MarshMcLennan

Marsh McLennan
1050 Connecticut Avenue, NW Ste 700
Washington, DC 20036
marshmclennan.com

Testimony of

Matt McCabe
Managing Director, Cyber Center of Excellence
Guy Carpenter

Before the

United States House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity and Infrastructure Protection

Sector Down: Ensuring Critical Infrastructure Resilience

June 27, 2024

Marsh McLennan

Marsh McLennan is the world's leading professional services firm in the areas of risk, strategy, and people. Our more than 85,000 colleagues advise clients in 130 countries. We work with corporate and public sector clients to navigate complex challenges through four market-leading businesses — Marsh, Guy Carpenter, Mercer, and Oliver Wyman.

These challenges include developing strategies for clients of all sizes and across all of industry to mitigate cyber risk. Marsh McLennan introduced some of the very first insurance policies that addressed data privacy and cybersecurity risks, and we remain leaders in that business today.

We appreciate the opportunity to share our perspective on the cyber threat to critical infrastructure, how cyber insurance works to mitigate that risk and enhance resilience, and potential government solutions that harness the mechanism of cyber insurance.

Executive summary

The responsibility for building cyber resilience in the infrastructure sector is shared among its owners, the insurance industry, and government.

Cyber threats to critical infrastructure

There is an ongoing threat of cyberattack against US critical infrastructure — financial institutions, communications providers, healthcare, energy, transportation, and water utilities infrastructure — including from activity sponsored by nation-states and others.

- The FBI's Internet Crime Complaint Center (IC3) received nearly 1,200 complaints in 2023 from the critical infrastructure sector regarding ransomware attacks, a persistent and growing threat across all industries.
- In 2023, Marsh McLennan received more insurance claims related to ransomware than in any prior year.

Cyber insurance helps build organizational resilience

Over time, insurance has proven effective at turning potentially ruinous risks into manageable components — whether it's responding to natural catastrophes, cyberattacks, or the broad range of other risks.

- Cyber risk ranks among the top threats facing companies today, requiring vigilance and continuous monitoring in order to build resilience.

- Cyber insurance is a critical tool in managing the financial risk associated with cyber risk.
- Insurance underwriting contributes to organizational readiness for cyberattacks by, among other benefits, acting as an annual assessment of cyber risk preparedness.
- Marsh McLennan's Cyber Risk Intelligence Center provides data-driven analyses to help companies identify where to invest in effective cyber risk management.

The cyber insurance protection gap

The potential damage to US critical infrastructure from an attack or other major event has the potential to produce financial losses beyond the insurance industry's ability to accept. The cyber protection gap is difficult to quantify; some estimates put the global gap as high as $900 billion.

Establishing a public-private partnership

There is increasing discussion regarding the role a public-private partnership (PPP) might play in managing the cyber risk protection gap. Doing so would not be without precedent as other risks — including nuclear, terrorism, and flood — have established PPPs.

