MarshMcLennan | ZURICH

Closing the cyber risk protection gap

Table of contents

1 Foreword

The cyber risk protection gap is an important societal issue that needs to be addressed

As dependence on digital technologies deepens, cyber risks are an ever-growing concern for societies around the globe. According to the World Economic Forum's *Global Risks Report 2024*, nearly 40% of experts surveyed consider cyberattacks to be a paramount risk with the potential to trigger a material crisis in the near future, placing cyberattacks within the top five in the report's current risk landscape.

Cyber threats are outpacing the ability of traditional insurance and risk management approaches to fully mitigate them. The resulting cyber risk protection gap is a societal challenge that urgently needs collective action from both the insurance industry and the public sector.

In this report, Zurich, the global multi-line insurer, and Marsh McLennan, a global professional services firm in the areas of risk, strategy and people, have joined forces to suggest ways of addressing the cyber risk protection gap.

We consider strategies to enhance the functionality and risk–bearing capacity of the private cyber insurance market, identify areas of limited insurability and non-insurability, and suggest principles for public-private partnerships to address these critical issues.

From strengthening resilience to managing catastrophic risk, re/insurers, governments, and technology providers should strive to establish the right partnerships so that the industry is better placed to offer more cyber risk protection, and to ensure that there are viable solutions in place should an extreme cyber incident occur.

Better risk models and knowledge-sharing partnerships will help insurers expand the scale and scope of cyber protection. However, given the potential impact of connected cyber risk and the high claims cost related to extreme cyberattacks on, for instance, critical infrastructure, there are limits to the amount of financial loss the re/insurance industry can absorb.

The global cost of cybercrime is projected to increase to nearly USD24 trillion by 2027, up from close to USD8.5 trillion in 2022. And this does not include the cost of non-malicious events, such as witnessed in the recent CrowdStrike outage.

We hope this paper will serve as a call to action so that the right partnerships can be put in place to help reduce the cyber risk protection gap in service of society.

John Q. Doyle
President and
Chief Executive Officer,
Marsh McLennan

Mario Greco
Group Chief Executive Officer
Zurich Insurance Group

2

A cyber continuum:

From strengthening resilience to managing catastrophic risk

As technology innovations continue to drive the digitization of the global economy, many businesses perceive an increasing sense of cyber vulnerability. For example, 87% of global decision makers in the Munich Re Cyber Risk and Insurance Survey 2024 believe their organizations are inadequately shielded against cyberattacks.

The reality underpinning this perception is even more troubling: The cost of cyberattacks is projected to increase to nearly USD24 trillion by 2027, up from close to USD8.5 trillion in 2022. Ransomware payments hit a record-breaking USD1.1 billion in 2023, and attackers are employing increasingly sophisticated methods to break into systems, exploiting technological advancements, such as generative artificial intelligence (AI). The challenging cybersecurity environment is further exacerbated by intensifying geopolitical tensions as the digital domain has become a strategic environment for states or state-sponsored actors.

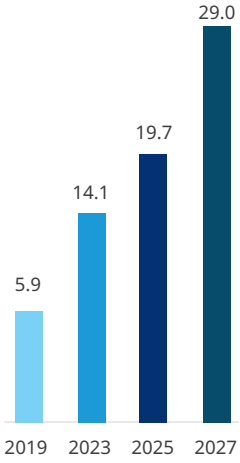
Significant strides have been and continue to be made in increasing cyber hygiene and resilience, such as linking available data with the effectiveness of various cyber controls. And while much more remains to be done, with each cyberattack — including increasingly frequent ransomware incidents — new lessons are learned and risk management strategies are modified and deployed.

