GENEVA ASSOCIATION

Strengthening Cyber Resilience Through Insurance

March 2026

GENEVA ASSOCIATION

Strengthening Cyber Resilience Through Insurance

Darren Pain
Director of Research, Geneva Association

Sasha Romanosky
Senior Policy Researcher, RAND

Geneva Association

The Geneva Association was created in 1973 and is the only global association of insurance companies; our members are insurance and reinsurance Chief Executive Officers (CEOs). Based on rigorous research conducted in collaboration with our members, academic institutions and multilateral organisations, our mission is to identify and investigate key trends that are likely to shape or impact the insurance industry in the future, highlighting what is at stake for the industry; develop recommendations for the industry and for policymakers; provide a platform to our members and other stakeholders to discuss these trends and recommendations; and reach out to global opinion leaders and influential organisations to highlight the positive contributions of insurance to better understanding risks and to building resilient and prosperous economies and societies, and thus a more sustainable world.

Photo credits:
Cover page – AI-generated
Section 1 – Getty Images for Unsplash+
Section 2 – metamorworks for Shutterstock
Section 3 – Adobestock
Section 4 – giggsy25 for Shutterstock
Section 5 – AI-generated
Section 6 – Philip Oroni for Unsplash+

Geneva Association publications:
Pamela Corn, Director Communications
Simon Woodward, Communications Manager & Editor
Jooin Shin, Digital Content & Design Manager

Suggested citation: Geneva Association. 2026. *Strengthening Cyber Resilience Through Insurance.* Authors: Darren Pain and Sasha Romanosky. March.

www.genevaassociation.org

Contents

ACKNOWLEDGEMENTS

This report has benefited significantly from the input of the members and affiliates of the Geneva Association's Cyber Working Group as well as external interlocutors who kindly agreed to share their expert insights. Special thanks go to:

- Rishi Baviskar, Rachel Carter and Sabrina Sexton (Allianz Commercial)
- Lori Bailey, David Schluger and Nick Steinmann (AXIS Capital)
- Hélène Chauveau and Sophie Farhane (AXA)
- Henry Skeoch, Wil Powell, Christian Taube and Michelle Waldron (Beazley)
- Matt Prevost (Chubb)
- Sezaneh Seymour and Daniel Woods (Coalition)
- Jonas Schwade (Cysmo)
- Kevin Sherry (DarkWeb IQ)
- René Buff (Helvetia Insurance Company)
- Martin Kreuzer and Franz Gromotka (Munich Re)
- Tom Egglestone (Resilience)
- Simon Parten (Schroders Capital)
- Philipp Skucha (securance.de)
- Colin Cowan (Standard Life Insurance)
- Stefan Frei (Techzoom.net)
- Andre Zapp (Toa Re)
- David Pym (University College London)
- Dingchen Ning (University of St. Gallen)

The views and conclusions presented in the report are solely those of the authors.

Foreword

Cyber resilience is becoming a core requirement for organisations operating in an increasingly digital and interconnected economy. Cyber incidents are no longer exceptional events; they are a persistent feature of the modern risk landscape. The financial impact is rising sharply, with median annual losses from cyber incidents increasing roughly 15-fold over the past 15 years. Strengthening resilience – ensuring organisations can prevent, absorb, and recover from cyber disruptions – has become an essential priority for firms, insurers, and policymakers alike.

This report examines the growing urgency around cyber resilience, and the role insurance can play in strengthening it. Geopolitical tensions, the rapid adoption of cloud services and artificial intelligence, expanding digital supply chains, and increasingly sophisticated threat actors are intensifying the risk environment. Yet many incidents still stem from basic, preventable weaknesses such as phishing attacks, weak passwords, unpatched software, and misconfigured systems – highlighting persistent gaps in cyber hygiene and risk management.

Preparation alone is not enough: organisations must also be able to absorb cyber shocks, respond effectively, and recover quickly. Cyber insurance is a potentially powerful, though still under-realised, governance mechanism – one that can complement cybersecurity investment, incentivise better practices, and provide critical expertise and financial support when incidents occur, particularly for small- and medium-sized enterprises.

This report sets out practical recommendations to expand awareness, improve insurance design, enhance data sharing, and promote common cyber hygiene standards. By acting together, stakeholders can help ensure that cyber insurance continues to evolve into a trusted and effective tool for managing cyber risk and supporting resilience across the economy.

Jad Ariss
Managing Director

Executive summary

Cyber insurance does not just cover losses – insurers work with partners and policyholders to anticipate risk and respond to cyber incidents.

Cyber incidents are becoming more frequent and more costly. The median annual loss of a cyber-security 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 on average USD 28 million within the top 10% of loss events in 2024, almost five times the level recorded in 2008.

Given geopolitical tensions, rapid digitalisation and use of artificial intelligence (AI), shifting regulatory requirements, and evolving threat actors, this trend is unlikely to reverse. 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.

Understanding cyber resilience goes beyond conventional risk management and the actions firms take to limit potential losses. Instead, resilience requires attention to how firms prevent, absorb, and recover from disruptions. Some shocks can be anticipated and mitigated in advance, but others cannot. The speed and scale of recovery depend on built-in redundancies and segmentation of IT systems, access to backup resources, and effective incident response (IR). More resilient organisations work to reduce both the depth and duration of performance losses following an incident, as well as to enhance their abilities to restore operational capacity and minimise any long-term damage to their reputation.

Cybersecurity investment and cyber insurance are complementary tools for strengthening resilience. Beyond providing financial compensation for losses arising from an incident, cyber insurance can positively shape firm behaviour and incentivise risk prevention and mitigation, especially among small and medium-sized enterprises (SMEs) who may have limited cybersecurity expertise. Insurers often require minimum security standards before underwriting, encourage risk controls during the policy period, monitor global threats and alert clients to vulnerabilities, and provide expert support in responding to and remediating breaches. As insurers observe cybersecurity patterns across many firms, they are also well positioned to promote resilience within the broader economy.

The market for cyber insurance has expanded rapidly, both in scale and scope of coverage, since it first emerged in the mid-to-late 1990s and especially over the past decade. During that time, it has persistently demonstrated its worth by paying claims, improving policyholders' cyber hygiene through effective underwriting, and supporting IR. Data for the US, Canada and the UK show that cyber insurance payouts represent a material share of overall incident costs, close to 70% in the case of SME policyholders. Furthermore, insurance broker data indicate 92% of notifications of potential losses fell within cyber insurance coverage, which compares favourably to other insurance lines.

However, the promise of a more powerful governance role for cyber insurance – where insurers proactively raise security awareness among their customers, incentivise continuous improvements in cybersecurity, and help expedite recovery when cyber defences are breached – is yet to be fully realised, particularly among SMEs, where adoption is low. Most insurers still struggle to accurately assess cyber risks and how they are evolving due to limited visibility into clients' internal security environments as well as the fast-moving threat landscape. Meanwhile, policyholders often underuse pre-incident risk prevention services, due to limited awareness, operational constraints, or concerns that sharing information may affect future pricing and coverage. The involvement of third-party service providers during IR can add legal and operational complexity at moments when speed and coordination are essential.

Ultimately, some cyber risks are simply uninsurable because the scale and/or uncertainty about potential losses is too great for insurers to underwrite. Nonetheless, cyber insurance can be a key enabler of the needed upgrade in cybersecurity to cope with more routine and often preventable cyber incidents that can still be highly disruptive.

Expanding the uptake of cyber insurance and enhancing its role as a vital tool in boosting firms' overall cyber resilience, especially among SMEs, will require coordinated action across insurers, firms, intermediaries, technology providers, and government. Key priorities include:

- **Improving awareness and education** of cyber risks and the preventative services embedded in insurance policies, particularly for SMEs with limited technical capacity.
- **Developing more flexible and accessible insurance products**, including clearer coverage terms and innovative approaches such as parametric or agreed-value solutions for business interruption.
- **Streamlining underwriting and claims processes** and clarifying policy language to ensure ease of understanding and relevance across sectors and jurisdictions.
- **Modernising customer engagement**, including digital distribution channels that simplify the buying process for brokers and smaller firms.
- **Partnering with IT and cybersecurity vendors** to access high-frequency data on vulnerabilities and support more accurate, continuous cyber risk assessment.
- **Working with government to promote common cyber hygiene standards** that can form the basis for coverage eligibility and security expectations.
- **Supporting systemwide resilience initiatives**, such as funding coordinated vulnerability discovery (e.g. bug bounty programmes) or advancing automated defence tools.

The insurance sector is already making progress in many of these areas. By helping establish and reinforce widely adopted standards of good cyber hygiene, cyber insurance can evolve into a more trusted and effective mechanism for building resilience across companies, industries, and economies.

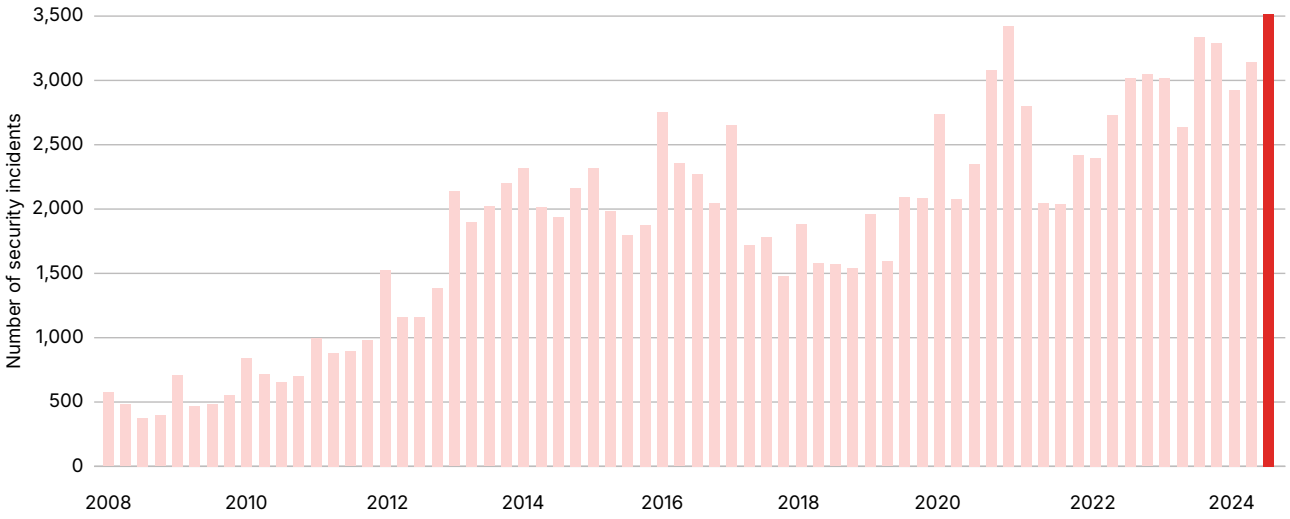
1 Introduction

Introduction

In today's more dangerous digital environment, cyber insurance is helping narrow still significant protection gaps.

The cyber risk environment appears to be worsening. According to published data, while the overall number of cyber incidents varies year-on-year, there has been a clear upward trend over the past two decades (see Figure 1).[1] Malicious cyber operations are becoming ever more prolific – ransomware and distributed denial of service (DDoS) attacks accounted for close to 50% of events in 2024 and contributed most to the increase in incidents over the past five years (see Figure 2). Moreover, many cyberattacks go unreported.[2]

FIGURE 1: GLOBAL CYBERSECURITY INCIDENTS PUBLICLY REPORTED OR DISCOVERED EACH QUARTER

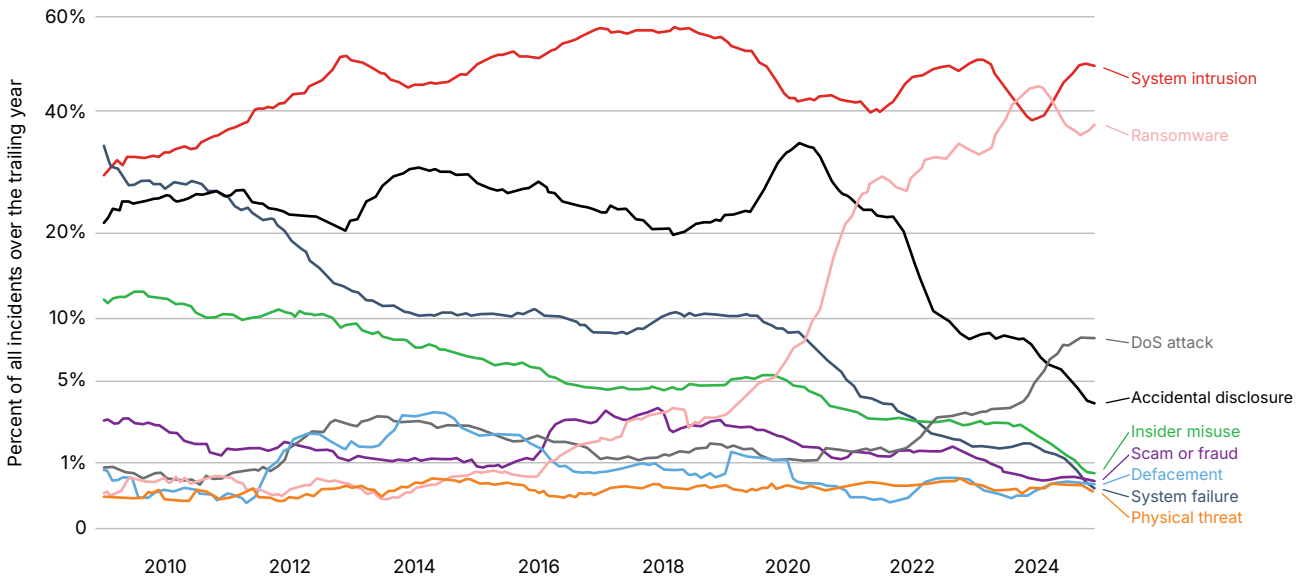


Sources: Cyentia, Feedly Threat Intelligence (Q4 2024)

1 This is especially the case given there are structural reporting delays surrounding cyber events which mean that the most recent incidents are underreported.

2 According to one recent survey of cybersecurity leaders across the US, the UK, and Ireland, 71% of respondents indicated that they might not report a data breach. The main reasons for failing to report a breach were concerns over a negative response from senior leadership (40%) and fear of reputational or financial harm if the news became public (44%). Viking Cloud 2025.

FIGURE 2: GLOBAL CYBERSECURITY INCIDENTS PUBLICLY REPORTED OR DISCOVERED EACH QUARTER



Source: Cyentia

Indicators of severity (based on partial data) likewise suggest cyber incidents are becoming more expensive. One study estimates the annual median loss from cyber-security incidents has risen 15-fold over the past 15 years, from USD 190,000 to almost USD 3 million.[3] The financial impact of major incidents has likewise increased markedly. In 2024, the average loss among the top decile of events surpassed USD 28 million – nearly five times the levels recorded in 2008.[4]

1.1 Cyber risks are a growing business concern

With geopolitical tensions, increasing digitalisation, an evolving regulatory and privacy law landscape, and a constantly changing group of threat actors, businesses see little prospect of a reversal of these trends. The Allianz Business Barometer ranked cyber as the top global risk in 2025, marking its fifth consecutive year at the top. Ten years ago, cyber risk ranked only eighth globally with 12% of responses, compared to 42% in 2025.[5]

The rapid adoption of emerging technologies such as AI only seems likely to amplify cyber risks as cybercriminals and other cyber adversaries successfully harness them to achieve greater sophistication and scale. While AI has benefits for security professionals, it supercharges the abilities of malicious actors, even among technically unsophisticated cybercriminals (see Box 1). AI can improve the targeting of vulnerabilities such as legacy systems, under-resourced IT departments, and human error.

3 Cyentia 2025.
4 Cyentia 2025.
5 Allianz 2026.

Box 1: Generative AI and cybercrime

Generative AI (GenAI) is a double-edged sword for cybersecurity: it strengthens the capabilities of both attackers and defenders, making the threat landscape more dynamic and challenging. On the defence side, it can enhance threat detection, automate incident response, and improve vulnerability analysis. Simultaneously, it can increase the speed, scale, and sophistication of cyberattacks, by enabling:

- **Malware creation and code generation.** GenAI models can create malicious code that previously required advanced expertise. While humans still need to prompt GenAI to create malware, improving models and datasets increase the potential for self-evolving malware that can evade traditional security measures.[6]
- **More sophisticated phishing and social engineering.** Hackers can use GenAI to craft highly convincing phishing emails and messages, particularly personalised, context-aware content.[7]
- **Attack automation and scaling.** GenAI can automate reconnaissance, vulnerability identification, and execution of attacks. This includes hunting for security loopholes and vulnerabilities in applications and systems, and autonomously deploying malware.[8]

As corporates integrate GenAI technologies into their own operations, they also potentially increase their vulnerabilities to cyber intrusions. Context poisoning and prompt injection – techniques using carefully crafted inputs to manipulate how a model responds and change its behaviour – represent a growing threat vector.[9] The increasing adoption of agentic AI, with added layers of autonomous decision making, is likely to amplify cybersecurity risks.[10]

Source: Geneva Association

It is not just that cyberattacks are growing in volume and creativity. The attack surface is expanding as more companies rely on a dense web of third-party vendors, each one a potential threat vector. In 2024, 23.3% of all cyber incidents were caused by intrusions through third-party IT and technology companies, up from 10.9% in 2020, highlighting the growing indirect threat of compromised supply chains.[11] Increased reliance on cloud computing capabilities opens up another key operational vulnerability, especially among SMEs, who are often critically dependent on such services.[12] Managed service providers (MSPs), which oversee their clients' systems, are another potential entry point increasingly targeted by cyberattackers.[13]

1.2 Many firms underinvest in cybersecurity

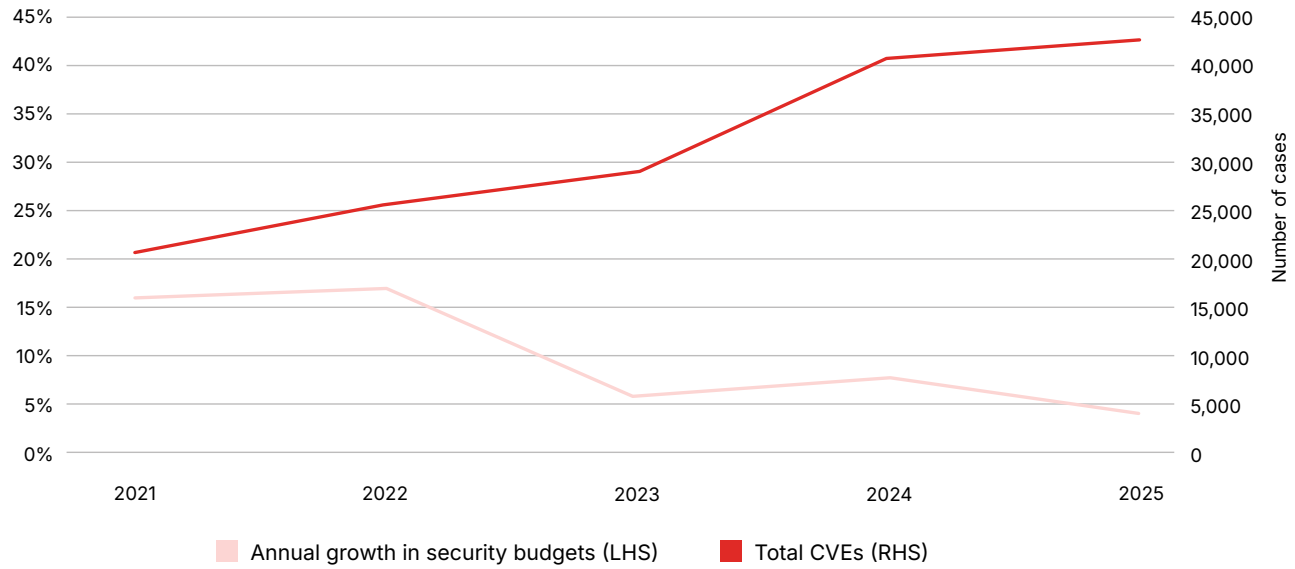
Despite growing cyber risks, established security weaknesses remain common, such as phishing emails, weak or reused passwords, unpatched software, and misconfigured systems. Targeting such vulnerabilities remains highly effective because many organisations still struggle to implement basic cybersecurity hygiene (e.g. effective firewalls, intrusion detection, or employee training). The Identity Theft Resource Center (ITRC) reports that more than 94% of data breaches in 2024 could have been prevented with simple cybersecurity protocols like multifactor authentication (MFA – a security method that requires users to provide more than one form of authentication to access an account).[14]

6 The Alan Turing Institute 2024.
7 Chipeta 2025.
8 In November 2025, Anthropic reported the first documented case of a cyberattack largely executed without human intervention at scale. A state-sponsored threat actor used Anthropic's GenAI tool, Claude Code, to autonomously conduct cyber operations against multiple targets, performing a wide range of post-exploitation activities from analysis, lateral movement, privilege escalation, data access, to data exfiltration. Anthropic 2025.
9 Arghire 2025.
10 McKinsey 2025.
11 A companion QBE-commissioned survey across nine Western countries revealed that among small businesses (100 to 2,000 employees) experiencing a cyberattack in 2024, 59% of incidents were linked to third-party suppliers, underscoring the rising threat of supply-chain cyber risk. QBE 2024.
12 According to a recent survey by Cyber Cube and Munich Re, small and mid-sized firms with revenues between USD 10 million and USD 100 million were found to be the most reliant on cloud services. Larger organisations showed declining dependence, likely due to more robust on-premise and hybrid architectures. CyberCube and Munich Re 2025.
13 Vakulov 2024.
14 According to ITRC, there were six major breaches in 2024, in which at least 100 million victims were affected. Four of those breaches could have been prevented if the organisations had deployed multifactor authentication. Delaney 2025.

An estimated 95% of data breaches can be prevented with simple cybersecurity protocols.

Many companies lack awareness of how rapidly cybercriminal business models evolve to exploit known and newly discovered weaknesses in IT systems. This is reflected in declining annual growth in security budgets in recent years, despite continuing security vulnerabilities (Figure 3).

FIGURE 3: GLOBAL CYBERSECURITY SPENDING VERSUS RISING IT VULNERABILITIES



Common vulnerabilities and exposures (CVEs) is a standardised dictionary/list of publicly known cybersecurity flaws.

Source: IANS and SecurityScorecard

1.3 Insurance as a risk governance mechanism

Insurance can play an important role in boosting cyber resilience, enabling firms not only to withstand an adverse disturbance (i.e. robustness) but also recover afterwards.[15] Besides compensating financial losses arising from a malicious or accidental incident, insurance can align incentives to upgrade risk prevention and provide resources and expertise to expedite remedial actions, mitigate losses, and hasten recovery. That applies not just to direct or indirect victims of a cyber incident who might shoulder most of the associated costs. It also includes encouraging strong security guardrails among MSPs, cloud platform providers, and hardware/software developers.

15 Brunnermeier uses the analogy of the oak tree and the reed to illuminate the distinction. An oak tree is robust. In a windstorm, it will stand strong – until it breaks. A reed, however, is resilient, designed to bend and move with the wind. Brunnermeier 2021.

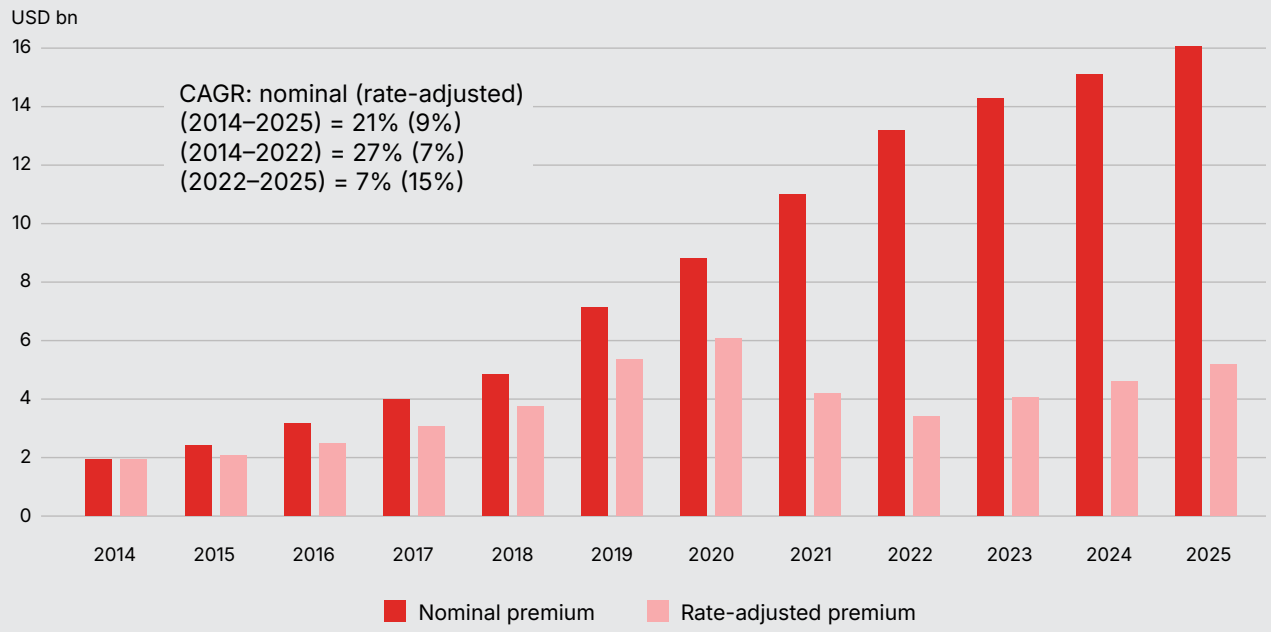
Box 2: Cyber insurance

Cyber insurance first appeared in the mid-to-late 1990s. Originally providing protection against liability claims from customers or business partners for harms caused by online content or data breaches, the scope of coverage has progressively broadened. Cyber policies now typically offer both first-party coverage (for own company losses like business interruption and data recovery) and a wide range of third-party liabilities, including expenses incurred during litigation and regulatory investigations. Cover can be purchased either as an endorsement to existing insurance or as a standalone cyber policy.

Notably, coverage has expanded to include claims arising from business practices, not just security breaches. For instance, protection against liability for wrongful collection – unauthorised or improper gathering of personal data – is often included in cyber insurance. More recently, some cyber policies now cover specific GenAI risks such as malicious interference with a firm's AI training data (i.e. data poisoning) and potential liability claims from third parties alleging copyright or intellectual property infringement.[16]

The standalone cyber insurance market has grown rapidly, especially over the past decade. Globally, premiums were worth around USD 16 billion in 2025, up from less than USD 1.5 billion in 2013. North America is the dominant region, commanding approximately two thirds of all cyber premiums. Europe is the second largest region, with a 21% premium share, while APAC is the third-largest market for cyber premium with a 10% share.[17]

FIGURE 4: GLOBAL CYBER INSURANCE PREMIUM GROWTH (2014–2025)



Source: Geneva Association, based on data from Howden and Swiss Re

Despite its rapid growth, cyber insurance still represents only around 1% of total property and casualty insurance revenues. Moreover, much of the market's recent expansion reflects higher premium rates in 2021 and 2022, when strong demand for protection pushed up the cost of coverage. As a result, rate-adjusted (i.e. real) premium growth was far lower than headline nominal growth (see Figure 4). Over the past two years, this has reversed: rising risk exposures have offset falling rates to support overall market growth. Future expansion will largely depend on boosting uptake in currently underserved regions and market segments.

Source: Geneva Association

16 AXA XL 2024.
17 Swiss Re 2025.

Different insurance policies may respond to a cyber incident depending on the specific policy wording, how the incident occurred and the losses that arise. As discussed in Box 2, a dedicated market for cyber insurance – the main policy intended to cover financial losses arising from cyber incidents, including those caused by third-party vendors – has developed rapidly. However, cyber insurance penetration in certain market segments and regions remains low. Estimates suggest only around 10% of SMEs globally have cyber insurance – and in some countries it could be much lower, especially among the very smallest firms.[18,19] Data from the North American and European markets show that cyber insurance take-up remains well below 10% for micro SMEs (Figure 5).[20] This is the case even though many have trouble safeguarding their cybersecurity. According to the World Economic Forum (WEF), 35% of small organisations believe their cyber resilience is inadequate, a proportion that has increased sevenfold since 2022.[21]

Estimates suggest only around 10% of SMEs globally have cyber insurance, with even less take-up among the smallest firms.

FIGURE 5: PERCENTAGE OF EACH CUSTOMER SEGMENT PURCHASING CYBER INSURANCE – NORTH AMERICA AND EUROPE

Source: Swiss Re

1.4 Report structure

Against this background, this report investigates how insurers can play a larger role in strengthening firms' resilience against cyber incidents, and how market developments could reinforce the value proposition of cyber insurance.

Section 2 of this report discusses the notion of cyber resilience and how firms can bolster resistance against cyber intrusions and system failures, as well as how to recover should they experience an incident. Section 3 considers how insurance can support resilience building, not only through indemnification of losses but also in the provision of vital pre- and post-incident services. Section 4 evaluates the resilience benefits of cyber insurance, how its role could be enhanced, and how adoption could be increased, especially among SMEs. The final section provides concluding remarks.

18 Swiss Re 2024.
19 WEF 2025.
20 Swiss Re 2025.
21 WEF 2025.

2 Understanding cyber resilience

Understanding cyber resilience

Resilience is not just about having effective risk management. It captures the ability of a firm to anticipate, absorb, and recover in the face of disruptive incidents.

Resilience describes how well a system maintains its structure and continues to function in the face of a disruption (see Box 3). The less it will be affected by a disturbance – both in terms of the degree and duration of any dysfunction in operability – the more resilient is the system. The state of a system depends on how it was designed and how it is operated. These choices influence whether and how output/service is degraded during a disruption, how quickly it recovers, and how completely it recovers. Like physical capital, the stock of resilience may depreciate naturally over time as new weaknesses or vulnerabilities emerge.

Box 3: Roots of resilience

Resilience is a widely used term, but its meaning can vary depending on the context. It entered into the English language in the early 17th century from the Latin verb resilire, meaning to rebound or recoil. Early uses were often related to the ability of materials to withstand severe conditions.[22] Modern-day applications of resilience emerged independently in ecology, psychology, and the social sciences in the 1970s.[23] The common thread is interactions within and among complex systems. At its core, it refers to "[t]he capacity of a dynamic system to adapt successfully to disturbances that threaten system function, viability, or future development of the system."[24]

Resilience in human and natural systems is often associated with sustainability in the face of constant change. That typically involves two kinds of response:

- **Adaptation:** Supports the resilience of a system by helping it stay in essentially the same state.
- **Transformational change:** If the maintained state becomes untenable, the system may move to a different stable state. Resilience is not always a matter of bouncing back, it may also suggest bouncing forward to a new state.

Narrow interpretations of resilience stress the ability to accommodate and recover from abnormal threats and events, be they enemy actions, natural disasters, or economic shocks. Broader definitions embrace awareness, detection, communication, reaction (and if possible, avoidance), and recovery.

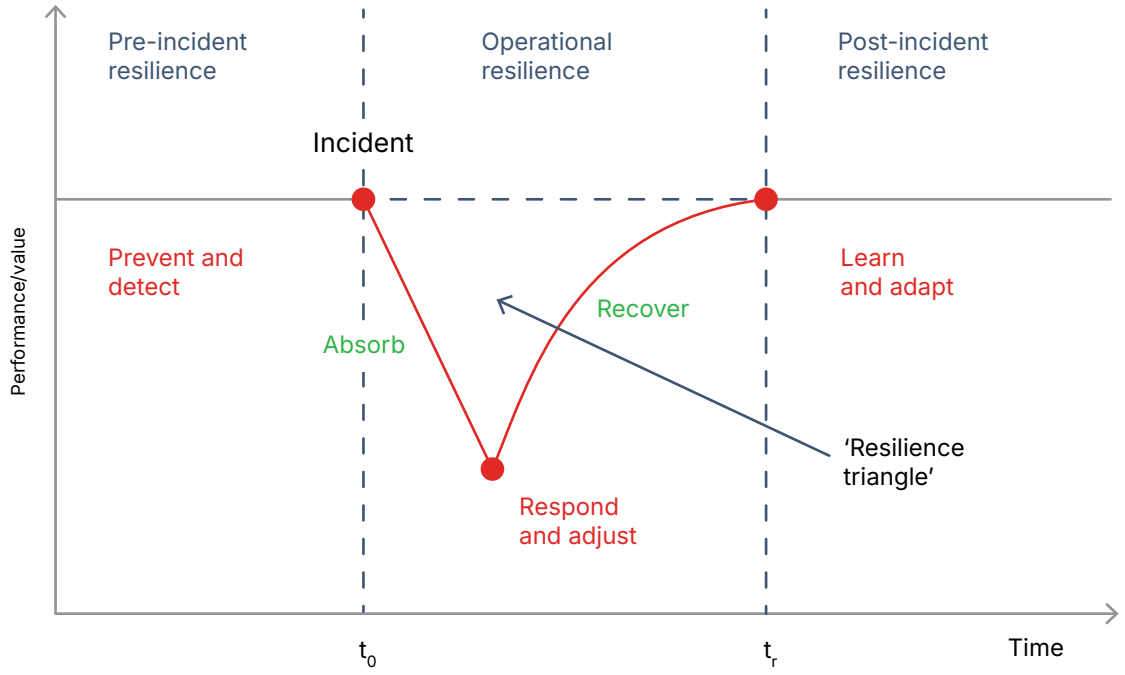
Source: Geneva Association

22 Torrens Resilience Institute 2010.
23 Knuth 2019.
24 Masten 2014.

2.1 The resilience triangle

The resilience triangle conceptually 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, perhaps because measures are in place to anticipate them and ameliorate their impact. Inevitably, however, some disturbances will be totally 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/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 6).[25]

FIGURE 6: A HOLISTIC VIEW OF RESILIENCE



Source: Geneva Association[26]

In the context of cyber incidents, a firm must decide how to manage the risk that a cyber event could seriously disrupt its operations (and ultimately impair its economic value). This involves the measures it can take to avert a cyber incident as well as those it can deploy to recover should it be hit. These actions might include investing in tougher cybersecurity controls, reconfiguring business processes and supply chains, taking steps to reduce legal or regulatory liability, and purchasing insurance to protect against unforeseen events.