Cyber threats to critical infrastructure

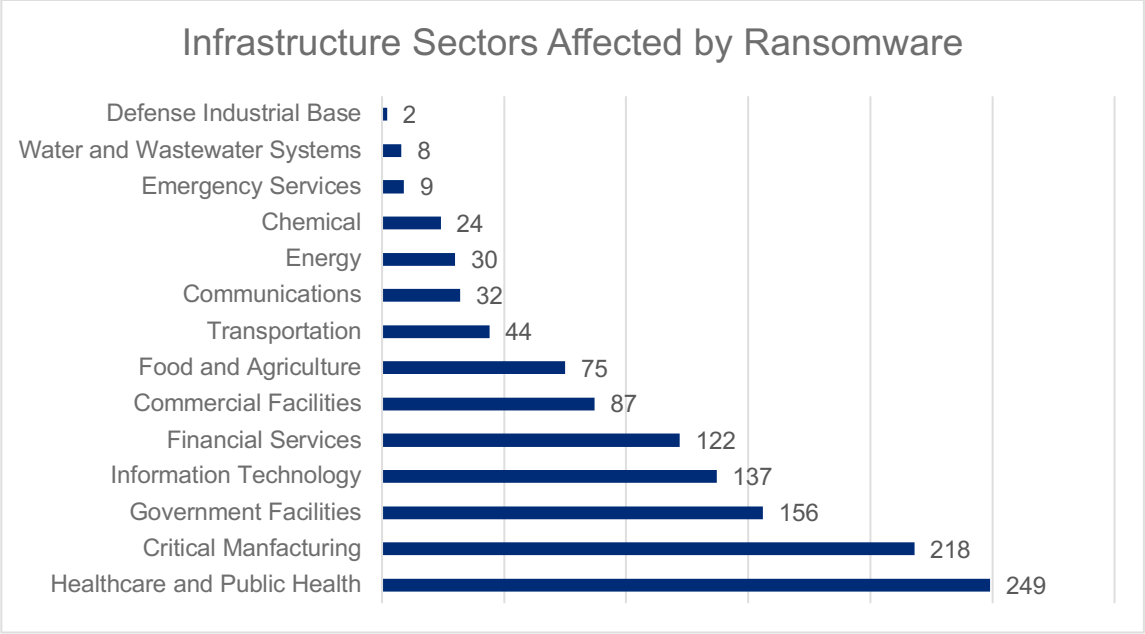
There is a clear and present cyber threat against the US companies that own and operate critical infrastructure. US officials acknowledged the threat in a recent Joint Cybersecurity Advisory that warned operators of critical infrastructure that nation-state cyber threat actors had already compromised their cyber defenses and were "pre-positioning themselves on IT networks to enable lateral movement to [operational technology] assets to disrupt functions." The report, whose authors included the Cybersecurity & Infrastructure Security Agency (CISA), the FBI and the National Security Agency (NSA), noted that nation-state cyber threat actors targeted multiple critical infrastructure organizations — in areas including healthcare, communications providers, energy, transportation, and water utilities — throughout the United States and its territories.

In its annual report on industrial controls systems, the cybersecurity company Dragos found that ransomware remains the number one cyber threat. Dragos observed 50 active ransomware groups impacting industrial organizations in 2023 and tracked 905 reported ransomware incidents impacting industrial organizations in 2023.

Also in 2023, the FBI's Internet Crime Complaint Center (IC3) received 1,193 complaints from organizations belonging to critical infrastructure sectors that were affected by a ransomware attack. Although ransomware represented less than 20% of claims reported to Marsh in the US in 2023, the

number of Marsh clients reporting cyber extortion events in 2023 was the highest annual level to date. It remains a top concern for our clients given its increased frequency, sophistication, and potential severity.

On a positive note, the percentage of companies paying ransom demands continued to decline, signaling that organizations are growing more resilient to ransomware threats.



Source: FBI IC3 Report 2023

In some instances, cyber operations against critical infrastructure threaten cyber physical systems, where there is the potential for kinetic consequences including machinery breakdown, pipeline leakage, train derailment, and disruption of the global supply chain. Today, the risk of disrupting cyber physical systems has grown more acute through the Internet of Things (IoT), which connects cyber physical systems to the internet, as well as the increasing standardization of technologies that makes industrial control systems more easily recognizable to adversaries.

Cyber insurance helps organizations build resilience

Industry and government face an unrelenting barrage of cyber threats. As a result, cyber risk ranks as one of the leading challenges facing organizations today, as seen in analyses such as is found in the annual *Global Risks Report* from the World Economic Forum, to which Marsh McLennan is a key contributor. Despite the resources invested, cybersecurity remains a dynamic and evolving risk that requires continuous management in order to build organizational resilience.

Cyber insurance has become an essential component of cyber risk management, as it fulfills the critical role of helping organizations manage capital through the transfer of financial risk for potential cyber incidents. Cyber insurance can also play a key role in bolstering cyber resilience.

Underwriting for cyber insurance serves as an annual assessment of an organization's cyber hygiene. Those insureds that do not demonstrate effective technology, practices, and procedures to mitigate cyber risk typically will receive "feedback" in the form of higher policy premiums and/or less favorable terms and conditions. Cyber insurance underwriting has grown increasingly demanding as insurers seek a fuller understanding of their potential exposures and how individual risks might aggregate and impact their overall portfolios.

Marsh McLennan has established the Cyber Risk Intelligence Center, which provides leading solutions for cyber analytics and modelling. For example, the center has undertaken focused research on the prioritization of cyber risk controls. Its research evaluated controls including endpoint detection and response (EDR), multifactor authentication (MFA), and privileged access management (PAM) and provided a weighted scoping for each control's effectiveness, which can help businesses decide where to prioritize their cybersecurity investments.

Cyber insurance supports many vital aspects of cybersecurity. For example, cyber insurers typically provide risk engineering services to insureds, and some will provide active threat detection monitoring. Cyber insurance has also introduced incident response planning services to thousands of companies. This aspect is especially valuable for small and midsize businesses. Insurers have helped these

organizations navigate through numerous ransomware events and data breaches. Lastly, the financial risk transfer provided by insurance will support companies in their recovery from cyber events.

For these reasons, insurance is an increasingly vital component of cyber risk management, although uptake varies by company size — 47% of Marsh clients with annual revenues greater than $1 billion purchase cyber insurance, compared to 34% of clients with annual revenues below $1 billion.

The cyber insurance protection gap

The potential impact from some cyber events — whether due to an attack by a nation-state or other cause — could disable and disrupt some of the most critical US infrastructure to such an extent and at such a cost that the insurance industry alone could not accept the risk. By definition, such an event could have a global economic impact and overwhelm the cyber insurance marketplace, individual insurers, and others.

It is difficult to quantify the delta between the ceiling for a catastrophic cyber event and the current limits of insurance coverage, but the Global Federation of Insurance Associations estimates that this protection gap may be as high as $900 billion. Such gaps primarily represent two categories: underinsured losses and uninsurable losses.

Underinsured losses: Global cyber insurance premium today is approximately $15 billion, which is roughly three times the size of the cyber insurance market five years ago. In comparison, Marsh McLennan projects a catastrophic global event loss at the once-in-200 years level would range between $15.6 billion and $33.4 billion. These figures indicate that the cyber insurance market remains in an early stage, with insurers carefully managing limits to avoid large losses from catastrophic cyber events. As a result, large organizations with significant risks may struggle to purchase sufficient limits to offset their potential exposure.

Uninsurable losses: Like other insurance lines, cyber coverage will exclude events that could result in large losses that cannot be easily modeled. The most prominent examples of this are exclusions for failure of critical infrastructure and losses arising from cyber operations supporting acts of war or hostilities. If a large cyber event meets the thresholds of these exclusions, then losses would be fully borne by the insured.

A public-private partnership to address the cyber protection gap

There are now discussions regarding the potential benefits of a public-private partnership (PPP) for catastrophic cyber risk, where the government would become the reinsurer of last resort if a cyber event resulted in losses deemed too large for the insurance industry to absorb. Such a partnership would

reduce the cyber protection gap and incentivize providers of capital to share in the risk because it would limit the ceiling of exposure.

A federal framework to address catastrophic cyber risk would respond to a gap in a manner that could only be fulfilled by the US government. As last year's National Cybersecurity Strategy recognized: "When catastrophic incidents occur, it is a government responsibility to stabilize the economy and provide certainty in uncertain times … Structuring that response before a catastrophic event occurs — rather than rushing to develop an aid package after the fact — could provide certainty to markets and make the nation more resilient."

Precedent exists for the government to undertake this role. Current risk-sharing mechanisms include the Price Anderson Act of 1957 for providers of nuclear power; the National Flood Insurance Program (NFIP); and the Terrorism Risk Insurance Program (TRIP), established following the attacks of September 11, 2001. The establishment of a federal framework to address the cyber coverage gap would be a natural evolution of the government's role. Without discussion and planning today about the government's role in a catastrophic cyber event, there would, in all likelihood, be a period of confusion to determine how to meet the need when such a crisis occurs. Therefore, we believe the time is now to have that conversation.

Conclusion

We appreciate the Homeland Security Committee dedicating a hearing to this important matter, and we encourage the Committee to hear from critical infrastructure owners and operators to better understand their cyber risk.

If we start preparing now, we can bend the risk curve for catastrophic cyber events. Insurance creates the right economic incentives to drive change in society. Analyzing this issue now, and leveraging the benefits of risk management, will help to build a more resilient US economy.

Appendix

Ransomware: A persistent challenge in cyber claims

Understanding cyber claims trends helps to inform an effective risk management strategy for one of the signature risks in today's tech-driven society.

