REINSURANCE ASSOCIATION OF AMERICA

STATEMENT

TESTIMONY
OF

ERIC CERNAK
VICE PRESIDENT, U.S. CYBER AND PRIVACY RISK PRACTICE LEADER
MUNICH RE AMERICA

FOR

THE REINSURANCE ASSOCIATION OF AMERICA

AND

PROPERTY CASUALTY INSURERS ASSOCIATION OF AMERICA

HOUSE SMALL BUSINESS COMMITTEE

HEARING ON

PROTECTING SMALL BUSINESSES FROM CYBER ATTACKS: THE CYBERSECURITY INSURANCE OPTION

July 26, 2017

1445 New York Avenue, NW
7th Floor
Washington, D.C. 20005
202/638-3690
www.reinsurance.org

Chairman Chabot, Ranking Member Velázquez, and members of the Committee, thank you for inviting me to testify. My name is Eric Cernak, and I am Vice President U.S. Cyber and Privacy Risk Practice Leader at Munich Re, US. Munich Re provides a range of reinsurance and insurance solutions through various companies that are part of the Group. In the U.S., Munich Re provides cyber- and privacy-related insurance for small businesses through Hartford Steam Boiler Group (HSB) headquartered in Hartford Connecticut. HSB has an A++ (Superior) financial strength rating from A.M. Best Company and has underwritten cyber reinsurance and insurance for over 12 years. Small business cyber insurance clients are served by over 1,500 HSB employees in our Hartford office and regional offices throughout the U.S.

I am testifying today on behalf of the Reinsurance Association of America (RAA) and the Property Casualty Insurers Association of America (PCI).

The RAA is the leading trade association of property and casualty reinsurers doing business in the United States. RAA membership is diverse, including reinsurance underwriters and intermediaries licensed in the U.S. and those that conduct business on a cross border basis. The RAA represents its members before state, federal and international bodies.

PCI is composed of nearly 1,000 member companies, representing the broadest cross section of insurers of any national trade association. PCI members write $202 billion in annual premium, 35 percent of the nation's property casualty insurance. Member companies write 42 percent of the U.S. automobile insurance market, 27 percent of the homeowners' market, 33 percent of the commercial property and liability market and 34 percent of the private workers' compensation market.

Today's hearing is an important discussion to highlight the success of the private sector in developing cyber insurance and to help raise awareness among the small business community about the option of securing cyber insurance, which can offer both preventative, risk-management tools and act as a critical safety net should a cyber event occur. My perspective today is from that of a reinsurer and insurer. Munich Re's Hartford Steam Boiler Group, as a reinsurer (insurance for insurers) for primary insurers, provides reinsurance to share in the risk of loss, helps primary insurers underwrite cyber risk and develop products, and provides other services to primary

insurers that are writing, for example, cyber insurance specifically for small businesses. HSB, as a primary insurer, also offers cyber insurance and services directly to customers (via brokers and agents).

ORIGIN AND DEVELOPMENT OF CYBER INSURANCE

Cyber is a rapidly evolving risk and reinsurers and insurers continue to develop products to meet the increasing demand and needs of the insureds, including small businesses. The magnitude of known attacks, development of new technologies and security measures to protect against such attacks are growing dynamically. As reported by Risk Management Solutions in its 2017 Cyber Risk Landscape Report, the number of large magnitude data exfiltration events has grown substantially in the years prior to 2016 (with 2016 showing some recent flattening of incident rates). To protect against these threats, companies are increasingly investing in their own cybersecurity systems. And, per the RMS report, global expenditure on cybersecurity is estimated to have grown 14 percent year-on-year, from $75B in 2015 to $86B in 2016.