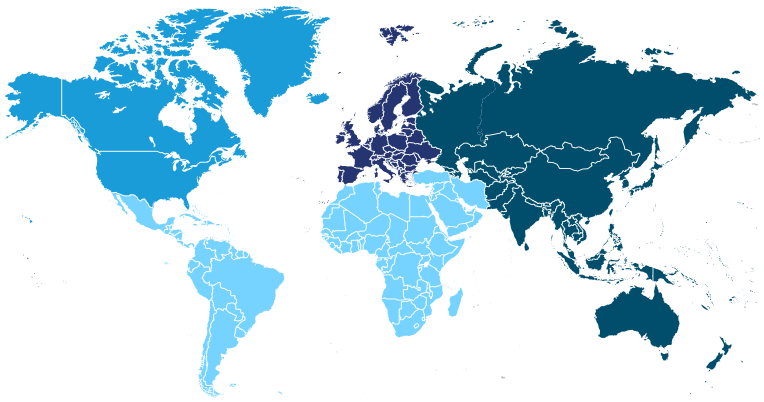
The cyber insurance market has seen strong growth over recent years, estimated at USD14 billion gross written premium (GWP) in 2023, and is projected to more than double by 2027. Yet, despite this growth, a substantial cyber risk protection gap persists — the chasm between insured losses and economic losses due to cyberattacks is estimated at a staggering USD0.9 trillion, or 99% of economic losses. In addition, while demand from organizations seeking to transfer their cyber risk has certainly been growing, this growth has been uneven and there remains a worrying trend of small- and medium-size businesses (SMBs) that are uninsured or underinsured.

It is evident that there is an urgent need to address these risks due to both their volatile nature and the ubiquitous use of technology. At the same time, we need to foster societies that are innovative, resilient, and adaptable, while safeguarding economic prosperity and national security. The insurance industry, with its proven track record of advancing societal objectives through offering its risk management and transfer capabilities, plays a critical role in this endeavor from both a risk transfer and cyber resilience perspective.

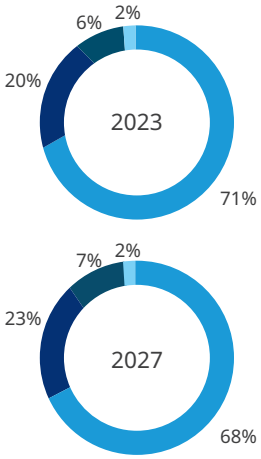
01| Strong growth anticipated for the cyber insurance market

Gross written premium (GWP) globally in USD billions





Regional percentage of global GWP



Regional GWP in USD billions	2019	2023	2025	2027
North America	4.4	10.1	13.5	19.7
Europe	0.9	2.8	4.3	6.6
Asia/Oceania	0.4	0.9	1.3	2.0
Rest of the world	0.2	0.3	0.5	0.7

Source: Estimates by Munich Re

02| Reducing the cyber risk protection gap

1. **Strengthen cyber resilience —** Focusing on ways to strengthen cyber resilience is critical to enabling the overall economy to resist, withstand, and recover quickly from cyber incidents. This can be accomplished through such measures as raising awareness and education regarding cyber risks, providing subsidies for investment into cybersecurity, using cyber resilience services offered by the insurance industry, and sharing structured data. Effectively bolstering cyber resilience will lessen some of the pressure around catastrophic risk issues.
2. **Address quantifiable catastrophic cyber risk —** Quantifiable catastrophic cyber risks are, in general, insurable. However, above a significant threshold, a loss event could have such severe financial accumulation potential that financing by the traditional or alternative (re)insurance markets could become challenging.
3. **Manage unquantifiable cyber risk —** When cyber risk becomes unquantifiable/uninsurable, a public-private partnership (PPP) could potentially sustain the market and the broader economy as catastrophic incidents arise.

3 Supporting society in a digital world:

Addressing the challenges of scaling the cyber insurance market

The insurance industry plays an essential role in helping businesses responsibly take risks in support of society's growth, innovation, and overall well–being — risks that are generally predictable and manageable, as opposed to those that would potentially shock the global economy or significant portions thereof.

The reality of today's interconnected world is that businesses, large and small, increasingly depend on digital technologies to drive their growth and innovation. With the convergence of the physical and digital comes the perception that catastrophic risk has dramatically increased in parallel to the corresponding cyber risk protection gap. The question then arises: How can the cyber insurance market — concerned with catastrophic cyber risk — scale to support societal cyber resilience without taking on an unmanageable amount of exposure?

Enhancing cyber resilience and maturity: It's important to raise awareness and incentivize organizations, via private and public activities, to enhance their cyber resilience and maturity. This can be done, for example, via cyber hygiene processes that reflect best practices, and employees who are digitally literate. Doing so will continuously improve the pool of insured risk and the ability of an economy to prevent and withstand catastrophic cyber incidents in general.

In recent years, the industry has begun to address one aspect of insurability by promoting adherence to best practices pertaining to cyber hygiene — including such controls as multi-factor authentication, identity and access management solutions, and immutable backups — that have proven effective in deterring and recovering from ransomware and other cyberattacks.

