can't directly pass these costs to consumers, they typically seek insurance to help cover their risk. The participants noted that the introduction of cyber risk into the terrorism protection conversation therefore raises a number of new questions for the insurance industry – including whether a cyber incident should be classified as a terrorist act that would entitle a company to rate recovery or a result of negligence that might otherwise spur demand

for cybersecurity insurance. Resolution of this issue one way or the other could profoundly impact the value of a repository.

- On a separate theme, an underwriter cited the challenge of consistently defining cyber incidents across international boundaries. In practice, he reported, disparate legal and policy requirements lead actors in different international jurisdictions to define cyber incidents very differently – resulting in generic terms such as "breach" being used as a catch-all to describe a wide and varied range of incidents. The underwriter commented that efforts to harmonize taxonomies therefore will be required to the extent a repository welcomes international participation.

Visibility

- Participants also described their current lack of visibility into cyber-related critical infrastructure loss incidents. They commented that without greater insight into such incidents as actually experienced, attribution of responsibility and incident characterization (i.e., accidental or malicious) is quite difficult. Underwriting efforts suffer as a result. Several participants noted, however, that data currently gathered by ISACs could potentially be leveraged to better characterize these incidents; identify which related losses warrant what amounts and kinds of coverage; and develop insurance packages in response that address those discrete needs.

Creating a Cyber Incident Data Repository

Despite these potential roadblocks to establishing a cyber incident data repository, the participants shared various perspectives on how to lay the groundwork for its development. Specifically, they described the need for a diverse working group to develop a cyber incident data template for repository information sharing purposes; identified stakeholders with potentially the "best" data for it; and described the catalyst role government could play in identifying and improving repository data sets.

Cyber Incident Data Repository Working Group

- An underwriter suggested that a working group, modeled on an organization such as the National Fire Protection Association (NFPA), should be established to advance repository conversations to the next stage. He advised that the NFPA hosts construction code officers, engineers, and other fire safety experts who know what information they need to help advance fire protection initiatives. The underwriter and several other participants identified various "cyber equivalents" to those experts whom they believed should constitute the core of a cyber incident data repository working group:

    - Technically savvy IT specialists, including IT system owners and managers;
    - CISOs and other information security professionals, especially those already involved in cyber incident information sharing efforts;

- Representatives from entities that currently receive cyber threat data through established mechanisms and/or aggregate such data and subsequently disseminate analytical reports (e.g., ISACs and IT and telecommunications companies that own and operate critical infrastructure);
- Insurance brokers and underwriters, especially those involved in communicating cyber risks to corporate boards; and
- Vendors.

- A broker and an underwriter emphasized the particular importance of bringing vendors into the conversation. They observed that vendors often possess unique viewpoints about cyber threats and exposures but do not have established channels to share their knowledge with carriers. The broker and underwriter asserted that vendor participation in a repository working group accordingly would provide valuable insight into how best to communicate with them about cyber incidents and how best to categorize and structure the data they have available.

Data Template

- Many participants recommended that after working through definition issues, a repository working group should develop a data template that clarifies the kinds of cyber incident information a repository should contain. The answers to this question, they explained, would directly inform a repository's design and organizational structure. Two underwriters asserted that while a common data template seeking the same basic information from all contributors would promote data consistency, such a template should be only a starting point. They explained that sector-specific and even sub-sector-specific templates should be developed to obtain additional relevant information from similarly situated organizations – including the dollar values associated with cyber-related asset and revenue loss. Many participants observed that whatever final form they take, a common data template and additional templates developed for specific sectors and sub-sectors should support the goal of establishing a "dynamic" repository. Specifically, the templates should include features that allow contributors to update previously submitted cyber incident data as new information becomes available.

- An underwriter recommended that a repository working group examine existing data templates before developing its own. He cited the Insurance Services Office (ISO) and other insurance solutions companies as potential sources for such templates and suggested that they might be willing to adapt and share them for repository purposes. The underwriter likewise mentioned the existence of several Energy sector data sets that include failure scenarios that also could be a good source for template data fields.

- An underwriter expressed concern that many companies would not know how to fill out an extensive data template that seeks more than the basic facts surrounding a breach. A second underwriter agreed, asserting that carriers would have to ask CISOs to investigate cyber incidents beyond their normal protocols in order to complete a lengthy form – potentially

requiring them to spend considerable time and resources determining, for example, the source of a particular cyber incident. A third underwriter responded that although there likely would be challenges with incentivizing CISOs to provide all the information desired by carriers, insurance industry representatives could and probably should volunteer to collaborate with CISOs on this task. Much of this information, he added, would likely be available anyway through claims forms filed by organizations seeking reimbursement for damages under existing cybersecurity insurance policies. The underwriter observed that significant and mutually beneficial information sharing already is occurring between CISOs and the insurance industry that could be expanded and leveraged to further support a repository's development.

Identifying Stakeholders with the "Best" Data

- In addition to discussing how to incentivize a wide range of large, mid-size, and small companies to contribute cyber incident data to a repository, several participants attempted to identify which kinds of organizations are positioned to contribute the most meaningful data – specifically, cyber threat and incident data that exists beyond the individual enterprise level. Such organizations, they asserted, should be similarly incentivized to contribute, as necessary:

    - A broker noted that major telecommunications companies own and operate critical communications infrastructure that allows them to "watch" cyber incident data streams through key nodes. He asserted that these companies are thus uniquely situated to provide overarching data about malicious activity observed at the system level. Anonymized versions of this type of data, he added, would be particularly useful to carriers because it could be aggregated and analyzed over time to show patterns and trends associated with known bad traffic.

    - A second broker stated that data about the impacts of cyber incidents may be even more relevant to repository users. She emphasized that managed security service providers (MSSPs) already possess the majority of this kind of data and may, in fact, possess a more detailed understanding of the cyber threats and vulnerabilities that particular companies face than do the companies themselves. A third broker agreed, noting that the "top twenty" cybersecurity service providers have a large amount of data about cyber incidents that – if they agreed to anonymize and provide it – would be invaluable.

    - The fourth broker commented that if organizations already are mandated to share information about cyber incidents with auditors, it would be worthwhile for repository planners to request those auditors to anonymize and aggregate that data for inclusion. She advised that it would be particularly helpful if the Federal Energy Regulatory Commission (FERC) leveraged data for this purpose from electric companies regarding their compliance or non-compliance with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards. For that matter, the broker concluded, whenever a Federal agency tells a specific organization that it has been breached in some way, the agency should similarly anonymize, aggregate, and contribute that cyber incident data.

- Finally, a reinsurer and a fifth broker agreed that cyber terrorism and other data from the Federal Bureau of Investigation (FBI) and the United States Secret Service (USSS) that help identify the potential causes of systemic risk would be a welcome repository contribution. Among other things, they noted, such data could help inform cyber incident consequence analysis efforts.

Government Catalysts

- Most of the participants identified the Federal government as being in a unique position to compile cyber incident data across sectors. In particular, they noted that it could help facilitate the sharing of anonymized information between the vendor and insurance industry communities regarding the top cyber risks that organizations face. The participants noted, however, that the Federal government should pay particular attention to filtering any vendor data that it aggregates before contributing it to a repository. They emphasized that such quality control would help ensure that shared information is indeed applicable and/or responsive to critical infrastructure protection needs.

- Many participants likewise noted that information about cyber-related law enforcement activities – e.g., cybercrimes – could be useful to carriers for underwriting purposes. Two underwriters noted, however, that similar challenges might arise if a repository were to receive cybercrime data about the same cyber incident from multiple (e.g., Federal, state, local, tribal, and territorial) sources. They asserted that a repository quality check process accordingly would need to be in place in order to ensure that cybercrime information obtained from different law enforcement parties does not lead to an outcome in which carriers provide coverage for the same cyber risk in different ways given variations in the data. Even so, several reinsurers responded that any cybercrime information that helps reinsurers understand how to insure against probable maximum loss would be highly valuable – especially when it comes to systemic cyber incidents.[15]

Characteristics of a Successful Cyber Incident Data Repository

- An underwriter observed that he and other carriers would know a successful cyber incident data repository "when they see it." While conceding that the concept is still notional, he and several other participants listed a number of repository attributes that together would indicate progress. They include:

  - Employment of an information sharing structure that adapts continually to evolving cyber threats and the shifting cyber risk landscape;
  - A critical mass of information about current cyber incidents and those that have occurred in the recent past that help inform present-day underwriting discussions;

[15] *See* probable maximum loss definition, *supra* note 9.