According to a report published last month by Aon titled, "Global Cyber Market Overview, Uncovering the Hidden Opportunities," the global stand-alone cyber insurance market in 2016 was around $2.3 billion in premium, up from $1.7 in 2015, and the U.S. accounted for 90% of the 2015 market. The report noted that "the market is still believed to be in its infancy and penetration levels are still relatively low." It estimated that globally "over 75%" of certain large businesses but "less than 5%" of small and medium-sized businesses secured some cyber insurance. In the U.S., around 19% of small businesses secured some cyber insurance. Aon's report projected that the U.S. stand-alone cyber insurance market gross written premium will continue to grow at 30% per year and could more than triple from 2015 to 2020, from $1.5 billion to $5.6 billion.

More insurers have become interested in offering cyber insurance over time. Less than a dozen insurers offered some cyber insurance in the early 2000s compared to more than 70 in 2016. Reinsurance risk transfer options for insurers with regard to cyber may also become increasingly available. Aon's report mentioned another study by Aon Benfield that "estimates the 2015 global reinsurance market to be worth c. $525m in annual premium." Further, "more than 15 reinsurers actively write standalone cyber treaties and the number is increasing."

Most cyber insurance policies have their roots in liability coverage. Initially, these policies were considered "stand-alone," meaning the business needed to purchase the coverage separately from any other insurance, such as general liability, they might be purchasing, as these policies did not provide explicit coverage for cyber-related losses. The first cyber policies were often expensive, difficult to obtain, and required a relatively cumbersome and confusing application process. For these reasons, the initial success related to cyber policies came from the larger end of the market— Fortune 1000 companies—and provided limits generally ranging from $10M to $25M+.

Early on, many insurers required the applicant to submit to an external data system penetration test. The results of the test were then submitted as part of the insurance application. As cyber insurance became more prevalent, most insurers dropped the penetration test requirement and focused on the application. As the market has evolved, it is now possible for an insured to obtain up to $5M in coverage by answering as few as 4 – 20 questions.

As more attacks on larger businesses occurred and media coverage increased, smaller business began to take notice of the exposure. The insurance market responded by creating cyber insurance endorsements, which is simply an insurance product that is added to policies the small businesses were already purchasing, such as their business owners' policy or commercial property policy. Business owners' policies typically cover small business property and liability exposures in one simple insurance package, and commercial property policies typically cover the property exposures of larger businesses. A cyber insurance endorsement can cover various exposures not addressed by Businessowners' or Commercial Property policies by providing coverage for costs resulting from a breach of personal information, cyber extortion, transmission of a virus to another entity, breaching another entity's propriety information, etc. These endorsements afforded the insured a streamlined product and application process (generally an application is not needed for base limits), and lower premium for a commensurate limit (e.g. $100,000). Often these cyber endorsements could be automatically quoted without the insured ever completing an application — greatly simplifying the process.

With either the stand-alone cyber insurance policy or the endorsement approach, a significant part of the value proposition is the value-added loss prevention services that can be "bundled" into the policy to reduce the insureds' exposure. For example, a cyber insurance policy could include risk-management services such as vulnerability assessments, next generation firewalls, IT security audits, and intrusion detection/penetration testing. These were ranked as the top five most helpful services related to cyber insurance in a 2016 survey of small businesses conducted by Hartford Steam Boiler.

In that same survey, 36% of participants gave three reasons why they did not purchase cyber insurance. The number one reason given was that they claimed they did not need it. The second was the expense of coverage, and the third was that the process was too complicated and confusing. These results suggest that education is key to increasing the take-up rate of cyber insurance by small businesses, particularly given that 86% of the respondents stated that they store Personally Identifying or Personal Health Information.

HOW TO INCREASE THE TAKE-UP RATE OF CYBER INSURANCE BY SMALL BUSINESS

The small business objections to cyber insurance noted above, two of the three speak to the misunderstanding of the value proposition of cyber insurance relative to the exposure. Small businesses would benefit greatly from better understanding the risks presented to their operations by cyber-related exposures and the cyber insurance option to address those risks. Almost every business now relies upon at least one computer to conduct business, whether it is for accepting payments, designing parts, or servicing customers. It is important for small businesses to better understand their reliance upon technology and the impact to their operations should it not perform as expected due to a cyber event.

