MARSH & McLENNAN COMPANIES

Marsh & McLennan Companies, Inc.
1166 Avenue of the Americas
New York, NY 10036
+1 212 345 5000
Fax +1 212 345 4808

Testimony of

Peter J. Beshar

Executive Vice President and General Counsel

Marsh & McLennan Companies

Before the Presidential Commission on
Enhancing National Cybersecurity

May 16, 2016
New York, New York

Good morning Chairman Donilon, Vice Chairman Palmisano, and members of the Commission. I am Peter Beshar, the Executive Vice President and General Counsel of Marsh & McLennan Companies. I am grateful for the opportunity to participate in this important hearing about enhancing our national cybersecurity.

Marsh & McLennan operates through four market-leading brands — Marsh, Guy Carpenter, Mercer and Oliver Wyman. Our 60,000 employees provide 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.

I would like to focus my remarks this morning on three core points. First, what role can cyber insurance play in enhancing our nation's cyber resilience? Second, how can big data strategies be utilized to assess and mitigate cyber risk? Third, what specific strategies can be deployed by the business community to mitigate cyber risk against critical infrastructure?

The Need for A Public-Private Partnership

As cyber attacks in both the public and private sectors have shown, neither government nor business can solve this problem alone. Much of the focus in the past two years has been on data breaches involving credit cards at large retailers and social security numbers from health care companies.

As events earlier this year in Ukraine and elsewhere have shown, however, we are now confronting a stark new reality of threats against physical assets - including electric grids, dams, telecommunications networks, transportation systems and civilian nuclear facilities. Ubiquitous connections to the Internet have increased vulnerability in the industrial systems that control these physical assets. As the vast majority of critical infrastructure in this country is owned and operated by the private sector, it is vital that government and industry lock arms in confronting this risk.

We need a mindset that we are all in this together and that we are engaged in a race without a finish line.

Why is Cyber Insurance Important?

Throughout our nation's history, the insurance industry has played an important role in developing strategies to mitigate emerging risks. The underwriting process, by identifying a set of best practices across industries, creates important incentives that drive behavioral change in the marketplace.

A brief historical analogy. In 1730, a disastrous fire swept through the city of Philadelphia. Benjamin Franklin stepped into the fray and made it his mission to devise strategies to mitigate the risk posed by fire. Incredibly, Franklin introduced the first all-volunteer fire brigade and invented both the "Franklin" stove and, of course, the lightning rod.

Franklin then took another critical step that is less widely known. He founded the first insurance company in the colonies - the Philadelphia Contributorship. Anyone wishing to become a "subscriber" for insurance coverage had to embrace a specific set of best practices. An example was having an access point from the attic to the roof to reduce the risk of the roof catching on fire. For the first time, premium rates, rather than being uniform, were set relative to the risk posed by each property.

This combination of technological innovation and a defined set of best practices worked. Unlike other major cities of the era, Philadelphia did not suffer another catastrophic fire after 1730. Franklin had engaged in a textbook example of what we would today call "enterprise risk management."

So, what role can cyber insurance play to mitigate cyber risk? Broadly stated, there are three core types of cyber insurance.

The most basic coverage provides protection for out-of-pocket expenses that a company incurs directly in the wake of a cyber incident. Most commonly, these expenses include the cost to respond to a data breach, including notifying individuals, setting up call centers and providing credit monitoring. This may also include the cost of restoring data or paying "ransomware" demands that have recently plagued the healthcare industry.

Next, "business interruption" coverage protects a company if its computer network is disrupted for a defined period of time, typically at least 8 hours. With this coverage, a company can recover the actual harm it suffers in the form of lost profits or extra expenses. These first two forms of coverage are called first-party coverage.

The final form of coverage is for liability that could result if a third party, a client for example, is economically damaged as a result of the company's breach. This is called third-party coverage.

Why Does Cyber Insurance Matter?

If all that cyber insurance did was pass the risk of harm from one party to another, that would be helpful as a financial matter, but not significant as a policy matter.

Fortunately, the underwriting process creates a powerful set of economic incentives that drive behavioral change in the marketplace. That is the potential that cyber insurance offers.

First, the act of applying for insurance prompts the policyholder to take a number of constructive actions. Companies typically conduct a benchmarking analysis against an established industry standard, whether the NIST Framework, an ISO standard like 27001 or another proprietary system such as Marsh's Information Security and Privacy Self-Assessment.

The policyholder and oftentimes broker assess the company's cyber protocols. Has the enterprise identified its high value assets? Has it implemented two-factor authentication for remote access by employees and vendors? How robust are its software patch management protocols? Does the company have, and has it tested, its incident response plan?

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.

Given the barrage of cyber breaches in the headlines, these incentives are driving strong economic forces in the market. According to the Betterley 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.

The number of Marsh clients purchasing stand-alone cyber insurance increased by 27% in 2015 after an increase of more than 30% in 2014. In addition, companies are purchasing higher limits. Coverages, which formerly were in the tens of millions, are now climbing up to $500 million for companies in particularly vulnerable industries. Indeed, the average limit placed for large communications, media, and technology organizations is approaching $100 million.

Utilizing Big Data Strategies to Mitigate Cyber Risks

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

In a recent report entitled "Cyber Resilience in the Fourth Industrial Revolution" that Marsh & McLennan issued together with FireEye and Hewlett-Packard, we identified two core approaches that insurers are utilizing.

The first is the more common "inside-out" approach that involves hiring a forensic investigations firm to conduct an on-site assessment of a company's policies, practices and potential vulnerabilities. Experts conduct "penetration" tests and compromise assessments to probe the resilience of a company's security protocols.

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 on Glassdoor 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.

So, data is critical.

We urge the Commission to recommend that the government engage the finest minds in the tech community to expand the use of big data strategies. In addition, the vision articulated in the Cybersecurity Act of 2015 to create a real-time information sharing platform of cyber threat indicators needs to be made operational.

The Emerging Threat Against Critical Infrastructure

The escalation in the sophistication and potential severity of cyber threats has been stunning. Data breaches relating to credit cards, social security numbers and personal health records have proven to be only the tip of the iceberg. The emerging, and far more troubling, threat is that posed to our nation's critical infrastructure.

The members of this Commission will be all too familiar with recent attacks on critical infrastructure including the German iron plant and the Bowman dam in New York. The attack on the Ukrainian power grid earlier this year represents a significant escalation in that threat. Lloyd's of London conducted an important review of the potential vulnerability of the power grid in the US and concluded that a significant attack on the northeast grid could cause up to $1 trillion in damages. As a measure of comparison, the tsunami in Japan caused approximately $350 billion in economic damages.

We are growing increasingly concerned about the risk that cyber presents to the operations of large corporations across the US and urge this Commission to make protecting our nation's critical infrastructure a key priority.

Given this threat landscape, we recommend that the Commission improve national cyber resilience by facilitating broader use of the SAFETY Act. Adopted in the wake of the attacks on 9/11, the SAFETY Act has played an important role in encouraging companies to develop innovative anti-terrorism technologies. Under the SAFETY Act, a company submits a specific technology, either a product or service, designed for anti-terrorism purposes to DHS. Upon finding that the product has the potential to be effective, DHS grants SAFETY Act protection which limits the legal damages that may result from a failure of the technology. This process encourages innovation while also shielding an organization from catastrophic liability.

Our country now confronts a growing threat of cyber terrorism. In its current form, the SAFETY Act can help companies manage their cyber risk. Power and water utilities, chemical plants and telecommunications providers can mitigate their exposure by submitting their information security protocols and controls for SAFETY Act approval. The SAFETY Act offers particular promise in the area of new technologies for network monitoring.

At present, application of the Act can only be triggered by a declaration by the Secretary of DHS that an act of terrorism has occurred. As there are political ramifications of any declaration of an act of terrorism as well as policy implications under the Terrorism Risk Insurance Act, this requirement might prove unduly limiting in practice. Moreover, particularly in the realm of cyber terrorism, the issue of attribution can be exceedingly complex. Accordingly, we recommend that the Commission consider mechanisms to broaden the application of the SAFETY Act where there is widespread damage to critical infrastructure.

If necessary, a congressional amendment to the SAFETY Act would expand application, subject to legislatively set thresholds, for cyber attacks that threaten material harm to the US economy or national security.

This type of action would likely foster greater collaboration between government and industry. Those industries that own and operate critical infrastructure would have a financial interest in collaborating with security experts on what controls are expected. In turn, government would have greater visibility into an arena where it relies on voluntary collaboration because regulatory authority is more limited.

Here again, the insurance industry could potentially play a constructive role. The SAFETY Act requires DHS to set the limit of liability for each applicant based on the amount of insurance available and the burden to purchase coverage up to that limit. Modeling and analysis performed within the insurance industry can help guide these determinations.

As a whole, the process could lead to companies implementing stronger controls while establishing greater financial certainty in the face of catastrophic risk. Both serve the ultimate goal of building cyber resilience in the private sector.

Conclusion

The federal government has taken a leading role in cybersecurity. The NIST Cybersecurity Framework in early 2014, the Cybersecurity Act of 2015 and now this Commission point to the Administration's commitment to bolster our country's cyber resilience.

Cyber insurance in particular and the insurance industry in general have the potential, in our judgment, to serve as important contributors to enhancing our cyber resilience.

I look forward to answering any questions you might have.