Addressing the underinsured SMB market: Despite the prevalence of cyber risk, a significant portion of SMBs remain uninsured or underinsured. These companies often lack the necessary funds to invest in cybersecurity, in the same way as they may forego purchasing insurance due to affordability, lack of risk awareness, or not understanding the coverage. To overcome such challenges, our industry should seek to simplify all elements of the procurement process, provide holistic solutions, and support and enable public-private partnerships. Some are further along in this journey than others.

It is important to provide insureds with appropriate coverage while avoiding unnecessary limitations and exclusionary language, which often overlap, lack universal consensus on applicability, and create new protection gaps.

Creating a common framework for structured data: Creating a common framework for collecting cyber loss and insurance data will help position brokers, insurers, and government agencies to analyze aggregated information and provide deeper insights to insureds.

Existing examples of public-private collaboration suggest that they can be the cornerstone of an effective cybersecurity strategy. One such effort in the United States was the 2023 "relaunch" by the Cybersecurity & Infrastructure Security Agency (CISA) of the Cybersecurity Insurance and Data Analysis Working Group (CIDAWG). Originally created in 2014, CIDAWG aims to understand which security controls are working most effectively to defend against cyber incidents, with an initial focus on giving the government insights into the types of data available to the insurance industry.

In addition, threat intelligence, vulnerabilities, crime atlas (threat actors), CISA data, US Securities and Exchange Commission (SEC) incident data, resilience level of certain industries (benchmarked across countries), and the like could be considered as further elements of confidential data sharing between the public and private sectors to better combat cyber threats.

In late 2023, the UK government released two papers outlining concerns regarding ransomware and the need to make combatting it a "more pressing political priority." Meanwhile, in the EU, the Digital Operational Resilience Act is being rolled out and requires that financial services providers set up robust ICT risk management processes and that they remediate critical risk exposures. These are just a few instances of governments' commitments to supporting cyber resilience, with aspects of some campaigns aimed at SMBs.

It's not just governments that need to be involved. As the call for additional regulation evolves, the insurance industry should establish incentives for raising security levels through such measures as design approaches, cybersecurity tools take-up, and cyber hygiene measures. The involvement of systemically important technology and infrastructure providers is crucial given their expertise, experience, and unique vantage points. At the same time, software and digital infrastructure firms should strive to adopt state of the art security measures. Creating robust incentives for adoption of security could present a valuable alternative to additional regulation.

4 Navigating the frontier of cyber risk:

Understanding the spectrum of insurable and non–insurable cyber events

To effectively navigate the frontier of cyber risk, we should strive to understand the spectrum of insurable and currently non-insurable cyber events. This understanding will enhance the industry's ability to offer appropriate coverage and inform public sector policy on managing uninsurable risks.

We find ourselves in an evolving landscape of cyber incidents, where the scope of insurability transitions from manageable and quantifiable risks to a frontier of obscurity with limited visibility and no clear path to credible quantification. This frontier, however, is not static; it evolves with accumulating experience, data collection, technological advancement, evolving modelling capabilities, and increasing cyber resilience.

It is important to note that tail risk events — those with a low probability of occurrence, but a high impact should they occur — do not automatically equate to non-insurability. The insurance industry has demonstrated resilience in absorbing cyber events that spread systemically, as shown by events such as hardware and software supply chain attacks. The future holds the likelihood of similar attacks, but with potentially more significant scale, resources, and coordination, which could bring higher financial impact.

Catastrophic cyber incident scenarios can be classified into two main categories: 1) incidents that are considered insurable up to a certain level, and 2) incidents that are generally considered non-insurable, due either to lack of insurer risk appetite or being against conventional public policy. The categorization is based on criteria including the nature of the cyberattack, its spread, the nature of the damages caused, and the economic loss at stake. Mass malware and mass cloud outage are examples of cyber incidents that are currently considered insurable up to a certain level of financial loss.

Simultaneously, there is a commonly held view of non-insurability. If a cyber incident results in a critical infrastructure failure — related to areas including power outage, financial market infrastructure, utility supply, telecommunications, internet access, or satellite systems — the risks have a significant accumulation potential. Potentially accumulating risks are currently regarded as unmanageable due to a lack of visibility regarding the resilience of connected entities to manage the dependencies on these critical infrastructures.

