Marsh & McLennan Companies, Inc.
1166 Avenue of the Americas
New York, NY 10036
212 345 5000
Fax 212 345 4808

Statement of

MATTHEW P. McCABE

Senior Vice President

Marsh, LLC

Before the Advisory Council
on Employee Welfare and Pension Benefit Plans

June 7, 2016

New York, New York

Introduction

Good morning Chairman Schmidtke, Vice Chairwoman Tretheway, and members of the Council. My name is Matthew McCabe, and I am a Senior Vice President at Marsh and an adviser in the field of cyber risk management. My testimony today will focus on defining the product of cyber insurance, explaining how it supports resiliency to defend against cyber threats, and how data analysis is helping to quantify the exposure. I am grateful for the opportunity to participate in this meeting.

Marsh & McLennan operates through four market-leading brands — Marsh, Guy Carpenter, Mercer and Oliver Wyman. Each organization provides advice to clients across an array of industries in the areas of risk, strategy and human capital. As the leading insurance broker in the world, Marsh has a unique perspective on the cyber insurance market. Marsh's role is to work with clients to analyze their risk exposures and, where appropriate, help our clients implement solutions to address and mitigate the financial impact of a cyber incident.

Cyber Insurance is a Vital Component of Risk Management

Over the past decade, we have witnessed an astonishing evolution of cyber risk. Companies have lost hundreds of millions of customer records containing personally identifiable information, suffered rampant pilfering of intellectual property and endured the theft of funds and sensitive financial information. Concern has also recently elevated for cyber threats against physical assets - including electric grids, dams, telecommunications networks, transportation systems and civilian nuclear facilities. However, breaches related to the confidentiality of data remains predominant.

The number of Marsh U.S.-based clients purchasing standalone cyber insurance increased 27% in 2015 compared with 2014. That followed a 32% increase of clients purchasing cyber insurance in 2014 over 2013, and a 21% increase from 2012 to 2013. This purchasing is supported by more than 50 carriers from around the world that potentially can provide more than $500 million in capacity. According to the *Betterly Report*, the total amount of annual gross written premium in the cyber market reached $2.75 billion in 2015. Experts have estimated that the market could grow to $10 billion in global premium by 2020. In short, the sharp increase in cyber insurance purchasing has increased rapidly and continues its growth as a vital part of risk-based cybersecurity management strategies.

Despite the large losses sustained in past years, there is no reason to believe the level of risk is abating. First, the attack surface for hackers to target data continues to expand. The mobility of data continues to increase, with individuals and institutions exchange data through various intermediaries and via mobile or cloud-based

environments. As the Council is aware, this is applicable for benefit plans, where administration of the plan requires information sharing among participants, third party administrators, actuaries, auditors, and trustees. Second, addressing the origin of the threat remains a challenge. Technically sophisticated actors have the opportunity to carry out attacks at a relatively low cost, and they do so repeatedly by frustrating attribution or enjoying the protection of a jurisdiction where the ability to extradite or prosecute bad actors remains evasive. This paradigm has produced in an epic crime wave, with enormous consequences for our clients.

At Marsh, we endeavor to help clients understand, evaluate and protect benefit plan data and assets from cybersecurity risks. Marsh & McLennan recently considered this challenge in a report titled "Cyber Resiliency in the Fourth Industrial Revolution", which it co-authored with FireEye and Hewlett Packard Enterprise. (*See* Appendix A.) As noted in the report, experts predict that the number of Internet-connected devices will eclipse 30 million by 2020. Realizing that this boom in connectivity must be met with a better approach for securing the systems, the authors considered the challenge of how the private sector can develop greater resiliency. Importantly, the approach to cyber solutions must by scalable. There is no "one size fits all." This is apparent in the context of ERISA, where benefit plans vary widely in size and complexity.

The report's conclusion was that cyber risk advisers must present for clients a unified approach for building cyber resiliency of these systems. This is a similar approach to how the NIST Framework presents a process for end-to-end assessment that is flexible and scalable to every client, including small and large plans, service providers and plan sponsors. Cyber risk advisers must coalesce into an integrated solution tailored to a specific organization. Each stage of cyber risk advising should inform and reinforce the others. Thus, cyber insurance should not be viewed as a stand-alone solution; it is instead a key component of cyber risk management around which experts can coalesce and which can provide strong market incentives to pursue greater security.

The Value of Cyber Insurance

Broadly stated, there are three core components of cyber insurance. First, cyber insurance will reimburse the costs that a company pays to respond to a cyber incident. These expenses may come in the form of complying with requirements to notify and protect affected individuals in the wake of a data breach; paying the expense to recreate corrupted or destroyed data; or even paying the demand of an extortionist. Second, cyber insurance covers the fees and damages that a company may pay in response to litigation resulting from a cyber incident. Third, cyber insurance reimburses revenues lost or expenses incurred due to a disruption related to a cyber incident.