2.1.1 Pre-incident preparedness

Pre-incident (preventive) cybersecurity controls include intrusion prevention and detection systems (see Box 4), as well as training programmes to reduce the risk caused by staff. Verizon estimates human factors – including phishing, intentional misuse by insiders, unintentional actions (e.g. unintended downloads of malware, software/hardware misconfigurations), and compromised user credentials – play a role in about 60% of all data breaches.[27]

Cyber resilience refers to the measures firms can take to avert a cyber incident as well as those it can deploy to absorb and recover should it be hit.

25 There is an analogy with investment in physical capital, where to maintain its capacity to produce, a firm must invest in plant and machinery, at least to offset any natural depreciation in the usefulness of those assets in production.
26 Graphic adapted from Bruneau et al. 2003.
27 Verizon 2025.

Box 4: Types of cybersecurity controls

Pre-incident: Firms deploy tools and procedures to safeguard their cybersecurity, including:

- Intrusion detection and prevention systems (IDS, IPS, IDPS) which alert the firm to attempted cyberattacks and aim to actively block potential malicious threats in real time.
- Firewalls and perimeter access controls to prevent unauthorised activity.
- Endpoint detection and response (EDR) to help guide the firm to detect and remediate threats on endpoints – physical devices connected to a network, such as mobile phones, desktops, laptops – before they can spread throughout the network.
- Vulnerability management to prioritise patching and mitigation of software vulnerabilities.
- Security information and event management (SIEM) systems to act as a central collection point of all cyber activity across a firm and help separate benign from malicious activity.

During an incident: Containment practices and technologies are used to identify, isolate, and limit the initial impact of cyber incidents, such as identifying malicious activities swiftly, isolating affected areas, and preventing the spread of the threat to other parts of the network or connected systems. Forensic software and hardware solutions are used to search for and analyse digital evidence of an incident. These tools help in recovering, preserving, and analysing data from various electronic devices to identify the root cause, understand attacker tactics, and restore or repair systems.

Post-incident: Recovery strategies and backups are used to restore systems and data after a cyberattack or other disruptive events. These tools help minimise downtime, prevent data loss, and get operations back to normal quickly. Key tools include backup and recovery solutions, incident response plans, and cybersecurity awareness training.

Source: Geneva Association, RAND

Zero trust principles, operating on the basis that no user or system should be automatically trusted, can enhance cybersecurity. Unlike traditional security models that rely on a defined network perimeter, zero trust requires continuous authentication, authorisation, and validation of security configurations before access is granted to applications and data.

2.1.2 Operational resilience

Operational resilience captures the main component of the resilience triangle, depicting a firm's reaction to a disturbance, the magnitude of its effect on the firm's value or output, and the speed and form of recovery.

If prevention security controls are insufficient, the immediate fallout will depend on the degree of redundancy in a firm's IT systems and its ability to run back-up processes to ensure operational continuity. Post-incident response and associated costs will be influenced by the firm's ability to assess the nature and scope of the incident and activate incident response plans to absorb and contain the harms as well as the associated financial costs.

Once the incident has been contained, the firm engages recovery controls to repair and restore any affected systems. Expediting remedial actions will limit damage to the firm's productivity (i.e. reduce the magnitude and duration of the initial disruption and reduce the downward leg of the triangle) and influence its recovery path. Recovery controls include digital forensics to identify any affected IT devices, cleaning and repairing those devices, restoring data from backups, as well as reconfiguring business processes and supply chains, and acting to reduce legal or regulatory liability.

2.1.3 Post-incident recovery

Even though a firm may fully restore its operational capabilities following a cyber incident, residual effects may linger. For example, an incident such as disclosure of confidential customer or corporate information may undermine trust in the firm, affecting its brand and future sales or profitability. As a result, even if the firm's operations are restored, the demand for its goods or services, and hence actual output, may be significantly impacted. Companies hit by a cyber event could also face persistent effects on the cost and availability of finance.[28]

28 One recent study suggests firms targeted by cyberattacks are significantly less likely to undertake seasoned equity offerings, and they raise smaller proceeds when they do. This effect, which is driven by reputational loss and higher financing costs, persists for up to three years and spills over to industry peers, altering equity issuance across entire sectors. Liu et al. 2025.

In addition, other parties beyond the firm could be harmed by a cyber incident, justifying a civil or criminal legal claim. Such liability can be costly and affect the future financial viability of the firm. The firm may also be subject to regulatory fines or fees that could have further financial or organisational repercussions. For example, the US Federal Trade Commission often imposes, in addition to pecuniary sanctions, cyber-security audit and consent orders for up to 20 years following an enforcement action.[29]

The reputational fallout from cyber incidents is a growing concern (see Table 1). According to a recent survey by Hiscox, 61% of those responsible for their firm's cybersecurity believe that reputational damage from a cyberattack would significantly damage their business. Close to two thirds (64%) believe they risk losing business if they do not handle client and partner data securely.[30]

TABLE 1: SURVEY VIEWS ON THE IMPACT OF CYBERATTACKS (% OF SURVEY RESPONDENTS CITING A FEATURE)

	2024	2023
Greater difficulty in attracting new customers	47	20
Lost customers	43	21
Bad publicity, which impacted brand reputation	38	25
Lost business partners	21	16

Source: Hiscox

2.2 Beyond conventional risk management

While resilience is closely related to risk management, the two are not the same. Risk management focuses on the actions firms take before an uncertain event occurs to limit potential losses. These actions typically include reducing risk (for example, lowering the likelihood or size of losses through operational safeguards), financing risk (such as building financial reserves), and transferring risk to others (for example, through warranties or insurance). In combination, these measures aim to bring risk exposure within acceptable tolerance levels.

Resilience describes the effectiveness of the firm's preventative measures and how well it copes after a risk has materialised.

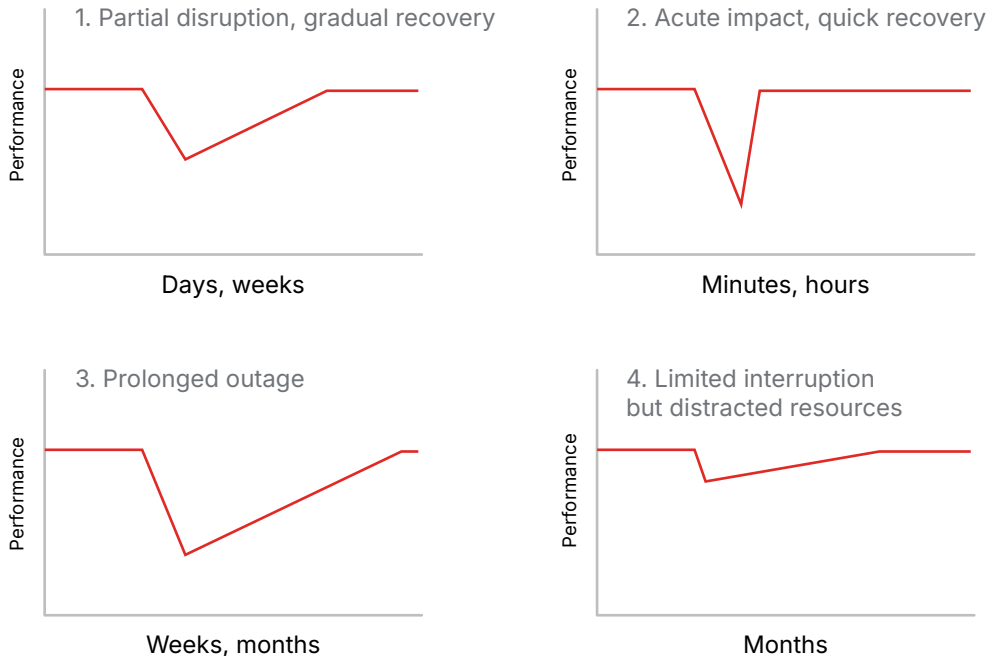
By contrast, resilience describes the effectiveness of the firm's preventative measures and how well it copes after a risk has materialised. Once an event occurs, uncertainty is no longer about whether it will happen, but about how severe its impact will be. Resilience, therefore, describes a firm's ability to prepare for, absorb and recover from operational and financial shocks in order to ensure their long-run sustainability.

2.3 The geometry of cyber resilience

A firm's resilience to a particular adverse event – and therefore the shape of the resilience triangle – will be influenced by: 1) its ability to reduce the probability of a successful intrusion or IT failure; 2) its ability to absorb the impact of that event; and 3) the time taken to fully recover from that event. Firms will be affected differently by different kinds of cyber incidents, and any one cybersecurity control may prevent or mitigate multiple kinds of adverse events.[31,32] Figure 7 outlines some notional resilience archetypes that illustrate different effects of incidents on firm performance.

29 In the US, cybersecurity consent orders are legally binding settlement agreements between a regulatory agency (such as the FTC, the Securities and Exchange Commission (SEC), or banking regulators) and a company that has violated cybersecurity, data privacy, or data protection laws. They are designed to correct security deficiencies, enforce compliance, and avoid full-scale litigation, typically lasting for a set period, such as 10 or 20 years. Atlantic Council. 2024.
30 Hiscox 2024.
31 Haimes 2009.
32 Weiss and Zobel 2024.

FIGURE 7: RESILIENCE ARCHETYPES



Source: RAND

1. Partial disruption, gradual recovery.
A firm suffers a relatively modest cyber incident, then recovers gradually over a period of days or weeks. Most ransomware attacks would fall into this category, given that these attacks typically target some, but not all, of a firm's operations, with firms experiencing an average recovery time of 21 days.[33] A 2024 IBM/Ponemon survey suggested 60% of firms took between 100 and 150 days to fully recover from a cyber incident.[34]

2. Acute impact, quick recovery.
This case reflects incidents that have an intense effect on a firm's output or performance but are resolved quickly. For example, DDoS attacks are usually temporary, typically lasting under 20 minutes, though some can extend to several hours.[35] Even one of the most serious and widespread DDoS incidents (the 2017 Dyn DDoS attack) lasted less than a day.[36]

Similarly, network or cloud service outages can dramatically affect a firm's services (either public facing, or internally). While they have the potential to cause losses across all of a cloud provider's customers, the effect on a single firm is generally short-lived. For example, the Amazon AWS outage in October 2025, while highly disruptive for affected firms, lasted around 15 hours.[37]

For most firms, the CrowdStrike incident of July 2024 would also be characterised as an acute impact with quick recovery.[38] A faulty software update caused a critical failure in Windows operating systems, but there was swift investigation into the cause, and a fix was available within hours. CrowdStrike reported that operations for 99% of their customers were restored by the end of the same day. Importantly, however, other firms such as Delta Air Lines faced a prolonged outage from the very same event, costing over USD 500 million and resulting in 7,000 cancelled flights.[39]

3. Prolonged outage.
Alternatively, a firm may experience a cyber incident and suffer considerable delay before it is able to restore all operations. For example, car manufacturer Jaguar Land Rover suffered a major cyberattack in the middle of 2025. After many months, it stated that it would restore partial operations in a 'controlled, phased restart' of some sections of its manufacturing facilities.[40] As a result of the cyberattack, it reported losing GBP 50 million in lost production per week, and required a government loan of GBP 1.5 billion.[41]

33 Coveware 2022.
34 IBM and Ponemon Institute 2025.
35 Akamai 2025.
36 Cloudflare 2025.
37 Butler and Jamali 2025.
38 CrowdStrike 2024.
39 Stempel 2025.
40 Bacon 2025.
41 UK Department for Business and Trade 2025.

Similarly, the cyberattack on the UK retailer Marks & Spencer in April 2025 disrupted many online and electronic services for 6 weeks, with some services unavailable for 15 weeks.[42] Even after operations resumed, it continued to experience backlogs and delays in order fulfilment.[43]

4. Limited interruption but distracted resources.
There is a final class of cyber incidents that may affect business operations only slightly but nevertheless distract the firm. These include fraud due to business email compromise, incidents of privacy violations, and even cases of data exfiltration and extortion. In these cases, there is little impact to business performance, though the firm may take weeks or months to resolve the issue.

42 Butler 2025.
43 Davey 2025.

3 The resilience-enhancing role of insurance

The resilience-enhancing role of insurance

Bundling pre- and post-incident services with loss indemnification strengthens the value proposition of insurers and enhances system resilience.

Cyber insurance has evolved from being 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 offer packages including security recommendations, cyber risk monitoring and alerts, and payment for the costs of experts should an incident occur.[44] In doing so, insurance can help firms 'shrink the V' of the resilience triangle by improving their pre-incident, operational, and post-incident resilience (see Figure 6).

3.1 A complement to cybersecurity investment

Some firms may regard cyber insurance and cybersecurity as substitutes – a firm could upgrade its cybersecurity to reduce its cyber risk, or purchase insurance to absorb the cost of large claims. However, when well managed, cybersecurity investment and insurance can be complementary and mutually reinforce each other.

Insurance can encourage best-practice cyber hygiene, including regular software and hardware patching, with improved terms and conditions for policyholders that strengthen their cybersecurity. Through their risk assessment procedures, insurers might also guide a firm to allocate resources to more advanced or cost-effective cybersecurity measures.[45,46] Likewise, experienced claim handlers can steer insureds to the best recovery solutions and help them efficiently respond to an event.

Cyber insurers have a vested interest in helping their policyholders minimise losses from a cyber incident.

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 the advice and guidance provided and coverage: prioritising more effective cybersecurity will reduce insurance claims.[47] By the same token, 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.

3.2 Cyber insurance-as-a-service

In assessing the potential synergies between insurance and cybersecurity, cyber insurers have progressively added services such as advisory, legal, and crisis management, to their product offerings (see Box 5). While technology-led start-up companies (InsurTechs) are often associated with this evolution, traditional carriers now also typically combine proactive protection and incident response (IR) services together with financial safeguards.

44 Romanosky et al. 2025.
45 Some academics model cyber insurance as a scheme where an insurer offers policies in which part of the premium is not set aside to cover losses but rather invested to decrease expected loss. Wang 2019.
46 A weak interpretation of Wang's insurance scheme is that it can be seen as assistance to insureds who are less than fully informed in selecting their appropriate level of investment in cybersecurity. Franke and Orlando 2025.
47 The Institutes 2025.

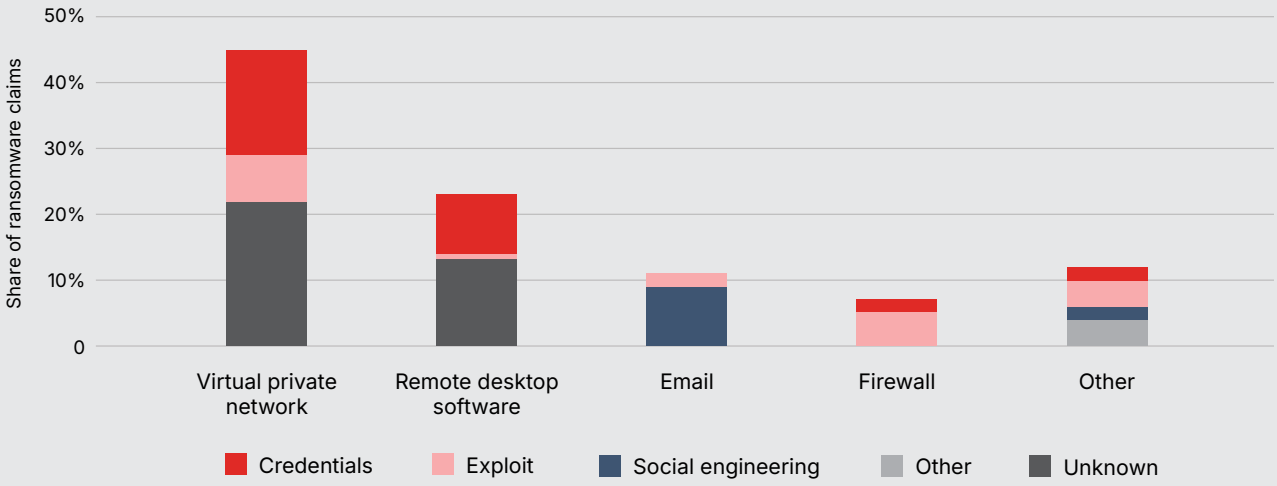
Box 5: Strengthening cyber hygiene through insurance

The insurance industry has learned it must go beyond pure risk transfer to sustainably offer cyber coverage that boosts policyholders' resilience. Modern cyber insurance typically provides ancillary cybersecurity services that guide businesses toward effective risk prevention and mitigation, in addition to covering crisis response.