- Validation that the cyber incident consequences that carriers anticipate – based on analysis of repository data – are actually experienced by affected entities;
- Inclusion of historical information that over time helps carriers identify cyber loss patterns and trends and answer the "looming question" of cyber incident frequency;
- An improved ability to support the mapping of critical infrastructure nodes and modeling of critical infrastructure dependencies and interdependencies; and
- An improved ability to monitor risk accumulation across critical infrastructures.

NEXT STEPS

- Many participants agreed that although a repository likely will not deploy at a mature level initially, efforts in this direction must begin somewhere. They suggested that repository planners begin with a pilot that involves only a few critical infrastructure sectors. An underwriter specifically recommended that a pilot should focus on several utilities sectors, including the Energy Sector or the Healthcare and Public Health Sector, before expanding to others.

- A reinsurer commented that whatever sectors participate, pilot operations likewise should start small. As a first step, he asserted, planners should define the characteristics of the kinds of entities that they want to engage, considering such factors as organization size and services provided. Second, the reinsurer continued, planners should limit the pilot to a few well-defined categories of cyber incidents and corresponding data that they want engaged entities to contribute. Third, he recommended that planners develop core data template fields for participating entities to use in describing themselves – including, obviously, the cyber incidents that they have experienced as well as their infrastructure and cyber incident response capabilities. Finally, the reinsurer stated, planners should develop a process to translate the impact of reported cyber incidents into financial and other cost terms.

- Other participants added that an ISAC or other industry body that might benefit from cyber incident information sharing – i.e., *not* the Federal government – would be the best option for leading the development and execution of a pilot and, eventually, the operation of a repository itself. These participants nevertheless stated that government data sharing and other repository participation would be critical to a pilot's success.

TOPIC 2: CYBER INCIDENT CONSEQUENCE ANALYSIS

DESCRIPTION: During NPPD's prior events, many of the participants asserted that a second major obstacle to advancing the first-party cybersecurity insurance market arises from ongoing uncertainty about how large cyber-related critical infrastructure losses might become. One participant noted that although effective cyber risk management is a necessary prerequisite for promoting that market, IT culture does not include an ingrained process for collecting data about cyber attacks and learning from them. Without such a process, data that might otherwise be available to estimate first, second, and

third-order effects from cyber attacks on industrial control systems, for example, is largely absent. Under these circumstances, participants indicated that carriers would benefit from an alternate source of information to understand the probable consequences of such cyber attacks. This foundational information, in turn, would help them develop truly attractive first-party policies in response. Several participants asserted that there accordingly should be a new focus on cyber incident consequence analysis – involving enhanced cyber risk models and simulations – that helps them at least to "ballpark" potential losses from cyber attacks on critical infrastructure and assess the effectiveness of available cyber risk controls to prevent or mitigate those losses. The purpose of this working session discussion therefore was to identify more specific insurance industry requirements for models, simulations, and exercises supporting such analysis going forward.

DISCUSSION POINTS:

CONSEQUENCE INFORMATION NEEDS

- An underwriter stated that the insurance industry needs an improved baseline understanding of what losses typically occur, or could be anticipated to occur, during a variety of potential cyber incidents, along with the likelihood that those incidents will come to pass. This information about losses, he continued, needs to be translatable to business consumers such as Chief Financial Officers (CFOs), CISOs, Chief Risk Officers (CROs), and most especially General Counsels – all of whom have obligations to corporate owners and shareholders when it comes to highlighting their company's financial risks from cyber incidents.

- Beyond this financial information, several participants asserted that effective cyber incident consequence analysis should optimally convey information about critical infrastructure interconnectedness – a "huge" issue that carriers seek to better understand. A broker and reinsurer agreed, stating that the insurance industry needs to know more about the cascading effects that might flow from a cyber incident. Specifically, they observed that carriers need:

    - Clarification about what critical infrastructure is actually most critical when it comes to mitigating and/or preventing such cascading effects through targeted cyber risk management investments;
    - An improved sense of which cyber risk management investments/controls would offer the most benefit in this regard; and
    - A means to better capture the actual risks faced by specific organizations that find themselves in the path of a cascading critical infrastructure failure caused by an initiating cyber incident.

    "We can't and don't want to eliminate all cyber risk," the reinsurer explained. "We just want to help manage it if we can."[16]

[16] An underwriter emphasized that not all incremental cybersecurity improvements are successfully driven by insurance and that expectations in the critical infrastructure protection space should be managed accordingly. He cited as an

- A second underwriter referred to the earlier cyber incident data repository discussion when asserting that the insurance industry needs and wants to leverage an enhanced understanding of critical infrastructure interconnectedness into an improved understanding of risk accumulation, the "big kahuna" of cyber risk exposures.[17] He and other participants reiterated that a focus on risk accumulation contrasts in some ways from the Federal government's focus on critical infrastructure sectors by highlighting instead specific technical areas that present significant cyber risk exposures (i.e., where risk "accumulates"). When discussing this point, the participants referenced cloud computing as just one area that does not fall neatly within a particular critical infrastructure sector but that still raises major concerns. "Companies are saving so much money with the cloud," the underwriter explained, "that they can't place pressure on cloud service providers to increase their cybersecurity." He concluded that effective consequence analyses that highlight this and other areas of risk accumulation will help companies better recognize, prioritize, and address their key cyber risks.

- A reinsurer asserted that the Federal government has likely "mapped out" a variety of cyber-related critical infrastructure failure/loss scenarios and thus may possess greater insight into critical infrastructure interconnectedness than does the insurance industry. She surmised, however, that national security considerations preclude the government from sharing a significant amount of this information with carriers and other cyber risk management professionals. The reinsurer nevertheless emphasized that, whatever factors may be in play, the challenge of underwriting cyber risk stemming from critical infrastructure and critical system interconnectedness is significantly more difficult without this information. She asserted that if the Federal government could share just some of its insight – particularly about "where the weaknesses are in the system" – it would be a boon to both underwriters and reinsurers in terms of educating them about the full extent of a cyber incident's potential cascading effects. At the same time, she concluded, such sharing could help promote the development of a community of practice that includes both risk mitigation and risk transfer professionals. Other participants observed that such a community is a necessary foundation for sustaining cyber risk management conversations among carriers, CISOs, critical infrastructure owners and operators, and others over the long term.

- An underwriter concurred, and emphasized that carriers typically struggle to understand what will happen during a cyber incident – a situation that has resulted in large part because existing cyber incident consequence models are based on limited public information and not detailed and regular self-reporting. While national security considerations might make some

---

example U.S. banks that historically have not put a value on the cyber risk inherent in swipe credit cards and that consequently have been slow to adopt more secure "chip and PIN" technology that is widely used across the U.K. and Ireland banking systems. *See* Tom Gara. "October 2015: The End of the Swipe-and-Sign Credit Card," *The Wall Street Journal*, 6 February 2014, http://blogs.wsj.com/corporate-intelligence/2014/02/06/october-2015-the-end-of-the-swipe-and-sign-credit-card/ (June 12, 2014). The underwriter nevertheless stated that the Cybersecurity Framework, *supra* note 3, could incentivize better cyber risk management behavior if Framework users are shown over time to have a better cyber loss experience than Framework non-users.

[17] *See* risk accumulation definition, *supra* note 11.

private/public collaboration in this area difficult, he continued, the Federal government still could greatly assist the insurance industry's own analytic efforts by identifying which cyber threats should be prioritized in light of the government's specialized knowledge. The underwriter likewise urged the Federal government to apply its considerable analytic capabilities against information contained in any future cyber incident data repository in order to identify emerging cyber incident patterns and trends. Such government involvement, he continued, could lead to the development of highly credible, and therefore commercially viable, cyber incident consequence models that focus on the "right" cyber risks. In addition, government input could also inform the identification of available and/or needed controls to address the cyber risks that the consequence models identify. Put simply, knowing better how cyber threats are evolving and what companies are likely to be affected will help carriers more confidently advise their clients about appropriate and available risk mitigation and risk transfer options. The underwriter concluded that whatever their initial level of maturity, such models, and the simulations and other exercises that utilize them, must be updated frequently to reflect not only new patterns, trends and threats but also the evolving nature of critical infrastructure itself.

- Various participants cited other potential approaches that might help the insurance industry capture the cyber incident consequence information it needs. For example, an underwriter suggested that models used to anticipate pandemics might be adapted for use in the critical infrastructure domain. A second underwriter likewise suggested that Cold War nuclear attack scenarios could also be viable templates on which to base cyber incident consequence models, simulations, and exercises with a critical infrastructure focus.

Utility of Cyber Incident Consequence Analytics

- Many participants spoke positively about the benefits that enhanced cyber risk analytics could bring to cyber risk management generally and to the cybersecurity insurance market specifically. They advised that greater access to information about specific cyber incidents as well as cyber risk trends could enable the insurance industry to move beyond existing static service outage models to new models that provide a better understanding of *potential* cyber incidents. In particular, participants expressed interest in better understanding the credible threats that might occasion cyber incidents, the probability of those incidents, and their likely consequences.

- Two brokers and an underwriter asserted that properly constructed models, simulations, and other exercises could be of great use in articulating cyber risks to boards of directors and other corporate leaders and incentivizing more informed cyber risk management investment accordingly. As one of the brokers explained, "Credibly determining how long a cyber-caused power outage will last before recovery efforts succeed will be hard without [such] models and simulations." Other participants noted that before many boards of directors commit to making major cybersecurity investments, they need to actually "see" such cyber incident consequence examples. They stated that illustrative models, simulations, and other exercises that provide

those examples, and which closely reflect reality as corporate leaders understand it, consequently could be highly effective communications tools in this regard.

- A broker added that improved cyber risk analysis of this nature could provide the insurance industry with a strong basis to move beyond case-by-case cybersecurity insurance coverage determinations for clients toward offering more generic, overarching policies to potential insureds. She added that cyber incident consequence analytics likewise could go a long way toward closing the gap between real property exposure, which is widely insured, and cyber exposure, which is not. "In the energy industry," the broker advised, "companies are paying $20 to $30 million dollars each year in property insurance but they won't pay a million dollars for cybersecurity insurance." She explained that when customers compare prices for property cover versus cyber cover, they see cyber cover as too expensive – primarily because they haven't had much experience with cyber incidents. Cyber incident models, simulations, and other exercise, she asserted, could provide them with that experience vicariously and could incentivize them to explore investments in cybersecurity insurance as a means to address associated risks in a more cost-effective manner.

- An underwriter commented that software failure represents a potentially huge risk accumulation, and that its probability therefore should be an integral part of any future cyber risk model, simulation, or exercise. He asserted that software vendors are in the best position to answer questions about their product vulnerabilities but acknowledged that they often are reluctant to do so. The underwriter emphasized, however, that if software vendors provided data, as well as the geographic locations of their customers, then carriers could build a heat map of exposure to those vulnerabilities that would support the development of tailored cybersecurity insurance products for impacted parties.[18] In short, he continued, such information sharing would allow carriers to create something analogous to the heat maps that enable carriers to identify the zip codes most likely to be significantly impacted by earthquakes, flood damage, and other natural disasters. The underwriter nevertheless recognized that without a breakthrough with software vendors on this front, credible models, simulations, and other exercises that support cyber incident consequence analysis at a generic level are the next best alternative for "mapping out" cyber risk. "The value of a generic model and cyber risk scenario, a reinsurer added, " is that it can help companies understand that they're vulnerable, what questions they accordingly should be asking their service providers – including cloud service providers – and what cybersecurity requirements to put on those providers as a condition for doing business."

[18] A "heat map" is a visual representation of data using colors. *Investopedia Financial Dictionary, s.v.*, "heatmap," accessed June 2, 2014, http://www.investopedia.com/terms/h/heatmap.asp. A heat map can be used with all sorts of data. *Id*. For example, a heat map of foreclosures data could show parts of the U.S. experiencing high rates of foreclosure in a dark color and states with low foreclosure rates in lighter colors. *Id*. A color-gradient legend typically accompanies a heat map to specify the data. *Id*.

Characteristics of Successful Tools and Platforms

The participants then described a variety of qualities that successful cyber incident consequence analysis tools and platforms should have from a risk mitigation/ risk transfer point of view. Specifically, such tools and platforms must:

- **Capture reality**. Several participants emphasized that analytic tools and platforms will be useful only insofar as their underlying data sets represent real-world conditions and circumstances. When asked about the security concerns associated with using actual and/or identifiable critical infrastructure data as part of an analytics effort, many participants stated that they would find value in generic models so long as "the fidelity of the data set underlying them can be defended." They explained that such data must capture true-to-life critical infrastructure characteristics that stakeholders could then use to compare their own situations.

  An underwriter commented that the Federal government is in the best position to provide the initial data set for such generic models but emphasized the importance of private industry expanding and refreshing it over time with appropriate industry-specific information. He added that private industry should do so on a consistent, periodic basis so generic models can provide maximum risk management benefit. He then referenced the ongoing development of building codes for fire protection as an example of model refinement that has increased safety margins over time. A broker responded that the underwriter's fire analogy was not overly helpful, however, because cyber standards cannot be developed to avoid all cyber exposures – most notably, because malicious hackers, unlike fire, typically adapt to outsmart cyber defenses. Under these circumstances, several participants recommended that future models assess infrastructure at a higher, more holistic level – focusing especially on architecture "weak points" and areas of high risk accumulation. They added that a generic model that includes refreshed data relevant to these areas of greatest insurance industry concern would be particularly helpful.

  Two brokers and an underwriter suggested that a table top exercise, hosted by DHS, could provide a useful starting point for cyber incident consequence analysis of this nature. The underwriter stated that hurricanes would be a good model for this work and described the cascading impacts that such storms cause across multiple critical infrastructures as a reasonable parallel for how impacts might proliferate during a major cyber incident. He accordingly suggested that the same first responders, utilities, and other entities that join hurricane table top exercises should be similarly engaged in the planning and execution of an equivalent cyber incident exercise. If possible, he added, a table top exercise should be designed to offer insights into the likelihood that particular consequences will result from the initiating cyber incident.

Several participants asserted that participation by members of the so-called "three-legged stool" – brokers, underwriters,[19] and vendors – would provide additional credibility to such a table top exercise and would likely increase the level of confidence that the insurance industry would place in its results. A broker explained that while brokers and underwriters collaborate frequently on risk transfer solutions, vendors tend to "look at issues through their own lens" and likely will have different but very useful perspectives. An underwriter agreed and asserted that the accumulation exposure occasioned by cloud services is the "800 pound gorilla" in the room. He accordingly suggested that cloud service providers, among other vendors, should be centrally involved in the planning and execution of a table top exercise.

Although they concurred that cyber incident consequence analysis holds promise for expanding first-party cybersecurity insurance coverage, a number of participants cited various difficulties faced by those already engaged in critical infrastructure interdependency modeling efforts:

- An underwriter and a reinsurer highlighted the fact that data sets about "domino" (i.e., cascading) impacts in this area are fairly limited, making models, simulations, and other exercises difficult to corroborate. For this reason, a broker noted, current models don't even attempt to capture the impacts of truly catastrophic critical infrastructure loss events – precisely the events of greatest interest to the insurance industry.

- A second broker added that it will remain difficult to calculate the impact of "downed service" on a company's reputation and revenue stream given the ongoing dearth of available data about those particular losses.

- Other participants advised that in order to make the "cyber ecosystem" safer, new and as yet undeveloped collaboration protocols will be needed to prod companies to share sensitive vulnerability and other critical infrastructure information in ways that they previously have not. Despite the growing realization that systemic cyber risk requires a collaborative response, they added, building the necessary trust to do so will take time.

