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

September 9, 2016

Ms. Nakia Grayson
National Institute of Standards and Technology,
100 Bureau Drive, Stop 2000
Gaithersburg, MD 20899

Re: Input to the Commission on Enhancing National Cybersecurity

Dear Ms. Grayson:

We write on behalf of the National Association of Insurance Commissioners (NAIC)[1] regarding the Commission on Enhancing National Cybersecurity's request for information about current and future states of cybersecurity in the digital economy.

State insurance regulators are keenly aware of the potentially devastating effects cyber attacks can have, and we have taken a number of steps to enhance data security expectations across the insurance sector. In the past year, the NAIC has adopted twelve Principles for Effective Cybersecurity, a Roadmap for Consumer Cybersecurity Protections, updated guidance for examiners regarding IT systems and protocols, and we are currently working on drafting a new Insurance Data Security Model Law. However, we also understand the pressure these increased risks put on other industries, creating unprecedented demand for products to manage and mitigate some of their cybersecurity risks through insurance.

State Insurance Regulation of Cybersecurity Insurance Policies

When it comes to regulating cyber insurance, policies and insurers are scrutinized just as closely as other insurance lines. While the complexity of cyber insurance policies and new product language will present some novel issues, policy forms and rates are still subject to review to ensure the contracts are reasonable and not contrary to state laws. Insurers providing cybersecurity insurance are subject to the same solvency regime as other insurers. Insurance regulators also have market conduct authorities to examine insurers and policies as well as significant enforcement powers to curtail misconduct.

[1] Founded in 1871, the NAIC is the U.S. standard-setting and regulatory support organization created and governed by the chief insurance regulators from the 50 states, the District of Columbia and the five U.S. territories. Through the NAIC, state insurance regulators establish standards and best practices, conduct peer review, and coordinate their regulatory oversight. NAIC members, together with the central resources of the NAIC, form the national system of state-based insurance regulation in the U.S.

Cybersecurity Insurance Market

Though demand is increasing, the cyber insurance market is still relatively small as cybersecurity risk remains difficult for insurance underwriters to quantify due in large part to a lack of actuarial data. Today, in the absence of such data, insurers compensate through pricing that relies on qualitative assessments of an applicant's operations, vendors, risk management procedures, and security culture. As a result, policies for cyber risk tend to be more customized than others and, therefore, more costly. From a state insurance regulatory perspective, we would like to see these qualitative assessments coupled with robust actuarial data based on actual incident experience.

As a still nascent market for coverage, accurately assessing exposure or the size of the cybersecurity insurance market is a work in progress. In light of the uncertainty and many questions surrounding these products and the market, the NAIC developed a new mandatory data supplement. This supplement requires all insurance carriers writing either identity theft insurance or cybersecurity insurance to report on their claims, premiums, losses, expenses, and in-force policies in these areas. With this data, regulators will be able to more definitively ascertain the size of the market, and identify trends that will inform whether more tailored regulation is necessary.

Last month, the NAIC publicly released a report on the initial results from the cybersecurity insurance coverage supplement and we have attached a copy to our comment letter. Some of the highlights include:

- Over 500 insurers have provided businesses and individuals with cybersecurity insurance, with the vast majority of these coverages written as endorsements to commercial and personal policies.
- From a market perspective, the year-end 2015 data indicates that U.S. insurers' most common form of risk related to cybersecurity is in the form of identity theft coverage, where insurers wrote approximately 16.6 million policies including identity theft coverage as part of a package policy. This compares to only 496,000 policies that were stand-alone identity theft coverage.
- $1,415,843,707 is the reported and estimated total direct written premium for cybersecurity insurance coverage on a standalone and package policy basis for 2015. Compare this with the nearly $2 trillion in total direct written premium across all insurance lines.
- Insurers writing standalone cybersecurity insurance products reported approximately $500 million in direct written premium. The top ten insurers wrote 78.7% of total U.S. market with the top 20 writing 95.8% of the market.
- Insurers writing cybersecurity insurance as part of a package policy reported roughly $1 billion in premium writings.

The expansion of cyber risks and the growth of the cybersecurity insurance market are a tremendous opportunity for the insurance sector to lead in the development of cyber-hygiene across our national infrastructure. Insurance has a long history of driving best practices and standardization. It creates economic incentives through the pricing of products, and the underwriting process can test risk management techniques, and encourage policyholders to make their businesses more secure. As insurers develop more sophisticated tools for underwriting and pricing, state regulators will continue to monitor and study cybersecurity products, always remembering that our fundamental commitment is to ensuring that policyholders are protected and treated fairly by financially sound insurance companies.

As policymakers and stakeholders increasingly look at insurance as part of the cyber risk management framework, we agree that there is great potential but would urge caution to allow the insurance market to

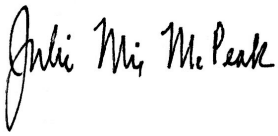
grow and evolve organically and be wary of policies that artificially pressure the supply or demand for this product. The insurance carriers that are writing these products are often the same carriers the economy relies upon to cover liability losses, hurricane damage, or other costly events that can put pressure on solvency. Insurance regulators must balance the industry's exposure to this product with all the other risks the industry is asked to absorb.

We appreciate the Commission's attention to this important subject and we look forward to continuing to share our data and analysis with you as our work progresses.

