CIPR Event Examines Cyber Liability Risk and Issues Facing the Insurance Industry

By Anne Obersteadt, CIPR Senior Researcher

Cyber risk is increasingly cited as a significant emerging threat to businesses. Growth in technology has brought with it a rising number of data breaches and a greater awareness of cyber risk and the need to manage it. In 2013, several well-known retailers, such as Target and Neiman Marcus, were subjected to cyber-attacks. In the wake of these high-profile data breaches, organizations are becoming more aware of their exposure to potential cyber threats. According to Marsh, demand for cyber liability insurance coverage increased 21% from 2012 to 2013.[1] However, cyber risk remains difficult for insurance underwriters to quantify due in large part to a lack of actuarial data. Insurers compensate by relying on qualitative assessments of an applicant's risk management procedures and risk culture. As a result, policies for cyber risk are more customized than other risk insurers take on, and, therefore, more costly. However, despite the challenges to insuring cyber risk, insurers and other stakeholders appear to be moving the market forward through the development of industry risk management standards and other collaborative efforts.

The NAIC Center for Insurance Policy and Research (CIPR) recently held a four-hour event, titled "Insuring Cyber Liability Risk," to bring together various high-level experts to take a closer look into cyber liability risk issues facing the insurance industry. This informative event took place March 28, 2014, at the NAIC Spring National Meeting in Orlando. Close to 200 attendees from a variety of segments—including insurance regulators, industry representatives, consumer advocates, information technology professionals and journalists/reporters from various media outlets—registered for the event. The event was moderated by Mississippi Insurance Commissioner Mike Chaney and included three sessions on the following topics: the cyber risk landscape; cyber liability insurance coverage issues; and federal regulatory initiatives related to managing cyber risk.

◆ The Cyber Risk Landscape

Session one, "The Cyber Risk Landscape," covered operational cyber risks, cybercrime and legal trends related to cyber liability. Speakers for this session included:

- Brian Peretti, acting director, U.S. Department of the Treasury, Office of Critical Infrastructure Protection and Compliance Policy
- Kenn Kern, chief of staff, Investigation Division, New York County District Attorney's Office
- Jeremiah Posedel, associate attorney, Drinker Biddle & Reath LLP

Mr. Peretti began the session by providing an overview of the cyber liability threat landscape and how the Treasury Department's Office of Critical Infrastructure Protection seeks to facilitate threat information-sharing and improve resiliency with the financial sector. He noted that cyber attacks may come from nation states, terrorists, criminals, activists, external opportunists and company insiders (both intentional and unintentional). Cyber criminals attack to gain some type of political, military or economic advantage. They usually steal money or information that can eventually be monetized, such as credit card numbers, health records, personal identification information and tax returns.

Mr. Peretti stated criminals are becoming more sophisticated. For example, cyber criminals are employing several new social engineering tactics. Social engineering is designed to trick victims into offering additional personal information by providing just enough information to appear legitimate. "Spear phishing" emails are one of the recent twists on this technique. In this type of attack, the identity thief targets a specific organization or person using information personal to the victim to appear to be from a trusted source.

Mobile devices were also identified by Mr. Peretti as an emerging risk. Cyber criminals frequently use phishing techniques in social media attacks, such as when a victim unknowingly clicks on a "friend request" which initiates malware. Mr. Peretti said a whole set of malware specific to mobile devices is now being deployed. Additionally, he noted most companies' security systems are not designed for mobile devices, increasing the risk for insider threats in workplaces that permit the use of personal mobile devices. He also emphasized cyber criminals seek to exploit the "weak link" in an organization's supply chain, rather than take it head on. For this reason, financial institutions need to ensure their entire supply chain is secure.

Mr. Kern spoke about the impact of cybercrime on businesses, individuals, and the economy at large from a law enforcement perspective. He said more than 30% of all of the New York County District Attorney Office's felony complaints involve some sort of cybercrime or identity theft. From a prosecutorial law enforcement perspective, the cyber risk landscape encompasses four key threats: 1) distributed denial of service (DDoS) attacks (which are designed to make a machine or network resource unavailable to its intended users); 2) hacking; 3) theft of personal identifying information; and 4) intellectual property theft.

(Continued on page 23)

[1] "Purchase of cyber insurance policies on the rise: Marsh." *Business Insurance*. March 31, 2014.

