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

Recent Regulatory Initiatives to Tackle the Growing Threat of Cyber Risk

By Shanique (Nikki) Hall, CIPR Manager and Sara Robben, NAIC Statistical Advisor

"There are only two types of companies: those that have been hacked and those that will be."
–Robert S. Mueller III, former FBI Director

◆ Introduction

The threat of a cyberattack is widely regarded as one of the greatest emerging risks for businesses, consumers and the financial system at large. Earlier this year, Mary Jo White, U.S. Securities and Exchange Commission (SEC) chairman, said cyberattacks represent the "biggest systemic risk" facing the U.S.[1] The list of cyberattack victims is long and includes household names such as Sony, Home Depot, Microsoft and Target, as well as the CIA and the U.S. military. The cyber threat landscape is evolving quickly. New exploits frequently emerge and are accelerated by the proliferation of smartphones, tablets, and most recently the "Internet of Things[2]."

Every business, regardless of size, is subject to cybersecurity risk. U.S. businesses suffered 43 million known security incidents in 2014, a 48% increase compared with 2013 and equaling some 117,000 attacks daily.[3] The increasing frequency, cost and sophistication of cyberattacks, combined with business structures that are ever more reliant on technology, has augmented demand for cyber insurance. While the insurance industry is fast becoming a source of risk transfer in this space, insurers have also become victims of cyberattacks. Insurers maintain unique and sensitive personal information—including medical and financial information—about individual insureds and claimants, which makes them more vulnerable to a cyberattack. This year is referred to as the "year of the health insurer data breaches." A number of high-profile data breaches at several health insurance providers, including Anthem Inc. and Premera Blue Cross, exposed data on more than 90 million customers, and placed an increased focus on cybersecurity as it relates to insurers.

As the cyberattacks against health insurers were announced, state insurance regulators began working with the breached companies, the FBI, and the cybersecurity firms they retained to evaluate the attacks. Insurance regulators held daily discussions with company executives to ensure appropriate steps were taken to protect the data that may have been compromised. The companies then repaired their systems to help prevent future attacks.

Cybersecurity issues are also being addressed through the NAIC Cybersecurity (EX) Task Force. The NAIC formed the Task Force in late 2014 to centralize state insurance regulatory activities related to cybersecurity. The Task Force had a fairly aggressive work plan this year, which involved coordinating with various NAIC groups on specific aspects of cybersecurity. In April, the NAIC published *Principles for Effective Cybersecurity: Insurance Regulatory Guidance*, which provides best practices for insurance regulators and companies, focusing on the protection of the sector's infrastructure and data from cyberattacks. The Task Force also developed the Cybersecurity and Identify Theft Coverage Supplement for insurer financial statements to gather financial performance information about insurers writing cyber-liability coverage nationwide. Moreover, in October, the Task Force adopted the *Cybersecurity Bill of Rights*[4], and the NAIC updated its *Financial Condition Examiners Handbook* and will be updating the *Market Regulation Handbook*.

The IT Examination (E) Working Group enhanced the guidelines, processes and procedures regarding cybersecurity risks in the *Financial Condition Examiners Handbook*, which is actively used by insurance regulators as they examine companies. The guidance included principles from the National Institute of Standards and Technology (NIST) Cybersecurity Framework, as well as strengthens the existing guidance. The Working Group updated the narrative guidance, as well as Exhibit C, which is the work program for the general information technology review of controls. The Working Group finalized its work in September and it will be included in the 2016 publication.

State insurance regulators also continue to work collaboratively with other financial regulators, Congress and the Obama Administration to identify specific threats and develop strategies to protect the financial infrastructure of the U.S. insurance commissioners, state insurance regulators and NAIC staff are active members of the Treasury Department's Financial Banking and Information Infrastructure Committee (FBIIC)[5], as

(Continued on page 3)

[1] Ackerman, Andrew. *"Cyberattacks Represent Top Risk, SEC Chief Says."* Wall Street Journal. May 8, 2015.
[2] The Internet of Things extends internet connectivity beyond traditional devices like desktop and laptop computers, smartphones and tablets to a diverse range of devices and everyday things that utilize embedded technology to communicate and interact with the external environment, all via the Internet (webopedia).
[3] Are Your CEO and Board Ready? AT&T'S Cybersecurity Insights Report Helps Executives Prepare for Cyberattacks. October 2015.
[4] The Cybersecurity Bill of Rights was adopted by the Task Force in October 2015. It was recently renamed the NAIC Roadmap for Cybersecurity Consumer Protections (Roadmap). The Roadmap was adopted by the NAIC Executive (EX) Committee and Plenary on Dec. 17, 2015.
[5] The FBIIC is chartered under President Barack Obama's Working Group on Financial Markets and is charged with improving coordination and communication among financial regulators, enhancing the reliability of the U.S. financial system.

well as the White House's Regulatory Cybersecurity Forum for Independent and Executive Branch Regulators.

The Cybersecurity (EX) Task Force follows the activities of information-sharing and analysis centers, such as Financial Services—Information Sharing & Analysis Center (FS-ISAC), HITRUST, the National Health ISAC, and the U.S. Department of Treasury. Information-sharing and analysis centers provide information regarding threats and vulnerabilities for specific sectors, such as banks, securities, and insurance. Their missions are to enhance the ability of the banking, securities, and insurance sectors to prepare for and respond to cyber threats and physical threats, vulnerabilities and incidents, and to serve as the primary communications channel for the sector. The goal regarding the information-sharing efforts of the Treasury Department is to get the best information possible tied to cyber threats and vulnerabilities in the hands of network defenders as quickly as possible. One of their key efforts is to ensure that government is able to get the most beneficial information out to the private sector that it has available.

This article is an update to a previous CIPR Newsletter article published earlier this year titled, *Cybersecurity Takes Center Stage*.[6] It will discuss the current cyber liability insurance landscape, and detail recent state insurance regulatory efforts to combat the growing threat of cyber risk.

◆ CYBER-LIABILITY INSURANCE MARKET

The evolving threat of cyberattacks is persistent and continues to rise across all industries. According to a recent Moody's Investors Services (Moody's) report, industries which house significant amounts of personal data—such as financial institutions, health care entities, higher education organizations and retail companies—are at greatest risk to experience large-scale data theft attacks resulting in serious reputational and financial damage.[7] In the same report, Moody's notes it will begin placing more weight on considerations related to cyber risk when issuing credit ratings, underscoring the importance that companies should begin to view cybersecurity in financial terms. Standard & Poor's (S&P) has also noted it would downgrade credit ratings of financial institutions that have poor cybersecurity protections.[8]

With cyberattacks creating increasing financial and liability risks for U.S. business and consumers, demand for insurance covering cyberattacks is mounting. However, insurance specific to cyber risk remains a relatively new product; although the market is expected to grow dramatically in the coming years. Many are calling cyber-risk coverage one of the fastest-growing insurance products today. According to Lloyds estimates, the cyber insurance market more than doubled in 2014 to $2.5 billion from less than $1 billion in 2012.[9] Some estimate that the cyber insurance market will more than triple to approximately $10 billion by 2020.[10]

The cyber insurance market is rapidly growing as a separate type of insurance. Most traditional commercial insurance policies do not cover cyber risks. Currently, most carriers either sell a standalone policy, or both a standalone policy and an endorsement. Very few carriers offer endorsements only. The majority of endorsements are provided in conjunction with Errors & Omissions coverage.

Generally, cyber liability policies cover a business' obligation to protect the personal data of its customers. The data may include personally identifiable information, financial or health information, and/or other critical data that, if compromised, might create a liability exposure for the business. The policy will cover liability for unauthorized access, theft or use of the data or software contained in a business' network or systems. Many policies also cover unintentional acts, errors, omission or mistakes by employees; unintentional spreading of a virus or malware; computer thefts; or extortion attempts by hackers.

It is important to recognize that cybersecurity policies, as well as businesses differ. Each cyber insurance policy is unique and highly customizable to fit the needs of a business. A business needs to understand the cyber risks it faces to ensure its policy is tailored its risks.

There are two types of cybersecurity coverage sold in the U.S. cyber insurance market today, namely: 1) first-party coverage; and 2) third-party defense and liability coverage. First-party coverage may include forensic investigation of a data breach; legal advice to determine a company's notification and regulatory obligations; notification costs of com-

(Continued on page 4)

[6] The article, published in May 2015, is available on the CIPR website at: www.naic.org/cipr_newsletter_archive/vol15_cybersecurity.pdf.

[7] "Moody's: Threat of cyber risk is of growing importance to credit analysis." Nov. 23, 2015. Retrieved from: https://www.moodys.com/research/Moodys-Threat-of-cyber-risk-is-of-growing-importance-to--PR_339656.

[8] "Looking Before They Leap: U.S. Insurers Dip Their Toes in the Cyber-Risk Pool." Standard and Poor's. June 9, 2015.

[9] "More Small and Mid-Sized Companies Buying Cyber Insurance." Insurance Information Institute. August 13, 2015. Retrieved from: www.iii.org/insuranceindustryblog/?paged=4.

[10] Advisen Research: " Cyber insurance market to reach $10B by 2020." July 2015. Retrieved from: www.advisenltd.com/2015/07/30/abi-research-cyber-insurance-market-to-reach-10b-by-2020/.

municating the breach; offering credit monitoring to customers as a result; public relations expenses; and loss of profits and extra expense during the time that a company's computer network is down, also known as business interruption.

Third-party coverage may include legal defense; payment for settlements, damages and judgements related to a breach; liability to banks for re-issuing credit cards; cost of responding to regulatory inquiries; and regulatory fines and penalties, including Payment Card Industry fines.[11] Additionally some insurers are starting to offer value added tools and consultation services to help a business continue operating in the event of a security breach by evaluating the extent of the problem, restoring a company's reputation, and preventing future data breaches.

While the market for cyber insurance is expected to grow dramatically in the coming years, U.S. businesses are still saying it is challenging to secure the coverage they need. Although more U.S. insurers are testing the waters, insurers have thus far been cautious to take on cyber risk due to the absence of sufficient actuarial data to price policies and develop probabilistic models. In its report, S&P notes insurers are not jumping into the market with both feet because cyber risk is fast moving, impossible to predict, and difficult to understand and model. Thus, insurers are approaching the market cautiously, offering relatively low limits and a large number of exclusions.[12] Cyber insurance is offered by roughly 50 insurers; however, the market is currently dominated by five writers: American International Group Inc., ACE Ltd., Chubb Corp., Zurich Insurance Co. Ltd., and Beazley Group Ltd.

◆ STATE INSURANCES REGULATORY EFFORTS

State insurance regulators and the NAIC are aggressively monitoring cybersecurity issues in the insurance sector. The NAIC appointed the Cybersecurity (EX) Task Force in late 2014 to monitor developments in the area of cybersecurity and to advise, report and make recommendations to the NAIC Executive (EX) Committee regarding cybersecurity issues. This involves coordination with various NAIC groups on specific aspects of cybersecurity. The Task Force has made substantial progress towards achieving its goals. The following will outline several of the Task Force's major accomplishments to date.

Guiding Principles

The Task Force's first initiative was to develop of a set of guiding principles. Due to ever-increasing cybersecurity risks, it became vital for state insurance regulators to provide effective cybersecurity guidance regarding the regulation of the insurance sector's data security and infrastructure. The insurance industry looks to state insurance regulators to develop uniform standards, to promote accountability across the entire insurance sector and to provide essential threat information. State insurance regulators look to the insurance industry to join forces in identifying risk and offering practical solutions. The guiding principles are intended to establish insurance regulatory guidance that promotes these relationships and protects consumers.

> *"A question we often get asked as financial regulators is: 'What keeps you up at night?' The answer is 'A lot of things.' But right at the top of the list is the cybersecurity at the financial institutions we regulate."*
> –Benjamin Lawsky, former superintendent at the New York State Department of Financial Service (prepared remarks from speech at Columbia Law School, Feb. 25, 2015.)[13]

After extensive comments from the insurance industry and consumer groups, the NAIC adopted the *Principles for Effective Cybersecurity: Insurance Regulatory Guidance* (Guiding Principles) in April 2015. The Guiding Principles consists of 12 primary principles for regulators and industry to follow. The 12 principles are centered on steps the insurance sector can take to help protect it from data breaches. The guiding principles serve as the foundation for protecting consumers' personally identifiable information that is held by insurers as well as insurance producers. They will also guide regulators who oversee the insurance industry.

The 12 Principles for Effective Cybersecurity:

- Principles 1-3 deal with the various obligations to safeguard personally identifiable consumer information.
- Principles 4 and 5 address the need for guidance to be risk-based, practical, scalable and flexible.
- Principle 6 addresses regulatory oversight including examinations.
- Principle 7 addresses the importance of planning for incident response.
- Principle 8 suggests regulated entities need to monitor what vendors and other service providers do to protect sensitive data.
- Principles 9 and 10 address incorporation of cybersecu-

(Continued on page 5)

[11] Floresca, Lauri. "Cyber Insurance 101: The Basics of Cyber Coverage." Retrieved from: www.wsandco.com/about-us/news-and-events/cyber-blog/cyber-basics.
[12] "Looking Before They Leap: U.S. Insurers Dip Their toes in the Cyber-Risk Pool." Standard and Poor's. June 9, 2015.
[13] Ha, Young. "N.Y.'s Lawsky: Cybersecurity Likely Most Important Issue DFS Will Face in 2015." Insurance Journal. February 26, 2015.

rity into enterprise risk management (ERM) and attention by the board of directors.
- Principle 11 stresses the importance of participating in an information-sharing and analysis organization (ISAO).
- Principle 12 discusses the importance of employee training.

The guidance encourages insurers, agencies and producers to secure data and maintain security with nationally recognized efforts such as those represented in the NIST Cybersecurity Framework. The NIST Cybersecurity Framework provides guidance on managing and reducing cybersecurity risk for organizations of all sizes.

Cybersecurity Bill of Rights

The Task Force's second initiative was to develop a Cybersecurity Consumer Bill of Rights (Bill of Rights) for insurance policyholders, beneficiaries and claimants. The Bill of Rights is designed to assist consumers when their personal information is compromised. It covers statutes and regulations regarding security breach notification. The Bill of Rights is intended to provide a roadmap for regulators as they draft model regulation codifying consumer protections related to cybersecurity. It also will eventually be made available for state insurance departments to publish for local consumers once legislation is enacted.

The Task Force released a discussion draft earlier this year and received more than 40 pages of comments on the initial draft. Since issuing the initial draft, the Task Force has worked extensively to develop a Bill of Rights detailing what consumers can expect from their insurance companies following a breach. After extensive review and discussion of the comments received, the Cybersecurity Bill of Rights was adopted by the Task Force on Oct. 14 2015. The Bill of Rights was considered by the NAIC Executive (EX) Committee and Plenary on Dec. 17, 2015. A motion was made to amend the title to the "NAIC Roadmap for Cybersecurity Consumer Protections (Roadmap)." Another motion changed the placement and text of a disclaimer on use of the document. It clarified the "rights" listed in the document may not be currently contained in state law and emphasized the use of the document as a starting point for developing a model law.

The Roadmap, as amended, was unanimously adopted by the NAIC Executive (EX) Committee and Plenary on Dec. 17, 2015.

The Roadmap includes six major expectations for insurance consumers, including the right to:

- Know the types of personal information collected and stored by an insurance company, agent or business they contract with (such as marketers and data warehouses).
- Expect insurance companies/agencies to have a privacy policy posted on their website and available in hard copy explaining: what personal information is collected, what choices consumers have about their data, how consumers can see and change/correct their data if needed, how the data is stored/protected, and what consumers can do if the company/agency does not follow its privacy policy.
- Expect the insurance company, agent or any business they contract with to "take reasonable steps to keep authorized persons from seeing, stealing or using" personal information.
- Receive a notice from the insurance company, agent or any business they contract with if an unauthorized person has (or it seems likely they have) seen, stolen or used personal information. The notice should, among other items: be sent as soon after a data breach, and never more than 60 days after the data breach is discovered; describe the type of information involved in a data breach and the steps that can be taken to protect the consumer from identify theft or fraud; describe the actions taken to keep personal information safe; include contact information for the three nationwide credit bureaus; and include contract information for the company or agent involved in the breach.
- Receive at least one year of identity theft protection paid for by the company or agent involved in a data breach.
- Other rights in the cases of identity theft, such as a 90-day initial fraud alert on credit reports (the first credit bureau contacted will alert the other two) and having fraudulent information related to a data breach removed or blocked from credit reports.[14]

The Roadmap outlines expectations of insurers if and when they experience data breaches or cybersecurity lapses. This is part of the NAIC's effort to strengthen the insurance industry's security posture by building a framework for insurance companies to follow in the event of a cyberattack. Portions of the Roadmap will be incorporated into a model law or regulation to convert the expectations into consumer rights.