With widespread use of digital technologies, single points of failure could have far-reaching implications. As evidenced by the recent CrowdStrike incident, major IT outages — including those caused by a simple, yet apparently defective, "content update" — could potentially cascade into catastrophic cyber incidents when there is a lack of public-private coordination.

It's important to acknowledge that, at times, things will go wrong. In the case of the CrowdStrike incident, organizations that had tested resiliency plans generally resolved the issue in relatively short time — hours in some cases, a few days in others. Only a handful faced longer-term challenges. A silver lining in this recent example was the coordination we saw between public and private entities in mitigating further impact. More of that kind of coordination is needed, and on a much larger scale.

Scenarios where resiliency is not as expected can be compounded by advanced persistent threats, often initiated by state or state-sponsored actors, which due to their resources and patience — as compared to the economic efficiency preferred by financially motivated actors — can pose a threat to commercial defenses, potentially causing catastrophic damage through specific actions. Indeed, the industry still faces the widespread implications of zero-day vulnerabilities such as Log4j and MOVEit.

Such large-scale cyber incidents could have caused extensive damage if, for example, adversaries' motivations had been different, or if mitigating factors had failed. It is also possible that some organizations might have experienced less damage had they built in measures including quicker patching of systems, information sharing, and stronger defenses of downstream entities.

With the accumulation of catastrophic vulnerabilities, the ways to execute future attacks multiply, and the number of threat actors grows, raising the need for alternative mitigation measures that include some sort of public sector involvement.

5

The potential for partnership:

A public sector role in managing catastrophic cyber risk

Developing a better understanding of how to include more prominent public sector involvement in effectively addressing potentially catastrophic cyber risks will help bring much needed clarity to businesses, brokers, and insurers alike.

The insurance industry and the public sector must continue to work together to educate and incentivize insurance buyers by fostering cybersecurity maturity and ensuring its affordability — if necessary, through the use of measures such as governmental subsidies. Many governments around the world have developed education and information–sharing resources. For example, in the US, CISA's Shields Up program focuses on providing guidance to SMBs and others. In response to the Russia-Ukraine war, a Shields Up alert regarding the increased risk of cyberattacks was sent to every US organization, reminding companies of the need to maintain strong cybersecurity controls and awareness.

In the EU, a February 2024 report from the European Union Agency for Cybersecurity (ENISA) states objectives such as providing overviews of cyber risk, cyber insurance, and existing research and modelling approaches, as well as identifying knowledge gaps that can be filled by upcoming research projects.

It is not without precedent for the public sector to play a prominent role in addressing potentially catastrophic risks. For example, government intervention has addressed the potential impacts from nuclear risk, natural disasters, and terrorism.

Nuclear energy risk led the US government to enact the Price Anderson Act of 1957 to cover liability claims of members of the public for personal injury and property damage caused by a commercial nuclear power plant accident. The legislation placed a ceiling on the total amount of liability facing any nuclear power plant in the event of an accident. Other international pooling arrangements also exist for nuclear risk.

Flood risk financing exists in many developed countries, with the predominant model a government-backed program, such as the US National Flood Insurance Program (NFIP). The UK government has focused on making flood insurance more affordable by improving reinsurance options for insurers through its flood reinsurance program, Flood Re.

Terrorism risk following the attacks of September 11, 2001, led the US government to pass the Terrorism Risk Insurance Act (TRIA). The backstop has enabled insurers to access affordable reinsurance for terrorism coverage. Other countries have developed similar terrorism backstops, such as Pool Re in the UK.

Cyber risk is now akin to these other risks. The need for a public-private approach for cyber risk has emerged from the continuing transformation of the digital economy, the blending of physical processes with virtual control, and the growing role and expanding capabilities of new technologies, most recently, generative AI.

The insurance industry has turned its attention to risks affecting critical infrastructure or nation-state attacks that result in a "major detrimental impact" on essential services, reflecting the potential magnitude of losses from an unquantifiable cyber incident. This has led to the development of evolved infrastructure exclusions and a new style of war exclusions in cyber policies. These, in turn, shine a spotlight on the ensuing coverage gap stemming from those risks that are considered unquantifiable, and therefore call out for some sort of public-private partnership.