Sharing threat intelligence

In most insurance lines, knowledge about effective loss controls accrues slowly as claims evidence accumulates.[48] However, cyber insurers cannot wait for insights from actuarial analysis years after the loss, as attackers may have changed tactics in the meantime. Instead, insurers must monitor vulnerabilities in real time and notify customers about emerging attack vectors. For example, the majority of 2024 ransomware claims started via unauthorised access to either the victim's virtual private network (VPN) (45%) or remote desktop protocol (RDP) systems (18%) (see Figure 8).[49] If one of these services is not secure, insurers can proactively inform insureds.

FIGURE 8: KNOWN INITIAL ACCESS VECTORS FOR RANSOMWARE CLAIMS



Note: Initial access vectors are methods cybercriminals use to gain a foothold in a network, primarily involving stolen credentials, social engineering (e.g. phishing), and exploiting software vulnerabilities.

Source: Coalition

Coalition, for example, gathers threat intelligence to send out alerts about new software vulnerabilities that are under active exploitation. This includes operating a global honeypot network – decoy systems that lure cybercriminals and reveal new attack methods – to collect real-time intelligence on ransomware tactics. This telemetry allows early detection of new ransomware campaigns, often before their impact is made public.

Hands-on support

However, this kind of information is useless if the customer does not have the capacity to take remedial action. Small businesses often lack the resources and/or expertise to resolve cybersecurity issues. Many insurance carriers mitigate the impact of an ongoing attack by providing access to 24/7 helplines to triage a potential event (even before confirming a breach and initiating a claim). In addition, Coalition runs a dedicated security support centre to guide policyholders to fix issues before they turn into incidents.

Policyholder incentives

Insurers have progressively sought to better differentiate prospective insureds according to the strength of their cybersecurity posture. This includes meeting certain security criteria as a condition of coverage. Aligning incentives can also work by rewarding good cybersecurity behaviour. For instance, policyholders who engage with recommended risk reduction services may benefit from reduced loss retention levels or lower deductibles.[50]

Source: Sezaneh Seymour and Daniel Woods, Coalition

48 For example, it took years for insurers in the late 1800s to discover that fire sprinklers reduced fire claims and offer corresponding discounts on property insurance. Canute 2025.
49 Coalition 2025.
50 Colletti 2025.

3.2.1 Pre-loss prevention

As part of their underwriting assessment, insurers may require their clients to undergo formal cyber penetration testing.[51] This involves deploying cybersecurity specialists, who actively attempt to breach the security defences of a system, network, or application to uncover weaknesses that could be exploited in real-world attacks.[52] Some carriers also work with bug bounty organisations to leverage the expertise of the broader ethical hacking community (see Box 6).

Box 6: Cybersecurity at SMEs: Leveraging bug bounty schemes

Cyber insurers increasingly emphasise protection services alongside loss indemnification to raise security awareness among their customers and encourage better security practices. One tool that some carriers are exploring is bug bounty programmes. These offer ethical hackers financial incentives to discover security vulnerabilities and weaknesses in a policyholder's IT systems. For example, Helvetia has partnered with GObugfree, a Swiss expert in bug bounty programmes, to develop a simplified vulnerability testing version called the Community Bugtest. This one-time security check helps SMEs identify and close vulnerabilities before they can be exploited. The service is not part of the cyber policy; rather Helvetia acts as an intermediary to introduce its customers to GOBugfree.[53]

How does the Community Bugtest work?

While similar in nature to a traditional penetration test, the Community Bugtest differs in scope and depth. Specifically, it is limited to a fixed timeframe (two days) and offers a streamlined, high-level overview of the company's security weaknesses. A penetration test, by contrast, typically examines a predefined scope in greater depth using a structured methodology.

GObugfree's employees simulate an external cyber-attack, relying solely on publicly available information to gain access to the firm's systems. Any resulting recommendations can then be prioritised and addressed by the company's own IT team or with the support of a specialised security partner.

The Community Bugtest serves as an entry point for small firms to understand how they might benefit from a full-scale bug bounty programme where outside ethical hackers are rewarded for discovering individual vulnerabilities in systems or software. However, the Bugtest itself does not involve any bounty payments. Instead, a company pays a one-time fee for this service.

Insurance benefits

Companies that implement security recommendations from vendors such as GObugfree reduce the cyber risks they face and as a result can make themselves more insurable. This can lead to better terms and conditions on their cyber insurance, including more favourable pricing as well as possibly higher coverage sums. Customers who additionally opt for ongoing monitoring schemes like a full bug bounty programme may benefit from even more favourable insurance terms.

Source: René Buff, Helvetia

Penetration tests are usually performed at the inception of the cyber insurance policy or at the annual renewal and include scanning exercises that automatically check for known software and hardware vulnerabilities, lack of security controls, and common network misconfigurations. External scans assess publicly accessible systems to identify vulnerabilities in perimeter defences, like firewalls and exposed ports. Internal scans focus on weaknesses within a network's internal infrastructure, with vendors often using authorised access to detect unauthorised or unpatched software.[54]

Alongside periodic scanning, cyber insurers also offer proactive monitoring and risk assessment. Many insurers now own or partner with cybersecurity firms – including third-party vendors providing Security Operations Center as a Service (SOCaaS) services – to offer endpoint protection or multifactor authentication and other cyber risk prevention and mitigation services. Such services seek to screen the public internet, as well as the dark web, for information about potential threats and vulnerabilities that could impact their policyholders.

Many insurers now own or partner with cybersecurity firms to offer endpoint protection.

Other insurers go even further, using offensive tactics to gather threat intelligence and build up a dynamic picture of the attacks to which their policyholders

51 Artais 2025.
52 Control Gap 2024.
53 The customer signs a separate contract with GObugfree, and the cost of the Community Bugtest is also borne by the customer. Thanks to the existing partnership between Helvetia and GObugfree, the customer benefits from a reduced price for this service.
54 Lockton Re 2024.

may be vulnerable. This includes partnering with tech start-ups that aim to disrupt cybercriminals' activities. For example, DarkWebIQ and Hudson Rock help identify potentially compromised accounts sourced directly from threat actors on the dark web and offer remediation advice to vulnerable firms.[55]

In addition to technical cybersecurity improvements, preventive organisational measures are another means to increase cyber resilience. These include, but are not limited to, regular training to raise employee awareness, a robust backup strategy, the definition and enforcement of access and authorisation policies, and the implementation of a cyber incident response/business continuity plan.

3.2.2 Post-incident response

If a policyholder's cybersecurity is compromised – whether the result of an accidental failure or malicious attack – insurers also arrange services to help businesses recover. These include forensic investigations to identify the cause and extent of a cyberattack to support remediation efforts, as well as legal, public relations, and communications support to manage the longer-term fallout of the cyber incident on a firm's reputation.

Insurers typically provide policyholders with a panel of pre-approved incident response firms and cover the associated fees.

Insurers typically provide policyholders with a panel of pre-approved incident response (IR) firms and cover the associated fees incurred by policyholders. The victim, or in many cases the firm's legal adviser, will choose and contract with the specific IR firm.[56] A key benefit of using an on-panel IR firm is that insurers can negotiate fixed upfront prices for IR services often below market rates. Insurers may still reimburse the fees of off-panel firms, but this will depend on the terms of the cyber insurance policy and usually must be agreed prior to the incident.[57]

Close cooperation between the insurance carrier and IR firms helps accelerate insurance payouts, which can be crucial in financing essential remedial and recovery work. Speedy claims handling relies on ensuring that the necessary forensic data and documentation are compiled and cross-checked against the terms of the policy. This can be aided by IR firms that are familiar with the insurer's claims procedures and can quickly provide additional information for the loss adjustment process.

3.3 A coordinating mechanism for resilience

One firm's cybersecurity depends not only on its own effort but also on the efforts of others in the same ecosystem (e.g. vendors and suppliers). In principle, insurance can function as a coordinating mechanism by fostering effective security investment that expressly considers the interdependence of cyber risks across firms.

Several academics have proposed approaches for an enhanced coordinating role for insurers, especially because they have visibility of multiple firms' cybersecurity postures, including vulnerabilities arising from the use of third-party service providers. For example, one study demonstrated that provided insurers can effectively evaluate and monitor policyholders' cybersecurity, they could design insurance contracts that incentivise security investments that take account of spillover effects across firms.[58,59] Another study considers a service provider and shows that an insurer will insure all agents (the service provider and its customers) as long as it can appropriately incentivise the provider to improve its security.[60]

Such policy features remain theoretical and have yet to find a commercial application. Nonetheless, an insurer's ability to leverage knowledge about interdependent cyber risks holds considerable promise to foster improved systemwide cyber resilience.[61] Short of re-working contract design, some authors also highlight how insurers might use insights from systems modelling. These models can assess cybersecurity interdependencies across firms and promote good security governance through the auxiliary services embedded in cyber insurance (see Box 7).

55 Henriques 2024.
56 In the US, the hotline that victims contact in the wake of a cyber incident tends to be run by a law firm as this helps to mitigate litigation risk. Woods and Böhme 2022.
57 Woods et al. 2023.
58 Khalili et al. 2017.
59 Similar results were derived by Franke and Orlando 2025.
60 Khalili et al. 2019.
61 One highly stylised model shows how an insurer may have an incentive to subsidise risk mitigation across different policyholders when a cyber disruption could trigger multiple losses across their insured portfolio. Zeller and Scherer 2023.

Box 7: Systems modelling for cyber insurance

Many companies now outsource key elements of their IT ecosystem, such as storage of customer data or security monitoring, creating critical external security dependencies. This calls for greater appreciation of how shocks can propagate and their effects be amplified across firms, as well as the systemwide benefits of key risk mitigation mechanisms like insurance.

Systems thinking: Building a framework for modelling based on computer science

A useful starting point is the concept of a distributed system, which is formed of:

- Connected locations, such as the rooms where servers and databases reside, connected by network cables, offices, and storerooms.
- Resources, such as computers, people, and inventory, which reside at the system's location.
- Processes that execute using the available resources at their locations to deliver the system's intended services.

Seen through this lens, the security properties of the ecosystem can be framed as an interdependent network of individual locations, resources, and processes.[62] Each firm – as owners of those digital assets – should decide its cybersecurity posture based on an understanding of how interconnections across firms will influence its chances of being affected by a cyber incident at another firm within the ecosystem. The more resilient the system, the better able it is to withstand cyber threats and keep operational capacity within agreed tolerances.[63]

Modelling these interactions is mathematically challenging and requires rigorous analysis.[64] A well-constructed model of a system can nevertheless help identify security weaknesses and guide decision making around firms' cyber resilience. In turn, it can inform insurers in underwriting cyber risks.

A systemwide resilience role for cyber insurance

By aggregating and disseminating information about threats and vulnerabilities across firms and shaping coverage to incentivise best-practice cyber hygiene, insurers can enhance systemwide cyber resilience. In this way, insurers can function as decentralised enforcers of good security governance, expressly taking into account that weak cybersecurity by some firms can impose negative externalities on others.[65]

Such a stewardship role for insurers is most obvious when they possess full information about threats and vulnerabilities and have the ability to steer policyholders' appropriate investment in cybersecurity. In practice, insureds may have better knowledge of their internal risk posture than insurers and disclosure may be resisted. Cyber threats also change rapidly and dependencies and externalities shift, meaning that what is good practice today may be insufficient tomorrow.

Significant progress has been made in recent years in helping to understand the dynamic characteristics of the cyber risk ecosystem, but further work is required. For cyber insurance to fulfil its potential to contribute to overall cyber resilience, there needs to be common understanding of the processes that influence the frequency and severity of cyber losses, otherwise the market will always be inherently inefficient.[66]

Source: David Pym, University College London (UCL), and Henry Skeoch, Beazley

62 The concept of an ecosystem of distributed systems — based on locations, resources, and processes — is scale-free: it can be deployed to describe systems that are of essentially any scale, from chips, through an organisation's network or business architecture, to a whole sector of an economy. Baldwin et al. 2021; Arnold et al. 2021.
63 This concept is often described as security maturity.
64 Ilau et al. 2025.
65 Ioannidis et al. 2019.
66 Skeoch and Ioannidis 2024.

4 How effective is cyber insurance at improving cyber resilience?

How effective is cyber insurance at improving cyber resilience?

Insurers should do more to emphasise the full benefits of cyber insurance to policyholders, especially for smaller firms, and how bundled services can strengthen cybersecurity.

High hopes have been placed on the ability of cyber insurers to enhance firms' cyber resilience.[67] Nevertheless, doubts persist about whether cyber insurance can fulfil that promise. This section reviews the available empirical evidence on how well cyber insurance supports cyber resilience, drawing on existing studies and market intelligence gathered from industry participants.

4.1 Insurers pay claims and influence insureds' cybersecurity posture

Insurance broker Willis Towers Watson analysed 4,650 cyber claims in over 90 countries, finding that 92% of notifications of potentially covered losses fell within cyber insurance coverage.[68] By comparison, while insurers paid out on more than 90% of claims on motor insurance in the UK, the acceptance rate was around 70% on home buildings and contents policies, and closer to 50% for some lines such as legal insurance.[69]

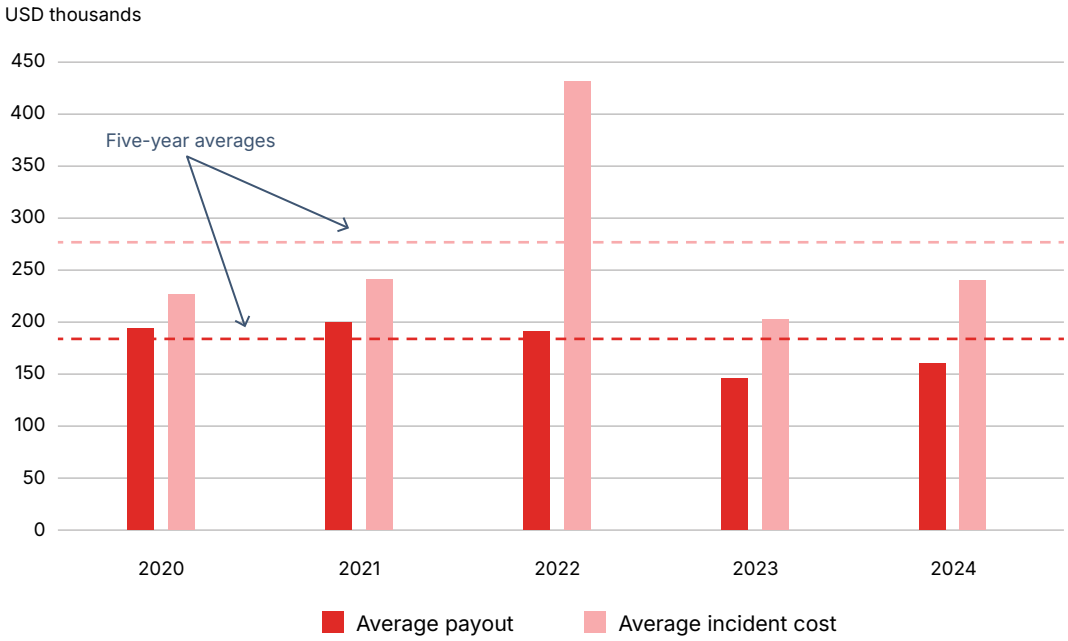
Claims analysis found that 92% of notifications of potentially covered losses fell within cyber insurance coverage.

Data for the US, Canada and the UK also show that the average cyber insurance payouts represent a material share of overall costs of an incident, close to 70% in the case of SMEs (see Figure 9).[70] Across the industry, the majority of claims funds are spent paying for professionals to help respond to incidents.[71] Crisis costs (including the costs to engage a privacy attorney to help navigate an incident and establish privilege, a digital forensics incident response firm (DFIR), and specialists to handle public relations, notification, and credit monitoring) average about 52% of expenses. Such services are crucial as publicly funded emergency services, such as the police, do not typically provide operational support to recover from cybercrime.