(Continued on page 6)

[14] "U.S. National Association of Insurance Commissioners adopts Cybersecurity Bill of Rights." Canadian Underwriter. October 16, 2015.

Cybersecurity Exam Tool – Enhancing Exam Standards

A third initiative the Task Force worked on this year was to enhance examination standards. State insurance regulators are conducting examinations of insurers to check whether companies are doing enough to protect sensitive data and confidential information. Insurer examination protocols have been updated to find out how prepared insurance companies are to handle data breaches. Whenever an examiner conducts a financial exam of an insurance company, there will be a set of best practices to test for security protocols and processes to protect policyholders.

Cybersecurity requirements currently vary from state-to-state; there is no uniform set of cybersecurity practices. As many as 48 states currently have data breach laws that govern how a company must respond in the event of a cyberattack; however, they are not insurance-specific. Many of these state laws provide different definitions of personally identifiable information. A few states provide triggers by access of data and many states require a risk of harm analysis in determining when notification is triggered.

The Task Force worked with the IT Examination (E) Working Group to compare its current examination procedures to the technology standards of the NIST Cybersecurity Framework. Using the identify, prevent, detect, respond and recover approach favored in the NIST standards, the IT Examination (E) Working Group exposed several documents for comment in June 2015.

In September, the Task Force adopted amendments to the IT section of the NAIC *Financial Condition Examiners Handbook* (the Handbook). The Working Group enhanced existing guidance and provided additional guidance for examiners to use when addressing cybersecurity risks. The Working Group also included principles from the NIST Cybersecurity Framework to strengthen the existing guidance. The Working Group updated the narrative guidance, as well as exhibit C, which is the work program for the general information technology review of controls. This guidance is included in the 2016 *Financial Condition Examiner's Handbook*. The NAIC will also be updating the *Market Regulation Handbook.*

Cybersecurity Annual Statement Supplement

In addition, the Task Force worked with the Property and Casualty Insurance (C) Committee to develop a cybersecurity supplement to the annual financial statement filed by property and casualty insurers. The supplement establishes requirements for insurers that provide cyber coverage. It will collect both identity theft insurance and cyber insurance information—including; direct written premium, direct earned premium, paid and incurred losses—as well as adjust and other expenses and direct defense and cost containment information. The supplement additionally collects information regarding the number of claims reported and number of written policies in force. This will allow regulators to monitor growth and claims experience as the insurance industry becomes more comfortable with writing cybersecurity products.

"The threat of a cyberattack is very real, and state regulators are committed to developing the tools we need to ensure effective regulation in this area."
–Adam Hamm, North Dakota insurance commissioner and chair of the NAIC Cybersecurity (EX) Task Force.[15]

This is an important step, as it allows regulators to monitor the development of this relatively new line of business. Regulators will begin receiving information in 2016 to respond to the many questions about the size and performance of the cybersecurity insurance markets. This also enhances regulators solvency surveillance efforts.

◆ CYBERSECURITY SYMPOSIUM

The NAIC also co-sponsored a symposium on Sept. 10, 2015, *Managing Cyber Risk and the Role of Insurance*, with the Center for Strategic and International Studies (CSIS) in Washington, D.C.[16] The forum featured a notable line-up of senior government officials and cyber experts. The aim of the forum was to increase the understanding of the escalating threat environment, emerging best practices in cyber-risk management, and the importance that cyber insurance plays in mitigating cyber risks. Roughly 300 individuals attended the symposium including more than 30 regulators from state insurance departments across the country.

NAIC President and Montana insurance commissioner Monica J. Lindeen gave the opening comments, noting "Ramping up our efforts in this critical area will help state insurance department's better address both the threats and responses

(Continued on page 7)

[15] Tuohy, Cyril. Industry Groups Press NAIC on "Consumer Cybersecurity Bill of Rights." Insurancenewsnet.com. September 3, 2015.

[16] More information on this event, as well as the video recordings, are available on the CSIS website at http://csis.org/event/managing-cyber-risk-and-role-insurance.

to cyber breaches." Sarah Bloom Raskin, deputy secretary of the U.S. Department of the Treasury, gave a keynote address describing the changing nature of cyber risks as society becomes more interconnected and digitalized through social media and the Internet, and as threats become more malicious. Deputy Secretary Raskin also stressed the importance of the insurance sector in developing cyber insurance and noted how the underwriting process itself can bolster the nation's cyber defenses.

There were two panel sessions; 1) a panel on the cyber threat landscape and 2) a second panel on financial sector cyber-risk management. The first panel characterized the cyber landscape as an "aggressively predatory environment." It stressed how cybersecurity should be a "deep and immediate concern" for everyone in business, and that businesses must adopt "intelligent courses of action to mitigate the risks." Concerns were raised about the growing use of social media and the Internet of Things in commerce without the necessary cyber guardrails to protect the integrity of highly sensitive business and personal data.[15]

Suzanne Spaulding, undersecretary for the National Protection and Programs Directorate (NPPD) at the U.S. Department of Homeland Security, delivered the second keynote address. Spaulding noted that taking an ERM approach to fighting cybercrime is critical. She also stressed the need for faster detection, more effective responses and prompt recovery, as well as identified the importance of developing a robust cyber insurance market.

During the second panel, Adam Hamm, North Dakota insurance commissioner and chair of the NAIC Cybersecurity (EX) Task Force, provided an update on steps the NAIC was taking with regard to protecting consumers and industry from network attacks. Hamm identified the major work streams of the Task Force, including its work on revising the NAIC privacy models, and updating financial examination protocols to assess cybersecurity preparedness.

In closing, NAIC CEO Senator Ben Nelson said "State regulators identified the threat to our sector early, and have worked continuously through the NAIC to develop the tools and resources state insurance departments need to protect consumers."

◆ SUMMARY

Cybersecurity is one of the biggest challenges facing businesses today. As cyberattacks become a reality in the business world, U.S. businesses need to assess their risks and take proactive steps to manage them. There is a new and growing market where insurers are offering risk management advice and insurance coverage for a wide-range of cybersecurity risks.

State insurance regulators have a significant role in monitoring insurers efforts to protect the data they receive from policyholders and claimants. State insurance regulators also need to monitor insurers sales of risk management services and risk transfer solutions. This article has summarized some of the efforts by state insurance regulators to proactively address these important regulatory issues.

ABOUT THE AUTHORS

Shanique (Nikki) Hall is the manager of the NAIC Center for Insurance Policy and Research (CIPR). She joined the NAIC in 2000 and currently oversees the CIPR's four primary work streams; 1) the CIPR Newsletter; 2) studies; 3) events; and 4) website. Ms. Hall has extensive capital markets and insurance expertise and has authored copious articles on major insurance regulatory and public policy matters. She began her career at J.P. Morgan Securities as a research analyst in the Global Economic Research Division. At J.P. Morgan, Ms. Hall analyzed regional economic conditions and worked closely with the chief economist to publish research on the principal forces shaping the economy and financial markets. Ms. Hall has a bachelor's degree in economics from Albany State University and an MBA in financial services from St. John's University. She also studied abroad at the London School

Sara Robben is a statistical advisor at the NAIC. She has worked in the Research and Actuarial department for the past eight years. Her current projects include staff support for the Cybersecurity (EX) Task Force, the Catastrophe Response (C) Working Group, the Catastrophe Insurance (C) Working Group, the Transparency and Readability of Consumer Information (C) Working Group and the Affordable Care Act Medical Professional Liability (C) Working Group. Ms. Robben has her Bachelor of Science in mathematics and statistics, and her master's degree in project management. She taught technology courses for DeVry University for 10 years, including computer networking, Web architecture, database administration, and network and operating systems security. Ms. Robben worked for AIG early in her career as a claims adjuster, financial analyst, LAN administrator and technical trainer.

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