Strengthening Cyber Resilience Through Insurance

Research summary | March 2026

Darren Pain, Director of Research, Geneva Association
Sasha Romanosky, Senior Policy Researcher, RAND

Cyber incidents are becoming more frequent and more costly. The median annual loss of a cybersecurity breach has risen 15-fold over the past 15 years, from USD 190,000 to nearly USD 3 million. Losses from major incidents have also grown sharply, exceeding an average of USD 28 million within the top 10% of loss events in 2024, almost five times the level recorded in 2008.[1]

Businesses increasingly identify cyber risk as a core operational concern. Yet many cyber incidents still stem from basic, preventable vulnerabilities such as susceptibility to phishing, weak passwords, unpatched software, and misconfigured systems. Insurers can play an important role in helping to raise firms' cybersecurity hygiene and enhancing overall cyber resilience. However, cyber insurance penetration in certain market segments and regions remains low. Estimates suggest only around 10% of small and medium-sized enterprises (SMEs) globally have cyber insurance – and in some countries it could be much lower, especially among the very smallest firms.[2]

Cyber resilience and insurance

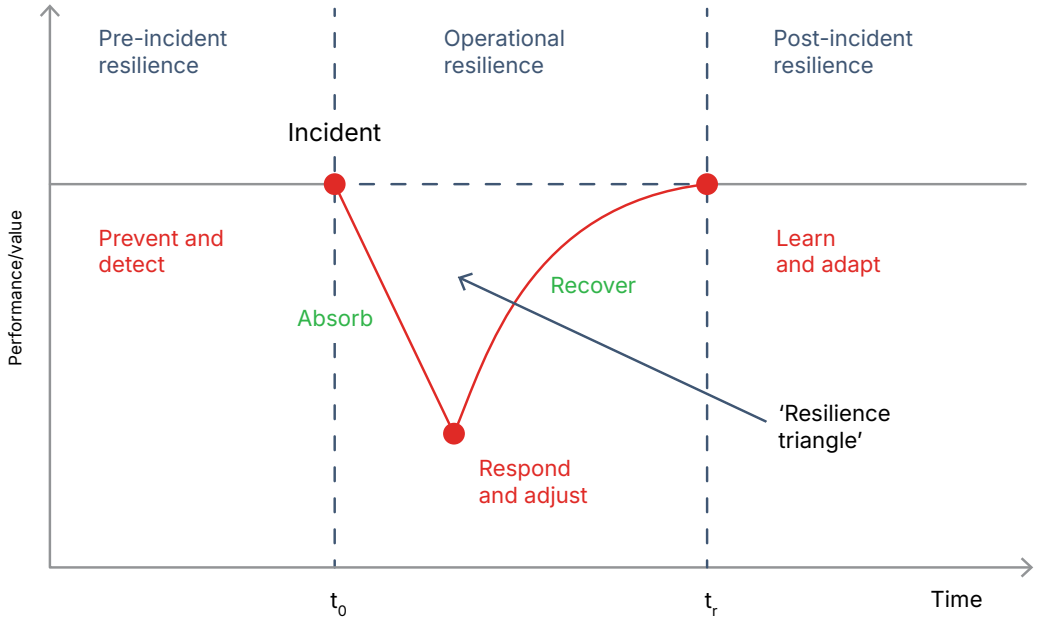
A 'resilience triangle' traces how a firm's performance is impacted by an adverse disturbance. Depending on the structure of a firm's systems, some shocks may be absorbed with no change in performance, if measures are in place to anticipate them and ameliorate their impact. But inevitably some disturbances will be unforeseen. Their effects will be determined by the firm's ability to rely on backup systems, isolate parts of its business functions to limit the spread of any disruption, and access financial and physical resources to respond to and remediate the incident. The triangle framework reflects the actions a firm takes to build and maintain system resilience – before, during, and after a disturbance – and helps ensure reliability and maintain firm-level performance (sales, output, etc.) (see Figure 1).

Cyber insurance has evolved from being just a risk-transfer mechanism to also helping companies manage and reduce cyber threats and their impacts. Insurers require baseline security standards from policyholders. They may also bundle services, including security recommendations, cyber-risk monitoring and alerts, and payment for the costs of experts should an incident occur. In doing so, insurance can help firms 'shrink the V' of the resilience triangle by improving their pre-incident, operational, and post-incident resilience.

Unlike cybersecurity vendors, who might offer standalone warranties offering compensation should their specific product or service fail, cyber insurers have a vested interest in helping their policyholders minimise the full suite of losses from a cyber incident, including damages incurred by third parties. There is a feedback loop between advice, guidance, and coverage: prioritising more effective cybersecurity will, in turn, reduce insurance claims. Equally, if investing in cybersecurity enables an insurer to provide better coverage terms or more effective incident response support, the investment increases the value of cyber insurance.