Properly designed, a government framework can create a mechanism that enhances efficiency, thus reducing the economic impact of a catastrophic cyber incident. Any solution, regardless of its precise design and in order to be effective and efficient, should follow a set of principles that:

- Addresses the connected and/or catastrophic nature of these risks.
- Recognizes the different needs and behaviors between SMBs and large firms.
- Reflects the need for widespread accessibility and affordability.
- Enhances the cyber resilience of the global economy.
- Uses efficient delivery mechanisms by leveraging insurers' actuarial, financial, administrative, and distribution expertise.
- Respects the fundamental need for risk-oriented pricing to avoid misaligned incentives.

Government plays multiple essential roles in addressing catastrophic cyber risks. For example, government can marshal resources at a scale beyond any private sector organization. In addition, government can establish policies and regulations to bring a "whole of government" approach to develop preparedness and build resilience.

Such initiatives should derive from a collaborative effort between government and industry. The majority of US critical infrastructure remains owned or controlled by the private sector. In addition, industry may bring expertise and innovation that lift the effort to success.

Collaboration with industry also brings the opportunity to share data, so that both may close vulnerabilities and combat threats. Doing so will require overcoming a number of obstacles to creating a common framework for data sharing, including current legal constraints regarding privacy, the lack of a common language regarding incidents, conflicting data guidelines, and limited incentives.

6 Conclusion

Strengthening society's cyber resilience is inextricably linked to the evolution of the cyber insurance market. Creating a virtuous cycle — via incentivizing cyber hygiene best practices, fostering public-private collaboration and recovery mechanisms, and establishing a common framework for structured data collection/sharing — positions the market to protect businesses against their most pressing cyber risks, fulfilling its ultimate purpose.

Both the insurance industry and the public sector are urged to collaborate, share, and innovate to confront the growing cyber risk protection gap, foster resilience, and safeguard our society and economy from the escalating cyber threat landscape. For industry and government to implement a cyber framework for cyber resiliency, they will need to address a number of issues, including the following:

What will be covered?

From the standpoint of national preparedness, the most pressing need is to address the gap created by war exclusions and infrastructure exclusions that appear in insurance policies.

Because these risks are the subject of exclusions, a cyber incident resulting in these losses will not impact the insurance market, but instead would require a government response post-incident. Creating a cyber framework provides the opportunity to engage in planning of how such compensation would be applied.

How will coverage be triggered?

Triggering events could be defined based on what current policies treat as uninsurable. Potentially, the framework could allow for a difference-in-condition product that is triggered when policy exclusions are applicable.

Additionally, it would be important to ensure that the program serves to respond to only truly catastrophic losses.

Who will participate?

To provide for flexibility and buy-in from industry, any government framework should be voluntary for eligible insurers. At the same time, this will require insurers to acknowledge their support and their belief in the viability of a cyber framework.

Ultimately, all insureds would benefit from the option to purchase coverage for catastrophic cyber risk.

How will claims be handled?

Currently, concern exists that the volume of claims arising from a catastrophic cyber incident might overwhelm the resources available to resolve such claims. Government policymakers should consider that the expertise and capabilities currently held by the insurance sector provide strong motivation for the government to create a framework in partnership with industry. In addition, policymakers should consider the tools and resources that government could provide for claims administration.

About Marsh McLennan

Marsh McLennan (NYSE: MMC) is the world's leading professional services firm in the areas of risk, strategy and people. The Company's more than 85,000 colleagues advise clients in over 130 countries. With annual revenue of $23 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses. Marsh provides data-driven risk advisory services and insurance solutions to commercial and consumer clients. Guy Carpenter develops advanced risk, reinsurance and capital strategies that help clients grow profitably and pursue emerging opportunities. Mercer delivers advice and technology-driven solutions that help organizations redefine the world of work, reshape retirement and investment outcomes, and unlock health and well being for a changing workforce. Oliver Wyman serves as a critical strategic, economic and brand advisor to private sector and governmental clients. For more information, visit marshmclennan.com, or follow us on LinkedIn and X.

About Zurich

Zurich Insurance Group (Zurich) is a leading multi-line insurer serving people and businesses in more than 200 countries and territories. Founded 150 years ago, Zurich is transforming insurance. In addition to providing insurance protection, Zurich is increasingly offering prevention services such as those that promote wellbeing and enhance climate resilience. The Group has about 60,000 employees and is headquartered in Zurich, Switzerland. Further information is available at www.zurich.com.