The public and private sectors have a role to play in helping businesses, small and large alike, to overcome the "it won't happen to me" mentality and constructively address cyber vulnerabilities while preparing for the aftermath of a cyber event. Cyber attacks may not be a matter of "if" but "when." It is essential for businesses, which are increasingly interconnected, to be prepared, protected, and resilient, and insurance can help with all three. Businesses are no longer being

attacked solely for the data they have but increasingly for the access to larger businesses with which they conduct business. This exposure is now being recognized by larger companies as they frequently require smaller business partners to carry cyber insurance as part of their contractual relationship.

In addition to education efforts, the insurance marketplace needs to continue to refine the process and coverage to reduce the complexity associated with purchasing cyber insurance. One significant challenge is that the terminology in a coverage form can vary greatly from insurer to insurer, thus making it harder for an applicant to understand what is covered in different policies. Last year, Munich Re's Hartford Steam Boiler Group participated in a Treasury-led project to develop a glossary of cyber insurance terms to help simplify and standardize cyber insurance terminology.

LIABILITY THAT MAY STILL BE PRESENT EVEN IF AN INSURED PURCHASES CYBER COVERAGE

As previously discussed, the terminology used in coverage forms can vary greatly from insurer to insurer, which makes understanding coverage difficult when a business is evaluating its needs.

Typical cyber-related coverages can include:

- Data Breach Response
- Data Breach Liability
- Computer attack
- Network Security Liability
- Media Liability
- Cyber Extortion
- Misdirected Payment Fraud (e.g. Business Email Compromise)
- Fines and penalties (may not be insurable in all jurisdictions)

Some cyber policies also are beginning to examine and/or address the exposure related to:

- Property and bodily injury resulting from a cyber event
- Failure of the Internet and the potential impact to business operations

However, the insured may still need to examine other policies for potential coverage for cyber-related exposures. These other polices may include:

- Crime
- Directors & Officers (which covers legal actions against top company executives)
- Contractual Liability (which protects a policyholder from liabilities assumed under a contract)
- Technology Errors & Omissions for exposures resulting from IT products the insured creates

MINIMUM SECURITY EXPECTATIONS FOR OBTAINING COVERAGE

Where an application is required for a cyber product, insurers may want to understand if the applicant complies with various security requirements (when applicable for the industry in question) such as the Payment Card Industry Data Security Standard (PCI-DSS), Health Information Technology for Economic and Clinical Health Act (HITECH), Gramm-Leach-Bliley Act (GLBA), Red Flag Rule, and Sarbanes-Oxley.

Additionally, from a technical perspective, many applications will inquire about encryption being deployed, systems patching cadence, back-up procedures, password management, firewalls installed, anti-malware software, intrusion detection/protection devices deployed, etc.

However, there is growing recognition that strengthening companies' security culture, embodied by various policies (privacy/security and document retention/destruction), criminal and credit checks conducted on employees, and robust training programs, deserves strong consideration as part of the underwriting process. This also is supported by the above-referenced Hartford Steam Boiler survey finding that nearly half (47%) of all data breaches were attributed to a vendor/contractor, followed by employee negligence or malfeasance (21%), and lost or stolen mobile device (20%). Hacking or other cyber-attack only represented 11% of data breaches.

By contrast, when no application is needed for an endorsement-based cyber product, often the form may contain language stating that the insured needs to comply with reasonable and industry-accepted protocols. These protocols may include:

- Providing and maintaining appropriate physical premises, computer, and Internet security
- Maintaining and updating at appropriate intervals backups of computer data
- Protecting transactions, such as processing credit card, debit card and check payments
- Appropriate disposal/destruction of files containing sensitive personal or corporate information/data

HOW INSURERS DETERMINE COVERAGE AND PRICE

Cyber insurance is unlike most other insurance coverages in four fundamental areas. Insurers are grappling with the following factors in offering cyber coverages and at what premium/limit.