Sincerely,

John M. Huff
NAIC President
Director, Missouri Department of Insurance, Financial Institutions and Professional Registration

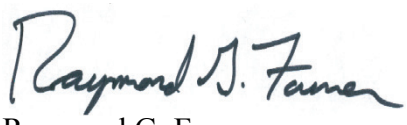
Theodore K. Nickel
NAIC President-Elect
Commissioner, Wisconsin Department of Insurance



Julie Mix McPeak
NAIC Vice President
Commissioner, Tennessee Department of Commerce and Insurance

Eric A. Cioppa
NAIC Secretary-Treasurer
Superintendent, Maine Department of Professional and Financial Regulation, Bureau of Insurance

Adam Hamm
Chair, NAIC Cybersecurity Task Force and NAIC Past President
Commissioner, North Dakota Department of Insurance



Raymond G. Farmer
Vice Chair, NAIC Cybersecurity Task Force
Director, South Carolina Department of Insurance

Enclosures:
Report to the NAIC Cybersecurity Task Force on Cyber Supplement, August 2016
Testimony of North Dakota Insurance Commissioner Adam Hamm before the U.S. House Committee on Homeland Security Regarding "The Role of Cyber Insurance in Risk Management," March 2016
NAIC *Principles for Effective Cybersecurity: Insurance Regulatory Guidance*, April 2015
NAIC *Roadmap for Consumer Cybersecurity Protections*, December 2015

TO: Cybersecurity (EX) Task Force

FROM: Eric Nordman, CPCU, CIE, MCM
Director, Regulatory Services Division & the CIPR

Dan Daveline,
Director, Financial Regulatory Services Division

DATE: August 27, 2016

SUBJECT: Report on the Cybersecurity Insurance Coverage Supplement

The purpose of this report is to inform the Cybersecurity (EX) Task Force about the information filed by insurers in the Cybersecurity Insurance and Identity Theft Coverage Supplement (the Supplement) to the Property and Casualty Annual Statement for 2015. The report will also address some shortcomings in the data collection process and make some suggestions for future actions for the Task Force to consider.

Overview

Cybersecurity is crucial to effective and efficient operation of U.S. businesses. Cybersecurity breaches can cause a major drain on the U.S. economy. Insurers face cybersecurity risks in their daily operations as do banks and securities firms. The Financial Services Sector is perhaps the most under attack from cyber criminals. The reason for the attacks is multifaceted. Financial firms receive, maintain and store sensitive personal financial information from their customers. Insurers, in many cases, receive personal health information in addition to personal financial information. For insurers, information may be provided by policyholders or claimants. Cyber criminals are interested in this sensitive information as it can be used for financial gain by stealing a person's identity for fraudulent purposes. We know from observation of the dark web that personal health information is much more valuable these days than personal financial information. Nation states are also known to sponsor cyber-attacks for espionage or gaining access to corporate trade secrets and business processes.

Insurers are selling cyber risk management services and cybersecurity insurance products to businesses and individuals. It is to gain information and understanding about the cybersecurity insurance markets that led regulators to design and implement the Supplement. The first year the Supplement was required to be filed was with the 2015 Annual Statement filed in April of 2016. The data filed provides some interesting results. The initial results of these filings indicate over 500 insurers have provided businesses and individuals with cybersecurity insurance, with the vast majority of these coverages written as endorsements to commercial and personal policies. An overview shows a market of roughly $1.5 billion in direct written premium for insurers required to file the Supplement. Insurers writing standalone cybersecurity insurance products reported approximately $500 million in direct written premium and those writing cybersecurity insurance as part of a package policy reported roughly $ 1.0 billion in premium writings. The remainder of the report will provide figures filed for each category and explain assumptions used to arrive at the $ 1.5 billion in direct written premium. It will also discuss the entities reporting data and which entities might be missing from the data set. The report concludes with some recommendations for the Task Force to consider going forward.

Cybersecurity Insurance Coverage

The Supplement requires insurers to report the following information on standalone cybersecurity insurance policies:

- Number of claims reported (First Party & Third Party)
- Direct premiums written and earned
- Direct losses paid and incurred
- Adjusting and other expenses paid and incurred
- Defense and cost containment expenses paid and incurred
- Number of policies in-force (claims-made and occurrence)

The Supplement requires insurers to report the following information on cybersecurity insurance coverage sold as part of a package policy:

- Number of claims reported (First Party & Third Party)
- Direct premiums written and earned, if available or estimable
- Direct losses paid and incurred
- Adjusting and other expenses paid and incurred
- Defense and cost containment expenses paid and incurred
- Number of policies in-force (claims-made and occurrence)

Standalone Cybersecurity Insurance Policies

Perhaps the most interesting information is the size of the standalone cybersecurity insurance marketplace. Insurers writing this coverage reported $483,197,973 in direct written premium spread among 48 insurer groups (116 individual insurers). Direct earned premium reported was $373,742,189. Having less earned premium than written premium is indicative of a growing market. The top ten insurers wrote 78.7% of total U.S. market with the top 20 writing 95.8% of the market.

Loss ratios for standalone cybersecurity insurance were all over the map ranging from zero to over 500%. This too was not overly surprising. The market for cybersecurity insurance products is a new one and it is one with an element of catastrophe exposure. A zero loss ratio might be indicative of sound underwriting, but it might also simply be luck in selecting businesses that did not get hacked in 2015. The over 500% loss ratio occurred in an insurer group with less than $400,000 in direct written premium. Again, it could be indicative of poor underwriting or simply bad luck to insure a policyholder having a breach in 2015.

To keep things in perspective, the reader should remember $1.5 billion in direct written premium is only a very small percentage of the $522.4 billion in net written premium reported by the property and casualty insurers for 2015. All of these writings are supported by $703.6 billion in policyholder surplus held by insurers.

Package Policies

The reported direct written premium for cybersecurity package policies totaled $515,100,239. However, 257 insurers of the 574 insurers reported no premiums, generally because they could not break out the premium change for the cybersecurity coverage from the remainder of the package policy. To arrive at a figure representing a complete market NAIC staff assumed the 257 insurers writing cybersecurity package policies where premiums were not reported would have reported premiums in the same ratio as those insurers reporting actual premiums.

The actual mathematical calculation to extrapolate the premium dollars not reported under package policies follows:

- 257 insurers of 574 insurers reported no premium, representing 44.77% of the insurer population.
- The inverse of 44.77% is 55.23%.
- Then divide the actual package premium of $515,100,239 by 55.23% to get $932,645,734.
- As a result, by extrapolation we estimate approximately $933 million was the direct written premium sold through package policies.

Thus, we wish to inform you $1,415,843,707 is the reported and estimated total direct written premium for cybersecurity insurance coverage on a standalone and package policy basis for 2015.

Another interesting observation about the cybersecurity insurance policies sold on a standalone basis is most of the third party coverage is written on a claims-made basis. Approximately 82% of the policies were claims-made. From a solvency risk management perspective for insurers, the claims-made contract generally serves to limit exposure to the insurer compared to an occurrence policy by placing time limits on when the insured event must be reported to the insurer. While this is good for insurers, it is a coverage limitation from a policyholder perspective.

Identity Theft Coverage

From a market perspective, the year-end 2015 data clearly indicates that U.S. insurers' most common form of risk related to cybersecurity is in the form of identity theft coverage, where insurers wrote approximately 16.6 million policies including identity theft coverage as part of a package policy. This compares to only 496,000 policies that were stand-alone identity theft coverage.

From a risk perspective, the year-end 2015 data for identify theft coverage indicates the stand-alone premium on the 496,000 policies was $21.2 million, or approximately $42 per policy. Based upon this average of $42 per policy, the total amount of estimated annual premium on the 16.6 million policies with identify-theft as part of a package policy is still only approximately $700 million.

Caveats

When one uses data to gain information, it is important to understand its source, its attributes and its limitations. There are some important limitations for readers of this report to consider. The first limitation is the reported information is limited to only those insurers required to file a Property and Casualty Annual Statement with the NAIC. To evaluate this limitation, one must understand the types of insurers writing property and casualty business in the U.S. and whether each type is required to report information to U.S. regulators. With apologies to regulators who already understand what is said in this section, we believe it is important for readers not completely familiar with the U.S. regulatory framework to understand, from a state insurance regulators' perspective, the admitted and surplus lines markets.

The U.S. regulatory system for property and casualty insurance views insurers as belonging in one of three classifications. They are: domestic, foreign and alien. A domestic insurer is one

licensed or admitted in a state it selects to be its home state. A foreign insurer would be one licensed or admitted in a state that is domiciled in another state. An alien insurer is one domiciled in another country. Generally states insist insurers be licensed or admitted in the state as a prerequisite for selling property and casualty insurance products. However, state legislatures recognize not every person or business seeking coverage for unique risks can find it from a licensed or admitted insurer. Thus, state legislatures have allowed non-licensed insurers to write property and casualty business under certain circumstances. The insurers doing business as non-licensed or non-admitted insurers are known as surplus lines insurers. They serve as an alternative marketplace to provide coverage for unique exposures and often serve as a testing ground for product innovations before they become mainstream. Such is the case for cybersecurity insurance products. Offering coverage on a surplus lines basis allows the insurer greater freedom in pricing and does not require formal prior approval of contract language.

If an insurer is licensed or admitted in one or more states, it is required to submit an Annual Financial Statement, including the Supplement. Thus, all domestic and foreign insurers are required to file the Supplement as they will be considered an admitted insurer in at least one state. Alien insurers can choose to be licensed or admitted in one or more states if they wish. If they do choose to be licensed or admitted, then they too must file the Supplement. However, if an alien insurer decides not to become licensed in any state, the District of Columbia or U.S. territory, then no Supplement filing is required. The premium writings by alien surplus lines insurers are missing from the information contained in this report. Since we believe there may be a significant amount of premium written by alien surplus lines insurers, the reader should be cognizant of this potentially important missing element.

What Others are Saying about the Cybersecurity Insurance Markets

"Cyber coverage is the fastest growing surplus lines business in history and it was caused by a regulation, not by some other market factor. It's a $1 billion line right now."—Benjamin J. McKay, Executive Director of the Surplus Line Association of California

"The cyber insurance marketplace has grown to over $2 billion in gross written premiums with industry prognosticators forecasting it to double by 2020. The number of carriers offering cyber insurance has increased following a spate of cyberattacks that have brought the potential and need for such insurance into sharper focus."—PartnerRe

"We expect worldwide spending on Cybersecurity products and services to eclipse $1 trillion for the five-year period from 2017 to 2021"—Steve Morgan, Founder and Editor-In-Chief at Cybersecurity Ventures

"Cyber insurance is a potentially huge, but still largely untapped, opportunity for insurers and reinsurers. We estimate that annual gross written premiums are set to increase from around $2.5 billion today to reach $7.5 billion by the end of the decade."—PwC Report—Insurance 2020 & beyond: Reaping the dividends of cyber resilience

"Annual premium volume information about the U.S. cyber-risk market is hard to come by, but in reviewing the market, we have concluded that the annual gross written premium may be as much as $3.25 billion (up from $2.75 billion in last year's report)."— Richard S. Betterley, CMC, President, Betterley Risk Consultants, Inc. from Cyber/Privacy Insurance Market Survey—2016

"The cyber market is growing by double-digit figures year-on-year, and could reach $20 billion or more in the next 10 years. …fewer than 10% of companies are thought to purchase cyber insurance today."—Nigel Pearson, Global Head of Fidelity, Allianz Global Corporate & Specialty

Recommendations for the Task Force

A major caveat contained in this report is the missing information on the amount of premium written by alien surplus lines insurers. Staff believes there may be significant premium writings, particularly for standalone cybersecurity insurance policies, in this segment of the overall markets. Staff recommends the Task Force consider approaching the Surplus Lines (C) Task Force to request making submission of some or all of the information contained in the Supplement a condition for continuing to be listed on the *Quarterly Listing of Alien Insurers*.

A second staff recommendation is for the Task Force to take comments from interested parties on how the instructions or the format of the Supplement could be improved.

Conclusion

While the first report of any data collection exercise is challenging, the quality of the data improves with subsequent filings. This report summarizes some interesting findings. If information can be obtained from the alien surplus lines insurers, a more complete picture of the 56 U.S. cybersecurity insurance markets will emerge. Having a time series will allow regulators to track market growth and pinpoint areas where further regulatory oversight is needed.

Testimony of

Adam W. Hamm

Commissioner

North Dakota Department of Insurance

On Behalf of the National Association of Insurance Commissioners

Before the

Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

Committee on Homeland Security

United States House of Representatives

Regarding:

The Role of Cyber Insurance in Risk Management

March 22, 2016

Introduction

Chairman Ratcliffe, Ranking Member Richmond, and members of the Subcommittee, thank you for the invitation to testify today. My name is Adam Hamm. I am the Commissioner of the Insurance Department for the state of North Dakota and I present today's testimony on behalf of the National Association of Insurance Commissioners (NAIC).[1] I am a Past President of the NAIC, and I have served as the Chair of the NAIC's Cybersecurity Task Force since its formation in 2014. On behalf of my fellow state insurance regulators, I appreciate the opportunity to offer our views and perspective on cybersecurity challenges facing our nation and the role cybersecurity insurance can play in risk management.

The Cyber Threat Landscape Creates Demand for Coverage

On one hand, threats to data privacy are not new for businesses, regulators, or the consumers we protect. Regulators and legislatures have required businesses to protect consumer data for decades. On the other hand, the modern size, scale, and methods of data collection, transmission, and storage all present new challenges. As society becomes more reliant on electronic communication and businesses collect and maintain ever more granular information about their customers in an effort to serve them better, the opportunity for bad actors to inflict damage on businesses and the public increases exponentially. Rather than walking into a bank, demanding bags of cash from a teller, and planning a speedy getaway, a modern thief can steal highly sensitive personal health and financial data with a few quick keystrokes or a well disguised phishing attack from the comfort of his basement couch. Nation states also place great value on acquiring data to either better understand or disrupt U.S. markets, and are dedicating tremendous resources to such efforts.

As these cyber threats continue to evolve, they will invariably affect consumers in all states and territories. State insurance regulators are keenly aware of the potential devastating effects cyber-attacks can have on businesses and consumers, and we have taken a number of steps to enhance data security expectations across the insurance sector, including at our own departments of insurance and at the NAIC. We also understand the pressure these increased risks are putting on other industries, creating unprecedented demand for products that allow purchasers to manage and mitigate some of their cybersecurity risks through insurance. Whether attacks come from nation states, terrorists, criminals, hacktivists, external opportunists or company insiders, with each announcement of a system failure leading to a significant business loss, awareness grows, and companies will seek additional coverage for security breaches, business interruptions, reputational damage, theft of digital assets, customer notifications, regulatory compliance costs, and many more liabilities that arise from doing business in the modern connected universe.

Most businesses carry and are familiar with their commercial insurance policies providing general liability coverage to protect the business from injury or property damage. What they may not realize is that most standard commercial lines policies do not cover many of the cyber risks

[1] The NAIC is the United States standard-setting and regulatory support organization created and governed by the chief insurance regulators from the 50 states, the District of Columbia, and five U.S. territories. Through the NAIC, we establish standards and best practices, conduct peer review, and coordinate our regulatory oversight. NAIC members, together with the central resources of the NAIC, form the national system of state-based insurance regulation in the U.S.

mentioned above. To cover these unique cyber risks through insurance, businesses need to purchase a special cybersecurity policy.

I want to urge some caution regarding the term "cybersecurity policy" because it can mean so many different things – while it is a useful short-hand for purposes of today's conversation, I want to remind the Committee that until we see more standardization in the marketplace, a "cybersecurity policy" will really be defined by what triggers the particular policy and what types of coverage may or may not be included depending on the purchaser and insurer. Commercial insurance policies are contracts between two or more parties, subject to a certain amount of customization, so if you've seen one cybersecurity policy, you've seen exactly one cybersecurity policy.

All these nuances mean securing a cybersecurity policy is not as simple as pulling something off the shelf and walking to the cash register. Insurers writing this coverage are justifiably interested in the risk-management techniques applied by the policyholder to protect its network and its assets. The more an insurer knows about a business's operations, structures, risks, history of cyber-attacks, and security culture, the better it will be able to design a product that meets the client's need and satisfies regulators.

Insurance Regulation in the U.S. – "Cops on the Beat"

The U.S. insurance industry has been well-regulated at the state level for nearly 150 years. Every state has an insurance commissioner responsible for regulating that state's insurance market, and commissioners have been coming together to coordinate and streamline their activities through the NAIC since 1871. The North Dakota Insurance Department, which I lead, was established in 1889 and employs approximately 50 full-time staff members to serve policyholders across our state. It is our job to license companies and agents that sell products in our state, as well as to enforce the state insurance code with the primary mission of ensuring solvency and protecting policyholders, claimants, and beneficiaries, while also fostering an effective and efficient marketplace for insurance products. The strength of our state-based system became especially evident during the financial crisis – while hundreds of banks failed and people were forced from their homes, less than 20 insurers became insolvent and even then, policyholders were paid when their claims came due.

