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[2] 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 cyber 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 improve 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 demands 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,

---

[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.

[2] Attachment A – NAIC Cybersecurity (EX) Task Force Membership List

reputational damage, theft of digital assets, customer notifications, regulatory compliance costs, and many more liabilities that may 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 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 facilitating 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. 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 other risk insurers take on, 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 insurance regulators' expectations of the C-Suite at insurers – 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*[3] 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.

---

[3] Attachment B.

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.[4] 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.[5]

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.[6] 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 4th iteration of data security and breach notification laws. Some of

---

[4] Attachment C.

[5] Attachment D.

[6] Attachment E.

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.