Closing the cyber risk protection gap

Table of contents

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

tensions as the digital domain has become a strategic environment for states or state-sponsored actors.

02| Reducing the cyber risk protection gap

Strisk protection gap

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

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

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

other cyberattacks.

Addressing the underinsured SMB market:
uninsured or underinsured. These companies often lack the necessary funds to invest in cybersecurity, in the same way as

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

the spectrum of insurable and currently non-insurable cyber events. This

and inform public sector policy on managing uninsurable risks.

not static; it evolves with accumulating experience,aa7Dit ea collicyion, technologie8hM0052005800u80560003ng ea co300370043rlogie8hM00

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

Developing a better understanding of how to include more prominent public

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

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 _____ states objectives such as providing overviews of cyber risk, cyber insurance, and existing research and modelling approaches, as well as identifying knowledge gaps that

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

Terrorism risk following the attacks of September 11, 2001, led the US government to pass the Terrorism Risk Insurance

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.

critical infrastructure or nation-state attacks that result in a

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

private partnership.

Properly designed, a government framework can create

economic impact of a catastrophic cyber incident. Any solution,

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

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: