National Association of Insurance Commissioners

& The Center for Insurance Policy and Research

CIPR Event:

Cybersecurity Issues, Challenges and Solutions

May 18, 2016
1:00 p.m. – 5:00 p.m.
Kansas City, Missouri

WELCOME MESSAGE

Welcome to the NAIC Center for Insurance Policy and Research (CIPR) Event: *Cybersecurity Issues, Challenges and Solutions.* The mission for the CIPR is to serve federal and state lawmakers, federal and state regulatory agencies, international regulatory agencies, and insurance consumers, by enhancing intergovernmental cooperation and awareness, improving consumer protection and promoting legitimate marketplace competition. To help achieve this mission, the CIPR hosts four annual events that bring together a number of dynamic and informative speakers and panelists. These events offer a forum for opinion and discussion on major insurance regulatory issues.

Recent high-profile data breaches underscore the growing significance of cybersecurity risks. This event will provide an overview of cybersecurity issues and recent insurance regulatory initiatives to address cybersecurity issues, including examination and model law development. Emerging trends and the benefits of engaging in a cybersecurity information sharing group and interacting with federal entities will also be covered.

While you are here, I encourage you to take some time to explore the Crown Center and downtown areas of Kansas City. I hope you enjoy the event and your stay!

Sincerely,

Eric Nordman
Director of CIPR and Regulatory Services

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

Table of Contents

MEET THE CIPR TEAM

Eric Nordman, CPCU, CIE, is the director of the NAIC Regulatory Services Division and the CIPR. He directs the Regulatory Services Division staff in a wide range of insurance research, financial and market regulatory activities, supporting NAIC committees, task forces and working groups. He has been with the NAIC since 1991. Prior to his appointment as director of the Regulatory Services Division, Mr. Nordman was director of the Research Division and, before that, the NAIC senior regulatory specialist. Before joining the NAIC, he was with the Michigan Insurance Bureau for 13 years. Mr. Nordman earned a bachelor's degree in mathematics from Michigan State University. He is a member of the CPCU Society and the Insurance Regulatory Examiners Society.

Kris DeFrain is the NAIC Director of the Research and Actuarial Department. She is currently charged as primary NAIC staff for the Principle-Based Reserving and the Casualty Actuarial and Statistical Task Forces. She manages a staff of actuaries, statistical analysts, insurance contract experts, and research analysts working on regulatory solvency and market-related issues, providing regulatory services, and conducting research for the Center for Insurance Policy and Research. She received her bachelor's degree in finance/ actuarial science from the University of Nebraska in 1989. Ms. DeFrain received her FCAS designation from the Casualty Actuarial Society (CAS), where she previously served as Vice President—International. She is a member of the American Academy of Actuaries and a Chartered Property and Casualty Underwriter.

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 primary work streams, including: the CIPR Newsletter; studies; events; webinars and 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 of Economics.

Anne Obersteadt is a researcher with the NAIC Center for Insurance Policy and Research (CIPR). Since 2000, she has been at 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 for U.S. Bank. Ms. Obersteadt has a bachelor's degree in business administration and an MBA in finance.

Dimitris Karapiperis joined the NAIC in 2001 and he is a researcher with the NAIC Center for Insurance Policy and Research. He has worked for more than 15 years as an economist and analyst in the financial services industry, focusing on economic, financial market and insurance industry trends and developments. He studied economics and finance at Rutgers University and the New School for Social Research, and he developed an extensive research background while working in the public and private sector.

Tiffany Fosgate joined the NAIC in 2012 and is the administrative assistant to the Research and Actuarial department, including the CIPR team. She assists with preparing for CIPR events, organizes speakers' accommodations and prepares CIPR newsletters for print and distribution. She previously worked in the Financial Regulatory Services department before coming to the Research and Actuarial team. Prior to the NAIC, she was employed with UMB at a branch primarily known for its commercial business. She continues her education in insurance regulation while assisting her team with the newsletter and event preparation.

Learning Objectives

At the completion of this program, attendees will be able to:

- **Identify the biggest breaches of the last three years, their common factors and cost reduction techniques**
- **Explain current and future cyber threat vectors**
- **Identify information sharing entities, their function, and collaboration benefits**
- **Explain the coordination role of the Financial and Banking Information Infrastructure Committee (FBIIC) and the Financial Services Sector Coordinating Council (FSSCC)**
- **Explain the potential benefits of the Cybersecurity Information Sharing Act (CISA) and the CIBAR Objective Database**
- **Explain recent insurance regulatory initiatives to address cybersecurity issues**
- **Identify how insurers are responding to the increased need for cyber insurance coverage and which coverages are in highest demand**
- **Identify solvency and financial strength rating concerns cyber-security exposure may pose to an organization**
- **Explain concerns insurance regulators have with pricing, policy forms and data collection efforts**

This is a NAIC Insurance Regulator Professional Designated program eligible for 3.5 hours of continuing professional development credit. To receive credit, you will need to write down the codes provided periodically throughout the program and provide them in a survey that will be sent to the email address you provided during registration.

CIPR Event: Cybersecurity Issues, Challenges & Solutions

As of 5/4/2016

May 18, 2016
Sheraton, San Francisco/Chicago Room
Kansas City, MO

1:00 Introduction and Overview

~ *Raymond G. Farmer, Director*
South Carolina Department of Insurance

1:05 The Cybersecurity Landscape

You would have to live under a rock to not have heard about cybersecurity; but the landscape changes constantly. This presentation will bring you up-to-date, provide insights as to what is going on in the industry and ensure your understanding of the hot issues is up to date.

~ *Walter Powell*
Optiv Security

1:50 Break

2:00 Information Sharing

This presentation will provide an understanding of the various information sharing entities, their function, and benefits from collaborating with both public and private entities on critical security threats. Discussion will include the function of the National Council of ISACs (NCI) and member benefits of participating in information sharing organizations, such as the Financial Services Information Sharing Analysis Center (FS-ISAC) and the National Health ISAC (NH-ISAC). It will also discuss the coordination role of Financial and Banking Information Infrastructure Committee (FBIIC) and the Financial Services Sector Coordinating Council (FSSCC). The impact and potential benefits of the Cybersecurity Information Sharing Act (CISA) will also be discussed. Additionally, the development of the CIBAR Objective Database to assist in more precise underwriting will be covered.

~ *Rick Lacafta*
FS-ISAC

2:50 Networking Break

CIPR Event: Cybersecurity Issues, Challenges & Solutions (continued)

3:30 Keynote Address

The presentation will provide an overview of cybersecurity issues, why cybersecurity is important to the insurance industry, and recent insurance regulatory initiatives to address cybersecurity issues, including financial reporting and data collection enhancements and examination and model law development. The expected impact of recent legislative efforts will also be covered.

~ *Adam Hamm, Commissioner*
North Dakota Insurance Department

4:00 Insurance Regulatory Initiatives to Address Cybersecurity

Panelists will discuss financial solvency concerns related to cybersecurity. Additionally, panelists will discuss the state of the insurance market for cyber policies, including underwriting and pricing concerns. The types of data related to cybersecurity collected by the NAIC will also be covered.

Moderator:

~ *Raymond G. Farmer, Director*
South Carolina Department of Insurance

Panelists:

~ *Pat McNaughton, Chief Financial Examiner*
Washington State Office of the Insurance Commissioner
~ *Beth Dwyer, Superintendent*
Rhode Island Division of Insurance
~ *Robert Parisi Jr., Senior Vice-President & National Technology Network Risk & Telecommunications Practice Leader*
Marsh USA
~ *Tracy Dolin*
Standard & Poor's

5:00 Adjourn

CIPR Event: Cybersecurity Issues, Challenges and Solutions

TRACY DOLIN-BENGUIGUI
DIRECTOR
INSURANCE RATINGS

Tracy Dolin-Benguigui is a director in the North American Practice of Standard & Poor's Insurance Ratings. She has analytic responsibilities for a portfolio of the largest property casualty insurance and reinsurance companies in North America and Bermuda. She also is the analytical lead for publication of commentaries related to the U.S. personal and commercial lines sectors, including the semi-annual P/C insurance sector & economic outlook and topical research including cyber, G-SII/US SIFI, M&A trends and TRIA. In addition, she chairs the Americas analytical oversight consistency council, North American standing research council, and co-chairs a focus team covering the global multiline insurance market and global regulatory & accounting developments. Ms. Dolin-Benguigui has spoken on property casualty insurance industry and ratings trends at numerous conferences and maintains a regular dialogue with investors, media, industry groups, intermediaries, and rated insurers.

Prior to joining Standard & Poor's in 2005, she was an insurance broker at AON Risk Services. Her responsibilities included client relationship management and insurance placements for middle market, healthcare and Japan based clients.

Ms. Dolin-Benguigui holds a B.A. from Brandeis University with a double major in Economics and Health, Law and Society interdisciplinary program. She acquired a New York Property & Casualty Insurance Brokerage License during her tenure at AON.

ELIZABETH KELLEHER DWYER
SUPERINTENDENT OF INSURANCE
RHODE ISLAND DEPARTMENT OF BUSINESS REGULATION, DIVISION OF INSURANCE

Elizabeth Kelleher Dwyer was appointed Deputy Director and Superintendent of Insurance and Banking on January 11, 2016. Prior to this appointment, she had been employed by the Rhode Island Department of Business Regulation for 15 years, first as General Counsel to the Insurance Division and later as Associate Director. Prior to government service, she was engaged in private law practice in California and Rhode Island, specializing in insurance regulation and litigation.

Superintendent Dwyer is a past president of the Rhode Island Women's Bar Association and served on the Rhode Island Supreme Court Advisory Committee on Gender in the Courts. In 2010, she was awarded the Rhode Island Attorney General's Justice Award for Consumer Protection. She has served as chair of a number of NAIC working groups and has achieved the designation of Professional in Insurance Regulation from the NAIC.

Superintendent Dwyer was admitted to practice law in California in 1985, Rhode Island in 1994 and Massachusetts in 1996. She is also admitted to practice before the Federal District Courts of California and Rhode Island and the Ninth Circuit Court of Appeals. She received a bachelor's degree in political science and public administration from Providence College in 1982 and a Juris Doctor from Pepperdine University in 1985.

RAYMOND G. FARMER
DIRECTOR
SOUTH CAROLINA DEPARTMENT OF INSURANCE

Raymond G. Farmer was appointed by South Carolina Governor Nikki Haley to serve as Director for the South Carolina Department of Insurance on November 13, 2012. With more than 40 years' experience, Director Farmer earned his bachelor's degree in insurance from the University of Southern Mississippi and earned his law degree from Atlanta's John Marshall Law School.

Director Farmer served as the Deputy Insurance Commissioner of the Enforcement Division for the Georgia Department of Insurance and more recently as vice president for the American Insurance Association. As a part of his service, he has served for more than 30 years on the board of directors of the Georgia Arson Control Program, an organization aiding firefighters and prosecutors combating arson. He is a member of the State Bar of Georgia and a member of the Tort and Insurance Practice section, as well as the Workers' Compensation section.

In 2012, Director Farmer was awarded the Herman Hass Award by the Independent Insurance Agents of Georgia for service to the insurance industry. Also in 2012, he received a Presidential Citation for Outstanding Service to the insurance industry from the Professional Insurance Agents of Georgia. Recently, he received the 2014 Industry Person of the Year from the Independent Agents and Brokers of South Carolina.

ADAM HAMM
COMMISSIONER
NORTH DAKOTA INSURANCE DEPARTMENT

Adam Hamm was appointed Insurance Commissioner in October 2007. He was elected to a four-year term in November 2008 and again in 2012. Commissioner Hamm has a strong and varied background that includes experience in public service and in the private sector. Hamm's dedication and desire to serve the public was in part borne out of his experiences seeking justice for personal crime victims as a prosecutor for the Cass County State Attorney's Office.

Commissioner Hamm also worked as an attorney in private practice, advocating for North Dakota businesses and individuals. He specialized in a number of areas, including commercial litigation and administrative agency law.

Commissioner Hamm is a graduate of Sam Houston State University and earned his Juris Doctor degree, with distinction, from the University of North Dakota School of Law.

Commissioner Hamm is very active in the NAIC, the association made up of the chief insurance regulators from all 50 states, the District of Columbia and the five U.S. territories. He is a past president of the NAIC, serves as the chair of the Cybersecurity (EX) Task Force and is on numerous committees.

In September 2014, Commissioner Hamm was appointed by the NAIC to the U.S. Financial Stability Oversight Council as the state insurance commissioner representative. In this role, he represents the interests of all the nation's state insurance regulators. The Council was created by the federal Dodd-Frank Wall Street Protection and Consumer Protection Act in 2010 to monitor the safety and stability of the nation's financial system and coordinate a response to any threats.

RICK LACAFTA
DIRECTOR OF INSURANCE SERVICES
FINANCIAL SERVICES INFORMATION SHARING AND ANALYSIS CENTER (FS-ISAC)

Rick Lacafta has over 40 years of experience in information technology, information security and legal compliance management with Travelers Insurance, Citigroup, Primerica and CitiFinancial and most recently, FS-ISAC, on diverse assignments. Mr. Lacafta was Chief Information Security Officer for Travelers Insurance from 1999 to 2011, and Senior Legal Compliance Officer from 2008 to 2011.

Mr. Lacafta has served on several committees on the FSSCC (Financial Services Sector Coordinating Council), the Threat and Intelligence Committee of the FS-ISAC, the Independent Insurance Agents Council on Technology, IBM Privacy Council and AT&T Technical Advisory Committee.

Mr. Lacafta currently serves as Director of Insurance Services for the FS-ISAC, a Washington, DC based non-profit organization providing cyber intelligence to leading financial services companies. He is managing the Insurance Risk Council and Compliance and Audit Council for the FS-ISAC.

Mr. Lacafta is a frequent presenter at information security and business conferences, as well as managing content for FS-ISAC's US and international information security summits. He also works with several businesses as an information security advisor.

PATRICK H. MCNAUGHTON
CHIEF EXAMINER, COMPANY SUPERVISION DIVISION
WASHINGTON STATE OFFICE OF THE INSURANCE COMMISSIONER (OIC)

Since joining the OIC in 1999, his primary duties have been to direct and lead staff in the financial solvency examinations of domestic insurance companies. He was recently appointed Chair of the OIC Executive Management Team's CyberSecurity Task Force. He has also represented Washington State as the Chair of several NAIC working groups, and task forces as follows: Information Technology Examination Working Group; Financial Examination Coordination Working Group; NAIC Chief Financial Regulators Forum; Financial Examination Coordination Regulator Issues Sub-Group and Health Industry Sub-group; Blanks Working Group Schedule T Sub-group; Financial Examiners Handbook Technical Group-Risk Retention Sub-group and Examination Reporting Sub-group; and the Health RBC Working Group. He has also served or serves as a member of the following groups: Cyber Security Task Force; Financial Examiners Handbook Technical Group; Financial Condition Committee; Examination Oversight Task Force; Risk Assessment Working Group; Risk Assessment Implementation Sub-group; Capital Adequacy Task Force; Reinsurance Task Force; Valuation of Securities Task Force; Solvency Modernization Initiative Working Group and the Corporate Governance Working Group. In 2008, he was named as the Western Zone representative for the Board of Directors of the NAIC Professional Designation Advisory Board.

He has also been an instructor at the Insurance Regulator Program at the Katie School of Insurance and Financial Services at Illinois State University since 2006. He has also taught numerous courses on Risk-Assessment for the NAIC and has been invited to teach at the annual Society of Financial Examiners Career Development Seminar, the annual Insurance Regulators Examiners Society Career Development Seminar, and the National Council of Insurance Guarantee Funds annual conference.

Prior to his employment in Washington State, Mr. McNaughton served as the Chief Examiner for the Federal Reserve Board of Governors in Washington, DC. He supervised the internal control reviews and financial assessments of the Federal Reserve System's nationwide banking, accounting, and computer operations. He also provided operational best-practice consultation to CEO's and CFO's of all Federal Reserve Districts including extensive risk assessments of all Federal Reserve investment portfolios, corporate governance; and effectiveness of control compliance, and problem management of Reserve Bank practices and reporting mechanisms.

Mr. McNaughton has provided consultant services through the US State Department and the US Treasury Department to the Directors of the National Bank of Russia, the National Bank of Kazakhstan, and the National Bank of Kirgizstan, on corporate governance, internal audit best practices, IT audit processes, and risk assessments of accounting and payments systems. In 2012 and 2014, he also provided consultant services to the Federal Financial Services Authority in Albania in the development of an insurer solvency early warning system.

Mr. McNaughton has a Bachelors of Science degree from Rockhurst University in Kansas City, Missouri, with majors in Accounting, Computer Science, and Economics.

In 2014, Mr. McNaughton received the Governor's Award for Leadership in Management as one of the top managers in Washington State.

ROBERT A. PARISI, JR.
MANAGING DIRECTOR & NATIONAL PRACTICE LEADER
FOR NETWORK SECURITY & PRIVACY RISK
MARSH USA

Robert Parisi, Jr. is a Managing Director and National Practice Leader for Network Security & Privacy Risk in Marsh's New York City headquarters. His current responsibilities include advising clients on issues related to intellectual property, technology, privacy, and cyber related risks as well as negotiating with the carriers on terms and conditions.

Prior to joining Marsh, Mr. Parisi was the senior vice president and Chief Underwriting Officer (CUO) of eBusiness Risk Solutions at AIG. He joined AIG in 1998 as legal counsel for its Professional Liability group and held several executive and legal positions, including CUO for Professional Liability and Technology. While at AIG, Mr. Parisi oversaw the creation and drafting of underwriting guidelines and policies for all lines of Professional Liability. He was also instrumental in the development of specialty reinsurance to address aggregation of risk issues inherent in cyber, privacy and technology insurance. In addition to working with AIG, he has also been in private practice, principally as legal counsel to various Lloyds of London syndicates.

While at Marsh, Mr. Parisi has worked extensively with Marsh clients in all industries, assisting them in analysis of their risk as well as in the placement of coverage for cyber and privacy risks.

Mr. Parisi holds a JD from Fordham University School of Law and a BA in economics from Fordham College.

WALT POWELL
SOLUTION ARCHITECT
OPTIV SECURITY

Walt Powell is a seasoned security professional with over ten years of technical leadership experience. As a solution architect he provides a variety of Fortune 100 and governmental clients with architectural and design support for security solutions. Mr. Powell delivers his clients product engineering, compliance, audit and assessment expertise to securely enable their businesses by aligning business goals with their security programs.

Mr. Powell began his sales engineering role in the Silicon Valley / San Francisco Bay area where he had the opportunity to work with many of the top security companies as both a vendor and a client. He has had the opportunity to visit EBCs for most of the top security control manufacturers.

Prior to joining the FishNet team, Mr. Powell served as the program director for the associate of networking security degree program at Wright College. In 2012, he brought his talents to Fishnet as a security training consultant, where he performed Security Governance, Management and International standards certification consulting in addition to delivering on site and classroom based instructor lead corporate security training. He has delivered and developed curricula, courseware and content for dozens of cyber security courses including CISSP, CISM, Security+, Checkpoint and F5 Networks.

Mr. Powell is a subject matter expert in security architecture but has additional focused expertise in application delivery and security. He heads the national Optiv Application Security SME Team and is a member of the F5 Certified Speaker's Bureau. Powell holds over 50 professional, technical, training, engineering and sales certifications including CISSP, CISM, F5TS, CCSA, etc. He is an active member of several industry and professional organizations, including ICS2, ISACA, ONF and CSA where he participates in exam development committees. Mr. Powell has also delivered several keynote and guest speaker engagements in addition to writing several technical papers and solution briefs.

www.naic.org Quick Guide

NAIC National Association of Insurance Commissioners

& The Center for Insurance Policy and Research

The CIPR serves: federal and state lawmakers; federal and state regulatory agencies; international regulatory agencies; and insurance consumers. It enhances intergovernmental cooperation and awareness, improving consumer protection while promoting legitimate marketplace competition. The site provides information on current insurance regulatory developments, ongoing CIPR projects, and coverage of a wide-range of insurance industry topics.

The CIPR's organization and navigation shares many of the same elements the NAIC home page as described on Page 1.

Here are the highlights unique to CIPR pages:

1. The NAIC's Central Office/CIPR staff can provide a great deal of information to regulators and lawmakers. Contact information providing direct access to them is vital to the CIPR site's function.

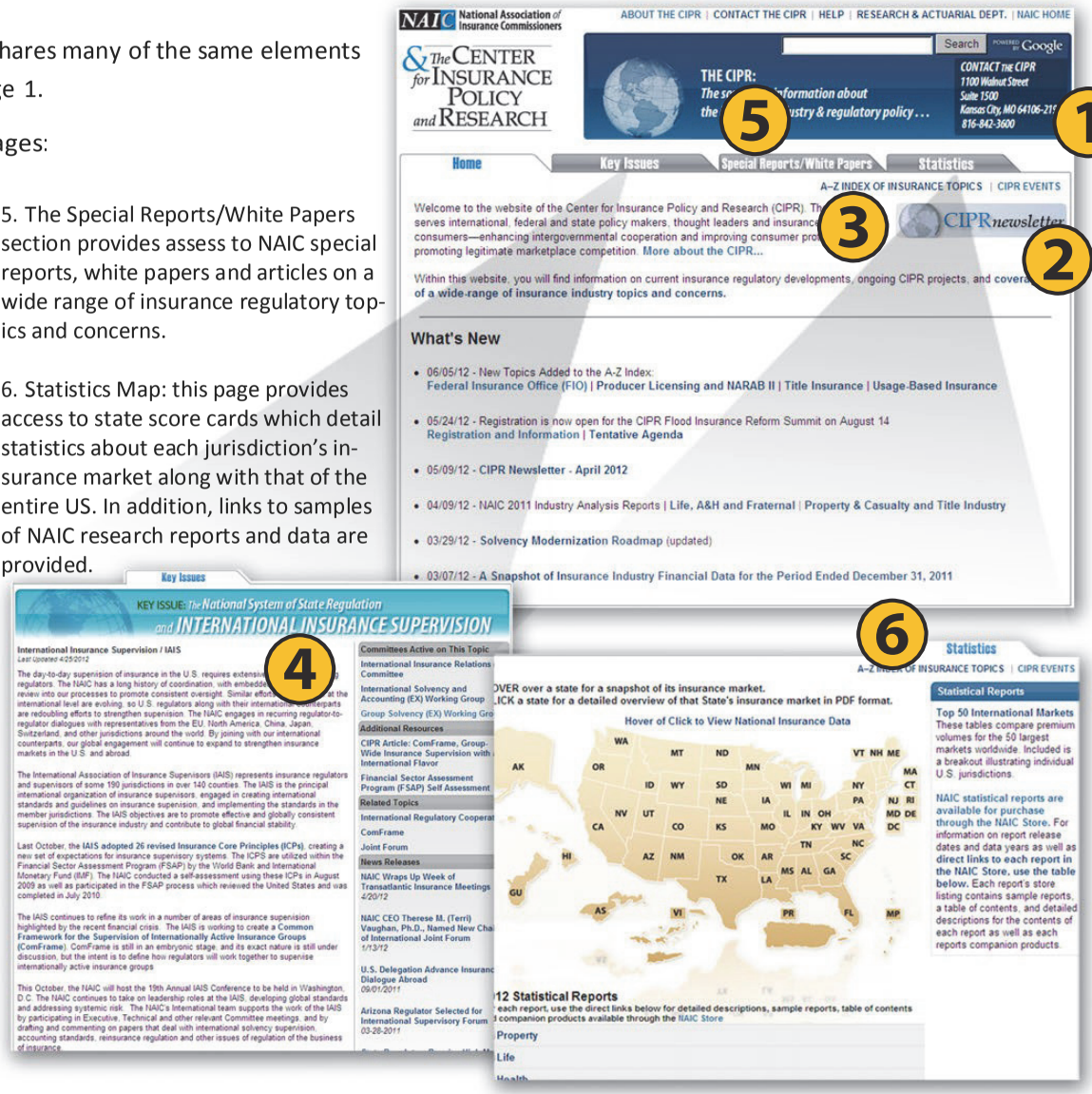
2. Click to see the most current as well as archived issues of the CIPR Newsletter.

3. The A-Z Index of Insurance topics and issues. Click to see detailed analysis and documentation on a wide range of insurance topics and issues.

4. The Key Issues section includes a topical listing of key insurance regulatory issues.

5. The Special Reports/White Papers section provides assess to NAIC special reports, white papers and articles on a wide range of insurance regulatory topics and concerns.