Mr. Kern told the audience that between 2011 and 2013, there was a significant volume of DDoS attacks on the financial sector. These attacks continue to the present day. Political dissent and ideological "hacktivism" continue to be one driver behind these cyber-attacks.

Intellectual property theft is another salient problem facing the private and public sectors, as well as the academic community. Intellectual property theft often involves the theft of data or source code, often by insiders or employees. Law enforcement has seen insiders leave their firm and then sell stolen data or use it to start their own firm. Mr. Kern said, "These trends indicate employees, while in and outside of the firm's employment, must be considered as both assets and potential threats."

Separately, the theft of personal identifying information (PII) is frequently monetized by selling it online, often on the "deep Web." Mr. Kern explained that the deep Web uses a series of encryptions to preserve seller and buyer anonymity.

Mr. Posedel provided an overview of how security and privacy are regulated in the U.S., and the potential liability an organization faces when cyber attacks and other breaches occur. He explained that many countries take an "omnibus" regulatory approach, meaning privacy and security rules relating to the processing of information in any manner are regulated under one law. However, the U.S. takes a "sectoral" regulatory approach, whereby numerous federal and state privacy laws address specific processing activities, industries, individuals and data types. "For instance," Mr. Posedel explained, "the Health Insurance Portability and Accountability Act (HIPAA) has privacy rules, security rules and breach notification obligations, but it only applies to specific entities covered by HIPAA (namely healthcare professionals, insurance companies, and healthcare exchanges)." Likewise, the federal Gramm-Leach-Bliley Act imposes privacy and security requirements, including recommending implementation of a risk-based breach response program, but applies only to financial institutions, including agents and brokers.

At the state level, a number of state privacy and security statutes add to the regulatory landscape. According to Mr. Posedel, most states require prompt notification be given following a breach, with 47 states requiring entities to send breach notification letters. "In addition," he added, "states can—and do—regulate privacy and security practices through their state unfair and deceptive trade practices acts."

While there has been a push for more overarching legislation in the wake of significant breaches, it is difficult for affected individuals to hold companies liable when breaches occur. Mr. Posedel told the audience that the courts routinely dismiss cases based on lack of actual damages and/or failure to establish causation, both necessary for a plaintiff to state a claim for relief. As Mr. Posedel explained, "This element of injury—a real tangible harm—is relevant and necessary for both specific causes of action and Article III standing. In a lot of cases, plaintiffs are unable to demonstrate any actual injury and, as a result, their claims are dismissed." He added this is because the expectation of future harm, such as the possibility stolen credit card information could be used to inflict financial damages, does not typically constitute an existing and real harm. Similarly, even where fraudulent credit card charges occur, affected individuals are normally reimbursed by the card-issuing financial institution, thereby eliminating any damages to the individual.

◆ Federal Initiatives Related to Managing Cyber Risk

Session two, "Federal Initiatives Related to Managing Cyber Risk," focused on the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure (Framework). Discussions centered on implementation considerations and the Framework's potential influence on the cyber security insurance market and cyber risk management. Speakers for this session included:

- Adam Sedgewick, senior information technology policy advisor, NIST
- Tom Finan, senior cybersecurity strategist and counsel, U.S. Department of Homeland Security, National Protection and Programs Directorate (NPPD)

The Framework provides a structure of standards, guidelines and practices to aid organizations, regulators and customers with critical infrastructures in effectively managing their cyber risks. On Feb. 13, 2014, NIST, a non-regulatory agency of the U.S. Department of Commerce, released the final draft of the Framework. Mr. Sedgewick said the Framework was the outcome of Executive Order 13636: Improving Critical Infrastructure Cybersecurity, issued by President Barack Obama in February 2013. The executive order asked NIST to work with the industry to identify core cyber security practices applicable to sectors exposed to evolving threats. Mr. Sedgewick said the diversity of critical infrastructures ranged from large multi-national corporations to small regional banks and water utilities. The goal, according

(Continued on page 24)

to Mr. Sedgewick, was to build off standards in use today, thereby allowing the Framework to become a tool for business-to-business relationships.