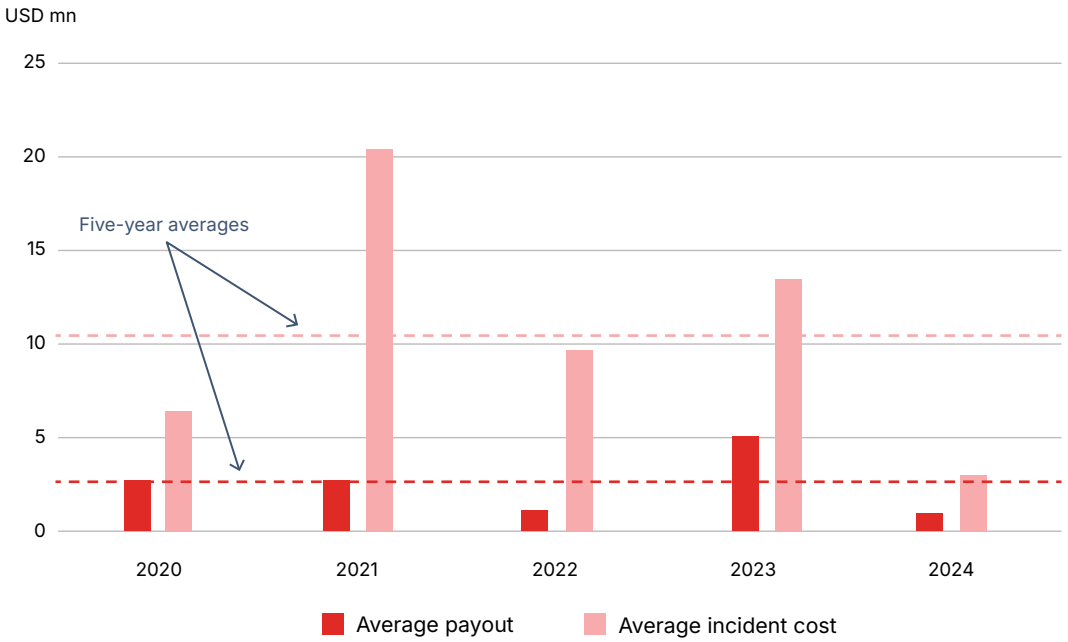
67 Franke and Orlando 2025.
68 Willis Towers Watson 2025.
69 Financial Conduct Authority 2025.
70 Data for other insurance lines are not readily available. However, comparing average UK home contents insurance claim with the costs associated with a burglary suggests a payout proportion of somewhere between 50% and 75%, depending on how much the insurance policy would respond to property damages from a break-in.
71 NetDiligence 2024.

FIGURE 9: CYBER INSURANCE PAYOUTS AND INCIDENT COSTS

Insurance payouts and incident costs – SMEs



Insurance payouts and incident costs – large companies



Source: NetDiligence

Surveys indicate that, through their underwriting procedures, cyber insurers have a positive impact on policyholders' cyber hygiene. In particular:

- According to cybersecurity provider Delinea, cyber insurance requirements are driving heavy investment in cybersecurity tools. Around 96% of companies surveyed purchased at least one cybersecurity solution before being approved for coverage.[72]
- A 2024 survey by cybersecurity solutions company Sophos 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 made increased investments in cybersecurity in order to apply for cyber insurance.[73]
- A survey commissioned by InsurTech At-Bay showed cyber insurance helps encourage security measures, mitigation strategies, and targeted spending. More than 70% of respondents said they view cyber coverage as important or critical to their company and reported increased spending on cybersecurity solutions over the past 12 months.[74]

Case studies also highlight how cyber insurance improves policyholders' cyber resilience (see Table 2). Likewise, past studies endorse the supportive role of cyber insurance in dealing with a cyber incident.[75]

TABLE 2: SELECTED CASE STUDIES OF SUCCESSFUL INSURER-LED UPGRADES IN FIRMS' CYBERSECURITY POSTURE

Issue		Insurer-led solution	Outcome
Improve insureds' cyber risk preparedness	• Global veterinary medicine company with immature internal security controls resulting in limited insurance coverage.	• Prioritised actions, enabling rapid approval and implementation of controls, including MDR and Privileged Access Management (PAM) capabilities.	• Established a mature security programme by fully implementing critical controls. • Shifted to a proactive security culture integrated with insurance.
	• A company in the tech and security industry experienced a data breach, with serious implications for its reputation and insurability.	• Built an actionable cyber-hygiene plan with the goal of prioritising targeted controls. • Engaged in monthly meetings with the client's IT team to ensure the cyber-hygiene plan was on track.	• Successfully demonstrated the company had a stable risk profile. • Helped client qualify for improved insurance coverage on better terms than previously available.

72 Delinea 2024.
73 Sophos 2024.
74 Jones 2024.
75 Woods and Böhme 2021.

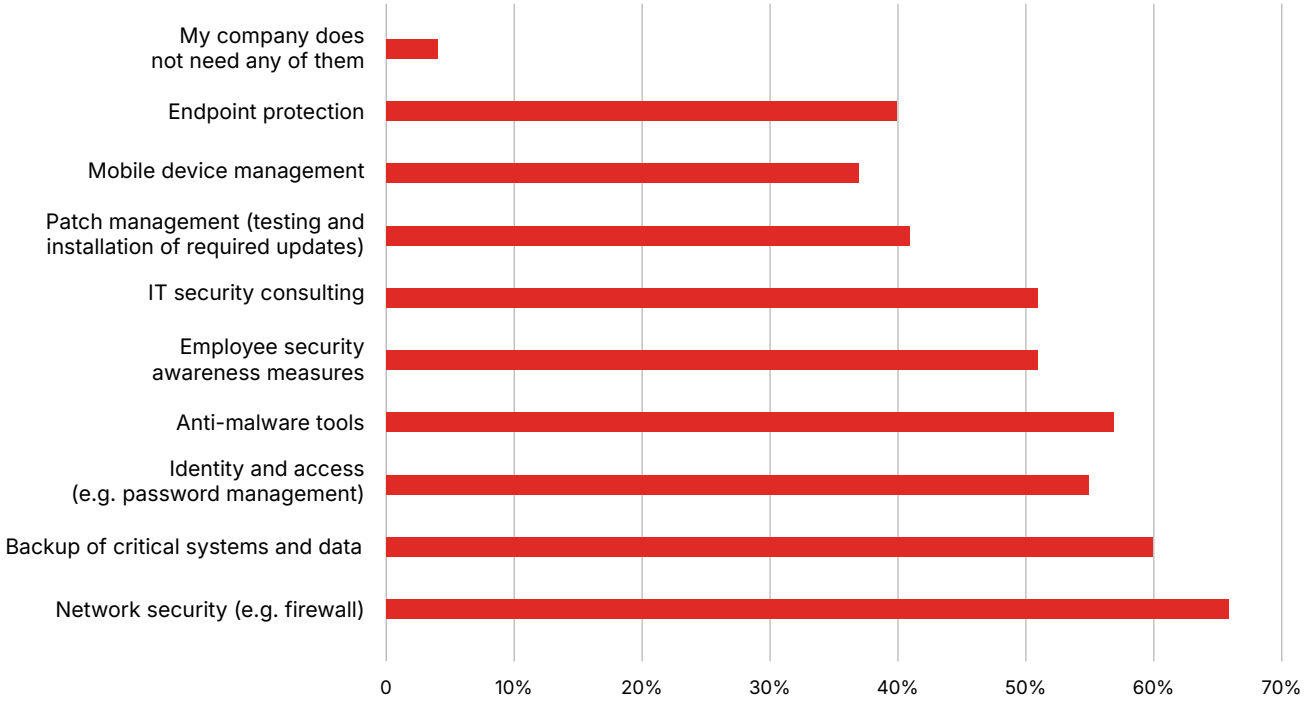
Issue		Insurer-led solution	Outcome
Contain and recover from a major cyber incident	• A medium-sized public sector organisation experienced a ransomware attack that disrupted its operations.	• Connected the client with partner firms specialising in forensic investigation and incident response. • Engaged legal counsel to advise on regulatory obligations.	• Forensic investigation provided a comprehensive understanding of the threat actor's activity and capabilities. • Avoided ransom payment and shortened incident duration. • Policy contributed to response and data recovery costs, including expenses for forensic investigation, legal counsel, and system restoration.
	• Law firm's administrative operations hit by a phishing email, potentially exposing sensitive client data.	• Engaged a forensic specialist to investigate the attack and determine the scope of the data breach.	• Policy paid for all forensic and legal response costs. • Client successfully navigated complex reporting obligations to its regulator.
Optimise insurance coverage	• Local government addressing critical IT challenges, including missing documentation, weak vendor risk management, and threat of ransomware attacks.	• Review of the organisation's cybersecurity posture. • Identified control gaps, compliance issues, and potential mitigation strategies.	• Aligned risk transfer with security initiatives to improve the organisation's risk profile and increase insurance coverage. • Developed an improved cybersecurity roadmap.
	• Technology firm facing difficulties aligning its IT and business teams on cybersecurity priorities in the wake of a recent company acquisition.	• Partnered with insurer to drive visibility, prioritisation, and cross-functional alignment. • Vendor risk reports commissioned to supplement regular due diligence for ongoing acquisitions. • Tabletop exercise to overcome communication gaps.	• Leadership and IT aligned on top risks and security investments across brands and functions. • Enhanced vendor risk visibility, reducing exposure in global supply chains. • Matured incident response and continuity planning to strengthen brand trust and investor confidence.

Source: Tom Egglestone, Resilience

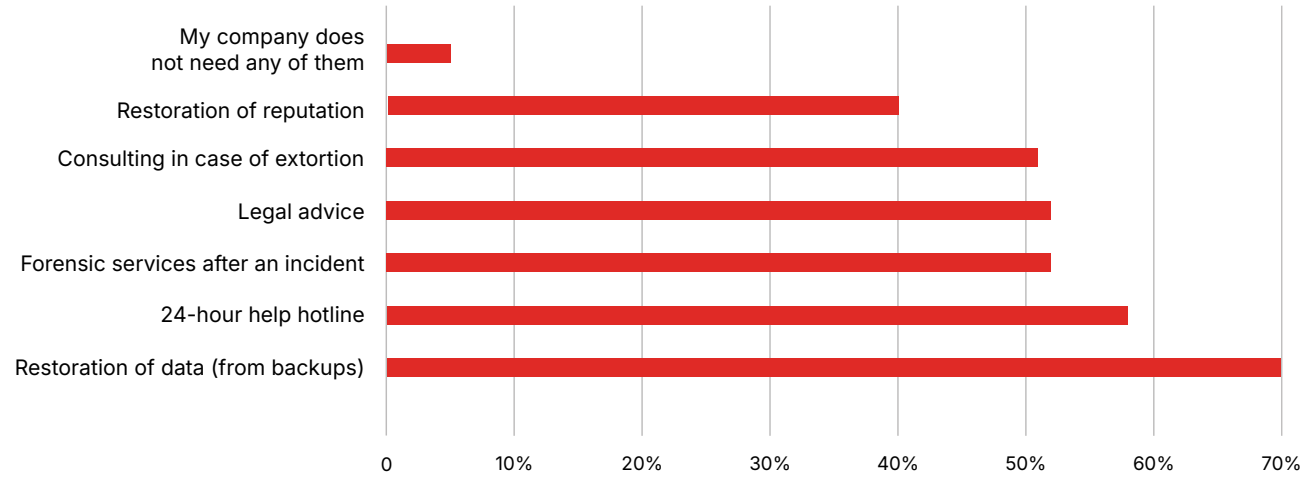
Organisations that have cyber insurance say they appreciate how it aids their overall security posture. A Munich Re survey indicates the majority of policyholders welcome the provision of ancillary services from carriers and see them as integral to cyber insurance (see Figure 10). Similarly, a recent Howden poll indicates that firms with insurance policies that include such services believe they significantly improve their capabilities to cope with a cyber incident.[76] As highlighted in Box 8, firms that deploy common security controls advocated by cyber insurers are much less likely to experience a breach.

FIGURE 10: CYBER INSURANCE SURVEY INDICATES THE MAJORITY OF POLICYHOLDERS WELCOME THE PROVISION OF ANCILLARY SERVICES FROM CARRIERS (% RESPONDENTS)

Which of these pre-incident services should be covered by cyber insurance solutions for protection against cyberattacks?



Which of these post-incident services should be covered by cyber insurance solutions for protection against cyberattacks?



Source: Munich Re

76 On average, 35% of survey respondents with cyber insurance report pre- and post-incident services improve their cyberattack-response capabilities. This compares with 15% of firms who are uninsured. Howden 2025.

Box 8: Insurance promotes good cybersecurity

Cyber insurers play a vital role in identifying cybersecurity weaknesses and providing access to specialised expertise to address them. In the first instance, insurers may refuse to cover entities that demonstrate poor cyber hygiene. For example, Allianz declined insurance to a prospective client in the financial sector due to inadequate endpoint and network protection controls. Similarly, an airport client was not offered protection because its cybersecurity posture was deficient, including the absence of MFA for remote access, limited vendor management processes, and weak backup management.[77]

Beyond the initial screening, cyber insurers' underwriting and risk prevention services provide actionable insights insureds can use to strengthen their cyber resilience. Cyber360 assessments, workshops, and risk scenario analyses, provide policyholders with enhanced transparency and control across their digital ecosystem. According to a recent study of security controls commonly used by cyber insurers when assessing risk, organisations that regularly test their cyber incident response plans are significantly less likely to face breach-related insurance claims.[78]

By developing and analysing tailored threat scenarios and emerging potential vulnerabilities, insurers help reduce their clients' potential exposures through targeted mitigation strategies. For example, in March 2024, insurers notified policyholders about a particular Citrix software vulnerability along with advice about implementing the required patch, enabling their policyholders to mitigate the threat of a ransomware attack.[79]

Source: Rishi Baviskar, Allianz Commercial

4.2 Market realities may blunt its governance role

Despite encouraging signs that cyber insurance contributes positively to firms' cyber resilience, several market features still restrict its potential to promote effective cybersecurity governance. These reflect factors affecting both the supply of and demand for coverage.

In some cases, companies buy cyber insurance simply because of contractual commitments with their customers or suppliers rather than a conscious decision to optimise their cybersecurity. Such contractual obligations often mandate vendors to purchase cyber insurance, specify incident response roles, and ensure timely breach notifications by affected firms. For example, contracts often include data protection and breach notification clauses aligned with insurance coverage requirements. Where those clauses do not exist, some companies may simply eschew cover.

4.2.1 Limits to risk differentiation

To underwrite and price cyber risks accurately, insurers must align discoverable risks and exposures with factors unique to each business. This includes details collected during the application process, as well as other factors, like individual cybersecurity controls deployed by the firm.[80] 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.[81]

To some extent, this situation stems from a lack of reliable data either because the underlying risks are rapidly evolving, or the information that insurers have about firm's cybersecurity posture is insufficiently granular or is incomplete. For example, despite advances in technographic data capture, insurers may have limited insight into clients' business continuity plans, cloud architecture, and intangible asset exposure.

Outside-in scanning tools offer additional information about a policyholder's vulnerabilities, but they provide only a partial snapshot and must be combined with details about the firm's internal IT infrastructure and configurations. Recent empirical research suggests insurers still largely base their risk selection on policyholders' self-assessed cybersecurity questionnaires, even though automated security scores produced by external vendors may have more predictive power about future claims (see Box 9). Furthermore, the same study finds that insurers primarily manage their exposure by capping coverage rather than fine-tuning prices according to the riskiness of the insured.[82]

77 Analysis shows that in over 80% of large claims, insureds' decisions significantly influenced loss size, with many incidents preventable through basic controls such as patching, segmentation, backups, and MFA. Allianz 2025.
78 Recamara 2025.
79 See, for example, Seymour 2024.
80 Coalition 2024.
81 Todyl 2025.
82 Improved terms and conditions on available insurance might not influence firms' cybersecurity decisions. A saving of USD 10,000 on a policy offering only USD 100,000 limit is unlikely to change incentives, especially if the required security investment itself costs USD 100,000.

Box 9: How cyber insurers select and price risk: insights from an empirical analysis

Advances in data collection and analytics have substantially improved the tools available to evaluate a firm's cybersecurity posture. Automated scanning tools, as well as techniques to detect, block or redirect malicious intrusions (e.g. honeypots and sinkholes), now routinely gather information on open ports, vulnerabilities, and malware infections.[83] Specialist vendors translate these observations into cybersecurity scores which, although imperfect, have been shown to be empirically useful in predicting cyber incidents.

A central question is the extent to which cyber insurers use these tools in risk selection and pricing. If insurers can accurately identify firms' risk characteristics and adjust premiums accordingly, they can mitigate adverse selection (where high-risk companies disproportionately seek coverage) and moral hazard (where insured firms face weaker incentives to maintain good cyber hygiene). Improved risk differentiation should, in turn, strengthen insureds' incentives to invest in their own cybersecurity.