An underwriter responded that all modeling and simulation efforts – and the potential risk solutions they help inform – necessarily begin from a point of maturity lower than ideally desired. The use of even generic data, he continued, nevertheless could result in the development of superior models than those currently in use. The underwriter explained that existing models start with nominal assumptions, and that lots of information is extrapolated from that starting point. He emphasized that those extrapolations still help translate otherwise

[19] An underwriter stated that actuaries should be included in the population of underwriters participating in any such exercise. An actuary is a business professional who analyzes the financial consequences of risk. "What is an Actuary?," Purdue University, accessed June 12, 2014, http://www.math.purdue.edu/academic/actuary/what.php?p=what. Actuaries use mathematics, statistics, and financial theory to study uncertain future events, especially those of concern to insurance and pension programs. *Id*. An actuary tells insurance companies how much they should charge people for insurance based on risks. *Merriam-Webster Online Dictionary, s.v.,* "actuary," accessed May 16, 2014, http://www.merriam-webster.com/dictionary/actuary.

academic or conceptual scenarios into viable simulations and other exercises, including table top exercises. The underwriter saw no reason why the same approach would not also work in the cyber context.

When asked if well-crafted models could actually help expand insurance coverage to physical losses arising from a cyber incident, the underwriter replied in the affirmative but noted the embryonic nature of first-party coverage in this area. He nevertheless stated that generic cyber risk models and simulations, based on defensible data, could lead to the discovery of new cyber risk management information that, in turn, could generate new ideas for new insurance products. The underwriter advised that the decision to proceed with such products would depend ultimately on the outcome of reviews by actuaries.

- **Enable refinement of benchmarks and standards.** The participants also discussed the role that standards play in security benchmarking. Several noted that corporate information security leaders – specifically, CIOs and CISOs – tend not to benchmark their security performance against an ideal scenario of perfect security breaches (i.e., no breaches) because such an ideal is a fundamentally unachievable goal. The participants noted that they instead tend to benchmark their performance against peer organizations. In short, companies compare their cybersecurity efforts against each other rather than against standards that describe ideal but unachievable cybersecurity postures.

  Given this dynamic, several participants advised that improved models, simulations, and other exercises could help companies better benchmark themselves by providing greater insight into systemic conditions that increase cyber risk for everyone. While many large companies already perform company-level modeling that is often directed internally, they explained, the development of cyber incident consequence analysis tools and platforms that capture external interconnections could drive more thorough conversations between companies and their underwriters about the full range of cyber risks they face. The participants stated that this hopefully would encourage companies to launch more effective cyber risk mitigation efforts in response.

  Several participants asserted that such tools and platforms also could provide the basis for improvements to existing, industry-developed cybersecurity standards – for example, by raising the profile of systemic risks that arise out of critical infrastructure interconnections and thereby creating momentum to provide them with more specific and thorough standards treatment. As companies start to use those enhanced standards as the basis for both cyber risk management investment and comparison against their peers, they continued, the baseline level of compliance could increase over time. The participants concluded that any such enhanced standards should be developed in light of existing industry-developed standards and frameworks that inform risk mitigation, such as the Cybersecurity Framework.[20]

[20] *See* Cybersecurity Framework, *supra* note 3.

- **Reflect cost drivers and supports refinement.** Many participants concurred that the ultimate goal of cyber incident consequence analytics is not to provide a "perfect capture" of all risks. Instead, they asserted, model and platforms should provide improved visibility into the drivers of cyber incident costs. They likewise should be sufficiently flexible to incorporate refinements and other updates that improve understanding of risk accumulation over time.

- **Address insurance needs.** Several participants likewise remarked on the need for cyber incident consequence analytics to meaningfully addressing probable maximum loss,[21] as well as the critical infrastructure interconnections that affect such loss. An underwriter explained that if the Federal government could help provide some idea of probable maximum loss arising from a particular cyber incident of heightened concern – up to and including catastrophic loss – then the insurance industry would be much better positioned to clarify which consequences flowing from it are insurable and which are not. A broker agreed, observing that it is important to "zero in" and determine cyber incident consequences that may never be insurable so companies can plan their risk management strategies accordingly. Other participants again underscored the significance of risk accumulation in the provision of insurance and emphasized that cyber incident models, simulations, and other exercises must help carriers understand risk accumulation not only within conventional critical infrastructure sectors but also domains such as the cloud.

CURRENT APPROACHES

- A reinsurer provided insight into his company's development of "plausible but challenging" disaster scenarios that are meant to elicit data about probable maximum loss events, including cyber events. He described how his company annually provides a description of a notional loss event to underwriters and then asks them to report on all the losses they likely would experience during and after such events. The reinsurer advised that this approach requires scientifically rigorous development of cyber incident scenarios – not through probabilistic approaches,[22] which he described as "impossible" for cyber risks until more loss data becomes available, but nevertheless in partnership with both government cyber risk experts and industry risk managers. Those scenarios, in turn, are reviewed by a broad set of analysts in the governmental, private, and academic risk management communities before they are modeled through the company's annual exercise. Academic partners, he noted, typically bring data to the exercise. The reinsurer characterized this effort as "a regular part of our business planning

[21] *See* probable maximum loss definition, *supra* note 9.

[22] For a general explanation of deterministic versus probabilistic approaches to risk assessment, *see* "Probabilistic Approaches for Assessing Environmental Risks of Pesticides," European Framework for Probabilistic Risk Assessment of the Environmental Impact of Pesticides (EUFRAM), http://www.eufram.com/probablistic.cfm (May 19, 2014) ("Probabilistic approaches enable variation and uncertainty to be quantified, mainly by using distributions instead of fixed values in risk assessment. A distribution describes the range of possible values (e.g., for toxicity), and shows which values within the range are most likely. The result of a probabilistic risk assessment can also be shown as a distribution, showing the range of environmental impacts that are possible, and which impacts within that range are most likely. This should provide a better basis for making decisions about pesticide risks [than deterministic approaches], because the full range of possible outcomes can be taken into account.").

process" and emphasized that information sharing with underwriters is a key part of its ongoing success. He explained that his company "shares back" aggregate data from all the contributing underwriters with those underwriters but keeps their individual contributions confidential for competitive reasons.

- The reinsurer added that major non-U.S. banks adopted his company's approach when modeling and exercising similar scenarios that addressed the impacts of a cyber attack in their shared geographic region. The result of that exercise, he advised, was the development and adoption of a new collaboration protocol among the participating banks to address a previously unrecognized information sharing gap.

- The reinsurer then identified several challenges with this analysis work. He advised that his company is testing a data aggregation tool to help it better leverage the information it receives from its scenario-based exercises. He noted, however, that feedback received to date suggests that his company has not yet successfully articulated a scenario that represents a "truly systemic capital hit." Put simply, his company can generate strong numbers describing a cyber attack on a specific industry but cannot yet effectively describe the "cross-over" effects – i.e., cascading effects – on other sectors. Limited data about actual cyber incidents, he noted, complicates the development of realistic scenarios much in the same way that attempts to model terrorist attack scenarios are complicated by the small number of terrorist attack "samples." The reinsurer added that while his company has had success in identifying specific risk accumulators within specific industries – typically mid-size and small companies that fail to manage their cyber risks well – it likewise has had a hard time pricing that identified risk accumulation.

- An underwriter stated that his company conducts similar scenario-based modeling – for example, defining the parameters of a hundred-year cyber event and running simulations based on those parameters – because it also has experienced difficulties with probabilistic modeling. Like the reinsurer, he explained, he and his colleagues are also struggling with how to further develop scenario-based modeling in the absence of more, and more defensible, data.

- In response to these challenges, several participants offered feedback and observations. A broker suggested that red team exercises, such as the recent GridEx II exercise conducted by NERC, could potentially provide useful data for understanding the cascading effects from a cyber incident.[23] She advised that the exercise included a scenario involving the simultaneous deployment of a computer virus and the detonation of a bomb – both of which initiated a three-day power outage that caused fatalities and considerable property damage. The broker cited resulting food shortages and their behavioral impacts on the population (e.g., looting) as particularly noteworthy exercise highlights. An underwriter added that ISACs also could be

[23] *See* North American Electric Reliability Corporation (NERC). *Grid Security Exercise (GridEx II) After Action Report* (Atlanta, Georgia, March 2014), http://www.nerc.com/pa/CI/CIPOutreach/GridEX/GridEx%20II%20After% 20Action% 20Report.pdf (June 7, 2014); *see also* NERC Web page, "GridEx," http://www.nerc.com/pa/CI/CIPOutreach/Pages/GridEX.aspx, accessed June 7, 2014.

useful sources of information about cascading effects. He re-iterated the point that cyber incident consequence models, simulations, and other exercises should be developed against actual, parallel incidents (e.g., hurricanes) in order to bring together the right stakeholders from multiple sectors for planning purposes.