Analysis of the 1,800+ cyber claims submitted to Marsh in the US and Canada in 2023 reveals the following:

- 21% of clients that purchased a cyber policy reported an event in 2023, consistent with the percentage over the past five years.
- In 2023, events were driven by factors including increased sophistication of cyberattacks; the MOVEit event, highlighting supply chain vulnerabilities; and privacy claims.
- Healthcare, communications, retail/wholesale, financial institutions, and education remain in the top five of most affected industry sectors.
- Ransomware represented less than 20% of claims reported, but remained a top concern for organizations given their increased frequency, sophistication, and potential severity.
- In managing claims, it's important to follow proper procedures, including notifying insurers, brokers, and other stakeholders and maintaining proper documentation.
- Organizations' cyber resilience strategy should incorporate a view of cyber risk across the enterprise, including its potential economic and operational impact and taking account of cybersecurity at vendors and other third parties.

Solving the cyber risk financial dilemma

The average cost of a data breach globally was US $4.45 million in 2023, increasing by 15% over a three-year period. The average cost of a data breach in the US was more than double, at US $9.48 million.

Today's digital-dependent world consists of unrelenting cyber threats. At the same time, macroeconomic conditions may place senior leaders under enormous pressure to reduce risk while managing constricted budgets. This can lead to senior leaders considering whether to invest in cybersecurity controls or purchase cyber coverage.

Instead of an either-or choice, organizations should strike a balance through a two-pronged approach to financially prudent cyber resiliency. This consists of investing in cybersecurity controls while purchasing insurance that aligns with risk tolerance to cover losses following a potential cyber incident.

To help make objective, informed decisions, senior leaders should consider the following questions.

- What are my contractual requirements?
- How much would a cyber incident cost my organization?
- What does cyber insurance cover?
- How much does cyber insurance cost?
- Is the cyber insurance application too time-consuming?

Public-private partnership examples

Significant loss events or changes in how risks are modeled can lead to market-wide capacity withdrawal.	TRIA was passed in 2002 following a widespread withdrawal of commercial terrorism cover by reinsurers after the September 11, 2001, terrorist attacks. Flood Re was developed to provide affordable flood risk cover to the approximately 3% of UK homeowners living in high flood risk areas. Industrywide Improvements in flood risk modeling had made coverage unaffordable for this cohort.
Extreme risks typically require some form of government backstop.	Government treasuries are the Insurer of last resort on multiple loss sharing schemes. For example, the US National Flood Insurance Program (NFIP), the UK's Pool Re, and France's CCR Cat Nat and Gestion de l'Asurance et de la Reassurance des risques Attentats et actes de Terrorisme (GAREAT) have unlimited guarantees. TRIA, the Australian Reinsurance Pool Corporation (ARPC), Germany's Extremus, and the Netherlands' Nederlandse Herverzekeringsmaatschappi| voor Terrorismeschaden (NHT) have limited guarantees.
Public-private partnerships provide credibility and can be structured to gradually shift risk to the private sector.	The US government's terrorism backstop enabled Insurers to access affordable reinsurance for terrorism coverage. Over time, federal reinsurance participation In the program has fallen from 90% In 2002 to 80% In 2020, while Insurer deductibles have risen from 7% of premium In 2002 to 20% In 2020. Insurer retentions have also Increased, from $5 million in 2002 to $200 million in 2020. The UK government's backing of Pool Re similarly enabled Insurers to access affordable terrorism reinsurance. Over time, the Pool Re fund

	grew and private reinsurer confidence was restored, to the point that £2.4 billion of reinsurance cover is now purchased. As a result, a loss fund of approximately £10 billion (including member retentions) sits between the consumer and the government needing to step in.
Programs can be used to Incentivize the adoption of preventive measures.	Eligibility for the US flood risk program, NFIP, requires communities to adopt and enforce strict floodplain ordinances and offers premium discounts for outstanding performance. While there is no direct requirement for risk mitigation by Pool Re stakeholders, premium discounts of up to 7.5% are available for Insureds that proactively undertake such initiatives. The US crop Insurance Industry supports continued agronomic research to determine how farmers can best incorporate risk management best practices in their operations and the impact those practices may have on Insured crops. The US SAFETY Act of 2002 was created to spur the adoption of Improved security measures by offering to limit liability of companies providing anti-terrorism products and services for qualified vendors. Similar policies, coupled with a robust public-private insurance market, could incentivize private sector adoption of prophylactic measures to drive down exposures. Flood Re Is Intended as a temporary solution to be phased out by 2039. As such, the government has committed to major Investments in preventive measures, while Flood Re has prompted Insurers to work to enhance their understanding, mapping, and modeling of flood risk and their collection of data for Improved underwriting.