Selecting and screening prospective policyholders

A recent study examined a proprietary dataset combining US data on cyber insurance take-up, cyber incidents, and firm-level cybersecurity risk indicators from one of the largest insurance brokers.[84] For contracts sold through the broker between 2019 and 2022, firms with higher cyber risk – measured either by past incidents or by external security vendor scores – were more likely to purchase cyber insurance. That result could reflect two effects: demand-side selection (riskier firms seek coverage) and/or supply-side screening (insurers selectively underwrite high-risk firms at higher premiums).

To investigate this issue further, the study deployed additional survey data from the broker. The surveys captured firms' self-assessed cybersecurity posture, allowing the researchers to distinguish between firms that intended to apply for insurance and those that ultimately obtained coverage.[85] Regression analyses – using as dependent variables the probability of applying for cyber insurance and the probability of obtaining coverage – indicated that:

- Firms intending to apply for insurance were generally more alert to their underlying cyber risk exposure, either because they experienced a cyber incident or their cybersecurity score declined.
- Most firm characteristics, including firm size and cybersecurity score, were not statistically significant predictors of being insured, suggesting limited screening by insurers based on these variables. In contrast, the survey-based score was a significant predictor, indicating insurers relied more heavily on self-reported assessments when screening applicants.

Alongside prior research highlighting how questionnaires often understate technical or infrastructural features that matter for accurate risk assessment, this empirical evidence suggests insurers still lean on imperfect survey metrics, even when more predictive indicators – such as external risk scores or incident histories – are available.[86]

Pricing and coverage of cyber risk

Additional regression results on the same dataset showed that while small firms with recent incidents received higher coverage limits, their cybersecurity scores did not meaningfully influence the premiums they paid. Instead, insurers appeared to manage exposure primarily by capping the amount of coverage – particularly for large firms – rather than by adjusting premiums to reflect changes in risk.

Combined with the previous finding that firms with higher risk are more likely to apply for cover, the regression analysis suggests that adverse selection may arise from insurers not fully incorporating certain risk factors into their screening and pricing decisions. Furthermore, capping coverage is consistent with insurer capacity constraints and the need to control aggregate exposure to potential catastrophic cyber losses, resulting in tighter policy limits for large clients.

83 A sinkhole is a cybersecurity tool that intercepts and redirects malicious internet traffic to a controlled server.
84 Ning 2025.
85 Due to data availability, the regression analyses focus only on the years 2021 and 2022, when survey responses are most complete.
86 Romanosky 2019.

Some caveats

As with any empirical study, we should exercise caution when generalising the findings. Insurers may not fully incorporate cybersecurity scores into underwriting procedures simply because these measures are typically accessible only to large carriers. In addition, the reliability of the scores takes time to establish, and retrospective adjustments after incidents reduce their usefulness for prospective underwriting.

Another consideration is moral hazard: obtaining insurance might prompt firms to scale back cybersecurity investment, thereby increasing their risk profile. Such behavioural changes could mimic patterns typically attributed to adverse selection. However, the study found no evidence that acquiring insurance led to an increase in cyber risk – whether measured by security scores or the likelihood of an incident.

Source: Dingchen Ning, University of St. Gallen

4.2.2 Practical obstacles to steering effective risk prevention and mitigation

Although cyber insurance can improve policyholders' cybersecurity posture, 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.[87]

A lack of awareness and understanding about cyber insurance products leads firms to underestimate their value.

There may be a lack of understanding regarding the relationship between cybersecurity controls and cyber insurance.[88] The Federation of European Risk Managers Associations highlights how a lack of awareness and understanding about cyber insurance products leads firms to underestimate their value.[89] One poll of UK insurance brokers, for example, revealed that almost half (49%) said that they had encountered a challenge from their client's IT department, stating that they did not need cyber insurance.[90] Some firms also reportedly prefer to design and draft their own cybersecurity programmes in advance of qualifying for insurance, rather than collaborating with carriers, while others dismiss non-risk transfer options altogether, either viewing them as unnecessary or irrelevant.[91]

Even if companies do make use of insurers' pre-incident security services, some firms may be reluctant to adopt recommended security measures that could disrupt daily operations or require significant changes to their IT systems.[92] This resistance may be especially severe if insurers insist not only on implementing initial security protocols, but in monitoring ongoing compliance with those security measures. Policyholders may also worry that sharing sensitive cyber information will affect future insurance pricing and coverage.

Similarly, in terms of supporting victims of cyber incidents, insurers may not always have the technical expertise to place the best vendors on their pre-approved IR panels. Instead, the main selection metric is often cost rather than competence. IR firms may prioritise speed and cost over understanding the underlying factors behind a security incident, which can lead to inadequate incident response plans, poorly trained teams, and ultimately more severe and costly incidents. [93] Recognised best practices in IR are emerging; the challenge is to ensure these are routinely followed, especially during an unfolding crisis, and actionable lessons can be extracted from insurance claims (see Box 10).

87 QBE 2024.
88 FERMA 2025.
89 FERMA 2025.
90 CFC 2023.
91 QBE 2024.
92 Resilience Forward 2025.
93 Woods et al. 2023.

Box 10: Incident response best practices

Cybersecurity requires continuous investment of time and resources to remain at the forefront of defence against a rapidly evolving risk. To many, that means purchasing tools and focusing on preventive capabilities, but the most effective approach also involves intentional and dynamic incident response planning. Such advanced planning features measures such as:

- **Commit to working with cyber specialists.** IR is best undertaken by experienced, qualified professionals focusing on specialised tasks such as containment (to limit disruption), digital forensics (to gather and preserve evidence), and recovery (to restore damaged systems).
- **Interview potential response partners.** Familiarisation with the response team enables the firm to vet the capabilities and open dialogue with key stakeholders, including the firm's cyber insurer.
- **Develop nimble, lightweight incident response playbook(s).** Clear roles and responsibilities speed up decision making in the event of a cyber incident. Too frequently, organisations develop overly complicated plans that hamper response.
- **Establish secure communication channels.** Prepare separate, independent communication methods (e.g. encrypted messaging or dedicated phone lines) in case primary systems are compromised. This is often overlooked in advance but becomes much more challenging in the face of disruption.
- **Integrate legal and regulatory requirements.** Map out notification timelines and compliance obligations for jurisdictions where the organisation operates. This is a key area to revisit periodically as regulations are continuously evolving.
- **Conduct regular tabletop exercises.** Realistic tests of the IR plan help prepare teams across the organisation and identify gaps in planning.
- **Establish rigorous documentation approach.** Ensure network configurations, critical system assessments, contact lists, plans/playbooks, and other pertinent documentation remain up-to-date and accessible offline.

When an incident does occur, the planning and preparation will be put to the test. Even well-trained teams can struggle with the complexities of a real incident, so it is important to stay focused on key operating principles, such as:

- **Resist the temptation to pursue quick technical fixes.** Without full knowledge of the incident and the integrity of digital records, knee-jerk reactions can hinder recovery efforts and jeopardise key forensic evidence.
- **Do not engage a threat actor.** Interaction with the perpetrators of a cyberattack should be delegated to experienced incident responders under the firm's supervision.
- **Ensure effective communication channels.** Good decision making requires a clear chain of command, ideally in a pre-established and road-tested structure.
- **Establish dedicated workstreams.** This ensures that issues like technical, legal and compliance, media and investor relations, and business continuity can be worked out in parallel with good collaboration across teams.
- **Set realistic goals.** By setting the anticipated recovery timeline, updated as the incident unfolds, the response team will be better able to prioritise actions. Information sharing may vary across different stakeholders, but too little communication can create confusion and undermine crisis management.

While not exhaustive, these tips represent good guidelines for an organisation to consider when preparing for and dealing with a cyber incident. Ideally, the IR process would be combined with a consistent approach to learning lessons internally from near misses and leveraging successful tactics from industry peers.

Source: David Shluger and Nick Steinmann, AXIS Capital

4.2.3 Misaligned incentives and institutional frictions

Insureds may be wary of the close relationships that insurers have with cybersecurity vendors, fearing they are being sold something they do not understand and may not need. 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. The reluctance to share information undermines transparency and trust.[94]

94 FERMA 2025.

Policyholders may not want to provide all the necessary information insurers need for loss adjustment.

Similarly, the involvement of MSPs can complicate the resolution process, if they fear inadvertently incriminating themselves should their actions have contributed to an initial malware infection or its subsequent propagation. The participation of third parties often introduces contractual and communication issues. These can slow down IR measures, incentivise IR practitioners not to write down remediation steps or to produce formal reports, and restrict access to any documents produced which adds to disruption costs.[95] Such institutional frictions hinder insurers' abilities to process claims quickly and efficiently.

4.2.4 Ambiguity surrounding potential cyber catastrophic events

The ambiguity over the likelihood and size of cumulative losses that might accompany a major cyber event – for example, possible accumulated claims from the common failure of IT systems or the contagious spread of malware – continues to restrict re/insurer appetite to underwrite cyber risks.[96] That casts a shadow over the development of the cyber insurance market.

The ambiguity over the likelihood and size of cumulative losses that might accompany a major cyber event continues to restrict re/insurer risk appetite.

Individual policy limits are often set low, and certain risks are excluded from regular cyber policies. Losses linked to acts of war, terrorism, or state-sponsored cyberattacks are typically not covered – due to the difficulty of attribution and the sheer scale of potential claims – although some carriers may offer coverage for hostile cyber activity not categorised as war.[97] Similarly, losses resulting from the failure of essential infrastructure like power, gas, or telecommunications services, are generally excluded. Moreover, the providers of capital to insurance companies must be compensated for the uncertainty surrounding future possible large cyber losses, which increases the premiums cyber insurers charge to policyholders.

The pragmatic use of exclusions and limits ensures insurers do not overstretch their own balance sheets and are able to keep promises to policyholders. However, if exclusions are too broad or poorly aligned with customer expectations, they may undermine long-run demand. This is especially the case if opaque and ambiguous policy wordings mean insurance payouts are perceived as unreliable. For some larger clients, individual policy limits may be too low to provide meaningful protection against cyber risks.

Firms may question the benefit of buying cyber insurance if largely unavoidable, or at least hard to mitigate, risks are not covered, even though insurance can offer crucial protection against many of the more regular cyber-hygiene risks, including pervasive cybercrimes like ransomware. Hence, it is imperative that insurers continually upgrade their products and services so that they remain relevant in protecting cyberspace. The next section evaluates the steps that insurers could take (and are starting to take) to enhance the value proposition of cyber insurance and boost adoption.

95 Woods et al. 2023.
96 Insurers face significant challenges in assessing and managing cyber accumulation risk. Geneva Association 2023.
97 Wolff 2023.

5 Fostering increased take-up of cyber insurance

Fostering increased take-up of cyber insurance

Insurers can tailor products, enter partnerships, and support security initiatives to more clearly demonstrate the value of cyber insurance.

There is no such thing as a risk-free organisation. Businesses must embed resilience into their technology systems, anticipate third-party vulnerabilities, and build continuity planning into their operations. Insurance can be a key enabler of the 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.

5.1 Raising awareness of cyber risks and the full benefits of coverage

Corporate boards often express confidence in their cyber readiness and cybersecurity oversight is increasingly a core governance priority.[98] However, awareness of heightened cyber risks needs to translate into effective cybersecurity controls. According to a recent Willis Towers Watson survey, most company boards report they have a cyber incident contingency plan, but only around two thirds (68%) have tested those arrangements over the past year.[99] Other studies suggest that the shortfall in preparedness is even bigger among smaller firms.[100]

Historically, many organisations have prioritised cybersecurity prevention, focusing on technical tools like firewalls and antivirus software to block attacks before they happen. Consequently, cyber insurance is often overlooked, even though insurers can frequently guide policyholders on cybersecurity best practices.[101] While eliminating the prospect of all cyber incidents is impossible, 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 risk is negligence and oversight.[102]

Insureds' risk profiles can be materially strengthened through the underwriting process and sustained engagement with their insurers.

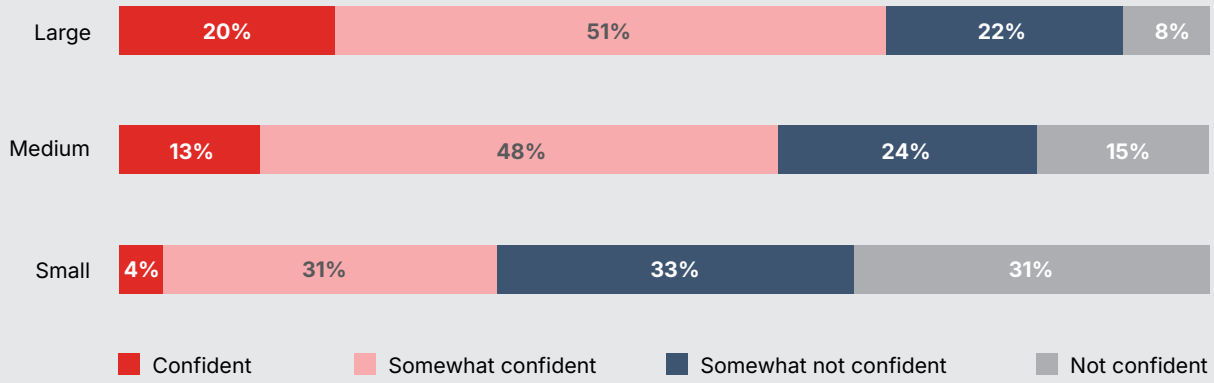
This suggests an opening for carriers (and brokers) to invest further in client education about cyber risks and the proactive and preventive cybersecurity options included in cyber policies. Forward-looking cyber insurers already understand this, stressing resilience in their interaction with policyholders, rather than focusing solely on either risk prevention, mitigation, or transfer (see Box 11).

98 Niemann 2025.
99 Willis Towers Watson 2025.
100 For example, a recent study revealed that while 61% of large organisations test their cyber incident response plans, this percentage falls to 40% for SMEs. Marsh 2025.
101 In a recent survey, 86% of business leaders reported confidence in the proactive cybersecurity guidance from insurance carriers – a higher proportion than for third-party vendors or service providers. Travelers 2025.
102 Palardy 2023.

Box 11: Expanding the uptake of cyber insurance by SMEs

Firms have finite resources to invest in cybersecurity tools as well as purchase insurance. This inevitably presents difficult choices, especially for SMEs with small budgets and who often lack technical expertise to assess their own cyber risk protection needs.[103] A World Economic Forum survey found that only 35% of small organisations are confident their cyber insurance will adequately cover potential losses (see Figure 11). Surveyed SMEs remain confused about the specifics of their coverage and the options available to them.[104] The cost of insurance may also be a significant barrier, with 36% of UK SMEs citing it as a prohibitive factor.[105]

FIGURE 11: CONFIDENCE IN CYBER INSURANCE, BY COMPANY SIZE



Note: The category of smallest organisations by annual revenue is up to USD 250 million; the category of medium is between USD 250 million and USD 5.5 billion; and the category of large is more than USD 5.5 billion.

Source: WEF

The insurance industry remains focused on developing products that offer essential coverage at prices small businesses can afford. However, increasing the number of SMEs that purchase cyber insurance requires more than well-designed and affordable policies. It also requires cyber education. Many SMEs are unaware of the full extent of their exposures to cyber threats. Cyber perpetrators are indiscriminate in who they attack, with no company too big or too small. According to the 2025 Verizon Data Breach Investigations Report, the majority of ransomware attacks now target small businesses, with extortion malware appearing in 88% of SME breach incidents, more than double the rate at larger enterprises.[106]

Besides risk education, greater efforts are needed to incentivise investment in cybersecurity hygiene among SMEs, to prevent potential incidents from occurring in the first place. Insurers have an important role to play in that process. The residual challenge is demonstrating to prospective clients the value in cyber insurance that goes beyond risk transfer, extending to threat intelligence, loss prevention, mitigation, and incident response.

Source: Rachel Carter and Sabrina Sexton, Allianz Commercial

5.2 Tailoring cover to meet policyholders' needs

Prompt reimbursement of cyber-related losses remains one of the primary ways insurance bolsters firms' resilience. However, large firms sometimes perceive cyber insurance coverage as overly rigid and not tailored to their specific needs.[107] At the same time, SMEs often require essential protection against common cyber risks like data breaches, ransomware, and business interruption without the need for extensive customisation. This calls for greater flexibility in product design to tailor cyber insurance to suit various policyholders' risk profiles. Insurers could provide, for example, coverage for specific perils (e.g. only ransomware or only data restoration), or different policy triggers, especially if policyholders choose to mitigate certain risks in other ways.

103 Salzberger 2025.
104 Lister 2025.
105 Grant Thornton and UK Department of Science, Innovation and Technology 2025.
106 Verizon 2025.
107 FERMA 2025.

Many carriers already offer modular cyber policies that provide firms with tailored coverage options.

