



Peter J. Beshar
Executive Vice President
and General Counsel

Marsh & McLennan Companies, Inc.
1166 Avenue of the Americas
New York, NY 10036
212 345 1071 Fax: 212 345 1074
peter.beshar@mmc.com

September 9, 2016

Attention:
Nakia Grayson
National Institute of Standards and Technology 100 Bureau Drive
Stop 2000
Gaithersburg, Maryland 20899

Dear Chairman Donilon, Vice Chairman Palmisano and Members of the Commission:

On behalf of Marsh & McLennan Companies, I wanted to thank you for the opportunity to testify before the President's Commission on Enhancing National Cybersecurity on May 16, 2016 and commend you for the professionalism and rigor that you have brought to this critical endeavor. Though sobering to fathom, the threat posed by cyber will be even graver for the next Administration than it has been for this Administration.

It is our hope that an overarching principle for the Commission's recommendations will be the importance of bringing government and industry closer together in this fight. As recent attacks have shown, no organization is immune. Not government. Not industry. Not even the not-for-profit sector. We are all in this together. Accordingly, we must find opportunities to collaborate, share threat information and forge stronger alliances and a more trusting relationship between the private and public sectors. My colleagues and I respectfully believe that the business community, keenly aware of its own vulnerabilities, is eager to step up and embrace this challenge.

I want to focus this submission on the actions that the insurance industry can take to strengthen this partnership. As a starting point, our industry is no different than other sectors of the business community. We are being confronted with daily attacks from malicious hackers interfering with critical systems and data.

In our judgment, there are three specific areas where the Commission can leverage the insurance industry, and market incentives, to bolster our national cyber resilience: (1) harness the power of cyber insurance to promote the adoption of best practices, (2) extend the SAFETY Act to cover cyber protocols; and (3) clarify TRIPRA's application to cyber terrorism.

Broaden the Adoption of Best Practices Through Cyber Insurance

We were heartened that the Commission, from the outset of its work, expressed interest in the potential role of cyber insurance. If all cyber insurance did was to transfer risk from one party to another, that would be helpful as a financial matter, but not significant as a policy matter. Cyber insurance contributes to resilience, however, because the underwriting process creates a set of incentives that drive behavioral change in the marketplace. The simple act of applying for insurance prompts the policyholder, whether a multinational company or a small business, to conduct an assessment of its vulnerabilities against an established industry benchmark. In this regard, the Administration made a significant contribution by developing, in consultation with the private sector, the NIST Framework.

The NIST Framework and other benchmarks prompt companies to confront a number of, at times, uncomfortable questions. For example, has the enterprise identified its high value assets or “crown jewels”? Has a process been established for patching software with known vulnerabilities? Has two-factor authentication been implemented for remote access for at least employees and vendors? And, importantly, does the company have, and has it tested, an incident response plan? Underwriters naturally prefer, and provide preferential pricing to, companies that implement best practices around cyber protocols.

Once an insurer underwrites the risk, further incentives are created. The insurance carrier then has every incentive to help its policyholders avoid, or at least mitigate, the potential harm of a cyber attack. Accordingly, insurers have begun to provide policyholders with access to experts and a suite of services that including monitoring and rapid response.

If the Commission accepts the premise that cyber insurance can play an important role in expanding the adoption of best practices, there are a number of potential tools that are available to encourage broader adoption of cyber insurance. Examples include utilizing the government’s procurement power by mandating that vendors bidding for government contracts maintain minimum levels of cyber coverage and signaling in public pronouncements, as the Treasury Department has done, that cyber insurance is one element that companies should consider as part of a holistic risk mitigation strategy.

In addition, the next Administration could support further development of the Cyber Incident Data Repository proposed by the Department of Homeland Security. In the wake of the passage of the Cybersecurity Information Sharing Act in late 2015, DHS has a vital role to play in aggregating, distilling and then disseminating cyber threat intelligence. Insurance claims filed by companies in the aftermath of cyber attacks are an important data source to model the financial impact of cyber incidents and implement risk-based cyber strategies.