In developing the Framework, NIST held a number of workshops to gather information from organizations on the challenges they experienced in securing their cyber infrastructure. Through these workshops, NIST found communicating cyber security risk throughout an organization was a major issue. Mr. Sedgewick noted, "It was often difficult [for organizations] to get executive buy-in and to transition the needed changes all the way to the person who needs to implement the solution." Organizations also expressed the need for tools to fuse threat information with business information and for a deeper talent pool. Additionally, they indicated there was a gap in industry-driven conformity programs and a need for models to assist organizations in evaluating and improving their capabilities.

The Framework is composed of three parts: the core; profiles; and implementation tiers. The core simplifies and groups the existing standards, requirements and best practices into five ascending structure levels of identify, detect, protect, respond and recover. "Identify is the most important of the broad categories," Mr. Sedgewick said. "To get started, you need to know what you have to be able to protect it." The profiles are used by organizations to define their existing and targeted set of cyber security standards. Mr. Sedgewick explained organizations can overcome difficulties in communicating threats, both inside and outside the organization, by using the profile tools. He added the implementation tiers provide a set of guidelines to assist organizations in determining how they should manage their cyber security risks in relation to their risk management practices and business needs.

Mr. Sedgewick stressed the Framework was designed to be a flexible tool for diverse industries and stakeholders to be able to use in improving their cyber security and privacy practices. Its structure is intended to complement, rather than replace, the various regulatory and business requirements employed today. "Now that we are done," he stated, "it is important the industry picks up [the Framework] and uses it. This will be the true measure of our success." Mr. Finan told the audience NPPD, which is responsible for helping federal civilian agencies protect themselves against cyber attacks, hopes engaging the insurance industry will lead to the implementation of cyber security underwriting practices designed to promote greater adoption of the Framework. In 2012, NPPD began identifying a series of challenges to first- and third-party cyber security markets. As Mr. Finan, who leads NPDD's efforts in this area, stated, "What piqued our interest was [the insurance industry's] potential to promote better cyber security. What we discovered was the market may in fact get us there, but we are not there quite yet."

According to Mr. Finan, a sizable and growing amount of actuarial data on data breaches has led to a functional third-party cyber security insurance market. This coverage covers various costs associated with a data breach, such as credit monitoring for impacted parties, cyber forensics and notification costs. However, Mr. Finan indicated the first party market, which covers an organization's own damages from things such as loss of profits, reputation and intellectual damages, is nascent due to a lack of actuarial data. "Perhaps, and unsurprisingly, companies are not publicly disclosing their own damages from cyber events they themselves are experiencing," he stated. "Consequently, there is just not enough actuarial data to lay the foundations for a robust first party market."

To compensate for this lack of actuarial data, insurers told NPPD they examine a potential insured's risk culture alone, or in addition to, their technical compliance with available standards when accessing qualifications for coverage. In so doing, they pay particular attention to the cyber security practices and procedures the organization has adopted, implemented and enforced. Oftentimes, this approach results in insurers drafting custom policies for their clients rather than broader template policies. Mr. Finan believes the increasing focus on engaged cyber risk cultures appears to be an emerging underwriting trend. This trend appears to be linked to the growing convergence of cyber risks with more traditional risks, resulting from the adoption of enterprise risk management (ERM) strategies.

Mr. Finan said NPPD held a workshop with the insurance industry in September 2013. The workshop aimed to gain insight from insurers on how the Framework could facilitate insurers' ability to incentivize better cyber security management within organizations. In these discussions, Mr. Finan said insurers identified three ways the Framework might help the market. First, the Framework could serve as a risk-management tool insurers could use immediately to access the current state of a potential insured's cyber security. Secondly, the Framework could increase capacity by incentivizing carriers to direct and simplify their discussions about developing new kinds of business interruption policies. "If cyber-related business interruption becomes more commonplace," Mr. Finan explained, "the current distinction

(Continued on page 25)

between physically caused physical loss and cyber-caused physical loss will likely become untenable." Third, the Framework might have a positive impact on policy pricing by improving an insured's ability to demonstrate a good cyber risk profile. Mr. Finan concluded by stating the NPPD's next workshop will focus on how to advance the first-party market. NPPD's proposed solutions center on improved cyber incident information-sharing, cyber risk consequence analytics and incorporating cyber risk into traditional ERM programs.