Barriers to Cyber Incident Consequence Analytics

In addition to describing the potential benefits associated with improved cyber incident consequence modeling, simulations, and exercises, participants identified various potential barriers to that progress. They include:

- **Availability of data.** A broker stated that it is no accident that the three existing lines of insurance with the most robust data and strongest predictability – workers compensation, automotive, and homeowners insurance – also entail mandatory coverage requirements. He asserted that more ubiquitous use of cyber insurance therefore may be required to generate the volume of data needed to inform more effective cyber incident consequence analytics in the future. The broker further noted that banks require proof of homeowners insurance before issuing home mortgages and posited that banks, rather than carriers, may ultimately drive up the rate of users applying for and receiving cybersecurity insurance. A second broker agreed, stating that she has seen a gradually increasing number of companies being contractually required to purchase cybersecurity insurance as a cost of doing business. She advised that her company has contributed to this trend by asking its clients to ask their vendors to buy policies. A reinsurer made similar observations and stated that as purchasing cybersecurity insurance becomes a business norm in the years ahead, carriers will be in an enhanced position to anonymize, aggregate, and analyze cyber incident claims data to support their actuarial needs.

  When asked what "still missing data" would be most helpful for cyber incident consequence analytics – and what data capture and development should accordingly be prioritized going forward – various participants responded with the following categories:

  - Probability of attacks on particular critical infrastructures;
  - Locations of risk accumulation/aggregation;
  - Impacts of cascading effects across critical infrastructure sectors;
  - Magnitude and value of losses from the cyber-related theft of intellectual property; and
  - Magnitude and value of losses stemming from reputational harm to companies following cyber incidents, such as data breaches and service failures (e.g., business interruption).

  Several participants likewise echoed comments made during the earlier cyber incident data repository discussion about existing data gathering efforts by sector ISACs. They asserted that those efforts might have uncovered information that could help close the insurance industry's data gaps in each of these categories and should be leveraged where possible.

- **Maturation of the modeling industry.** An underwriter indicated that current cyber incident consequence analytics seems to be driven more by the intuition of analysts than by actual risk

assessments. She explained that existing modeling software thus leaves more to be desired. As a result, she continued, many carriers have responded by *not* adopting model-based approaches to better understanding cyber risk. Several participants responded that the adoption and backing of risk assessment-based models by ratings agencies would significantly enhance their standing and would likely encourage their expanded use by carriers. "If ratings agencies start asking questions about what companies are doing to mitigate cyber risk," one participant observed, "everyone's likely to pay attention."

- **Adoption challenges.** Several participants noted that the reluctance of some organizations to engage cyber incident models, simulations, and other exercises stems from inherent tensions between identified risk areas and the cost saving that those risk areas enable. A reinsurer cited cloud computing as a prime example of a technology that provides significant cost savings but that also aggregates more risk than previous IT solutions. Cloud enthusiasts, he stated, do not always want to know the risks they are buying. A broker noted that vendors face similar tensions. He explained that they possess significant understanding about the risks presented by the use of new software, network configurations, cloud architectures and the like but understandably are not keen to publicize what could be perceived as shortcomings in those offerings. He asserted, however, that without a view into this information, carriers are unable to accurately capture accordant risks or develop responsive insurance policies to help address them. Many participants responded by emphasizing the need for greater information sharing among vendors and carriers about relevant vulnerabilities and the kinds of controls that should be developed to mitigate them. With more open lines of communication, they asserted, carriers could require those controls as a condition for coverage – safeguarding the value of vendor offerings while protecting consumers of those offerings in the process.

Potential Action to Support Cyber Incident Consequence Analytics Approaches

The participants thereafter identified a series of actions that they believed could help promote the development and adoption of better cyber incident consequence analytics. They include:

- **Development of a generic modeling structure.** An underwriter cautioned that truly effective cyber incident consequence modeling must reflect the type of underwriting assessment taking place. He explained that while generic model "archetypes" may be useful for describing cyber risk trends across companies, meaningful modeling ultimately needs to occur at the individual company level. Only at that level, he explained, can companies incorporate their unique circumstances into the analytics process and confidently ensure that the results apply to its actual risk situation. A company-specific underwriting assessment, he continued, "can't simply be a checkbox questionnaire." On the contrary, doing it right with company-specific data instead requires significant attention and resources from individual companies. Although several other participants also emphasized the need to refine generic models to assess cyber risks on an individual company basis, they nevertheless responded positively to the notion of developing a generic modeling structure on which to base those refined modeling efforts. Several underwriters, for example, noted that if a company participated in a generic but

industry-specific table top exercise, it could apply lessons learned from that exercise to evolve its own company-level model – tailoring it to provide more insights about where it might best direct limited risk management dollars against cyber risk based on its unique profile.

One underwriter replied that while this would be worthwhile advance, tying actual dollar values to the consequences demonstrated in a generic table top exercise – even if that exercise is industry-specific – will likely remain challenging. When asked if it nevertheless would be helpful for table top exercise planners to develop a series of follow-on valuation and other questions for individual companies to answer themselves (i.e., privately through such company-level models), he and several other participants responded emphatically, "yes." A reinsurer explained that, at a very minimum, a generic but industry-specific table top exercise – supported by more specific follow-on questions – could help carriers better advise potential insureds about specific vulnerabilities that they should address to enhance their cybersecurity.

- **Improved education about cyber risks.** A broker and several other participants noted the lack of awareness by many companies about the nature of their actual cyber risk. They consequently highlighted the value of a generic model as an educational tool that could teach companies about what their cyber vulnerabilities actually are, rather than what they think they are. For example, a reinsurer cited a recent study in which only 30% of companies believed that they had cyber risk exposure through their use of cloud services. In reality, he advised, fully 90% of them had such exposure. Under the circumstances, several participants suggested that a "foundational" generic model should be designed to inform companies that they are part of a wider cyber risk community of interest with shared vulnerabilities that require collaborative risk management attention.

TOPIC 3: CYBER RISK AND ENTERPRISE RISK MANAGEMENT

DESCRIPTION: During NPPD's prior events, participants commented that many boards of directors and other senior leaders continue to treat cyber risk as an IT problem separate and apart from the other risks they must address within their overall corporate risk management strategies. The primary reason appears to be that cyber risk still has not been reduced to terms that non-technical business leaders can readily understand – namely, the financial costs of cyber events and the potential damages to reputation they can cause. Many of the participants suggested that to overcome this hurdle, companies should adopt ERM programs that explicitly incorporate cyber risk into the family of other business risks they face.[24] By doing so, companies will be able to use common ERM vernacular to prioritize cyber risks and corresponding solution sets in relation to those other business risks. This will empower senior leaders – in many cases, for the first time – to move beyond addressing only the technical aspects of cyber risk to its broader potential impacts on customer satisfaction, reputation, sales, and supply chain resilience. In short, ERM "done right" could serve as a powerful tool to help companies determine how to move cyber risk out of the IT silo and into more holistic business discussions. This, in turn, will help

[24] *See* enterprise risk management (ERM) definition, *supra* note 2.

companies make more informed and effective cyber risk mitigation and transfer investments in the ongoing competition for limited risk management dollars.

While the promise of ERM for addressing cyber risks faces several challenges, it nevertheless remains a hopeful path forward for advancing both the first-party and third-party cybersecurity insurance markets. Many past event participants observed that the key differentiator between companies that purchase policies before a cyber incident and those that do is whether the company maintains a centralized ERM structure for cyber risk management. Participants concluded that more efforts are needed to evangelize the benefits of ERM to larger audiences in order to promote not only better cyber risk mitigation efforts but also the case for cybersecurity insurance as complementary parts of a comprehensive cyber risk management strategy. The purpose of this working session discussion was to identify insurance industry ideas on how to advance that message.

DISCUSSION POINTS:

THE CASE FOR ERM IN THE CYBER RISK SPACE

- Participants discussed the many motivations that lead a company to adopt or not adopt ERM programs in order to address its cyber and other risks. A broker noted the competing risk management interests that corporate leaders must continually balance. He explained that most large companies face a wide range of security concerns and employ different security professionals to address them. Those professionals, the broker asserted, often find themselves competing against one another for scarce risk management resources. Several underwriters responded by citing the utility of ERM when it comes to highlighting the interdependent nature of many corporate security concerns, including cyber risk. They emphasized the particular value that ERM brings to risk management tradeoff decisions – specifically, its core approach for helping companies decide which interrelated risks they should "assume, pass, or share." The underwriters likewise underscored the benefit that ERM provides to business continuity planning, which for many companies increasingly includes a cybersecurity component.[25] Finally, they noted the direct application that basic business continuity planning steps could have to broader questions about how society should maintain the essential functions that critical infrastructure provides and/or supports in the face of cyber and other risks.

- Most participants agreed that companies that use ERM programs to address their cyber risk have "many more options" when they decide to purchase cybersecurity insurance. An underwriter advised that while they do not formally require it, many carriers count the presence of an ERM program as a factor in favor of providing cyber risk coverage. Given the holistic risk

[25] Business Continuity Planning (BCP) is the process of developing prior arrangements and procedures that enable an organization to respond to an event in such a manner that critical business functions can continue within planned levels of disruption. Business Continuity Institute. *Dictionary of Business Continuity Management Terms*. (Caversham, Berkshire, United Kingdom: Business Continuity Institute, September 2011) (June 16, 2014). The end result of the BCP process is a business continuity plan. *Id*.

management focus that those programs presumably instill within an organization, he explained, ERM programs help carriers differentiate between those companies that are safer insurance investments from those that are less safe. "The outgrowths of ERM, such as insurance," he stated, "come with a certain confidence level in the security of the [company's] infrastructure." A second underwriter likewise noted that many carriers use the existence of an ERM program as the basis for an initial insure/do not insure decision – with more detailed assessments of a program's robustness as a necessary follow-on inquiry before actually writing a policy. These and other participants then described the elements of successful ERM programs that typically help companies better manage their cyber risk and, as a result, qualify them for more relevant and affordable coverage:

- **Engagement of senior leadership.** A reinsurer commented that effective ERM programs must be implemented at the senior leadership level. Specifically, he advised that they should reflect a corporate culture that features cyber-related ERM discussions at all board meetings and that subjects itself to regular oversight – including through periodic internal risk audits and audits by outside, independent organizations.

- **Engagement of general counsels.** A broker described general counsels and chief compliance officers as key players in successful ERM programs and stated that her company's risk assessment workshops for corporate leaders are always more successful when then these leaders are involved. She explained that corporate general counsels, in particular, are able to command senior management's attention in powerful ways and accordingly are well-positioned to help drive a company's cyber-related risk management investments. A second broker agreed, observing that a general counsel in some respects *is* a company's chief risk officer.

- **Engagement of CISOs.** An underwriter added that it is similarly valuable to include a company's CISO in the ERM process – particularly a CISO who understands the role that insurance can play as part of a comprehensive risk management strategy. A smart CISO, he observed, understands that the cyber risk controls that carriers require as a condition of coverage can help justify his or her cybersecurity budget request. A second underwriter agreed and emphasized that insurance is not so much a risk management "solution" as it is a tool to help manage (i.e., transfer) residual risk. He concluded that the company that "gets" this is in a better position to incorporate its cyber risk into its ERM program, mitigate it more effectively, and make more informed insurance purchases accordingly.

- **Establishing direct lines of communication.** A third underwriter asserted that when it comes to cybersecurity specifically, a company should establish a direct line for ERM reporting to its board of directors rather than a hierarchal chain that requires many approvals before funds can be spent on someone (e.g., outside cyber forensics support) or something (e.g., a new technology) to address a cyber risk or incident. At the same time, he added, ERM programs should promote connections among employees laterally across

organizations so IT and other professionals from different chains of command can be leveraged for assistance as needed.

Barriers to Implementing ERM in the Cyber Risk Space

Despite the promise of ERM, the participants cited a number of ongoing barriers that inhibit its more widespread adoption or otherwise prevent its extension to fully encompass cyber risk. They include:

- **Risk management resources.** A broker commented that not all companies are sufficiently large, resource-enabled, or sophisticated to support ERM programs. A second broker explained that establishing and leveraging ERM to bring proper attention to both a company's cyber risk issues and risk management options has met resistance by mid-size and small companies especially because "developing and implementing ERM sounds [to them] like a full-time job." She commented that this perception is misplaced. Regardless of whether a company is sophisticated enough to have an ERM program, it will have a board. A board-level review, the broker continued, could essentially serve as an ERM program substitute for a mid-size or small company.

  An underwriter added that a significant challenge with applying ERM in the cyber risk space is that some companies – regardless of size – don't want to address systemic issues associated with their older and outdated technology systems. He noted that the cost of replacing those systems typically is very high and that some corporate leaders therefore would "rather not know." Not implementing ERM, he concluded, allows these leaders to maintain a certain level of plausible deniability about their risk. A second underwriter agreed and added that companies without ERM programs often fail to acknowledge their cyber risks and, in some cases, actively seek to hide them. He described this situation as a missed opportunity, noting that companies with ERM programs tend to exhibit a clearer understanding of the implications of cyber risks to their organizations. They consequently tend to target limited risk management resources more effectively. The underwriter advised that these benefits result directly from ERM-based collaborative structures that companies have established between their boards of directors and CISOs and other IT professionals in order to address cyber risks.

- **Communication differences.** Several participants stated that semantic and other communications differences complicate discussions about ERM program implementation, both at the corporate leadership level and among security professionals within companies. An underwriter described marked differences in the language that IT security professionals and non-IT security professionals use to describe their respective challenges. She asserted that significant communications breakdowns between these two groups result frequently, even in companies with "mature" ERM programs. The underwriter likewise described a similar language barrier that exists between IT security professionals and carriers. Other participants concurred that ERM has not proven to be a panacea when it comes to translating cyber risk into terms of financial and reputational harm.

A second underwriter responded, however, that this problem is less prevalent in companies that include regular CISO briefings to boards of directors – a practice he described as a "leading indicator of a mature ERM program." Ideally, he added, CISOs and ERM leads should prepare those briefings together. He observed that such co-prepared briefings typically contribute to a greater cyber risk focus within organizations and consequently greater cyber risk understanding. In short, ERM-informed attempts to facilitate cyber risk management messaging to senior leadership can begin to bridge these persistent communications gaps.

Given these challenges, other participants suggested that carriers refrain from using ERM as the starting point for a cyber risk management discussion – at least with some potential insureds. An underwriter stated that ERM needs to be thought of as an operational risk management strategy of which cyber risk management is just one part. ERM itself, he emphasized, is not a cybersecurity strategy. A broker agreed, explaining that his risk management conversations with mid-size and small companies focus first on the need for more and better cybersecurity as a prerequisite to obtaining desired coverage. He advised that most such companies are unfamiliar with ERM, so he usually drops it from conversation in order to avoid "muddying the message." A second broker noted that this approach with mid-size and small companies makes sense because any increase in cybersecurity that a company funds in order to qualify for insurance will likely translate into increased security overall for the company. In short, ERM goals will be accomplished indirectly.

- **Leadership and alignment issues.** While most participants saw clear value in ERM as a means to more effectively manage cyber risk, a reinsurer noted that some 90 percent of companies don't have ERM programs of any sort. A broker noted that even if more companies were to enthusiastically adopt ERM programs tomorrow, many of them probably can't afford to address their cyber risks "in-house." As a result, he continued, they've likely already turned to MSSPs for assistance. The broker observed that the question of how to extend the reach of a company's ERM program to its MSSP presents significant difficulties. While other participants responded that ERM is focused "only within a company," an underwriter strongly disagreed. "Good ERM," he stated, "looks at the security and viability of a company's suppliers and vendors." He acknowledged, however, that the extent to which most companies engage in such "good ERM" remains an open question.