Expand the SAFETY Act to Cover Cyber Protocols

There are other important levers that the Commission can utilize to drive market behavior. A powerful example involves the Support Anti-Terrorism by Fostering Effective Technologies Act of 2002 ("SAFETY Act"). Adopted in the wake of the attacks on September 11, 2001, the SAFETY Act has played an important role in encouraging companies to develop and promote 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 or service has the potential to be effective, DHS grants SAFETY Act protection, which limits the sponsoring company's liability arising from a failure of its technology. Institutions like the New York Stock Exchange, the New York Yankees and the Green Bay Packers have been granted SAFETY Act protection because of the security measures they have adopted.

As our nation confronts a growing threat of cyber terrorism, the SAFETY Act, in its current form, can help companies mitigate their cyber terrorism risk. DHS has already taken initial steps to apply the SAFETY Act to cyber technologies, involving assessment, network monitoring and anomaly detection.

Yet, the SAFETY Act can be put to even greater use. A comprehensive risk mitigation strategy involves people, process and technology. Beyond covering solely new cyber technologies, the SAFETY Act could be applied more broadly to the people and process elements of cyber protocols. Companies that own and operate critical infrastructure, including power and water utilities, chemical plants, civilian nuclear facilities, dam operators and telecommunication providers, should be encouraged to submit their information security protocols and controls for SAFETY Act approval. These and other industries would have a financial incentive to collaborate with security experts, including at DHS, on what controls are considered industry leading. Several sector specific regulators, including FERC, have issued guidance on industry best practices that could serve as the basis for SAFETY Act evaluation.

Here again, the insurance industry could 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 in that amount. Modeling and analysis performed within the insurance industry can help guide these determinations. As a whole, the process could induce companies in critical sectors to implement stronger controls in return for greater financial certainty in the face of catastrophic risk. Both serve the ultimate goal of building cyber resilience in the private sector.

Clarify the Application of the Terrorism Risk Insurance Program Reauthorization Act of 2015 (TRIPRA) to Cyber Terrorism.

In the wake of the terror attacks of September 11th, the Terrorism Risk Insurance Act of 2002 provided crucial stability to the market for terrorism insurance. The availability of this coverage, which explicitly extends to losses occurring under property and casualty insurance, was crucial to enabling the aviation industry among others to recover. When TRIA was first passed, the threat posed by cyber was limited at best and cyber insurance was at a nascent stage. The subsequent reauthorizations of TRIA, including the passage of the Terrorism Risk Insurance Program Reauthorization Act of 2015 (TRIPRA), remained essentially silent on the question of how the program would respond to a large scale cyber terrorist attack.

As recognized by the Commission, cybersecurity is an increasingly systemic risk where an attack against one industry may create a cascading impact across the entire economy without necessarily causing physical damages. The reliance of critical infrastructure upon digital architecture has been demonstrated by the recent cyber attack against the Ukrainian power utilities. Indeed, Lloyd's has estimated that a large-scale attack on the power grid in the northeast of the United States could cause up to \$1 trillion in economic loss. Moreover, the risk of cyber terrorism extends far beyond the electric grid.

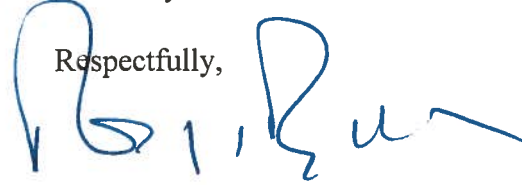
In our judgment, a cyber terrorism event that meets TRIPRA's prerequisites – including being certified as terrorism by the Secretary of the Treasury – should be eligible for coverage under TRIPRA. In this regard, it would be helpful for the Department of Treasury to provide a statement that it interprets TRIPRA to include network interruption losses caused by acts of cyber terrorism. We note that Senator Reed expressed his view in the deliberations over the reauthorization of TRIPRA that cyberattacks “would continue to fall within the scope of TRIA's covered lines, as they do today, provided that the statutory prerequisites are met.”¹

¹ See S. Rept. 113-199 - Terrorism Risk Insurance Program Reauthorization Act of 2014, 113th Congress (2013-2014) (<https://www.congress.gov/congressional-report/113th-congress/senate-report/199/1>)

Conclusion

We are engaged in a race without a finish line and fully expect that the threat posed by cyber will only intensify and broaden, including to the Internet of Things, in the coming years. Accordingly, we need to forge a greater partnership between government and industry and leverage our respective areas of expertise to respond to this dynamic threat.

Respectfully,



Peter J. Beshar