◆ Cyber Liability Insurance Coverage, Barriers and Pricing

Session three, "Cyber Liability Insurance Coverage, Barriers and Pricing," featured discussions on cyber coverage provided by traditional insurance and cyber-specific policies, underwriting and risk-management considerations for cyber risk policies, cyber insurance barriers and pricing considerations. Speakers for this session included:

- Robert Parisi, Jr., managing director and national technology, network risk and telecommunications practice leader, Financial and Professional Liability Practice (FINPRO) unit, Marsh USA
- John Coletti, vice president and underwriting manager, XL Group
- Dr. Lance Hoffman, director, The Cyber Security and Policy Research Institute, The George Washington University

Mr. Parisi explained insurers view cyber and privacy risks as a broad risk encompassing most organizations. Insurers, he added, view cyber events as a financial risk, coming from two basic places. The first is risk stemming from the collection or handling of information. The second is an organization's reliance on the use of technology in its business operations. "Generally," noted Mr. Parisi, "you'd be hard-pressed to find a company that doesn't qualify under at least one of these categories."

Mr. Coletti stated cyber policies have evolved from primarily covering online activity to including first- and third-party components. "The community," he added, "is innovative and constantly coming up with new ways to attack the exposure." In recent years, first-party business interruption coverage has expanded to cover not just damages triggered by a cyber attack, but those resulting from a network downfall (whether a breach or an internally caused network error). Mr. Parisi noted that coverage from a technology outage is an issue rarely highlighted publicly. "What we've seen over the last several years," he explained, "is that disruptions to a company's supply chain—the logistics behind a company's operation—is more likely to be due to a technology outage than adverse weather." Technology outages are not only more frequent than adverse weather, they are more severe, he added.

Mr. Coletti said dependent business interruption coverage is another recent addition. Organizations purchase this coverage for their critical activities performed, stored or accessed from the cloud. He added organizations commonly purchase coverage for data breach response and crisis management to pay for breach-related costs, internet technology forensics, credit monitoring, attorney fees and call center operating costs. "The reason for this," Mr. Coletti explained, "is it's the one cost everyone can rationalize and say, OK, that happened to my business." Insurers provide coverage on either a dollar-limit basis, a per-person basis or they cover costs on a certain number of records breached. Other typical coverages, he added, include costs incurred in restoring data damaged or lost from a computer virus and data extortion threats.

Mr. Parisi said privacy has also received a lot of public focus, as this risk impacts any organization handling data, regardless of their use of technology. He explained privacy coverage is different from network coverage provided under a traditional cyber liability policy in how it is triggered. Network coverage is triggered by a technology-related event and provides liability coverage for related damages. Privacy coverage is triggered by unauthorized disclosure, unauthorized access or wrongful collection of confidential information. Mr. Parisi further added, "The privacy coverage strips out the requirement there be any technological aspect to it. It doesn't have to be electronic data. It could be a three -ring binder with everyone's Social Security number in it."

Mr. Coletti said he has seen an increase in demand for cyber and privacy insurance in response to recent high-profile cyber breaches. He added, "We are seeing a huge increase in cyber purchases since the Target and subsequent breaches. Those industries are looking not only to buy limits for the first time, but to increase any current limits they already have." Regulated industries, such as financial institutions, healthcare providers, retailers and universities, are the traditional buyers of cyber liability policies. But, Mr. Coletti noted, this is changing, as he is seeing increased applications from nontraditional purchasers such as professional service firms, manufacturing firms and hospitality companies. "These companies are now recognizing the need for notification coverage provided only by cyber liability policies," he explained.

(Continued on page 26)

Mr. Coletti stated insurers do not know how to price cyber liability policies. Instead, he said, "It's a market-driven price historically based on error and omissions rates from the 1990s." Insurers are trying to build databases for solid actuarial algorithms. However, Mr. Coletti believes these databases are not complete enough to ensure accurate pricing. He also expressed concern, as an underwriter, over aggregation risk. "If you're in the situation where you are insuring multiple insureds that were breached by the same vendor," he explained, "you could have an aggregation exposure."

Dr. Hoffman shared the results of a recent Cyber Security Policy and Research Institute (CSPRI) commissioned report, "Insurance for Cyber Attacks: The Issue of Setting Premiums in Context." The report was authored by Costis Toregas and Nicolas Zahn and released in January 2014. Dr. Hoffman said the report outlines market barriers to cyber liability insurance and presented dialogue highlights with various market actors. It also suggested a collaborative research agenda designed to improve information security metrics and risk management in an expanded internet framework. Dr. Hoffman believes the report underscores the high cost of breaches, "with more than 17 million personal records breached in 2012, resulting in an average financial impact of $10 million."

As an outcome of its review of prior studies, the report identified several challenges specific to the cyber liability insurance market. In terms of the legal framework, there is uncertainty surrounding liability exposure, coverage gaps and insurance exclusions. Additionally, insurers face conceptual issues, such as knowing how to identify correlated, interrelated and global cyber risks. Additionally, the report indicated insurers struggle with how to quantify cyber-related risks and costs and how to integrate related decision-making beyond the information technology silo. Dr. Hoffman said the report found setting premiums was particularly challenging to insurers, given the lack of normative standards, reinsurance and actuarial data.

Dr. Hoffman discussed CSPRI's desire to collaborate with stakeholders to improve the viability of the cyber insurance market. He suggested a multi-disciplinary workshop—with participants from the insurance, academia, government and legal communities—could easily be used to identify points of consensus and disagreement. This type of research and cooperation between stakeholders, he said, could advance cyber liability insurance standards for premium rate setting. Dr. Hoffman stressed standards will become particularly important as technology continues to be integrated into everyday devices. He pointed out, "Industry can set standards, but if they don't, the technological firms are going to build their own devices with little or no privacy and security built in." For this reason, he continued, it is important for approaches to be developed before a solution is imposed that may be wrong or under-researched.

◆ SUMMARY

The CIPR event illustrated privacy and cyber breaches threaten all organizations. It also demonstrated, while organizations have made great progress in mitigating their cyber and privacy exposures, the risk is still not fully understood. Many organizations find it difficult to move cyber risk discussions beyond their IT department, inhibiting their ability to instill an organization-wide cyber risk culture. However, recent concerns about regulatory compliance standards have helped to push these conversations into the boardroom. Moreover, the proliferation of connected devices—such as cameras, cell phones, digitized equipment—will create new channels for cyber threats. As such, stakeholders must become more proactive in establishing cyber and information security practices and standards. Likewise, insurers must continue to evolve if they are to provide effective risk-transfer solutions specific to the emerging threats industries face. Additional information on this CIPR event, including the agenda, presentations and audio, can be found on the CIPR website at http://cipr.naic.org.

ABOUT THE AUTHOR

Anne Obersteadt is a researcher with the NAIC's Center for Insurance Policy and Research (CIPR). She has 14 years of experience with the NAIC performing financial, statistical and research analysis on all insurance sectors. In her current role, she has authored several articles for the CIPR Newsletter, a CIPR Study on the State of the Life Insurance Industry, organized forums on insurance related issues, and provided support for NAIC working groups. Before joining CIPR, she worked in other NAIC Departments where she published statistical reports, provided insurance guidance and statistical data for external parties, analyzed insurer financial filings for solvency issues, and authored commentaries on the financial performance of the life and property/casualty insurance sectors. Prior to the NAIC, she worked as a commercial loan officer at U.S. Bank. Ms. Obersteadt has a bachelor's degree in business administration and an MBA in finance.

National Association of Insurance Commissioners
& The Center for Insurance Policy and Research

NAIC Central Office
Center for Insurance Policy and Research
1100 Walnut Street, Suite 1500
Kansas City, MO 64106-2197
Phone: 816-842-3600
Fax: 816-783-8175

http://www.naic.org http://cipr.naic.org

To subscribe to the CIPR mailing list, please email CIPRNEWS@NAIC.org or SHALL@NAIC.ORG

The National Association of Insurance Commissioners (NAIC) is the U.S. standard-setting and regulatory support organization created and governed by the chief insurance regulators from the 50 states, the District of Columbia and five U.S. territories. Through the NAIC, state insurance regulators establish standards and best practices, conduct peer review, and coordinate their regulatory oversight. NAIC staff supports these efforts and represents the collective views of state regulators domestically and internationally. NAIC members, together with the central resources of the NAIC, form the national system of state-based insurance regulation in the U.S. For more information, visit www.naic.org.