Cyber insurance unpacked: the corporate digital safety net[1]

Executive summary

In a more digitalised world, particularly with emerging threats amplified by artificial intelligence (AI), cyber risk is increasingly recognised as a significant threat to financial and economic stability. Beyond the financial impacts of cyber attacks, these incidents can also disrupt critical infrastructure, global supply chains and consumer trust. For the financial sector, these risks are particularly acute, as cyber incidents can destabilise payment systems and lead to cascading failures and operational disruptions across interconnected institutions. The rise in cyber risk is driven by increasingly sophisticated threat capabilities, geopolitical tensions, growing digitalisation, concentrated digital dependencies and supply chain vulnerabilities. It remains to be seen whether the recent step change in frontier cyber AI models will yield net positive or negative effects on cyber resilience – which will depend on whether defenders or attackers prevail in exploiting such models. These dynamics raise systemic concerns, with severe cyber incidents having the potential to disrupt significant portions of the economy and financial systems.

Cyber incidents can arise from both malicious and non-malicious causes, including technical malfunctions, human error and internal or external attacks. Malicious incidents such as ransomware, social engineering scams and data breaches are on the rise, with ransomware becoming the leading source of cyber losses. These attacks have evolved into complex, multi-stage operations that can affect multiple organisations simultaneously, amplifying accumulation risk for insurers. Non-malicious incidents that involve widespread outages or disruptions have gained in importance and can lead to systemic risk, particularly given increasing interdependence among critical infrastructure. Cyber insurance can play an important role in supporting firms' efforts to prepare, prevent, recover and mitigate cyber-related losses.

Against this backdrop, the disconnect between the increase in cyber risk and the use of cyber insurance as a risk mitigation tool is remarkable. It is estimated that only 1% of global economic cyber losses are covered by cyber insurance, with small and medium-sized enterprises (SMEs) being the most underinsured commercial customers. Although the global cyber insurance market has been growing, the growth has stalled even as insurance availability continues to increase and premium rates fall. The protection gap can have direct and serious consequences on economic resilience. Yet, the market faces significant challenges, including coverage gaps, non-affirmative cover, pricing complexities and accumulation risk.

Ambiguity in cyber insurance policy terms persists, leaving uncertainty around the scope of coverage. Cyber insurance – offered as a standalone policy or add-on to other insurance products – typically provides coverage for both first-party risks (such as incident response and cyber extortion) and third-party liabilities (including privacy violations and regulatory fines). In recent years, the types of incidents and risks covered have converged among insurers, but variations and exclusions continue to challenge policyholders. In some jurisdictions, these terms have yet to be tested in the courts.

The issue of non-affirmative or "silent cyber" – where coverage is neither explicitly included nor explicitly excluded – remains a critical concern. Actual attacks have highlighted the risks of non-affirmative coverage, as most losses have been claimed under property policies not designed to

[1] Adrien Currat (Adrien.Currat@bis.org) and Jeffery Yong (Jeffery.Yong@bis.org), Bank for International Settlements; Joe Perry (Joe.Perry@iais.org), International Association of Insurance Supervisors. We are grateful to Jonathan Dixon, Conor Donaldson, Hanne van Voorden, Marie Kratz and Randy Miskanic for helpful comments. We also extend our appreciation to the insurers, reinsurers, brokers, cyber risk modelling companies, insurance regulators and cloud service providers who generously shared their perspectives during the interviews. We would also like to thank Anna Henzmann, who provided valuable administrative support.

cover cyber risks. Both the industry and regulators have taken measures to achieve clearer policy terms to address this ambiguity. However, exclusions for risks like state-sponsored cyber attacks, terrorism and systemic vulnerabilities continue to limit the scope of coverage. Emerging risks, such as AI-enabled cyber attacks, are transforming the threat landscape, with insurers facing the dual challenge of addressing increasing AI-related losses and avoiding unintended exposures.

The pricing of cyber insurance poses unique challenges due to limited historical data, the rapidly evolving nature of cyber threats and the interconnectedness of digital ecosystems. Traditional actuarial models, which assume stable risk distributions, struggle to account for the non-stationary and systemic characteristics of cyber risk. Insurers increasingly rely on advanced methodologies, such as scenario analysis, to estimate losses and set premiums, leveraging cyber catastrophe models provided by a small number of vendors. Like other business lines, the ultimate pricing of cyber insurance is influenced by market dynamics, reinsurance costs and insurers' risk appetite, which may lead to significant volatility in premium rates over time.

Accumulation risk is a major concern for cyber insurance underwriting. The industry's core challenge is not "average ransomware" but instead includes correlated, tail events such as cloud outages, widely exploited vulnerabilities, destructive malware or critical infrastructure attacks that can trigger losses across multiple policies. Shared dependencies on critical infrastructure, cloud providers and software platforms exacerbate this risk, as a single vulnerability can cascade across numerous organisations and geographies. Looking at isolated incidents may hide interdependencies that can drive correlated, systemic losses. While insurers can manage accumulation risk through limits and exclusions, systemic events could threaten their solvency. Careful monitoring of the nature and potential evolution of accumulation risk is critical, particularly given frontier AI models that can expose systemic vulnerabilities.

There is a significant protection gap, which is particularly pronounced in emerging markets and for SMEs, leaving large portions of the economy vulnerable to cyber risks. While large corporates dominate cyber insurance coverage, even they face limits that may fall short of potential losses from major attacks or non-malicious disruptions. The gap is expected to widen as cyber vulnerabilities grow faster than insurance adoption, driven by advancements in AI and increasing digital interconnectivity. Both supply and demand factors contribute to the protection gap, with demand factors being more pronounced.

Addressing the protection gap requires a multi-stakeholder approach. Governments, sometimes in partnership with the insurance industry, can promote cyber hygiene through education and regulation, while insurers can incentivise better risk management by linking premiums to cyber security preventive measures. Public-private partnerships like cyber terrorism pools may be necessary to cover uninsurable risks, such as state-sponsored attacks. Regulatory initiatives to improve incident reporting and data availability can also enhance underwriting and pricing practices, though they may inadvertently reduce coverage availability or affordability.

Given the increasing complexity and scale of cyber risks, growth in the cyber underwriting market needs to be prudent, acknowledging that the market cannot fully address all cyber threats and vulnerabilities. Risk-based pricing and prudent underwriting will play a key role in supporting this growth: driving risk awareness, supporting better cyber hygiene and encouraging the provision of cyber insurance. At the same time, efforts to increase awareness of the importance of cyber insurance as a risk mitigation tool need to intensify. While cyber insurance can never (and should not) replace the need for firms to exercise sound cyber resilience practices, it can serve as a digital safety net and ultimately contribute to safeguarding financial and economic stability in times of a cyber crisis. To achieve this, collective efforts must be made to improve cyber resilience of firms across the board.