1 Cyentia 2025.
2 Swiss Re 2024.

FIGURE 1: A HOLISTIC VIEW OF RESILIENCE

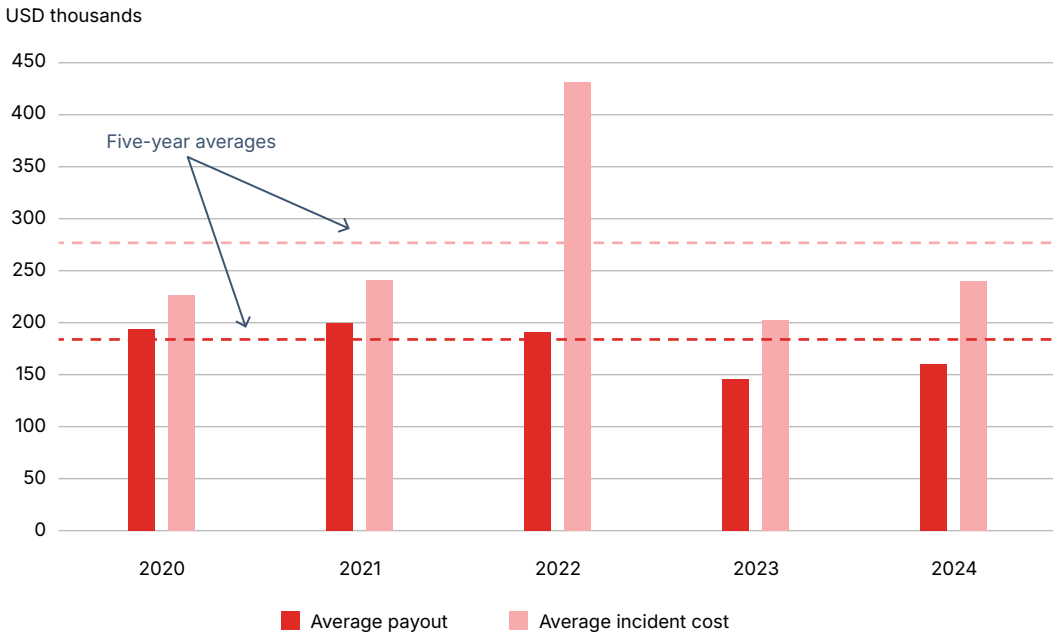


Source: Geneva Association[3]

How effective is cyber insurance?

Empirical evidence suggests cyber insurers pay claims and influence insureds' cybersecurity posture. One global study found that 92% of notifications of potentially covered losses fell within cyber insurance coverage.[4] By comparison, UK insurers paid out on more than 90% of motor insurance claims, around 70% of claims on home buildings and contents policies, and a little over 50% of legal insurance claims.[5]

FIGURE 2: INCIDENT COSTS AND INSURANCE PAYOUTS TO SMES



Source: NetDiligence[6]

3 Graphic adapted from Bruneau et al. 2003.
4 Willis Towers Watson 2025.
5 Financial Conduct Authority 2025.
6 NetDiligence 2024.

Data for the US, Canada, and the UK show that the average cyber insurance payouts represent a material share of overall incident costs, close to 70% in the case of SMEs (see Figure 2). Surveys and case studies also indicate that, through their underwriting procedures, cyber insurers have a positive impact on policyholders' cyber hygiene. For example, a 2024 survey reported that nearly all organisations that purchased a cyber policy also invested in improving their cyber defences to optimise their insurance position. Over three quarters (76%) of surveyed companies increased cybersecurity investments in order to apply for cyber insurance.[7]

However, several market features still restrict the potential of insurance, on both supply and demand sides, to promote effective cybersecurity governance:

- **Limits to risk differentiation.** While underwriting practices have advanced in recent years, insurers still struggle to precisely differentiate insureds by their level of cyber risk. As a result, insurance terms and conditions do not always provide sharp incentives for firms with weaker cybersecurity to improve their controls.

- **Practical obstacles to steering effective risk prevention and mitigation.** Many insureds do not take advantage of insurers' pre-incident security services. A recent survey found that nearly one third of respondents (32.5%) were unaware of any free risk management services included in their cyber insurance policy.[8]

- **Misaligned incentives and institutional frictions.** Efforts to manage risk after an accident or intrusion can also be undermined by potential conflicts of interest between insurers, intermediaries, and policyholders. For example, policyholders may not want to provide all the necessary information insurers need for loss adjustment, in case that reveals commercially valuable/sensitive data, or could lead to reputational harm and legal repercussions. A reluctance to share information undermines transparency and trust.

- **Ambiguity surrounding potential catastrophic cyber events.** The uncertainty over the likelihood and size of cumulative losses that might accompany a major cyber event – for example, possible accumulated claims from a common failure of IT systems or the contagious spread of malware – continues to restrict re/insurer appetite to underwrite cyber risks.