There is no significant historical loss data.

The exposure is relatively nascent as the Internet has only been commercially viable since the late 1990's. Further, the loss data generated even 10 years ago does not fully represent the exposure today. For example, virtual currencies and smartphones did not exist 10 years ago.

Due to the lack of loss data, insurers have adapted pricing, terms, and conditions from other lines of business, such as technology errors and omissions, crime, media liability, etc. Some insurers also have looked to conduct primary research and have interviewed experts in various fields, including IT forensics, attorneys, breach response service providers, public relations firms, and others. Through this process insurers can better understand the frequency of events, how long events may take to address, and the associated costs for the various services. These figures are then converted into insurance premiums. As experience develops, these initial figures can be blended with the actual insurance claims results to refine the premiums being charged.

Another tool insurers have deployed to improve cyber insurance products and pricing is the survey of potential customers (e.g., business owners) to understand specific kinds of concerns, the

frequency of issues they face, and the costs to address them. This helps insurers prioritize which coverages to develop and include in a cyber insurance product and determine associated terms and pricing.

The cause of loss is generated by an active adversary, which is capable of changing tactics and targets to suit their needs based on advances of technology.

As new technologies are introduced, exposures that previously did not exist become commonplace. For example, cyber extortion was typically limited in scope to targeted attacks where the attacker threatened to release data that had been stolen or to continue with a Denial of Service attack unless a ransom was paid. These attacks took significant time to conduct and often posed a significant risk to the perpetrator as they needed to interact with the company to receive payment. With the advent of virtual currency, ransomware exploded and is now a leading cause of loss.

Legislative and regulatory requirements continuously evolve.

Insurance companies need to monitor the evolving state, federal, and international privacy and data protection laws. While these laws are designed to protect consumers, they may create an exposure to small business owners. For example, there are 48 different state breach notification/data protection laws with which a small (or large) business must comply. Many of the first cyber insurance policies focused solely on liability exposures of third parties (as opposed to those faced by the entity purchasing the coverage) and only provided a small sublimit (the maximum amount for which the insurance policy would pay for in the event of this type of loss, which is less than the overall limit of the policy) for costs the insured might incur complying with various breach notification laws. As more states followed California in the mid-2000's with their own breach notification laws, insurers responded by expanding their breach response coverages.

Cyber poses potential aggregation or accumulation risk for insurers.

Cyber risk is not bound by geography, which greatly increases the aggregation risk from an insurer's perspective.

Many insurers will identify potential causes of aggregation (e.g. particular industry, service providers, failure of the Internet, etc.) and either decide to exclude that cause of aggregation or to monitor the amount of insurance being provided very closely. For example, an insurer may monitor the number of insureds using a particular cloud service provider.

CONCLUSION

As the private cyber insurance market continues to rapidly expand, reinsurers and insurers will continue to monitor and analyze cyber risks, survey and work to better understand the needs of existing and potential customers, develop insurance products and services accordingly, and help insureds following a cyber event. It is equally, if not more important, to U.S. businesses for federal and state governments' lawmakers, regulators, and other entities focusing on cybersecurity and evaluating potential regulatory changes, to develop clear, consistent requirements and to avoid a patchwork of different requirements and standards. Such a patchwork would impede companies' ability to effectively implement cyber security protocols and respond quickly and appropriately to a cyber security event. Although the nature of reinsurance means that reinsurers do not directly interact with consumers, and therefore reinsurers' obligations in the event of cyber security events differs somewhat from the primary insurance industry, the entire insurance and reinsurance industry (as well as consumers) benefit from uniform, consistent standards that are both proportional and flexible enough to work in an ever-changing cyber environment.

We also encourage the Administration to coordinate cybersecurity policy among federal agencies and designate lead agencies to coordinate discussions where appropriate. This should include discussions with state insurance regulators to encourage healthy cyber standards while eliminating conflicts and duplicative regulation.

Thank you for your time and your interest in this very important issue.