Many carriers already offer modular cyber policies that provide firms with tailored coverage options, including protection against enforced shutdowns, fines and penalties imposed by regulators, and losses resulting from cyber-related property damage and business interruption (BI).[108] Ongoing advances in underwriting practices will make unbundling even more feasible. In particular, cyber insurers are increasingly looking at parametric and agreed value solutions to speed up claim payouts for BI claims, either as add-ons to existing policies or as standalone coverage:[109]

- **Parametric coverage:** Insurance that pays out automatically once a pre-agreed, measurable event occurs, such as a major cloud outage. For example, Parametrix Enterprise Solutions offers parametric-based protection against losses due to both internal and external system interruptions, allowing for rapid compensation for downtime events.[110]

- **Agreed value cover:** Unlike regular parametric insurance, an agreed value policy is not triggered by a specific event like a cloud outage. Instead, any event that would trigger a cyber BI claim results in the agreed payout.

Moreover, product innovation should not be seen solely through the lens of standalone cyber insurance. Insurance policies ought to be complementary, ensuring clients are not left without coverage for cyber-related risks. The spate of supply-chain cyberattacks in 2025 has underscored the scale of upstream and downstream economic losses that can accompany a cyber incident. In doing so, they have revealed gaps in protection against cyber-related risks in non-cyber (i.e. property and casualty) policies. As technology becomes increasingly embedded in physical processes – such as manufacturing, transportation, and energy production – the potential for such coverage gaps will likely grow.[111]

Protection against contingent business interruption (CBI) losses has become a pressing need, as cyber incidents at major suppliers or key customers can quickly disrupt a firm's operations. Different types of insurance are available to cover CBI risks, although the terms and extent of cover vary.[112] Some cyber policies, for example, provide CBI cover for financial losses stemming from a cyber incident affecting a third party upon whom the policyholder depends. However, the scope of protection is often limited to specific named suppliers, for example losses arising from an incident at an outsourced IT service provider.[113] There may also be questions about policy triggers. While CBI insurance typically covers security failures, coverage for non-malicious system failures is less common and, when offered, is often more restricted.[114]

Cyber incidents at major suppliers or key customers can quickly disrupt a firm's operations.

Cyber CBI risk is challenging to assess and underwrite, especially gauging the potential for loss aggregation across policyholders. Both the probability and the severity of cyber-related losses are not only determined by the characteristics of the third party but also depend on the structure and the business model of the insured.[115] Expanding coverage will likely require more granular data on firms' supply chains, including vendors of a firm's vendors. Advanced analytics could help to map supplier networks more deeply and evaluate them, including spotting early warning signs of supplier vulnerabilities and potential disruptions.[116] There are promising signs that insurers are rising to the challenge. Some carriers recently extended CBI coverage to situations when a policyholder's key customer experiences a malicious cyber event that forces them to halt or reduce purchasing from the insured.[117]

108 Traditional cyber insurance policies do not normally cover property damage arising from cyber incidents. However, companies can purchase an affirmative property damage extension, either as an addition to their cyber policy or separately. Alternatively, they might choose a specially designed cyber gap policy, which 'un-excludes' those risks. Munich Re 2025.
109 MGAA 2025.
110 Wells 2024.
111 Risk Managers are increasingly concerned about insurance gaps: 53% fear that some of their activities might become uninsurable, with cyberattacks, digitalisation risks, and technological threats all considered to be in the top five areas where coverage is believed most likely to be withdrawn. FERMA 2025.
112 Traditional property insurance may provide cover for CBI losses, but such policies will typically only respond if one of the policyholder's main suppliers or customers suffers physical damage to their property that precludes them from fulfilling their contractual commitments. Non-damage BI (NDBI) and supply chain insurance (SCI) may in principle also provide cover for CBI losses resulting from a failure of information systems or a cyberattack. However, event triggers are often narrowly defined and coverage usually restricted to direct, first-tier, or named suppliers.
113 Corvus 2021.
114 Stanmore 2024.
115 Munich Re 2020.
116 Kshirsagar and Pawar 2023.
117 CFC 2026.

5.3 Simplifying policy language, underwriting and claims processes for SMEs

While large corporates have the luxury of dedicated experts to assess and scrutinise their cyber risks and required insurance coverage, this is not true for small firms, which frequently outsource at least part of their IT needs. Existing cyber insurance products can therefore be ill-suited for SMEs and particularly for micro-SMEs. Many are complicated, seemingly expensive policies originally designed for large corporates and simply scaled down, leaving SMEs with coverage that does not match their needs or budgets.[118]

Complex and time-consuming risk assessments, particularly lengthy questionnaires, which often include highly technical cybersecurity terminology, can discourage SMEs from purchasing cyber insurance. Often prospective policyholders struggle to identify which controls matter most, let alone prove to insurers they have implemented effective safeguards.

Insurers can target clear, jargon-free policy wording to ensure accessibility and relevance.

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 the 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. Similarly, streamlining documentation, establishing clear communication channels, and speeding up claim assessments and settlements would not only improve the policyholder experience but also increase the value customers derive from their cyber insurance.[119]

Policy simplification need not imply full product standardisation and uniform coverage across the marketplace. Insurance policies can still be aligned to customer preferences and needs. Rather, the emphasis should be on making individual policies easier for customers to comprehend. For example, there is still widespread confusion between cyber insurance and crime coverage.[120]

Insurers are already taking steps to bridge the information divide with SMEs. For instance, CyberAcuView – a coalition of leading cyber insurance underwriters, including AIG, AXIS, Beazley, Chubb, The Hartford, Liberty Mutual Insurance, and Travelers – has partnered to launch Control Assist™, a framework that maps technical security controls to typical cyber insurance questionnaires. This mapping allows SMEs to leverage existing tools to verify their cybersecurity posture, reducing the burden of manual documentation and accelerating the insurance application process.[121]

5.4 Aligning distribution with customer preferences and risk profiles

Collaboration with brokers or other intermediaries is often essential to ensure insureds have adequate cyber protection. Corporate risk managers, however, highlight that brokers and other intermediaries are frequently not adequately trained to address the full range of inquiries related to cyber risks. Likewise, a recent survey of UK SMEs found that 31% of respondents are deterred from purchasing cyber insurance because of unclear or limited advice from brokers, indicating significant confusion about policy details.[122] This underscores the need for continuous education and capability building across the industry.[123]

Traditional distribution models designed for large corporates are usually too complex and inefficient to scale profitably to SMEs. Hence, as well as the cyber insurance product itself, the ways in which customers interact with cyber insurers and intermediaries should also be upgraded. For example, digital distribution platforms (or application programme interfaces (APIs) to third-party platforms) can make the buying process easier for brokers and SMEs.

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. Designed for businesses with revenues of up to USD 250m, cyber insurance can be purchased directly through the online platform with only four pieces of information required for a quote.[124] Several carriers have also introduced embedded cyber insurance offerings

118 Swiss Re 2025.
119 Coker 2024.
120 FERMA 2025.
121 Centre for Internet Security 2025.
122 Grant Thornton 2025.
123 FERMA 2025.
124 Every client is pre-approved and eligible for insurance based on information about their name, industry, annual revenues and website. Supplementary data about the firms' cybersecurity are gathered remotely via public APIs, to uphold underwriting standards. Howden 2025.

that bundle coverage with the purchase of IT services, software, or security products in a bid to increase insurance penetration, especially among small firms.

5.5 Partnering with digital infrastructure providers

Integrating proactive risk control measures – like threat monitoring and well-practiced IR plans – within cyber insurance helps spot and contain threats before they escalate. This requires underwriters to have access to improved data capture of corporates' cyber exposures on an almost real-time basis. Static control checklists, siloed risk assessments, and one-off vendor snapshots (e.g. security ratings) significantly oversimplify risk exposure and leave organisations vulnerable to critical disruptions.[125] For example, cybercriminals often deploy tools and techniques to evade basic security controls like MFA.[126]

Static control checklists, siloed risk assessments, and one-off vendor snapshots significantly oversimplify risk exposure.

The dynamic nature of cyber risk means that simply focusing on basic cybersecurity hygiene at policy inception will be insufficient. 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.[127] This includes deploying AI tools to improve pricing accuracy, reduce claims, and enhance the resilience-building capabilities of cyber insurance.[128]

Such moves towards continuous underwriting will be aided by deeper connections between insurers and key infrastructure providers, as well as cybersecurity vendors (see Box 12). An existing example of that collaboration is the Risk Protection Program (RPP). A partnership between Google Cloud and leading cyber insurers (Beazley, Chubb, and Munich Re), the RPP blends cloud security insights with insurance industry expertise to offer Google Cloud customers customised cyber insurance. The RPP provides Google customers access to real-time reports on their cloud security posture, which can be shared directly with insurance carriers to facilitate faster and smoother underwriting decisions.[129]

Box 12: What's next for the cyber insurance industry?

The insurance industry must continue to explore new levers when it comes to protecting customers from cyber incidents. This includes making further strides to continuously monitor evolving cyber threats, identify and prioritise the most effective risk-reduction measures, and clearly communicate the practical steps to businesses. Cyber insurers' effectiveness will hinge on their capacity to actively influence policyholders' risk management decisions and behaviours.

Getting even more hands-on

Managed services have become a common solution for overseeing computer systems, particularly for small businesses that do not need a full-time IT employee. It is therefore unsurprising that some insurers are starting to offer support services that involve taking direct control over their customers' networks. Several insurers, including At-Bay, Beazley, and Coalition, have founded Managed Detection and Response (MDR) services, a paid add-on where security practitioners monitor networks and respond to alerts.

Such arrangements can create even faster feedback loops compared with simple customer alerts communicating emerging vulnerabilities or changing attacker tactics. One study found the value of claims from organisations using outsourced MDR services was 97.5% lower on average than those using in-house endpoint detection and response (EDR) teams, highlighting the benefits of external cybersecurity expertise.[130]

Despite its benefits, bundling – allowing policyholders to add optional paid-for security services like MDR from insurer partners or third parties – remains limited in some markets. Some researchers suggest inconsistent regulations and concerns about competition and conflicts of interest may have slowed adoption

125 Burn et al. 2025.
126 Threat actors have found multiple ways to bypass MFA. These include social engineering attacks, exploiting vulnerabilities in the implementation of the MFA process, and intercepting or redirecting communication containing authentication factors.
127 In cybersecurity, telemetry is used to not only gain broad visibility into an attack surface but to better identify and correlate actions that may signal a security threat or in-progress cyberattack. Arctic Wolf 2025.
128 One recent study found that compared with historical insurer risk ratings, AI-enabled underwriting materially improved the accuracy and efficiency of cyber risk assessment for SMEs. Specifically, machine learning models contributed an average 18% improvement in distinguishing between high- and low-risk SMEs and a reduced assessment time from two weeks to under 24 hours. Morgan et al. 2025.
129 Google Cloud.
130 Sophos 2025.

in the US.[131] This is problematic because barriers to bundling, whether real or perceived, prevent insurers from offering more proactive risk reduction services.

Strengthening partnerships with technology vendors

A crucial development for the cyber insurance market is more direct collaboration between technology vendors and insurers to facilitate real-time data sharing about an applicant's security posture. Currently, most insurers rely on self-reported questionnaires or PDF uploads, which are often incomplete and prone to errors, or outside-in scans that cannot quantify internal monitoring or system configuration. Active cooperation with vendors (including infrastructure providers) will allow more accurate risk assessments based on current, trustworthy information and streamline the insurance application process.

Structured integrations between a firm's own internal IT network and key external service providers allow insurers to see which controls are active, such as MFA or privileged access restrictions. Customers gain a tangible benefit - they can demonstrate their cyber hygiene easily and objectively, rather than describing technical details in freeform or static documents. With reliable data, insurers can confidently identify organisations that maintain strong security, reducing uncertainty and the chance of mispricing policies due to hidden risks.

Insurers are more willing to reward good security with better terms – lower premiums, higher policy limits, or fewer exclusions – when they have objective proof. This allows investments in cyber tools and configurations to translate into measurable reductions in insurance costs. Vendors also gain a competitive edge if their customers receive tangible rewards in the form of better insurance offers.

Source: Sezaneh Seymour and Daniel Woods, Coalition

5.6 Collaborating with government agencies

Enhanced collaboration between insurers and government security agencies can enhance the value of cyber insurance and strengthen firms' cyber resilience. 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. Similarly, when insurers' response teams and national cybersecurity centres share information and coordinate actions during an attack, this may facilitate faster containment and recovery at affected firms.

Enhanced collaboration between insurers and government security agencies can enhance the value of cyber insurance.

Such collaboration is already a feature in selected markets and further moves to deepen connections would be useful. For example:

- UK: The Cyber Security Information Sharing Partnership (CISP) connects the National Cyber Security Centre (NCSC) with private sector partners, including insurers.
- US: The Cybersecurity and Infrastructure Security Agency (CISA) established its Joint Cyber Defence Collaborative (JCDC) to work with insurers to understand systemic cyber risk.
- EU: The European Union Agency for Cybersecurity (ENISA) uses its Cyber Insurance and Resilience Framework to coordinate threat intelligence gathering and incident learnings.

Beyond information sharing, the insurance industry and the public sector, supported by a clear delineation of roles and responsibilities, must continue to work together to foster firms' cybersecurity maturity.[132] Together, insurers and governments can support the development and adoption of common standards for cyber hygiene, which underpin eligibility for insurance coverage. For example, firms registered for the UK government's Cyber Essentials scheme – a cybersecurity self-certification scheme designed to help SMEs and larger firms identify and address the most common security failings – automatically qualify for cyber liability insurance. According to the NCSC, 92% fewer insurance claims are made by organisations with the Cyber Essentials controls in place.[133]

131 Institute for Security and Technology 2025.
132 Marsh McLennan 2024.
133 National Cyber Security Centre 2025.

However, relying on voluntary minimum cybersecurity arrangements may be insufficient. Despite impressive rates of growth, overall registrations of UK firms for Cyber Essentials is still low. A little over 50,000 firms were signed up in 2025 (including recertified firms from earlier years), which represents only a fraction of the 5.5 million private sector businesses estimated to operate in the UK.[134] That might argue for mandating cybersecurity certification across all firms, as many governments already do for suppliers bidding on certain public sector contracts.

Moves towards mandatory cybersecurity standards would ensure a baseline level of protection across all sectors, reducing the likelihood of cascading failures and protecting not only individual firms but also supply chains and consumers. To ease the burden on SMEs with limited resources, public agencies might provide free or subsidised training, guidance, and threat intelligence to help smaller businesses meet the minimum requirements.

Mandatory cybersecurity standards would ensure a baseline level of protection across all sectors.

For insurers, minimum security standards would also simplify risk assessment and pricing, encouraging wider participation in the cyber insurance market. Well-designed regulation could drive cyber insurance market expansion – raising the average level of resilience without stifling innovation. At the same time, such mandates must remain flexible and proportionate – scalable to firm size and risk exposure, regularly updated to reflect technological change, and supported by practical guidance, training, and incentives rather than simply fines and penalties for non-compliance.

5.7 Exploring initiatives to promote systemwide resilience

Major technology companies already use bug bounty programmes, offering rewards to external researchers for responsibly reporting security flaws to improve vulnerability discovery. But emerging and open-source vendors face significant obstacles developing, operating, and financing such security programmes, even though this is a recognised area of security weakness. A 2024 report by cybersecurity vendor Synopsys revealed that 84% of analysed codebases contained at least one known open-source vulnerability, with 74% harbouring high-risk vulnerabilities – up from 48% in the previous year.[135]

This might provide an opportunity for insurers to channel some cyber insurance premiums to fund bug bounty schemes directly. The potential cybersecurity gains might be especially 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.

The extent to which identified vulnerabilities are patched/remediated before they can be exploited will lower the frequency and severity of insurance claims, offsetting the cost of the bounties. The security data gathered from ethical hackers could also be integrated into the insurers' risk modelling and underwriting procedures, helping to improve actuarial predictability.

Moreover, by targeting common dependencies across insured clients (e.g. critical open-source libraries, common software-as-a-service components), such initiatives could strengthen systemwide resilience. Insurers' use of bug bounty schemes could support their role as stewards that facilitate good cyber hygiene across firms and promote systemwide stability (see Section 3, Box 7).

Insurers' use of bug bounty schemes could support their role as stewards that facilitate good cyber hygiene across firms.