Fostering increased take-up of cyber insurance

Insurance can be a key enabler of a needed upgrade in firms' cybersecurity as well as strengthening their capabilities to cope with cyber incidents, even if some peak cyber risks ultimately remain uninsurable. However, increasing the take-up of cyber insurance and enhancing its role as a vital tool in boosting overall cyber resilience, especially among SMEs, will require a combination of initiatives involving multiple stakeholders. These include:

- **Raising awareness of cyber risks and the full benefits of coverage.** Insureds' risk profiles can be materially strengthened through the underwriting process and sustained engagement with their insurers, not least among SMEs, where the most significant risks are negligence and oversight. This suggests an opening for carriers (and brokers) to invest further in client education about cyber risks and the proactive and preventive cybersecurity options included in cyber policies. Forward-looking cyber insurers already understand this, stressing resilience in their interaction with policyholders.

- **Tailoring cover to meet policyholders' needs.** Ongoing advances in underwriting practices will make tailored coverage options even more feasible, including protection against enforced shutdowns, fines and penalties imposed by regulators, and losses resulting from cyber-related property damage and business interruption. In particular, cyber insurers are increasingly looking at parametric and agreed-value solutions to speed up claim payouts for business interruption claims, either as add-ons to existing policies, or as standalone policies.

- **Simplifying policy language, underwriting, and claims processes for SMEs.** The priority should be to simplify the customer experience. As far as possible, this means crafting policies that are easy to understand, delivering a seamless onboarding journey for new policyholders, and streamlining underwriting and claims processes. For instance, insurers can target clear, jargon-free policy wording, adapted to local regulations and industry contexts, to ensure accessibility and relevance. More transparent policy wording would make it clearer what perils are covered and which exclusions apply. This will help to build trust between policyholders and insurers, and cement stable, long-term cybersecurity partnerships.

7 Sophos 2024.
8 QBE 2024.

- **Aligning distribution with customer preferences and risk profiles.** As well as the cyber insurance product itself, the ways in which customers interact with cyber insurers and intermediaries should also be upgraded. New distribution models have already begun to emerge. In May 2024, the insurance broker Howden launched the first-of-its-kind SME cyber insurance platform.[9] Several carriers have also introduced embedded cyber insurance offerings that bundle coverage with the purchase of IT services, software, or security products, in a bid to increase insurance penetration, especially among small firms.

- **Partnering with digital infrastructure providers.** Insurers need to invest further in high-frequency telemetry – automatic gathering and analysis of data from multiple sources, including networks, applications, endpoints, and cloud environments – to better assess their insureds' IT vulnerabilities and cybersecurity postures. This includes deploying AI tools to improve pricing accuracy, reduce claims, and enhance the resilience-building capabilities of cyber insurance. The shift towards continuous underwriting will be aided by deeper connections between insurers, key infrastructure providers, and cybersecurity vendors.

- **Collaborating with government agencies.** Insurers possess rich data on incidents, losses, and vulnerabilities across industries; while government agencies often have access to classified or aggregated intelligence on emerging threats, attack techniques, and indicators of compromise. When these insights are shared securely and responsibly, firms benefit from earlier warnings, better risk assessments, and improved preparedness against emerging cyber threats. Beyond information sharing, insurers and governments can support the development and adoption of common cyber hygiene practices, which underpin eligibility for insurance coverage, including potential steps towards mandatory cybersecurity standards.

- **Exploring initiatives to promote system-wide resilience.** Major technology companies already use bug bounty programmes, offering rewards to external researchers for responsibly reporting security flaws, to improve vulnerability discovery. There is an opportunity for insurers to channel some cyber insurance premiums to fund bug bounty schemes directly. The potential cybersecurity gains might be significant if the skills of the ethical hacking community could be steered towards innovative defensive tools, such as automating vulnerability discovery or exploiting mitigation techniques. At the same time, operationalising such insurer-sponsored bug bounty programmes would take careful design and implementation, aligning the incentives of software vendors, policyholders, and insurance companies, while also overcoming any legal or regulatory hurdles.

References

Bruneau, M. et al. 2003. A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities. *Earthquake Spectra* 19 (4): 733–752.

Cyentia. 2025. *Information Risk Insight Study 2025*.

Financial Conduct Authority. 2025. *General Insurance Value Measures Data 2024*.

Howden. 2025. *Rebooting Growth: Howden's 2025 Cyber Insurance Report*.

NetDiligence. 2024. *Cyber Claims Study 2024 Report*.

QBE. 2024. *2024 Cyber Insurance Report*.

Sophos. 2024. *Cyber Insurance and Cyber Defenses 2024*.

Swiss Re. 2024. *Reality Check on the Future of the Cyber Insurance Market*.

Willis Towers Watson. 2025. *Boards Risk Costly Cyber Exposure as Confidence Outpaces Preparedness, According to Willis Report*.

9 Howden 2025.