Conceptually, insurance regulation in the United States is straightforward. Americans expect insurers to be financially solvent, and thus able to make good on the promises they have made. Americans also want insurers who treat policyholders and claimants fairly, paying claims when they come due. In practice, the regulation of an increasingly complex insurance industry facing constantly changing risks and developing new products to meet risk-transfer demand becomes challenging very quickly. The U.S. state-based insurance regulatory system is unique in that it relies on an extensive system of peer review, communication, and collaboration to produce checks and balances in our regulatory oversight of the market. This, in combination with our risk-focused approach to financial and market conduct regulation, forms the foundation of our system for all insurance products in the U.S., including the cybersecurity products we are here to discuss today.

Treasury Deputy Secretary Sarah Bloom Raskin stated at an NAIC/CSIS event last fall that "state insurance regulators are the cops on the beat when it comes to cybersecurity at insurance companies and the protection of sensitive information of applicants and policyholders." We take very seriously our responsibility to ensure the entities we regulate are both adequately protecting customer data and properly underwriting the products they sell, and we continue to convey the message to insurance company C-suites that cybersecurity is not an IT issue – it is an Enterprise Risk Management Issue, a Board of Directors issue, and ultimately a CEO issue.

Regulation of Cybersecurity Policies

Having discussed increasing demand for coverage, we can turn to the role my fellow insurance commissioners and I play as regulators of the product and its carriers. Let me start by putting you at ease: when it comes to regulation, cybersecurity policies are scrutinized just as rigorously as other insurance contracts. While they may be more complex than many existing coverages and new product language will present some novel issues, when insurers draft a cybersecurity policy, they are still required to file forms and rates subject to review by the state Department of Insurance. State insurance regulators review the language in the contracts to ensure they are reasonable and not contrary to state laws. We also review the pricing and evaluate the benefits we expect to find in such policies. State regulators also retain market conduct authorities with respect to examinations of these insurers and policies in order to protect policyholders by taking enforcement measures against bad actors.

Insurance regulation involves front-end, ongoing, and back-end monitoring of insurers, products, and insurance agents (or producers). The system's fundamental tenet is to protect policyholders by ensuring the solvency of the insurer and its ability to pay claims. Strict standards and keen financial oversight are critical components of our solvency framework. State regulators review insurers' material transactions for approval, restrict key activities, have explicit financial requirements, and monitor compliance and financial condition through various solvency surveillance and examination mechanisms, some of which we recently updated to incorporate cybersecurity controls. We can also take corrective action on insurers when necessary through a regulatory intervention process.

Financial Regulation

Financial regulation is focused on preventing, detecting, and resolving potentially troubled insurers. Insurance regulators carefully monitor insurers' capital, surplus, and transactions on an ongoing basis through financial analysis, reporting requirements, actuarial opinions, and cash flow testing. State insurance laws also restrict insurers' investments and impose capital and reserving requirements.

The monitoring of insurers is done through both on-site examinations and analysis of detailed periodic insurer reporting and disclosures. Insurers are required to prepare comprehensive financial statements using the NAIC's Statutory Accounting Principles (SAP). SAP utilizes the framework established by Generally Accepted Accounting Principles (GAAP), but unlike GAAP which is primarily designed to provide key information to investors of public companies and uses a going-concern concept, SAP is specifically designed to assist regulators in monitoring the solvency of an insurer. The NAIC's *Accounting Practices and Procedures Manual* includes the

entire codification of SAP and serves as the consistent baseline accounting requirement for all states. Each insurer's statutory financial statements are filed with the NAIC on a quarterly and annual basis and include a balance sheet, an income statement, and numerous required schedules and exhibits of additional detailed information.

The NAIC serves as the central repository for an insurer's financial statement data, including running automated prioritization indicators and sophisticated analysis techniques enabling regulators around the country to have access to national-level data without the redundancy of reproducing this resource in every state. This centralized data and analysis capability has been cited by the IMF as world leading.

Cybersecurity risk remains difficult for insurance underwriters to quantify due in large part to a lack of actuarial data. This has potential implications for ongoing regulation and the market for the product. If a product is priced too low, the insurer may not have the financial means to pay claims to the policyholder. If too high, few businesses and consumers can afford to purchase it, instead opting to effectively self-insure for cyber incidents, limiting the ability of the insurance sector to be used as a driver of best practices. Today, in the absence of such data, insurers compensate by pricing that relies on qualitative assessments of an applicant's risk management procedures and risk culture. As a result, policies for cyber risk tend to be more customized than policies for other risks, and, therefore, more costly. The type of business operation seeking coverage, the size and scope of operations, the number of customers, the presence on the web, the type of data collected, and how the data is stored will all be among the factors that dictate the scope and cost of cybersecurity coverage offered. From a regulatory perspective, though, we would like to see insurers couple these qualitative assessments with robust actuarial data based on actual incident experience.

Prior to writing the policy, the insurer will want to see the business' disaster response plan and evaluate it with respect to network risk management, websites, physical assets, intellectual property, and possibly even relationships with third-party vendors. The insurer will be keenly interested in how employees, contractors, and customers are able to access data systems, how they are trained, and who key data owners are. At a minimum, the insurer will want to know about the types of antivirus and anti-malware software the business is using, the frequency of system and software updates performed by the business, and the performance of the firewalls the business is using.

Examination Protocols and Recent Updates

Last year, the NAIC, through a joint project of the Cybersecurity Task Force and the IT Examination Working Group, undertook a complete review and update of existing IT examination standards for insurers. Prior to this year, regulatory reviews of an insurer's information technology involved a six step process for evaluating security controls under the COBIT 5 framework. Revisions for 2016 to further enhance examinations are based in part on the NIST framework "set of activities" to Identify, Protect, Detect, Respond, and Recover. Specific enhancements were made to the NAIC *Financial Examiner's Handbook* regarding reviews of insurer cybersecurity training and education programs, incident response plans, understanding cybersecurity roles and responsibilities, post-remediation analyses, consideration

of third party vendors, and how cybersecurity efforts are communicated to the Board of Directors.

Also evolving are regulators' expectations of insurance company C-suites – specifically Chief Risk Officers and Boards of Directors. Regulators expect improved incident response practice exercises, training, communication of cyber risks between the board and management, and incorporation of cyber security into the Enterprise Risk Management processes. There is now an expectation that members of an insurer's board of directors will be able to describe how the company monitors, assesses, and responds to information security risks.

Market Regulation

Market regulation is focused on legal and fair treatment of consumers by regulation of product rates, policy forms, marketing, underwriting, settlement, and producer licensing. Market conduct examinations occur on a routine basis, but also can be triggered by complaints against an insurer. These exams review producer licensing issues, complaints, types of products sold by insurers and producers, producer sales practices, compliance with filed rating plans, claims handling and other market-related aspects of an insurer's operation. When violations are found, the insurance department makes recommendations to improve the insurer's operations and to bring the company into compliance with state law. In addition, an insurer or insurance producer may be subject to civil penalties or license suspension or revocation. To the extent that we see any of these issues arising from claims made on cybersecurity policies, regulators will be able to address them promptly through our suite of market conduct tools, and enhancements made to the *Financial Examiner's Handbook* are expected to be incorporated into the *Market Conduct Examiner's Handbook* this year.

Surplus Lines

It is worth mentioning that some cybersecurity coverage is currently being written in the surplus lines markets. A surplus lines policy can be issued only in cases where the coverage cannot be found in traditional insurance markets because the coverage is unique or otherwise difficult to underwrite. Surplus lines insurers that are domiciled in a U.S. state are regulated by their state of domicile for financial solvency and market conduct. Surplus lines insurers domiciled outside the U.S. may apply for inclusion in the NAIC's Quarterly Listing of Alien Insurers. The carriers listed on the NAIC Quarterly Listing of Alien Insurers are subject to capital and surplus requirements, a requirement to maintain U.S. trust accounts, and character, trustworthiness and integrity requirements.

In addition, the insurance regulator of the state where the policyholder resides (the home state of the insured) has authority over the placement of the insurance by a surplus lines broker and enforces the requirements relating to the eligibility of the surplus lines carrier to write policies in that state. The insurance regulator can also potentially sanction the surplus lines broker, revoke their license, and hold them liable for the full amount of the policy.

Like any other insurance market, as the cybersecurity market grows and more companies offer coverage, we anticipate the regulation will continue to evolve to meet the size and breadth of the market as well as the needs of consumers. State insurance regulators have a long history of

carefully monitoring the emergence and innovation of new products and coverages, and tailoring regulation over time to ensure consumers are appropriately protected and policies are available.

Cybersecurity Insurance Market – New Reporting Requirements

As a still nascent market for coverage, accurately assessing exposure or the size of the cybersecurity insurance market is a work in progress. To date, the only analyses of the cybersecurity market come from industry surveys and estimates that consistently place the size of the market in the neighborhood of two to three billion dollars. In light of the uncertainty and many questions surrounding these products and the market, the NAIC developed the new *Cybersecurity and Identify Theft Coverage Supplement* for insurer financial statements to gather financial performance information about insurers writing cybersecurity coverage nationwide.

This mandatory new data supplement, to be attached to insurers' annual financial reports, requires that all insurance carriers writing either identity theft insurance or cybersecurity insurance report to the NAIC on their claims, premiums, losses, expenses, and in-force policies in these areas. The supplement requires separate reporting of both standalone policies and those that are part of a package policy. With this data, regulators will be able to more definitively report on the size of the market, and identify trends that will inform whether more tailored regulation is necessary. We will gladly submit a follow-up report to the Committee once we have received and analyzed the first batch of company filings, which are due April 1, and will keep all stakeholders apprised as we receive additional information. As with any new reporting requirement, we expect the terminology and reporting to mature over time as carriers better understand the specific information regulators need.

Having this data will enable regulators to better understand the existing cybersecurity market, and also help us know what to look for as the market continues to grow, particularly as we see small and mid-size carriers potentially writing these complex products.

NAIC Efforts Beyond Cybersecurity Insurance

The NAIC and state insurance regulators are also ramping up our efforts to tackle cybersecurity issues in the insurance sector well beyond cybersecurity insurance. We understand that the insurance industry is a particularly attractive target for hackers given the kind of data insurers and producers hold, and to that end we are engaged on a number of initiatives to reduce these risks.

The NAIC adopted twelve *Principles for Effective Cybersecurity: Insurance Regulatory Guidance* in April 2015. The principles set forth the framework through which regulators will evaluate efforts by insurers, producers, and other regulated entities to protect consumer information entrusted to them.

We also adopted an NAIC *Roadmap for Consumer Cybersecurity Protections* in December 2015 to describe protections the NAIC believes consumers should be entitled to from insurance companies and agents when these entities collect, maintain, and use personal information and to guide our ongoing efforts in developing formal regulatory guidance for insurance sector participants.