However, the benefits of cyber insurance extend far beyond reimbursement for financial loss. Cyber insurance has evolved into a product that serves as a key touchpoint for an organization to assess its cyber practices and coordinate its incident response plan to cyber incidents. The Department of Commerce Internet Policy Task Force recently commented that cybersecurity insurance is potentially an "effective, market-driven way" of increasing cybersecurity in the private sector.

For demonstrative purposes, the benefits attached to cyber insurance can be explained in the context of the NIST Cybersecurity Framework by mapping the components of a policy to the five cybersecurity domains proposed in the Framework: assessment, prevention, detection, response and recover.

As a threshold matter, the very act of applying for insurance forces an assessment of the applicant's cyber practices. The underwriting process will scrutinize a company's technical defenses, incident response plan, procedures for patching software, policies for limiting access to data and systems, monitoring of the vendor network and more. The very act of applying for insurance is therefore an important risk mitigation tool. Further, carriers assess the applicant's security practices and provide premiums based on their interpretation. Thus, cyber insurance premiums provide an important incentive that drives behavioral change in the marketplace.

Once a cyber insurance program is implemented, the insured can avail themselves of services and solutions to further mitigate cyber risk and strengthen cyber hygiene. The insurance marketplace thereby enhances access to detection and mitigation solutions and the large network of vendors that provide threat intelligence, vulnerability scanning, system configuration analysis, and technology to block malicious signatures.

Most prominently, cyber insurance can support an organization's incident response plans. In the example of a data breach, most cyber insurance policies provide the services needed to respond to breaches, including forensics to determine what customer records have been compromised, legal analysis of the insured's responsibilities, notification to affected individuals, and credit monitoring and restoration to protect its customers. A well-executed response plan will actually reduce the overall cost of a data breach and avoid many of the problems that may later surface in resulting litigation or regulatory scrutiny. These services can be especially valuable for small- and mid- size enterprises that will require a cyber incident response plan, but lack the resources to implement one on their own.

Naturally, the market will differentiate sharply among applicants depending on how the company approaches the people, processes and technology that affect cybersecurity. That differentiation comes in the form of premium dollars. Pricing pressures drive insureds to adopt best practices.

Once a policy has been placed with an insurer, further incentives are created. The insurer is now motivated to help its policyholders either avoid entirely or, at least mitigate, the risk of a cyber breach. Accordingly, insurance companies provide access to experts and a suite of services that include monitoring for anomalous behavior and rapid response capabilities. These services include technical advice from on-call consultants, vulnerability detection to examine network servers, and assistance developing incident response plans.

Cyber Insurance is Innovating Tools to Evaluate Cyber Risk

As the Council is aware, the insurance industry is data-driven. There are both internal and external drivers for strong modeling to enable more accurate forecasting for the likelihood and severity of events. As a rule of thumb, better data leads to better decisions.

A strength of the cyber insurance industry is that the underwriting process generates data on threats, vulnerabilities and potential consequences for each applicant. Indeed, the cyber insurance industry has risen to become a leader in incident analysis for informing trends in cyber threats and correlate best practices with the amount of loss.

For long-standing risks, actuaries rely on decades of claim data to set premium rates and reserves. For emerging risks like cyber, insurers were required to develop new approaches and techniques to guide their underwriting practices.

The first is the more common "inside-out" approach that requires scrutiny of a company's policies, practices and potential vulnerabilities. An alternative and emerging strategy is an "outside-in" approach that relies on big data methodologies. Without stepping foot inside of a company's offices, the cyber resilience of a company can be assessed by analyzing hundreds of externally available data points. For example, are employees accessing the Internet using an outdated web browser that is more vulnerable to spyware, malware and viruses? Does the company share web-hosting platforms and cloud storage with other companies? What information can be gleaned about a company's IT operating systems from help wanted postings when a company is looking to fill a position in its IT department? Does any data from the company, including stolen passwords, appear in the "dark web"? How does the company's ranking of employee satisfaction correlate to the risk that a disaffected insider will compromise its data security? How strong is the motivation of a potential hacker to breach a particular company's network?

None of these data points is dispositive. Utilizing algorithms to analyze hundreds of these data points, however, can yield important insights about the relative vulnerability of an organization in comparison to other firms in particular industries.

Conclusion

As our nation continues to grapple with cyber risk for the foreseeable future, we believe our industry will serve as important contributors to enhancing our cyber resilience. The insurance industry is at the vanguard with the tools and metrics to help companies understand risk and prioritize investment. However, cyber insurance is one piece of a puzzle complex puzzle that require deep collaboration and persistent vigilance.

Thank you for allowing me to present this testimony. I am happy to take your questions.