  Several participants noted that among those companies that run otherwise effective ERM programs, many continue to silo away cyber risk as an IT problem only – separate and apart from the other business risks they face. A broker commented that she is surprised that more companies that *do* have ERM programs have not incorporated cyber risk within them because, "cyber risk is a board issue." An underwriter replied that, "everyone is intimidated by cyber, so they go straight to their IT departments." A second underwriter observed, however, that any time a company segregates a portion of its risk from its ERM program, that company is no longer "doing ERM." He noted that cyber risk impacts the entirety of a company's structure and organization. Carriers, therefore, need to understand how a company's cyber risk relates to its other risks in terms of priority and risk management investment before they can make a

confident coverage and pricing determination for that company. The underwriter remarked that truncated ERM programs thus create a significant impediment for carriers that might otherwise provide policy premium discounts as a reward to those that manage their cyber risk well.

Factors Supporting the Case for ERM in the Cyber Risk Space

Despite these challenges, the participants discussed a number of factors that over time could support increased adoption of cyber risk-inclusive ERM by companies of all sizes, making it and the related purchase of cybersecurity insurance a standard business practice. They include:

- **Increased awareness of and education about cyber risks.** Multiple participants noted that recent cyber incidents, including the Target data breach in late 2013, have led to both an increased awareness of the present nature of cyber threats and a "humbling" on the part of many companies about their already compromised security postures. Once companies recognize their genuine vulnerability to cyber threats, they stated, they tend to be more open to adopting ERM approaches and exploring their cybersecurity insurance options. An underwriter observed that over the last five to 10 years, he has witnessed a gradual trend line of companies integrating cyber risk into their ERM programs – a phenomenon he described as increasingly evident, particularly among critical infrastructure owners, in the wake of the Target breach. A broker noted that CISOs likewise have become more accepting of cybersecurity insurance as a potential risk management tool because of growing uncertainty about the strength of their organizations' defenses. She cited this development as an advance and commented that the majority of CISOs previously considered the purchase of a policy as tantamount to an admission of failure on their part. Several other participants stated that, given these developments, they planned to use the Target breach and similar future incidents to make the case for ERM adoption to potential insureds.

  A reinsurer noted that insurance industry efforts to promote ERM as a best practice have been ongoing for at least the last four years. After direct and sustained engagement with various industry groups during that period, she stated, these efforts have begun to yield good results. She added that expanding these discussions to more thoroughly include cyber risk within the ERM paradigm will likely follow a similar trajectory. Specifically, she explained that she expected to see a similar multi-year "push" during which underwriters would continue to promote cybersecurity insurance products as part of an effective ERM program and brokers would continue to raise awareness within the critical infrastructure community about their value. The reinsurer nevertheless asserted that while these steps will help, "people have to be scared before they will buy insurance." In other words, she concluded, people have to see incidents happening to them, businesses similar to them, and/or their vendors and suppliers before they will be incentivized to act.

  Other participants cautioned that while carriers communicate effectively with some critical infrastructure owners about ERM and cybersecurity insurance, those owners represent only a

small subset of all critical infrastructure owners. They emphasized that significant education efforts are necessary to reach the many companies that lack even a basic understanding of what cybersecurity insurance is and how it is obtained. Several participants observed, however, that the insurance industry should not limit this education just to larger populations of critical infrastructure owners concerned about their cyber risk mitigation and transfer needs. On the contrary, they continued, carriers also should educate third-party vendors, specifically IT and cybersecurity service providers, about how they fall within a particular owner's ERM "tent" and why they need to be part of that owner's ERM conversations, including its conversations about cybersecurity insurance.

- **Regulatory regimes that include ERM.** Multiple participants noted the potential importance of the existing regulatory environment in driving ERM adoption by specific companies.

    - An underwriter asserted that if carriers offered economic incentives for companies to take up ERM, mid-size and small companies might do so. He noted, however, that current regulatory requirements that govern the provision of policy premium discounts might prevent carriers from taking this approach. A reinsurer responded that future regulation nevertheless may prove to be a more successful driver of ERM adoption for critical infrastructure owners than any market pressure from carriers – so long as regulation allows entities to demonstrate compliance through their ERM usage. A broker suggested that the U.S. Securities and Exchange Commission (SEC), for example, could play a role in encouraging public and "about to be public" companies to adopt ERM.

    - A second broker agreed, asserting that the magnitude of cyber risk is so great that a balance sheet equivalent for cyber risk/cyber posture might emerge in the years ahead. He explained that – similar to the Basel Accords standards for banks – there could come a point when the SEC will require companies to quantify and reserve amounts on their balance sheets to cover the public's risk from the cyber risks they face.[26] The broker added that this could create enough market incentive to drive adoption of ERM for cyber risk purposes.

    - An underwriter stated that existing regulations already are having that effect in the Healthcare and Public Health Sector. He cited as an example the ways in which the Health Insurance Portability and Accountability Act (HIPAA),[27] administered by the Department of Health and Human Services (HHS), has impacted both leadership decisions and third-party vendor offerings in ways that improve cyber risk profiles for many health care organizations.[28]

---

[26] *See*, *e.g.*, Wikipedia contributors, "Basel II," *Wikipedia, The Free Encyclopedia*, http://en.wikipedia.org/wiki/Basel_II, accessed May 28, 2014 ("Basel II, initially published in 2004, was intended to create an international standard for banking regulators to control how much capital banks need to put aside to guard against the types of financial and operational risks banks (and the whole economy) face.").

[27] The Health Insurance Portability and Accountability Act of 1996 (Pub.L. 104-191; 110 Stat. 1936).

[28] For an in-depth discussion of HIPAA and its impact on the cybersecurity of the Healthcare and Public Health Sector, *see* Office of the Under Secretary, *November 2013 Cybersecurity Insurance Event Readout Report,* Washington, D.C.: U.S.

- **Development and refinement of an ERM standard.** An underwriter cited the lack of a common, consistently applied ERM "standard" that prescribes baseline ERM approaches as a major challenge to more widespread ERM adoption – whether mandated by regulation or not. A broker agreed and described the role that the Federal government could play in helping to develop and refine such a standard. Building on the prior discussion, she asserted that the SEC could play a large role on this front by integrating more mature ERM-related best practices into existing regulatory regimes for public companies. While such an approach would only affect those companies already subject to SEC regulation, she added, it could represent an effective starting point for assessing available ERM approaches and processes, identifying the most effective options among them, and encouraging their use more broadly. A second broker agreed, adding that, in the event of a significant cyber incident, downstream impacts are inevitable and may involve potentially great losses to multiple critical infrastructure and other entities. Requiring public companies to purchase cybersecurity insurance policies that, in turn, require adherence to an emerging ERM standard, he continued, would likely help reduce the full magnitude of those losses. The broker concluded that doing so would likely incentivize similarly situated companies to adopt an ERM standard as well.

The Limits of "ERM-Lite"

- Several participants stated that the challenges associated with promoting the concept of ERM to mid-size and small companies frequently reflect reluctance by those companies to engage with programs that they believe require significant expertise, resources, and time for successful implementation. ERM often falls into this category, they noted, because it calls for at least some technical sophistication by implementers as well as a dedicated funding stream. An underwriter suggested that, under the circumstances, some kind of scaled-down version of ERM – a so-called "ERM-lite" approach – may need to be developed in order to reach these important economic players. While a second underwriter suggested that the U.S. Small Business Administration (SBA) might be a good advocate for an ERM-lite approach, other participants responded that the free market would be a better driver of its adoption. Still other participants countered that it is difficult to imagine how an ERM-lite program would operate in practice. They underscored the following challenges:

    - **Difficulties in segmenting ERM approaches.** A broker reiterated the point that a company that excludes the cyber risk "segment" from an otherwise comprehensive ERM program is no longer "doing ERM." A partial ERM program, he observed, leads to only a partial understanding of a company's total risk environment. The broker concluded that, for similar reasons, it would be very difficult to identify a subset of ERM activities for implementation as an ERM-lite program without compromising the underlying value proposition of ERM itself. Other participants added that an ERM-lite program likewise would fail to directly

---

Department of Homeland Security, National Protection and Programs Directorate, February 2014, http://www.dhs.gov/publication/cybersecurity-insurance (June 5, 2014).

address a fundamental challenge that exists for full ERM programs. They asserted that for any ERM effort to be successful, companies need to prioritize it above other funding priorities. Simply reducing the scope of current ERM approaches, they stated, will not change this requirement.