Most recently, on March 3rd, the Cybersecurity Task Force exposed its new *Insurance Data Security Model Law* for public comment – written comments should be submitted by Wednesday, March 23rd, and feedback will be discussed at the open meeting of the task force on April 4th in New Orleans. The purpose and intent of the model law is to establish the exclusive standards for data security, investigation, and notification of a breach applicable to insurance licensees. It lays out definitions and expectations for insurance information security, breach response, and the role of the regulator. Recognizing that one-size does not fit all, the model specifically allows for licensees to tailor their information security programs depending on the size, complexity, nature and scope of activities, and sensitivity of consumer information to be protected. Perhaps most importantly, the model is intended to create certainty and predictability for insurance consumers and licensees as they plan, protect information, and respond in the difficult time immediately following a breach. We welcome all stakeholders' input as we continue the model's development through the open and transparent NAIC process.

Related to the NAIC's new model, we are aware Congress is considering a number of Federal Data Breach bills. While Congress held its first hearings on data breaches 20 years ago, there has been no successful legislation on the issue. Meanwhile, 47 states have acted to varying degrees, and some are on the fourth iteration of data security and breach notification laws. Some of these bills, including S.961/HR 2205, the Data Security Act, would lessen existing consumer protections in the insurance sector and could undermine our ongoing and future efforts to respond to this very serious issue.

Coordinating with our Federal Colleagues

Lastly, we understand that state insurance regulators are not alone in any of our efforts. We work collaboratively with other financial regulators, Congress, and the Administration to identify specific threats and develop strategies to protect the U.S. financial infrastructure. State insurance regulators and NAIC staff are active members of the Treasury Department's Financial Banking and Information Infrastructure Committee (FBIIC), where I recently gave a presentation on insurance regulators' efforts in this space.

We are also members of the Cybersecurity Forum for Independent and Executive Branch Regulators, where we meet with White House officials and other regulators to discuss best practices and common regulatory approaches to cybersecurity challenges across very different sectors of the U.S. economy. While we certainly do not have all the answers yet, rest assured that regulators are communicating and collectively focused on improving cyber security posture across our sectors.

Current State of Play

I recently met with a group of insurance CEO's to discuss the NAIC's ongoing efforts in data and cybersecurity. Several baseball metaphors were used in the meeting, so when the discussion pivoted to cyber insurance, I asked how far along they felt that market was in its development. One CEO said it was only the top of the first inning, and the leadoff batter has just grabbed a bat from the rack before the first pitch has even been thrown – the rest of the room nodded in agreement. We are on the first leg of a long race when it comes to cybersecurity insurance.

There is no question that the expansion of cyber risks and the maturation of the cybersecurity insurance are a tremendous opportunity for the insurance sector to lead in the development of risk-reducing best practices and cyber-hygiene across our national infrastructure. Insurance has a long history of driving best practices and standardization by creating economic incentives through the pricing of products, and the underwriting process can test the risk management techniques and efficacy of a policyholder making a broader range of businesses secure. As insurers develop more sophisticated tools for underwriting and pricing, state regulators will continue to monitor and study cybersecurity products, always remembering that our fundamental commitment is to ensuring that policyholders are protected and treated fairly, and that insurance companies are able to pay claims when they come due.

Conclusion

As insurance markets evolve, state insurance regulators remain extensively engaged with all relevant stakeholders to promote an optimal regulatory framework—cybersecurity insurance is no exception. As the cybersecurity insurance market develops, we remain committed to effective regulation and to making changes when necessary. State insurance regulators will embrace new challenges posed by a dynamic cybersecurity insurance market and we continue to believe that well-regulated markets make for well-protected policyholders. Thank you again for the opportunity to be here on behalf of the NAIC, and I look forward to your questions.

Principles for Effective Cybersecurity: Insurance Regulatory Guidance[1]

Due to ever-increasing cybersecurity issues, it has become clear that it is vital for state insurance regulators to provide effective cybersecurity guidance regarding the protection of the insurance sector's data security and infrastructure. The insurance industry looks to state insurance regulators to aid in the identification of uniform standards, to promote accountability across the entire insurance sector, and to provide access to essential information. State insurance regulators look to the insurance industry to join forces in identifying risks and offering practical solutions. The guiding principles stated below are intended to establish insurance regulatory guidance that promotes these relationships and protects consumers.

Principle 1: State insurance regulators have a responsibility to ensure that personally identifiable consumer information held by insurers, producers and other regulated entities is protected from cybersecurity risks. Additionally, state insurance regulators should mandate that these entities have systems in place to alert consumers in a timely manner in the event of a cybersecurity breach. State insurance regulators should collaborate with insurers, insurance producers and the federal government to achieve a consistent, coordinated approach.

Principle 2: Confidential and/or personally identifiable consumer information data that is collected, stored and transferred inside or outside of an insurer's, insurance producer's or other regulated entity's network should be appropriately safeguarded.

Principle 3: State insurance regulators have a responsibility to protect information that is collected, stored and transferred inside or outside of an insurance department or at the NAIC. This information includes insurers' or insurance producers' confidential information, as well as personally identifiable consumer information. In the event of a breach, those affected should be alerted in a timely manner.

Principle 4: Cybersecurity regulatory guidance for insurers and insurance producers must be flexible, scalable, practical and consistent with nationally recognized efforts such as those embodied in the National Institute of Standards and Technology (NIST) framework.

Principle 5: Regulatory guidance must be risk-based and must consider the resources of the insurer or insurance producer, with the caveat that a minimum set of cybersecurity standards must be in place for all insurers and insurance producers that are physically connected to the Internet and/or other public data networks, regardless of size and scope of operations.

Principle 6: State insurance regulators should provide appropriate regulatory oversight, which includes, but is not limited to, conducting risk-based financial examinations and/or market conduct examinations regarding cybersecurity.

Principle 7: Planning for incident response by insurers, insurance producers, other regulated entities and state insurance regulators is an essential component to an effective cybersecurity program.

Principle 8: Insurers, insurance producers, other regulated entities and state insurance regulators should take appropriate steps to ensure that third parties and service providers have controls in place to protect personally identifiable information.

[1] These principles have been derived from the Securities Industry and Financial Markets Association's (SIFMA) "Principles for Effective Cybersecurity Regulatory Guidance."

Principle 9: Cybersecurity risks should be incorporated and addressed as part of an insurer's or an insurance producer's enterprise risk management (ERM) process. Cybersecurity transcends the information technology department and must include all facets of an organization.

Principle 10: Information technology internal audit findings that present a material risk to an insurer should be reviewed with the insurer's board of directors or appropriate committee thereof.

Principle 11: It is essential for insurers and insurance producers to use an information-sharing and analysis organization (ISAO) to share information and stay informed regarding emerging threats or vulnerabilities, as well as physical threat intelligence analysis and sharing.

Principle 12: Periodic and timely training, paired with an assessment, for employees of insurers and insurance producers, as well as other regulated entities and other third parties, regarding cybersecurity issues is essential.

W:\National Meetings\2015\Summer\TF\Cybersecurity\Guiding Principle Documents\Final Guiding Principles 4 16 15.docx

NAIC Roadmap for Cybersecurity Consumer Protections

This document describes the protections the NAIC believes consumers are entitled to from insurance companies, agents and other businesses when they collect, maintain and use your personal information, including what should happen in connection with a notice that your personal information has been involved in a data breach. Not all of these consumer protections are currently provided for under state law. This document functions as a Consumer Bill of Rights and will be incorporated into NAIC model laws and regulations. If you have questions about data security, a notice you receive about a data breach or other issues concerning your personal information in an insurance transaction, you should contact your state insurance department to determine your existing rights.

As an insurance consumer, you have the right to:

1. Know the types of personal information collected and stored by your insurance company, agent or any business it contracts with (such as marketers and data warehouses).
2. Expect insurance companies/agencies to have a privacy policy posted on their websites and available in hard copy, if you ask. The privacy policy should explain what personal information they collect, 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.
3. Expect your insurance company, agent or any business it contracts with to take reasonable steps to keep unauthorized persons from seeing, stealing or using your personal information.
4. Get a notice from your insurance company, agent or any business it contracts with if an unauthorized person has (or it seems likely he or she has) seen, stolen or used your personal information. This is called a *data breach*. This notice should:
   - Be sent in writing by first-class mail or by e-mail if you have agreed to that.
   - Be sent soon after a data breach and never more than 60 days after a data breach is discovered.
   - Describe the type of information involved in a data breach and the steps you can take to protect yourself from identity theft or fraud.
   - Describe the action(s) the insurance company, agent or business it contracts with has taken to keep your personal information safe.
   - Include contact information for the three nationwide credit bureaus.
   - Include contact information for the company or agent involved in a data breach.
5. Get at least one year of identity theft protection paid for by the company or agent involved in a data breach.
6. If someone steals your identity, you have a right to:
   - Put a 90-day initial fraud alert on your credit reports. (The first credit bureau you contact will alert the other two.)
   - Put a seven-year extended fraud alert on your credit reports.
   - Put a credit freeze on your credit report.
   - Get a free copy of your credit report from each credit bureau.
   - Get fraudulent information related to the data breach removed (or "blocked") from your credit reports.
   - Dispute fraudulent or wrong information on your credit reports.
   - Stop creditors and debt collectors from reporting fraudulent accounts related to the data breach.
   - Get copies of documents related to the identity theft.
   - Stop a debt collector from contacting you.

To learn more about the protections in your state or territory, contact your consumer protection office at *https://www.usa.gov/state-consumer* or your state or territory's insurance department at *www.naic.org/state_web_map.htm*.

Standard Definitions Under This Bill of Rights

Data Breach: When an unauthorized individual or organization sees, steals or uses sensitive, protected or confidential information—usually personal, financial and/or health information.

Credit Bureau (Consumer Reporting Agency): A business that prepares credit reports for a fee and provides those reports to consumers and businesses; its information sources are primarily other businesses.

Credit Freeze (Security Freeze): A way you can restrict access to your credit report and prevent anyone other than you from using your credit information.

Personal Information (Personally Identifiable Information): Any information about a consumer that an insurance company, its agents or any business it contracts with maintains that can be used to identify a consumer. Examples include:

- Full name.
- Social Security number.
- Date and place of birth.
- Mother's maiden name.
- Biometric records.
- Driver's license number.

Helpful Links:

"Credit Freeze FAQs" (Federal Trade Commission—FTC) – *www.consumer.ftc.gov/articles/0497-credit-freeze-faqs*

"Disputing Errors on Credit Reports" (FTC) – *www.consumer.ftc.gov/articles/0151-disputing-errors-credit-reports*

"Taking Charge: What to Do If Your Identity Is Stolen" (FTC, May 2012). Tri-fold brochure; online PDF; can order bulk copies at no cost – *https://bulkorder.ftc.gov/system/files/publications/pdf-0009-taking-charge.pdf*

"Know Your Rights" (FTC) – *https://www.identitytheft.gov/know-your-rights.html*

"What Is Identity Theft?" (video; FTC) – *www.consumer.ftc.gov/media/video-0023-what-identity-theft*

"When Information Is Lost or Exposed" (FTC) – *https://www.identitytheft.gov/info-lost-or-stolen.html*

State Consumer Protection Offices (USA.gov) – *www.usa.gov/directory/stateconsumer/index.shtml*

Directory of State Insurance Regulators (NAIC) *www.naic.org/state_web_map.htm*

World's Biggest Data Breaches (information is beautiful) – *www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/*