6. Statistics Map: this page provides access to state score cards which detail statistics about each jurisdiction's insurance market along with that of the entire US. In addition, links to samples of NAIC research reports and data are provided.



NAIC Web Site Support
Contact Information:

1. NAIC Help Desk:
   Phone 816.783.8500
   E-mail help@naic.org
   fax 816.460.7456
2. NAIC Web Team: webpost@naic.org
3. NAIC Communications: news@naic.org

CIPR EVENTS

The CIPR holds four events each year—three events during each of the NAIC National Meetings and one off-site event. For more information on our past events, including presentations and audio, please visit our website at: www.naic.org/cipr_events.htm.

2016 Events

- Insurance and Technology (Apr. 5)

2015 Events

- Regulation of Captives (Nov. 18)
- All About Earthquakes (Aug. 14)
- Boom or Bust? A Look into Retirement Issues Facing Baby Boomers Symposium (June 15-16)
- Risk of Pandemics to the Insurance Industry (Mar. 27)

2014 Events

- Navigating Interest Rate Risk in the Life Insurance Industry (Nov. 19)
- Implications for Increasing Catastrophe Volatility on Insurers and Consumers Symposium (Oct. 7-8)
- Commercial Ride-Sharing and Car-Sharing Issues (Aug. 16)
- Insuring Cyber Liability Risk (Mar. 28)

2013 Events

- The Future of Automobile Insurance: Telematics in the U.S. (Dec. 16)
- Exploring Insurers' Liabilities Summit (Aug. 27)
- Health Care Reform - Tools for Oversight and Assistance in the Marketplace Symposium (Apr. 30-May 1)
- Insurance for Acts of Terrorism (Apr. 9)

2012 Events

- Financing Home Ownership Luncheon (Nov. 30)
- State of the Life Insurance Industry: Implications of Industry Trends Symposium (Oct. 25-26)
- Flood Insurance Summit (Aug. 14)

2011 Events

- Conference on Transatlantic Insurance Group Supervision (Sep. 7-8)

Cybersecurity Takes Center Stage

By Adam Hamm, North Dakota Insurance Commissioner and NAIC Cybersecurity (EX) Task Force Chair

I recall the times when I thought it was a nuisance having to shred documents containing personal information so somebody wouldn't steal my identity by going through my trash each week. Now, I wish that was my only identity theft concern. With the proliferation of electronic communication, social media, emails and massive databases housing personal financial and health information, it's enough to make anyone lose sleep at night. It makes all of us wonder what can be done to protect ourselves.

In this article, I will discuss some steps being taken by state insurance regulators to proactively address cybersecurity issues.

◆ Defining the Problem

As people become more reliant on electronic communication, and as businesses collect and maintain ever more granular pieces of information on their customers, the opportunity for bad actors to cause difficulties for businesses and the public is exploding. Identity theft is a growing problem for consumers.

The statistics collected by the U.S. Bureau of Justice Statistics (BJS) confirm our fears related to identity theft. The BJS periodically collects information though a survey called the *National Crime Victimization Survey*. For purposes of the survey, the definition of identity theft includes three general types of incidents:

1. Unauthorized use or attempted use of an existing account.
2. Unauthorized use or attempted use of personal information to open a new account.
3. Misuse of personal information for a fraudulent purpose.[1]

The BJS report called *Victims of Identity Theft*, 2012 (the most recent year available) shows:

- About 7% of persons age 16 or older were victims of identity theft in 2012.
- The majority of identity theft incidents (85%) involved the fraudulent use of existing account information, such as credit card or bank account information.
- Victims who had personal information used to open a new account or for other fraudulent purposes were more likely than victims of existing account fraud to experience financial, credit, and relationship problems and severe emotional distress.
- About 14% of identity theft victims experienced out-of-pocket losses of $1 or more. Of these victims, about half suffered losses of less than $100.
- More than half of identity theft victims who were able to resolve any associated problems did so in a day or less; among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems.[2]

The BJS also collects information on cybercrime. However, the most recent data available from them is for 2005. There is another vehicle for gathering information about cybersecurity threats to the financial sector. Perhaps the best way for insurers to share information on cyber activity is through the Financial Services Information Sharing and Analysis Center (FS-ISAC). The FS-ISAC is a resource for the financial sector on cyber and physical threat intelligence analysis and information-sharing. The FS-ISAC is a member-owned non-profit entity providing an anonymous information-sharing capability across the entire financial services industry. For more information on the FS-ISAC visit *www.fsisac.com*.

Identity theft for individuals and cybercrimes for business are closely interrelated. There are a number of reasons why a business might be hacked. Some of these reasons are more critical than others for guarding against identity theft. One type of cybercrime is hacking by an individual just to show he or she can successfully perpetrate the act. The motivation is simply the challenge of being able to break through the firewall of a business and cause some form of disruption.

This type of hacking often shows itself as a denial-of-service attack. The intent of the hacker is to disrupt or degrade the Internet connectivity or email system of a business. This is accomplished by "ping" attacks, port -canning probes and by causing excessive amounts of data to arrive in a short period of time with the intent of disrupting service. From an identity theft perspective, this type of attack is relatively

(Continued on page 3)

[1] Bureau of Justice Statistics. *www.bjs.gov/index.cfm?ty=tp&tid=42*. Accessed April 8, 2015.
[2] Bureau of Justice Statistics. *www.bjs.gov/index.cfm?ty=pbdetail&iid=4821*. Accessed April 8, 2015.

benign. The intent of the hacker is not to steal and sell or use identities, but rather to be a nuisance to the business.

Other hackers, sometimes known as "hacktivists," are intent on using technology to deliver an ideological, political or religious message. Cyberterrorists are included in this category, as they use denial-of-service or Web defacement to damage a firm that fails to live up to the hacker's ideological expectations. Others hack to expose perceived wrong-doing or to make confidential information available to the public.

Another source of hacking is the nation state. We know some nations support hacking activities for various reasons. A rogue nation state might be interested in cyber warfare as a way to disrupt the economy of another nation or to do harm to its people. Other nations might simply be interested in spying on businesses in another nation or gaining information and insight from government websites. Sometimes, nation states target businesses to hack where access to trade secrets and business processes is the desired goal.

It is hacking for profit that is the cause of greatest concern. It could be an individual or an organized criminal gang who is engaged in hacking, with the goal to obtain personal financial and health information to exploit people and business for ill-gotten financial gain.

The bottom line is if you own a computer or a smart phone or other electronic equipment using the Internet, you are at risk. State insurance regulators are not going to be able to solve this broad public policy issue. However, state insurance regulators are in a position to help protect the public—policyholders, beneficiaries and claimants—by making sure that insurers implement the best practices for data security available.

From a state insurance regulator's perspective, the problem can be defined in four ways:

- Regulators know consumer information is at risk and want to do whatever is within their regulatory power to assist insurance consumers when consumer information is compromised by a breach from an insurer, an insurance producer or the regulator.
- Regulators have authority to monitor the market activities of insurers and insurance producers and are actively overseeing the cybersecurity capabilities of insurers and insurance producers.
- Regulators need to work together to make sure state computer networks and the computer network at the NAIC are state-of-the-art when it comes to cybersecurity measures.
- Regulators need to exercise authority over the insurers involved in selling cybersecurity insurance products to individuals and businesses in the U.S.

◆ THE NAIC CYBERSECURITY (EX) TASK FORCE

The NAIC Executive (EX) Committee recently appointed the Cybersecurity (EX) Task Force and asked it to serve as the central focus for insurance regulatory activities related to cybersecurity. I am honored to serve as chair of this new Task Force. The Task Force has a fairly aggressive work plan, which involves coordination with various NAIC groups working on certain aspects of cybersecurity.

The first project for the Task Force was establishing a set of guiding principles to plant a "flag in the ground" on cybersecurity. An initial draft set of eighteen guiding principles was released for public comment in March. After receiving and considering feedback from interested parties, the Task Force revised and combined some of the principles. The Task Force then adopted a final set of twelve guiding principles on April 16. These principles will serve as the foundation for protecting consumers personally identifiable information held by insurers as well as insurance producers and will guide state insurance regulators who oversee the insurance industry. A copy of the guiding principles can be found on the NAIC website.[3]

The Task Force will be working with the Property and Casualty Insurance (C) Committee on a proposal to add a cybersecurity supplement to the P&C Annual Statement. The purpose of this would be to get a clear picture of the size and breakdown of the cyber insurance market. The Committee recently adopted a motion to release the Annual Statement Supplement for public comment and asked for written comments to be submitted March 23. The Committee discussed the comments received during its March 29 meeting in Phoenix at the Spring National Meeting. Several states and interested parties made suggestions for im-

(Continued on page 4)

[1] www.naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf.

proving the draft Annual Statement Supplement. Commissioner Mike Chaney (MS), who chairs this Committee, convened a conference call to discuss the comments and suggested changes. The proposed supplement was then adopted during the call.

Additionally, the Task Force will be working with the IT Examination (E) Working Group. The Working Group plans to review existing guidance in the *Financial Condition Examiners Handbook* (Handbook) and will be working with the Task Force on improvements to the examination protocols for state financial examiners to check on the cybersecurity capabilities of insurers. Patrick McNaughton (WA) leads this Working Group.

Currently, every state is required to use specialists at companies when reviewing their data-security controls. These specialists generally have specialized training enabling them to successfully review insurer data security controls. These specialists typically have obtained the certified information systems auditor (CISA) designation, as well as the automated examination specialist certification from the Society of Financial Examiners (SOFE). Using these specialists is an accreditation requirement on all multi-state financial examinations.

The NAIC maintains the Handbook to provide guidance to financial examiners. The Handbook has an extensive section regarding the review of automated controls and uses the COBIT 5 standards, which are recommended and promoted by the Information Systems Audit and Control Association (ISACA). The standards are strict and robust with respect to evaluating and determining whether the general information technology controls at a company are operating as they should.

The difference between what a state financial examiner with data security skills and what a cybersecurity firm does is that the financial examiner ensures an insurer is evaluating its risks and hiring the necessary firms to examine its data and systems. A cybersecurity firm does actual penetration testing, monitoring, and ongoing reviews on behalf of the insurer.

The IT Examination (E) Working Group regularly revises its guidelines and standards. The Working Group has used the draft principles assembled by the Task Force to determine the Working Groups next steps to ensure the Handbook guidance includes a more robust look at cybersecurity. The Working Group is going to compare the National Institute of Standard Technology (NIST) framework to its existing framework to be sure there are no gaps between the two frameworks.

When financial regulators conduct a risk-focused examination of an insurer, they look at how the insurer identifies and defines its risks, as well as the steps taken to mitigate identified risks. The financial examiner will also weigh what the CEO and board members have to say regarding these risks. Often, the financial examiner finds data security and cybersecurity are not high enough on the list of risks identified by insurer management. The Cybersecurity (EX) Task Force, working together with the IT Examination (E) Working Group, plans to change that dynamic in the future.

The Task Force will also be looking to create a survey of the states to assess state cyber vulnerabilities. Work on this project is expected to occur over the summer. The Task Force plans to be able to discuss results of the survey during the Fall National Meeting.

Another important project for the Task Force is the creation of a Consumer Bill of Rights. I expect it will cover existing regulations and statutes regarding the security breach notification. It will also outline state insurance regulators' expectations of insurers if they experience a cybersecurity issue. Consumers deserve to know insurers are protecting their sensitive financial and health information. They also deserve to know when a breach occurs so they can take steps to safeguard themselves from identity theft or other fraud. Now that the guiding principles have been adopted, plans call for work on the Consumer Bill of Rights to begin.

The Task Force also plans to stay abreast of what is happening in the Financial and Banking Information Infrastructure Committee (FBIIC), the Cybersecurity Forum for Independent and Executive Branch Regulators and the FS-ISAC. Plans call for the Task Force to host a webinar to receive information from the FS-ISAC. The webinar will cover the benefits of information sharing through the FS-ISAC.

The NAIC maintains numerous model laws, regulations and guidelines. Some of them deal with issues related to cybersecurity. The Task Force will review several model laws and regulations to update them with regard to privacy and cybersecurity. Among the models under consideration are: the *NAIC Insurance Information and Privacy Protection Model Act* (#670); the *Privacy of Consumer Financial and Health*

(Continued on page 5)

Information Regulation (#672); and the *Standards for Safeguarding Consumer Information Model Regulation* (#673).

The Task Force may also take a look at the *Insurance Fraud Prevention Model Act* (#680). No definite timeframe has been set for this work. It is important to note the Model #670 and Model #672 were created in response to the federal Gramm-Leach-Bliley Act. They provide the basis of the annual privacy notifications for the insurance sector. Careful attention must be paid to these important models.

◆ CONCLUSION

These days, everyone who owns a computer is at risk. Hackers with a variety of motivations spend their days trying to stay one step ahead of the firms who sell cybersecurity tools. Sound firewalls and robust network security are able to turn away most hacking attempts, but we know no system is perfect. As such, I am proud to say state insurance regulators are stepping up to do their part to attempt to make the electronic world safer.

ABOUT THE AUTHOR

Adam Hamm was appointed Insurance Commissioner by Governor John Hoeven in October 2007, elected to a four-year term in November 2008 and reelected to a second four-year term in November 2012. He has a strong and varied background that includes experience both in public service and in the private sector.

Mr. Hamm's dedication to serve the public began with his work as a prosecutor at the Cass County State's Attorney's office. Hamm has also worked as an attorney in private practice advocating for North Dakota businesses and individuals. He is a graduate of Sam Houston State University and received his Juris Doctorate Degree, with Distinction, from the University of North Dakota School of Law in 1998

Mr. Hamm is currently the immediate Past President of the NAIC, and chairs its new Cybersecurity Task Force. He also serves on numerous NAIC committees, including the Executive Committee, the Accreditation Committee and the Government Relations Leadership Council. Additionally, he was selected by his fellow insurance commissioners to serve on the U.S. Financial Stability Oversight Council (FSOC). In this role, he represents the interests of all the nation's state insurance regulators.

Managing Cyber Risks

By Eric Nordman, CPCU, CIE, Director, Regulatory Services Division and the CIPR

◆ Introduction

As I write this article, I long for the days when life was simpler … when the post office brought my mail instead of a desktop computer … when I gave my handwritten notes or dictation to the typing pool and eventually a letter came back for my review … when people did not stand in line overnight to get the latest, greatest Apple iPhone. OK, so now you know that a curmudgeon is writing this article on cyber risk management. It is still worth reading, as my background tends to push me into evaluating everything from a risk-management perspective.

All of this new technology comes with risk. Once these risks are identified, understood and quantified, they can be avoided, controlled, combined, retained or transferred using insurance or other risk-management techniques. So now you get the picture. This article will discuss cyber risks and have some suggestions about what to do with them. Some creative insurers have already done much thinking about cyber risks and are offering innovative insurance products to meet businesses' risk management needs.

◆ Cyber Risk Management

If you own a computer, you are at risk. If you have the computer connected to the Internet, you are at greater risk. If you use the computer to send and receive email, you are at risk. If you store anything on the computer, you are at risk. If you let employees place sensitive information on a laptop, your risk increases. If you allow employees to use memory sticks or thumb drives, you are at risk. Nearly anything you do with a computer creates risk for you.

The cyber risks for a business are almost endless. As data breaches occur more frequently, there are additional pressures for business to step up efforts to protect the personal information in their possession. In fact, there is legislation requiring the protection of personal financial information and personal health information. Some of the key risks associated with owning a computer are:

- Identity theft as a result of security breaches where sensitive information is stolen by a hacker or inadvertently disclosed, including such data elements as Social Security numbers, credit card numbers, employee identification numbers, drivers' license numbers, birth dates and PIN numbers.
- Business interruption from a hacker shutting down a network.
- Damage to the firm's reputation.
- Costs associated with damage to data records caused by a hacker.
- Theft of valuable digital assets, including customer lists, business trade secrets and other similar electronic business assets.
- Introduction of malware, worms and other malicious computer code.
- Human error leading to inadvertent disclosure of sensitive information, such as an email from an employee to unintended recipients containing sensitive business information or personal identifying information.
- The cost of credit monitoring services for people impacted by a security breach.
- Lawsuits alleging trademark or copyright infringement.

Applying avoidance by selling all of your computers is probably tempting on some days, but is not generally the risk-management technique of choice. That leaves various forms of mitigation and risk transfer on the table for consideration. Because managing computer networks is outside my scope of knowledge, the remainder of this article will focus on managing cyber risks through insurance.

◆ Cyber Liability Policies

Most businesses are familiar with their commercial insurance policies providing general liability coverage to protect the business from injury or property damage. However, most standard commercial lines policies do not cover many of the cyber risks mentioned earlier. To cover these unique cyber risks through insurance requires the purchase of a special cyber liability policy. The markets for these policies are relatively new, with a growing number of insurers offering coverage. Like all new markets, coverage contained in the policy forms is evolving as risks evolve and competitive forces come into play. As a result, if you have seen one cyber liability policy you will have seen one cyber liability policy. It will be different than the cyber liability policy from the next insurer.

There are some risks that are commonly covered by cyber liability policies. Generally, cyber liability policies cover a business' obligation to protect the personal data of its customers. The data might include personal identifying information, financial or health information, or other critical data that, if compromised, could create a liability exposure

(Continued on page 29)

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.

Cyber liability policies tend to be customized to meet the risk-management needs of the policyholder. Because businesses are unique in many ways, this customization feature allows the insurer to tailor a policy to meet the unique nature of each business. Thus, the type of business operation will dictate the type and cost of cyber liability coverage. The size and scope of the business will play a role in coverage needs and pricing, as will the number of customers, the presence on the Web, the type of data collected and stored, and other factors.

Cyber liability policies might include one or more of the following types of coverage:

- Liability for security or privacy breaches. This would include loss of confidential information by allowing, or failing to prevent, unauthorized access to computer systems.
- The costs associated with a privacy breach, such as consumer notification, customer support and costs of providing credit monitoring services to affected consumers.
- The costs associated with restoring, updating or replacing business assets stored electronically.
- Business interruption and extra expense related to a security or privacy breach.
- Liability associated with libel, slander, copyright infringement, product disparagement or reputational damage to others when the allegations involve a business website, social media or print media.
- Expenses related to cyber extortion or cyber terrorism.
- Coverage for expenses related to regulatory compliance for billing errors, physician self-referral proceedings and Emergency Medical Treatment and Active Labor Act proceedings.