- **Insufficiency of a checklist approach to ERM.** A second broker commented that while ERM programs have generally proven effective for companies that adopt them, merely instituting an ERM program is no guarantee of improved cyber or other risk management. He explained that companies that implement effective ERM programs generally have the resources to follow through on the company-specific conclusions that they provide, empowering them to buy down risk across their specific enterprises. The broker commented that requiring a company to just "check the box" by adopting a generic ERM program – whether of the full or "lite" variety – as a condition for insurance coverage might not actually improve its risk management results. He concluded that a company instead must tailor its ERM program to its unique cyber and other risk circumstances and allocate risk management investments to the areas of greatest need in order to have greatest effect.

- To demonstrate this point, multiple participants referenced the Cybersecurity Framework as an example of a meaningful framework that highlights specific actions that companies can take to reduce their cyber risk.[29] They noted, however, that voluntary use of the Framework must be accompanied by specific, ongoing actions that apply its principles to a specific company's specific business processes. Absent this individualized application – *and measurement of results* – so-called "use" of the Framework loses much of its implied meaning for both insurance and other risk management purposes. A company's use of a full or ERM-lite program, they continued, must similarly transcend compliance considerations and directly address not only its implementation of specific security programs but also what mitigation impacts those programs produce.

- **Inability of the insurance market to provide ERM solutions.** An underwriter specifically noted that existing regulatory impediments directly restrict the insurance industry from offering ERM services as part of their market offerings to clients. He stated that this inability could present yet another barrier to ERM adoption by many companies.

Final ERM Remarks

- A broker commented that, beyond the regulatory sphere, the Federal government may be in the best position to drive awareness and education about cyber risk and, by extension, ERM. An underwriter agreed and stated that the Federal government could be especially helpful on two fronts: (1) by developing a ubiquitously recognized "Smokey the Bear" equivalent for cyber risk

[29] *See* Cybersecurity Framework, *supra* note 3.

that could be used in public education campaigns;[30] and (2) by creating a rating or symbol that publicizes the cybersecurity level of organizations. Several other participants asserted that greater public awareness about cyber risk – perhaps through these and other initiatives – will naturally feed a greater public appetite for ERM.

- A Federal government representative responded by describing the variety of awareness and education initiatives that DHS has undertaken to engage both citizens and the private and public sectors about cyber risks and options available for addressing them. Among other things, she described DHS' support for National Cybersecurity Awareness Month,[31] the Stop. Think. Connect. campaign,[32] and the many briefings and presentations that DHS provides on this topic to critical infrastructure leaders and other stakeholders. Many participants expressed interest in participating in these efforts in the future – not only for their own awareness and education, but also to inform their ongoing evangelization of ERM as a tool for effective cyber risk management.

[30] The Federal Government introduced Smokey Bear, also known as Smokey the Bear, through the Ad Council in August 1944 as part of a marketing campaign to encourage people to be more vigilant in the protection of forests. Meg James. "Smokey Bear, Nearly 70, Gets a Millennial Makeover," *Los Angeles Times*, 13 May 2014, http://www.latimes.com/entertainment/envelope/cotown/la-et-ct-smokey-bear-campaign-20140513-story.html (12 June 2014). Federal officials had been concerned that World War II enemies might try to set fire to U.S. forests to destroy wood, an important natural resource needed to support the war effort. *Id*. Smokey Bear became a ubiquitously recognized symbol among children and adults alike about the importance of suppressing activities that lead to forest fires and – in recent years – wildfires. *Id*. Accordingly, the underwriter here essentially suggested that a similar ubiquitously recognized symbol representing the need for safe practices online and suppressing activities that increase vulnerability online is important for public communications about cyber risks.

[31] From the U.S. Department of Homeland Security Web site, *National Cyber Security Awareness Month*, http://www.dhs.gov/national-cyber-security-awareness-month, accessed May 30, 2014.

[32] From the U.S. Department of Homeland Security Web site, *Stop. Think. Connect.*, http://www.dhs.gov/stopthinkconnect, accessed May 30, 2014.

CONCLUSION

At the close of the working session, the participants provided final thoughts summarizing their perspectives and big-picture takeaways on all three potential progress areas. They expressed strong support for continuing the conversation, particularly on the data-centered agenda items.

Regarding a cyber incident data repository, a broker, two underwriters, and a reinsurer suggested that actuaries should be invited to future sessions to explain how repository data could be used to develop new and enhance existing cybersecurity insurance products. They likewise advised that CISOs and other IT professionals, other corporate risk managers, industry associations, mid-size and small companies, law enforcement agencies, and software developers should be similarly engaged on their cyber risk information needs and how a repository could help meet them. Two brokers and two underwriters stated that such repository discussions should focus on: (1) developing a clear definition of "cyber incidents" that sets appropriate thresholds for nomination and inclusion; (2) designing a cyber incident data template that captures core characteristics of those incidents; (3) generating anonymization protocols to ensure that shared cyber incidents cannot be traced back to their originating sources; (4) identifying processes and procedures that help ensure a rigorous, quality effort that informs both risk mitigation and risk transfer professionals; and (5) formulating messages to different audiences (e.g., CISOs) not only to incentivize their repository participation but also to maximize their data contributions.

Three underwriters noted that more work must be done to enable a more complete understanding of the evolving nature of cyber risk exposure, including cyber-related systemic risk. They asserted that scenario-based risk modeling provides a significant value proposition for better understanding that risk. Informed by the "right" data, they explained, such modeling will help carriers establish, at a pre-competitive stage, the kind of foundational analytics they collectively need to develop a more methodological view about how cyber incidents might materialize, what consequences they probably will have, and what risk controls will probably best mitigate or prevent them. They added that a cyber incident data repository could be a major source of information for this work and accordingly should be designed with an eye toward supporting it.

A broker and a reinsurer emphasized that further promotion of ERM is an important activity for critical infrastructure and other supply chain companies. They stated that, rather than an ERM-lite approach, a tool that provides a step-by-step understanding of how to incorporate and implement ERM in full could be of significant value to mid-size and small companies. Such a tool, they advised, must be able to demonstrate how ERM can help make the business case for cybersecurity investments that help restore downed systems more quickly after a significant cyber incident. An underwriter and a second reinsurer responded that third-party vendors often are mid-size and small businesses and that more attention should be paid to what holds them back from enhancing their own cybersecurity postures and engaging the cybersecurity insurance market to address their own residual cyber risk. Whether through ERM or public awareness efforts more generally, they and other participants encouraged government and industry to collaborate on ways to educate companies and consumers alike about cyber risk, its potential impacts, and the actions they can take to address them.

APPENDIX: FULL AGENDA

Insurance Industry Working Session
"Insurance for Cyber-Related Critical Infrastructure Loss: Key Issues"

Monday, April 7, 2014

Eisenhower Executive Office Building (EEOB)
1650 Pennsylvania Avenue, N.W., Room 474
(Entrance at 17th Street, N.W. and New York Avenue, N.W.)
Washington, D.C.

AGENDA

8:00 – 8:30	Arrival/Registration
8:30 – 8:45	Opening Remarks from DHS/NPPD o *Tom Finan, Senior Cybersecurity Strategist and Counsel*
8:45 – 10:15	TOPIC 1: Cyber Incident Information Sharing (Facilitated Discussion)
10:15 – 10:30	Break
10:30– 12:00	TOPIC 2: Cyber Incident Consequence Analysis (Facilitated Discussion)
12:00 – 1:00	Lunch (Box Lunch On Site – $11)
1:00 – 2:30	TOPIC 3: Cyber Risk and Enterprise Risk Management (Facilitated Discussion)
2:30 – 2:45	Break
2:45 – 3:15	Summary Discussion/Q&A/Close

This page intentionally left blank