Operationalising such insurer-sponsored bug bounty programmes would take careful design and implementation, not least to align incentives of software vendors, policyholders, and insurance companies, as well as overcome any legal/regulatory hurdles. Scheme participation by an insured and a commitment to address identified vulnerabilities would need to be a condition for any premium discount or eligibility for coverage to incentivise good cybersecurity. To avoid non-participating insurers free-riding on intelligence gathered by others about systemic dependencies (e.g. flaws in widely used open-source components), an industry-wide bug bounty programme may be needed, or at least mechanisms that limit access to information about the vulnerability to participating insurers.[136]

On grounds that private IT companies also benefit from enhanced system resilience (e.g. via improved security reputation of their products), such a collective bug bounty scheme might be extended to include software and hardware vendors as co-sponsors. Co-funding

134 Muncaster 2025.
135 Synopsys 2024.
136 Some researchers highlight how such an industry-funded bug bounty scheme could expand the scrutiny of IT vulnerabilities to cover a wider set of critical technologies and vendors than current individually sponsored schemes. This reduces the pool of vulnerabilities available for cybercriminals to exploit. Frei and Rochford 2021.

allows for larger bounties and broader testing scope without overwhelming a single payer's budget. Equally, pooling funds across multiple organisations (to form a consortium) could create a shared bounty ecosystem to harvest network-wide security gains.

In certain jurisdictions, insurers funding or managing bounties may fall outside permitted underwriting activities or conflict with disclosure laws. More importantly, unauthorised access to an organisation's systems, even with good intentions, could lead to legal repercussions, potentially exposing sponsoring insurers to liability claims should harm ensue. Insurers would need to agree liability waivers with policyholders who participate in the scheme. Similarly, agreed vulnerability disclosure policies (VDPs) play a crucial role in the success of bug bounty programmes.[137]

137 Steele 2025.

6 Concluding remarks

Concluding remarks

If cyber insurance continues to evolve and innovate, including through partnerships with key stakeholders in cybersecurity, it will cement itself as a key pillar of digital resilience.

Cyber insurance occupies a distinct and increasingly influential position in promoting cyber resilience. Its value extends beyond the traditional function of indemnifying financial losses after an incident. Modern cyber insurance policies often incorporate a suite of pre-incident services such as security assessments, employee training, and vulnerability monitoring, as well as post-event IR coordination and forensic support. These services do not simply respond to risk, they actively seek to shape and reduce it. As such, cyber insurance can operate not only as a financial transfer mechanism but also as a proactive catalyst for stronger cybersecurity practices across firms.

Modern cyber insurance policies often incorporate a suite of pre-incident services as well as incident response coordination and forensic support.

However, the governance role that cyber insurance can play in affecting behaviour and organisational practices is currently constrained. Insurers still face significant challenges in accurately assessing and pricing cyber risk due to limited visibility of firms' internal security environments and the rapidly evolving cyber threat landscape. Many policyholders underuse the pre-incident services offered with policies, either from a lack of awareness, concerns about disruption to daily operations, or fear that sharing detailed security information may affect pricing or coverage. The involvement of third-party service providers in IR can add further legal complications, slowing down decision-making at moments where speed and open communications are crucial.

The upshot is that many firms, notably SMEs, remain uncertain whether the cost of cyber coverage justifies the perceived benefits, especially in a market characterised by technical policy language and complex underwriting and claims processes. Some organisations also find it hard to clearly attribute improvements in their cyber hygiene to insurance-driven interventions rather than other internal initiatives, even though the two should work as complements. If the insurance industry is to fulfil its potential role as a resilience enabler, it must work harder to make its value proposition more transparent, consistent, and demonstrably impactful.

The interconnected nature of digital risks makes the challenge even more pressing. A cyber incident at one organisation can cascade across supply chains, shared platforms, and critical infrastructure. In such an environment, the benefits of strong cybersecurity measures are partly public: one firm's security protects others, while one firm's weaknesses can expose others to harm. Cyber insurance has a unique opportunity to serve as a coordinating mechanism that helps internalise these externalities. By rewarding robust security practices and discouraging poor ones, insurers can help align individual incentives and promote collective cyber health.

Cyber insurance has a pedigree for innovation and continues to respond to the evolving risk landscape.

Even though it is only 30 years old, cyber insurance has a pedigree for innovation and continues to respond to the evolving risk landscape. Insurers must nonetheless redouble their efforts to demonstrate the value of the cybersecurity services they provide, while fostering clearer communication and more predictable coverage. There are ample signs the sector is keen to step up, with various current initiatives to increase the effectiveness of cyber insurance to bolster firms' resilience.

Yet insurers cannot accomplish the needed upgrade in firms' cyber resilience alone. Real progress requires active collaboration among insurers, governments, cybersecurity service providers, cloud and software

vendors, and critical infrastructure operators. These actors must work together to standardise baseline security expectations, improve threat intelligence sharing, and strengthen the reliability and usability of defensive tools. Regulatory frameworks can support this by clarifying responsibilities and encouraging risk-reducing behaviours, without stifling innovation.

By helping to build and sustain the conditions under which good cyber hygiene is recognised, rewarded, and widely adopted, the cyber insurance market can evolve into a more trusted and effective mechanism for reinforcing resilience. This applies not only at the level of individual firms but across the digital environment upon which societies increasingly depend.

References

Akamai. 2025. DDoS Attack Trends in 2024 Signify That Sophistication Overshadows Size.

Allianz. 2025. *Cyber Security Resilience 2025 – Claims and Risk Management Trends*.

Anthropic. 2025. *Disrupting the First Reported AI-orchestrated Cyber Espionage Campaign*.

Arghire, I. 2025. ChatGPT Tricked Into Solving CAPTCHAs. *Securityweek*.

Arnold, R. D. et al. 2021. Systems Thinking Assessment: A Method through Computer Simulation. *Proceedings of the ASME Design Engineering Technical Conference* (2).

Artais. 2025. How Penetration Testing Can Reduce Cyber Insurance Premiums and Improve Security Postures.

Arctic Wolf. 2025. Understanding Telemetry in Cybersecurity.

Aten, A. 2024. AI and the Future of Actuarial Science. *Coalition*.

Atlantic Council. 2024. *"Reasonable" Cybersecurity in Forty-seven Cases*.

AXA XL. 2024. AXA XL Unveils New Cyber Insurance Extending Coverage to Help Businesses Manage Emerging Gen AI Risks.

Bacon, A. 2025. Jaguar Land Rover to Partly Resume Output after Cyberattack. *Barron's*.

Baldwin, A. et al. 2021. Modelling Organizational Recovery. *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering* 424: 284–314.

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

Brunnermeier, M. 2021. *The Resilient Society*. Endeavor Literary Press.

Burn, J. et al. 2025. Too Big To Fail, Cyber Edition. *Forrester.*

Butler, E. 2025. Cyberattack on Marks & Spencer slices profits by more than a half. *MSN*.

Butler, G., and Jamali, L. 2025. Amazon Web Services Return to 'Normal Operations' after Mass Outage, Tech Giant Says. *BBC*.

Canute. *The Introduction to England of Automatic Fire Sprinkler 1881–1888*.

Center for Internet Security. 2025. Control Assist: A Path to Cyber Insurance Readiness for SMBs.

CFC. 2023. Poll: IT Departments the Biggest Obstacle to UK Brokers Selling Cyber.

CFC. 2026. Cyber Coverage Highlights: Customer Business Interruption.

Chipeta, C. 2025. 7 Deepfake Attacks Examples: Deepfake CEO scams. *eftsure*.

Cloudflare. Famous DDoS Attacks: The Largest DDoS Attacks of All Time.

Coalition. 2025. Coalition's Cyber Threat Index 2025 Finds Most Ransomware Incidents Start with Compromised VPN Devices.

Coker, J. 2024. How Cyber Insurance Can Work Better for Businesses in 2024. *Infosecurity Magazine*.

Colletti, J. 2025. How Vanishing Retention Rewards Security-Conscious Policyholders. *Coalition*.

Control Gap. 2024. Penetration Testing for Cybersecurity Insurance: What You Need to Know. Control Gap.

Corvus. 2021. Cyber Coverage Explained: Contingent Business Interruption.

Coveware. 2022. Fewer Ransomware Victims Pay, as Median Ransom Falls in Q2 2022.

CrowdStrike. 2024. Channel File 291 Incident: Root Cause Analysis is Available.

CyberCube and Munich Re. 2025. *Key Insights Into Systemic Cyber Risk*.

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

Davey, J. 2025. M&S Forecasts Rebound after Cyber Hack Halves First Half Profit. *Reuters.*

Delaney, A. 2025. 312% Surge in Breach Notices That Could Have Been Prevented. *DataBreach Today.*

Delinea. 2024. *2024 State of Cyber Insurance Research Report*.

Federation of European Risk Managers Associations. 2025. *Demystifying Cyber Insurance*.

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

Franke, U., and Orlando, A. 2025. Interdependent Cyber Risk and the Role of Insurers. *Research in Economics* 79 (3).

Frei, S., and Rochford, O. 2021. The Case for a Bug Bounty Program of Last Resort. *Techzoom.*

Geneva Association. 2024. *Cyber Risk Accumulation: Fully Tackling the Insurability Challenge*. Author: Darren Pain.

Google Cloud. 2025. Expanding our Risk Protection Program with New Insurance Partners and AI Coverage.

Grant Thornton and UK Department of Science, Innovation and Technology. 2025. *Insuring Resilience: Adoption of Cyber Insurance by UK Small and Medium Sized Enterprises*.

Haimes, Y. 2009. On the Complex Definition of Risk: A Systems-Based Approach. *Risk Analysis* 29 (12): 1647–1654.

Henriques, T. 2024. Cyber Threat Index 2024: Scans, Honeypots, and CVEs. *Coalition.*

Hiscox. 2024. *Hiscox Cyber Readiness Report 2024*.

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

IANS. 2025. *2025 Security Budget Benchmark Report*.

IBM and Ponemon. 2025. *Cost of a Data Breach Report 2025*.

Ilau, M.C. et al. 2025. Modelling and Simulating Organizational Ransomware Recovery: Structure, Methodology, and Decisions. *Journal of Cybersecurity* 11 (1): tyaf035.

Institute for Security and Technology. 2025. *Enhancing Cyber Resilience through Insurance: Revisiting Anti-Bundling Regulation*.

Insurance Journal. 2025. Travelers: Confidence High in Guidance From Cyber Insurers; Work to Do on Take-Up.

Ioannidis, C. P. et al. 2019. Resilience in Information Stewardship. *European Journal of Operational Research* 274 (2): 638–653.

Jones, D. 2024. Insurance Coverage Drives Cyber Risk Reduction for Companies, Researchers Say. *CybersecurityDive*.

Khalili, M. M., Naghizadeh, P., and Liu, M. 2017. Designing Cyber Insurance Policies in the Presence of Security Interdependence. *Proceedings of the 12th Workshop on the Economics of Networks, Systems and Computation*.

Khalili, M. M., Liu, M., and Romanosky, S. 2019. Embracing and Controlling Risk Dependency in Cyber-insurance Policy Underwriting. *Journal of Cybersecurity* 5 (1).

Knuth, K. 2019. The Term "Resilience" is Everywhere – but What Does It Really Mean? *Ensia*.

Kshirsagar, P. S., and Pawar, A. M. 2023. Predictive Analytics for Cyber Threats to Enhance Security in the Cyber Supply Chain. *Research Journal of Computer Systems and Engineering* 4 (1): 102–109.

Lister, S. 2025. Why Don't Small and Medium UK Enterprises Buy Cyber Insurance? *Binding Hook*.

Liu, X., et al. 2025. Equity Offering Following Cyberattacks. *Journal of Corporate Finance* 91: 102710.

Lockton Re. 2024. *The Art and Science of Cyber Risk Scoring Technologies*.

Marsh McLennan. 2024. *Closing the Cyber Risk Protection Gap*.

Marsh. 2025. *Why the Cybersecurity Gap between SMEs and Large Organisations Matters*.

Masten, A. 2014. *Ordinary Magic*. Guildford Press.

McKinsey. 2025. Deploying Agentic AI with Safety and Security: A Playbook for Technology Leaders.

MGAA. 2025. Insurance Insider: Parametric Solutions in Cyber on the Up as SME Coverage Needs Grow.

Morgan, A., Benslimane,Y., and Anoushka, Z. 2025. Enhancing Cyber Insurance Underwriting with AI-Powered Risk Analytics for SMEs. *ResearchGate*.

Muncaster, P. 2025. Has the UK's Cyber Essentials Scheme Failed? *Tech Monitor*.

Munich Re. 2020. Contingent Business Interruptions Due to Cyber Events.

Munich Re. 2025. Physical damage from cyberattacks: an underestimated risk in the age of automation and digitalisation.

NCSC. 2025. *Cyber Essentials*.

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

Niemann, P. 2025. Cyber and AI Oversight Disclosures: What Companies Shared in 2025. *Harvard Law School Forum on Corporate Governance*.

Ning, D. 2025. Selection and Screening in Cyber Insurance Markets. *Proceedings of World Risk and Insurance Economics Conference.*

Palardy, D. 2023. Small, Midsize Businesses Still Lack Cybersecurity Hygiene. *PropertyCasualty360.*

QBE. 2024. *2024 Cyber Insurance Report.*

QBE. 2025. The Cost of Catching Up.

RAND. 2025. Insuring Catastrophic Cyber Risk.

Recamara, J. 2025. Incident Response Planning Linked to Fewer Cyber Insurance Claims: Marsh Study. *Insurance Business.*

Resilience Forward. 2025. Setting Security Levels too High is a Risk in its Own Right. 'Right-sizing' Cybersecurity is the Way Forward...

Romanosky, S. et al. 2019. Content Analysis of Cyber Insurance Policies: How do Carriers Price Cyber Risk? *Journal of Cybersecurity* 5 (1).

Salzberger, A. 2025. An Empirical Analysis of the Behavioral Influences and Information Sources Affecting the Cyber Insurance Decisions of German SMEs. *Journal of Risk Finance* 26 (2): 213–240.

SecurityScorecard. 2025. CVEdetails.com.

Seymour, S. 2024. Ransomware Myths Busted: How Cyber Insurance Impacts Payments. *Coalition.*

Skeoch, H.R., and Ioannidis, C. 2024. The barriers to Sustainable Risk Transfer in the Cyber-insurance Market. *Journal of Cybersecurity* 10 (1).

Snape, G. 2025. Supplier Risk is Breaking the Size Myth in Cyber. *Insurance Business.*

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

Sophos. 2025. Quantifying ROI: Understanding the Impact of Cybersecurity Products and Services on Cyber Insurance Claims.

Stanmore. 2024. Contingent Business Interruption in Cyber Insurance.

Steele, J. 2025. Legal Perspectives on Bug Bounty Programs and Vulnerability Disclosure. *Steele Fortress.*

Stempel, J. 2025. Delta Can Sue CrowdStrike over Computer Outage that Caused 7,000 Canceled Flights. *Reuters.*

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

Swiss Re. 2025. Shifting Cyber Insurance Growth into the Next Gear.

Synopsys. 2024. *2024 OSSRA Report*.

The Alan Turing Institute and Centre for Emerging Technology and Security. 2024. *Generative AI in Cybersecurity*.

The Institutes. 2025. From Passive Policies to Active Cyber Protection.

Todyl. 2025. The Cyber Insurance Crisis: Why MSPs and Their Clients Are Struggling.

Torrens Resilience Institute. 2010. The Concept of Resilience: Understanding its Origins, Meaning and Utility.

UK Department for Business and Trade. 2025. Government Backs Jaguar Land Rover with £1.5 Billion Loan Guarantee.

Vakulov, A. 2024. Managed Service Providers: A Gateway for Cyber Attacks. *Cybersecurity Hub*.

Verizon. 2025. *2025 Data Breach Investigations Report*.

VikingCloud. 2025. *The 2025 Cyber Threat Landscape Report: How the Data Speaks to Key 2026 Trends for Cyber Leaders*.

Wang, S. 2019. Integrated Framework for Information Security Investment and Cyber Insurance. *Pacific-Basin Finance Journal* 57.

Weiss, R., and Zobel, C. 2024. Resist and Recover: Introducing a Spring Theory for Modeling Disaster Resilience. *Risk Analysis* 45 (2).

Wells, K. 2024. Parametrix Launches New Cyber Insurance Solution for Digital Interruption. *Reinsurance News*.

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

Wolff, J. 2023. The Role of Insurers in Shaping International Cyber-security Norms about Cyber-war. *Contemporary Security Policy* 141–170.

Woods, D., and Böhme, R. 2021. How Cyber Insurance Shapes Incident Response. *Proceedings of the 20th Workshop on the Economics of Information Security*.

Woods, D., and Böhme, R. 2022. Incident Response as a Lawyers' Service. *IEEE Security & Privacy* 20 (2): 68–74.

Woods, D. et al. 2023. Lessons Lost: Incident Response in the Age of Cyber Insurance and Breach Attorneys. *Proceedings of the 32nd USENIX Security Symposium*.

World Economic Forum. 2025. *Global Cybersecurity Outlook 2025*.

Zeller, G., and Scherer, M. 2023. Risk Mitigation Services in Cyber Insurance: Optimal Contract Design and Price Structure. *The Geneva Papers on Risk and Insurance – Issues and Practice* 48: 502–547.

INSURANCE FOR A BETTER WORLD

www.genevaassociation.org