Securing a cyber-liability policy will not be a simple task. Insurers writing this coverage will be interested in the risk-management techniques applied by the business to protect its network and its assets. The insurer will probably want to see the business' disaster response plan and evaluate it with respect to the business' risk management of its networks, its website, its physical assets and its intellectual property. The insurer will be keenly interested in how employees and others are able to access data systems. At a minimum, the insurer will want to know about antivirus and anti-malware software, the frequency of updates and the performance of firewalls.

◆ CONCLUSION

The market for cyber liability insurance policies is relatively new. Like many new markets, it is off to a good start, but expected to grow dramatically over time. New competitors are closely following what early entrants have done. Businesses are gradually becoming more aware that current business policies do not adequately cover cyber risks. With each announcement of a system failure leading to a significant business loss, the awareness grows. Soon, business leaders will recognize what their information technology staff has been telling them. Running a computer operation with exposure to the Internet is risky, but necessary, for a business to succeed in the modern world. Thankfully, there are ways to protect the business from financial ruin through this rapidly growing niche insurance market.

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.

benign. The intent of the hacker is not to steal and sell or use identities, but rather to be a nuisance to the business.

Other hackers, sometimes known as "hacktivists," are intent on using technology to deliver an ideological, political or religious message. Cyberterrorists are included in this category, as they use denial-of-service or Web defacement to damage a firm that fails to live up to the hacker's ideological expectations. Others hack to expose perceived wrong-doing or to make confidential information available to the public.

Another source of hacking is the nation state. We know some nations support hacking activities for various reasons. A rogue nation state might be interested in cyber warfare as a way to disrupt the economy of another nation or to do harm to its people. Other nations might simply be interested in spying on businesses in another nation or gaining information and insight from government websites. Sometimes, nation states target businesses to hack where access to trade secrets and business processes is the desired goal.

It is hacking for profit that is the cause of greatest concern. It could be an individual or an organized criminal gang who is engaged in hacking, with the goal to obtain personal financial and health information to exploit people and business for ill-gotten financial gain.

The bottom line is if you own a computer or a smart phone or other electronic equipment using the Internet, you are at risk. State insurance regulators are not going to be able to solve this broad public policy issue. However, state insurance regulators are in a position to help protect the public—policyholders, beneficiaries and claimants—by making sure that insurers implement the best practices for data security available.

From a state insurance regulator's perspective, the problem can be defined in four ways:

- Regulators know consumer information is at risk and want to do whatever is within their regulatory power to assist insurance consumers when consumer information is compromised by a breach from an insurer, an insurance producer or the regulator.
- Regulators have authority to monitor the market activities of insurers and insurance producers and are actively overseeing the cybersecurity capabilities of insurers and insurance producers.
- Regulators need to work together to make sure state computer networks and the computer network at the NAIC are state-of-the-art when it comes to cybersecurity measures.
- Regulators need to exercise authority over the insurers involved in selling cybersecurity insurance products to individuals and businesses in the U.S.

◆ THE NAIC CYBERSECURITY (EX) TASK FORCE

The NAIC Executive (EX) Committee recently appointed the Cybersecurity (EX) Task Force and asked it to serve as the central focus for insurance regulatory activities related to cybersecurity. I am honored to serve as chair of this new Task Force. The Task Force has a fairly aggressive work plan, which involves coordination with various NAIC groups working on certain aspects of cybersecurity.

The first project for the Task Force was establishing a set of guiding principles to plant a "flag in the ground" on cybersecurity. An initial draft set of eighteen guiding principles was released for public comment in March. After receiving and considering feedback from interested parties, the Task Force revised and combined some of the principles. The Task Force then adopted a final set of twelve guiding principles on April 16. These principles will serve as the foundation for protecting consumers personally identifiable information held by insurers as well as insurance producers and will guide state insurance regulators who oversee the insurance industry. A copy of the guiding principles can be found on the NAIC website.[3]

The Task Force will be working with the Property and Casualty Insurance (C) Committee on a proposal to add a cybersecurity supplement to the P&C Annual Statement. The purpose of this would be to get a clear picture of the size and breakdown of the cyber insurance market. The Committee recently adopted a motion to release the Annual Statement Supplement for public comment and asked for written comments to be submitted March 23. The Committee discussed the comments received during its March 29 meeting in Phoenix at the Spring National Meeting. Several states and interested parties made suggestions for im-

(Continued on page 4)

[1] www.naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf.

NAIC Insurance Regulator Professional Designation Program

- ***comprehensive, customizable, content-rich curriculum…directly from the NAIC***

Over 800 enrollments and growing…our designations have been designed to assure that regulators have a basic understanding of market, solvency, and rates and forms regulation at the APIR level, specialized training in regulatory concepts at the PIR level, leadership training at the SPIR level and a focused understanding of investments at the IPIR level. We continue to add new course opportunities at the PIR level and the new IPIR courses are rolling out at a rapid pace!

What Regulators Have to Say:

"The APIR program was a well- rounded program that gave me a clear picture of how I fit into the overall regulatory setting. The background obtained through these classes has improved my ability and confidence to perform as a regulator immensely, and I believe there is something here for everyone."…David

"The APIR has provided me with a wonderful opportunity to learn from and interact with regulators across the country (and our U.S. territories). I think the NAIC will be of growing importance to all of us in the future and we should not miss the opportunity to learn from the wealth of knowledge and experience it offers to us."…Richie

"I have really enjoyed the PIR program. It has enhanced my skills as a regulator by increasing my knowledge of both the industry and the regulatory tools that I have at my disposal. One of my favorite things about the program is the opportunity to attend instructor-led NAIC courses and associate with other regulators. There is no substitute for learning from other regulators personal experiences…Dan

"Through the NAIC Designation Program I have been able to work, learn, accomplish and excel in insurance regulatory areas outside of my duties. The program gave me the opportunity to broaden my knowledge beyond the basic insurance scope and think outside the box."…Vanessa

---

If you are a state insurance department employee, we invite you to sign up and learn how this program can help you achieve your personal goals.

Visit us at http://www.naic.org/education_designation.htm

NOTES:

NOTES:

NOTES:

NOTES:

NOTES:

NOTES:

NOTES:

NOTES:

NOTES:

NOTES: