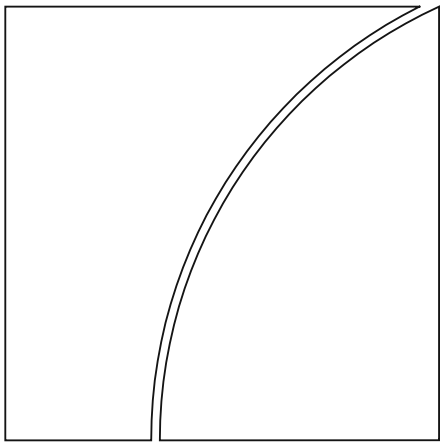
IAIS International Association of Insurance Supervisors

Financial Stability Institute | BIS

FSI Insights

on policy implementation

No 75



Cyber insurance unpacked: the corporate digital safety net

by Adrien Currat, Joe Perry and Jeffery Yong

June 2026

JEL classification: G18, G22

Keywords: cyber risk, insurance, operational resilience

FSI Insights are written by members of the Financial Stability Institute (FSI) of the Bank for International Settlements (BIS), often in collaboration with staff from supervisory agencies and central banks. The papers aim to contribute to international discussions on a range of contemporary regulatory and supervisory policy issues and implementation challenges faced by financial sector authorities. The views expressed in this publication are those of the authors and do not necessarily reflect the views of the BIS, its member central banks or the Basel-based standard-setting bodies.

Authorised by the Chair of the FSI, Fernando Restoy, and the Chair of the Executive Committee of the International Association of Insurance Supervisors, Toshiyuki Miyoshi.

This publication is available on the BIS website (www.bis.org). To contact the BIS Global Media and Public Relations team, please email media@bis.org. You can sign up for email alerts at www.bis.org/emailalerts.htm.

ISSN 2522-249X (online)
ISBN 978-92-9259-954-6 (online)

Contents

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

Executive summary

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

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

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

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

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

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

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

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

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

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

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

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

Section 1 – Introduction

1. **In an increasingly digitalised and uncertain world, cyber risk has become a significant risk, posing a threat not only to financial and economic stability but also to livelihoods at large.** Cyber risk is now the leading global business concern across sectors and jurisdictions.[2] Beyond immediate financial losses, cyber incidents can paralyse critical infrastructure, disrupt global supply chains and erode consumer trust, amplifying their impact on economies. For the financial sector, the threat is even more acute: cyber attacks can destabilise payment systems, compromise sensitive data and lead to cascading failures across interconnected institutions.[3] Although estimates of global economic costs of cyber incidents vary widely[4] – from around USD 1 trillion to above USD 10 trillion annually[5] – the amount and impact are clearly significant and have led to insolvencies.[6]

2. **The increase in cyber risk can be attributed to a combination of heightened threat capabilities, geopolitical tensions, growing digitalisation, concentrated digital dependencies and supply chain vulnerabilities.** The World Economic Forum highlights cyber-enabled fraud and phishing, ransomware attacks, artificial intelligence (AI) vulnerabilities and supply chain disruption as the leading cyber risk concerns (WEF (2026)). Cyber risk is further amplified by geopolitical conflicts, as cyber operations increasingly feature in hybrid warfare and may target critical infrastructure and essential services. At the same time, a high concentration of dependency on a limited number of third-party suppliers for critical data and digital services creates structural vulnerabilities (see Allianz (2026)).[7] The interconnected nature of supply chain networks across digital and physical borders makes companies vulnerable to shocks that can propagate through the entire system and expose multiple entry points for hackers (Swiss Re (2022)). IBM (2026) estimates a fourfold increase in the number of major supply chain or third-party breaches over the last five years.

3. **Unprecedented advancements in frontier AI models can significantly disrupt the cyber risk landscape.**[8] Frontier AI models such as Claude Mythos Preview and GPT-5.5-Cyber are capable of autonomously identifying vulnerabilities at outpaced scale and speed compared with human teams (Anthropic (2026); OpenAI (2026)). On the positive side, the models can enhance cyber resilience by enabling quicker detection and detection of previously unknown vulnerabilities at a lower cost and without needing specialist skills. On the negative side, the technology in the wrong hands can amplify cyber risk by increasing the speed and lowering the barrier to launch large-scale, automated attacks. Taken together,

[2] Allianz (2026) and Aon (2025) identified cyber risk as the number one risk in 2025.

[3] Munich Re (2026) reported that the financial sector was the fourth most attacked in 2025.

[4] See Vergara Cobos and Cakir (2024) for an explanation of why the estimates vary: for example, methodological uncertainty, difficulty in measuring indirect losses such as product chain disruption and reputational damage.

[5] For example, Cybersecurity Ventures estimates that cybercrime will account for USD 12.2 trillion annual global losses by 2031. This estimated loss is equivalent to the gross domestic product (GDP) of the third largest economy after the United States and China. Note that the figures exclude non-malicious losses that may be covered in certain cyber insurance policies.

[6] Lewis Silkin estimated that a successful cyber attack would force nearly one in five small and medium enterprises (SMEs) to close their doors (Vaziri (2023)). In the insurance sector, German insurer Einhaus filed for insolvency in August 2025 following a ransomware attack in 2023 (Jones (2025)). (For another example of insolvency caused by a cyber attack in the healthcare sector, see Finnish Government (2021).)

[7] More than three quarters of companies rely on cloud services across most or all areas of their operations, while only three providers (ie Amazon Web Services, Microsoft Azure and Google Cloud) account for over 60% of global cloud infrastructure. Each of these providers experienced separate significant outages in 2025.

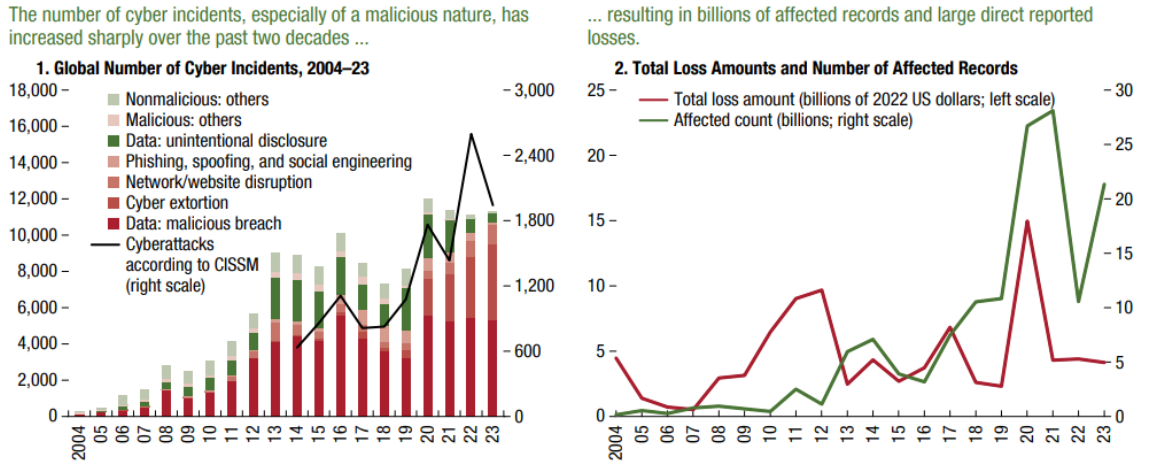
[8] CrowdStrike (2026) reported that in 2025, AI-enabled attacks increased by 89% and the average time for an attacker to move within a compromised network after gaining initial access fell to just 29 minutes, a 65% increase year on year. Beazley Security (2026) reported a 43% increase in active exploitation in the first quarter of 2026 compared with the previous quarter. The report noted increasing discoveries by AI tools used in bug bounty submissions and highlighted a significant AI-assisted multistage supply-chain attack affecting major public and private entities, including the European Commission.

these dynamics raise concerns that severe cyber incidents may generate systemic implications, potentially disrupting significant parts of the economy and the financial system.

4. **Cyber risks and incidents can arise from both malicious and non-malicious causes.**[9] The FSB (2023) defines cyber risk as "the probability of cyber incidents occurring and their impact" and a cyber incident as "a cyber event that adversely affects the cyber security of an information or the information the system processes, stores or transmits whether resulting from malicious activity or not". Cyber incidents may result from technical malfunction, human error and insider or external attacks (ENISA (2024)).

5. **Malicious cyber incidents are the dominant source of cyber losses and have been increasing significantly, while non-malicious incidents are growing in importance.** One study has found that the majority of cyber losses originate from four main types of malicious cyber incidents: (i) ransomware attacks, (ii) business email compromise,[10] (iii) distributed denial of service attacks[11] and (iv) data breaches.[12] Ransomware has become the leading source of cyber insurance losses (see Box A), while cyber-enabled fraud has become the leading cyber risk for chief executive officers (CEOs) (WEF (2026)). A study by the European Union Agency for Cybersecurity (ENISA) shows that distributed denial of service attacks accounted for more than three quarters of reported cyber incidents (ENISA (2025)).[13] Data breaches remain particularly costly, with the global average cost estimated at around USD 4.44 million per incident (IBM (2025)). Non-malicious incidents, such as human error or technical failures, are gaining significance and accounted for a third of Allianz's large claims in 2024 (Allianz (2026)).[14] Given the increasing trend of the number of cyber incidents and cyber losses (see Graph 1), measures to mitigate cyber risk are becoming increasingly important, including cyber insurance.

Number and cost of cyber incidents — Graph 1



The CISSM refers to the Center for International and Security Studies at Maryland, which provides data on malicious cyber attacks.

Source: FSI-IAIS staff. Adapted from International Monetary Fund, Global financial stability report: the last mile: financial vulnerabilities and risks, April 2024.

[9] Cyber is a generic term for all risks in the context of computer systems, hardware, software, data, the Internet or other digital network, any kind of Information Technology (IT) or Operational Technology (ENISA (2024)).

[10] Business email compromise , a subcategory of cyber fraud, is a "sophisticated scam in which cybercriminals impersonate trusted leaders to trick employees into sending money or data".

[11] A distributed denial of service attack "floods an online resource, such as a website or cloud service, with fraudulent connection requests or other malicious traffic, typically by using a botnet".

[12] See Munich Re (2026), whose data show overall ratio of three to one for malicious and non-malicious attributable loss events.

[13] ENISA (2025) analysed 4,875 incidents over a period from 1 July 2024 to 30 June 2025 in European member states.

[14] Large claims are defined as more than EUR 1 million.

6. **Cyber insurance can play a role in mitigating cyber-related losses.** The International Association of Insurance Supervisors (IAIS) defines cyber insurance as insurance providing "first-party and third-party coverage to mitigate risk exposure by offsetting costs involved with recovery of cyber losses" (IAIS (2020)). Appropriate cyber insurance coverage can help organisations mitigate losses associated with business interruption and the costs incurred from responding to and recovering from an attack or incident (BoE (2025)). Beyond payouts, many cyber policies include incident response services – such digital forensics, legal counsel and crisis communication – that can help speed up recovery and reduce economic damage. Moreover, the underwriting process may incentivise insured firms to strengthen their cyber security measures. While the cyber insurance market has grown in recent years alongside the rising frequency and severity of cyber incidents,[15] the protection gap remains substantial.[16] Estimates suggest that around 99% of global economic cyber losses remain uninsured (GFIA (2023)).

7. **While cyber insurance can support broader financial stability goals in mitigating the financial and operational impact from a cyber incident, it is important that the market grows sustainably.** The evolving nature and magnitude of cyber risk create substantial challenges for cyber insurance underwriting, while longstanding issues such as non-affirmative cyber coverage and accumulation risk remain a consideration (IAIS (2020); IAIS (2023b)). Furthermore, with a substantial protection gap and potential for growing demand for coverage, the development of the cyber insurance market must be grounded in sound practices.

8. **Against this backdrop, this paper takes stock of the cyber insurance landscape, covering market dynamics.** Based on a literature review and interviews with regulators and market players,[17] the paper covers cyber insurance product coverage, pricing and underwriting practices, and the protection gap, and it highlights key considerations in supporting a sustainable and sound growth of the cyber insurance market.[18] Section 2 describes core coverage components, exclusions and non-affirmative coverage. Section 3 analyses pricing methodologies and underwriting practices, including issues surrounding accumulation risk. Section 4 explores the protection gap and potential policy measures, and section 5 concludes.

Section 2 – Nature of cyber insurance product

9. **The cyber insurance market has expanded rapidly in recent years, although growth has moderated.** The global cyber insurance market was worth USD 15.3 billion in gross written premiums(GWP) in 2024, having doubled since 2020 (Munich Re (2025a)). North America remains the dominant market, with around two thirds of global premiums (see Graph 2). This dominance is driven by the early adoption of data breach laws and tightening of commercial insurance policy terms to exclude breach response costs for a cyber incident, leading to increased demand for cyber insurance coverage (American Academy of Actuaries (2025)). Europe represents the second largest market, followed by Asia/Oceania. The rapid expansion of the cyber insurance market was accompanied by sharp increases in premiums as insurers reacted to rising ransomware claims during the Covid-19 pandemic. However, recent

[15] Swiss Re (2025) estimates that the cyber insurance market has grown at a compound annual growth rate (CAGR) of 31% between 2017 and 2022, before slowing to 5% between 2022 and 2026.

[16] Munich Re (2025a) estimates that cyber insurance accounts for less than 1% of global property and casualty premiums. IAIS (2025) describes the evolution of the cyber insurance market.

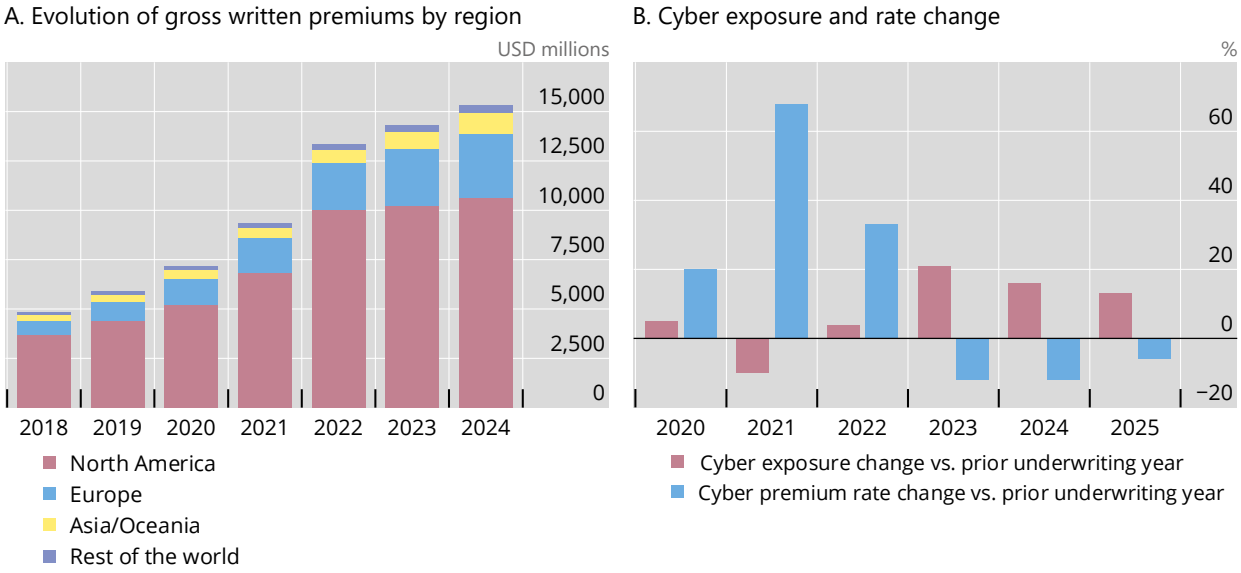
[17] This paper covers regulatory approaches in Bermuda, the European Union, the United Kingdom and the United States. Interviews were held with insurance authorities, insurers, reinsurers, brokers, model vendors and cyber risk experts.

[18] Quantum computing could eventually have important implications for cyber insurance if attackers can decrypt sensitive data, compromise authentication systems or disrupt digital infrastructure. To focus on more immediate threats, this paper does not consider quantum-related cyber risks.

developments indicate a moderation in pricing as underwriting discipline improved and additional market capacity entered the sector (S&P Global (2024)). In the United States, premiums declined for the first time in 2024. This potentially reflects cyclical pricing dynamics and improved cyber security controls among insured firms, though cyber risk remains elevated (NAIC (2025)). Graph 3 provides an illustration of average cyber insurance premium rates in the United States based on a sample of 10 insurers for a $1 million coverage with a $1,000 deductible.

Cyber insurance market

Graph 2

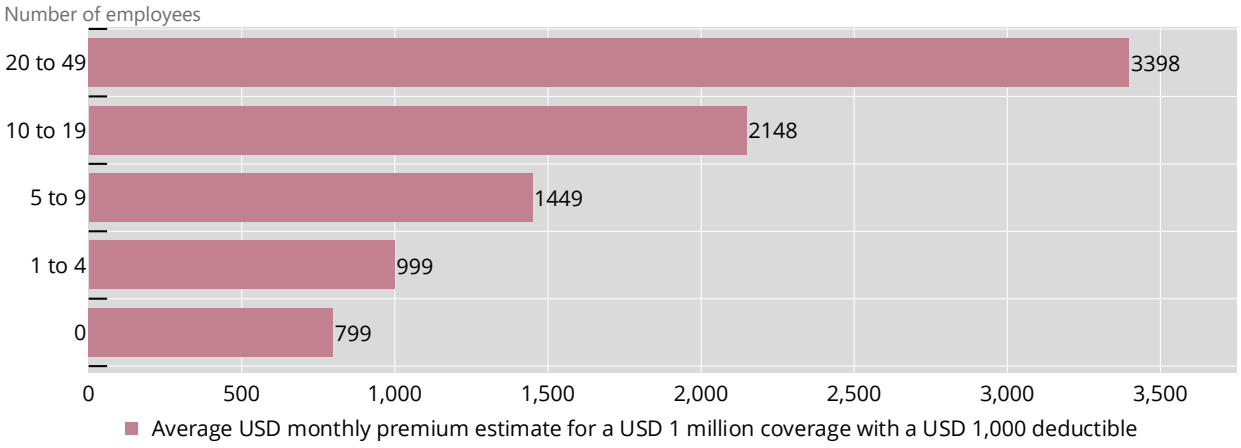


Gross written premiums are the total amount of premiums an insurance company receives from policyholders during a specific period, before deductions for reinsurance or other adjustments.

Sources: Adapted from Munich Re, "Cyber insurance: risks and trends 2025", 3 April 2025; and Swiss Re, "Shifting cyber insurance growth into the next gear", 3 September 2025.

Average cyber insurance premium rates by size of business

Graph 3

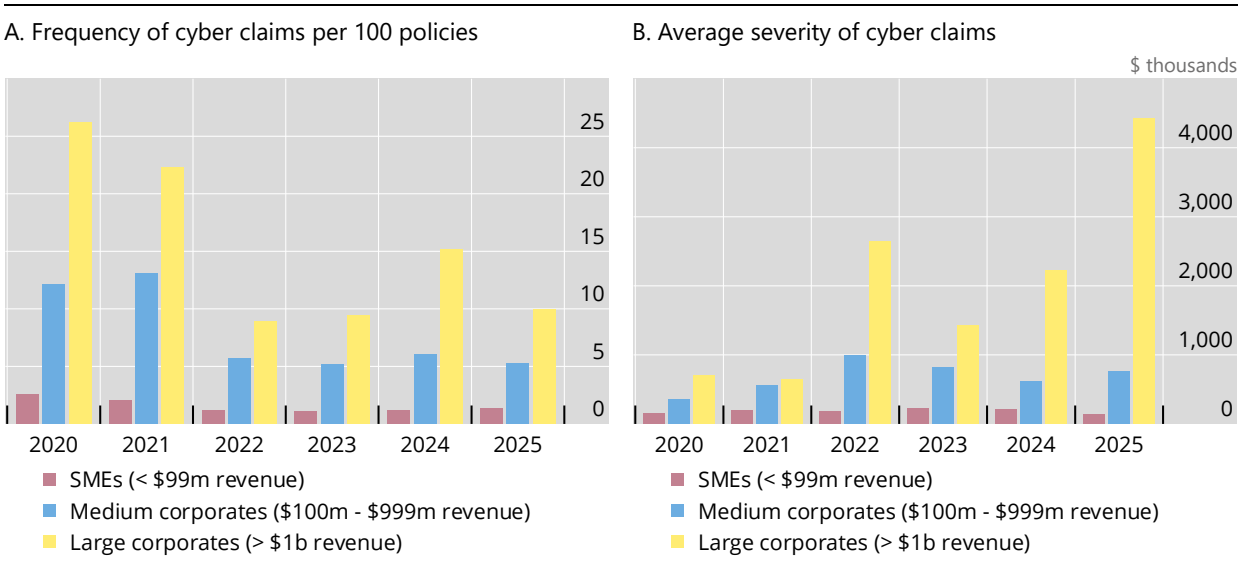


Source: Adapted from C Bolton, "Average cyber insurance cost 2026 report", *MoneyGeek*, March 2026.

10. **In major cyber insurance markets, claims frequency appears to be stabilising or even decreasing in some segments, while the average severity is increasing for large corporates** (Chubb

(2026)). Improvements in the cyber resilience[19] of insured firms are the main contributing factor in containing the number of cyber insurance claims. Nevertheless, the average cost of each cyber insurance claim has increased significantly for large corporates. This is attributable to increasing business interruption expenses, the cost of data breaches and privacy-related litigation, among other reasons. Graph 4 shows the evolution of the average frequency and severity of cyber insurance claims for different segments of corporates. The trend is similar in Europe but with lower average cost of claims due to less privacy-related third-party litigation. In the United States, Chubb (2026) reports that the average cost for a data breach in 2025 was a record USD 10.2 million – more than twice the global average of USD 4.4 million.

Frequency and average severity of cyber claims in the United States — Graph 4



SMEs are small and medium-sized enterprises.

Source: Adapted from Chubb, *2026 Cyber Claims Report*, 2026.

11. **Cyber insurance coverage is typically provided either through standalone policies specifically designed to address cyber risks or through endorsements[20] in other commercial insurance policies.** The standalone market has grown rapidly and is now estimated to be nearly twice as large as the packaged cyber market in terms of direct premiums written. Standalone cyber policies are purchased mainly by large corporates, which tend to have more data and financial resources at risk (Swiss Re (2022)). While cyber coverage also exists for individuals, personal cyber insurance remains a relatively small segment of the market. This paper focuses on issues related to cyber insurance for businesses, given the significance of this business line.[21]

[19] FSB (2023) defines cyber resilience as the ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents. IAIS (2026) considers an operationally resilient insurer to be "one that can encounter, withstand, mitigate, recover and learn from the impact of a broad range of events that have the potential to significantly disrupt the normal course of business by affecting critical services or operations".

[20] An endorsement is a written document attached to an insurance policy that changes its terms or coverage. It can be considered as an "add-on" coverage. See Chubb (2022) for an example of endorsement for widespread events, ransomware and neglected software vulnerabilities.

[21] It is acknowledged that there are conduct-related issues in cyber insurance underwriting for example, claims disputes arising from ambiguity in policy terms. This paper focuses on prudential issues, as these are more pertinent in the context of cyber insurance for businesses.

Coverage

12. **Cyber insurance policies vary significantly across insurers and jurisdictions, reflecting differences in market practices, insurers' business strategy and the needs of the policyholders** (Tsohou et al (2023)). This section provides an overview of the core component of cyber insurance policies and highlights two main issues related to cyber insurance coverage: (i) the lack of clarity or certainty over coverage and (ii) overlaps between cyber coverage and other insurance products.

13. **Cyber insurance policies typically provide two main types of coverage: first-party and third-party.** When cyber insurance emerged in the market, the product coverage varied significantly from the different insurers. Over the years, there has been some convergence on the common risks that are covered in cyber policies. Among them are system malfunctions, data breaches, loss of integrity or availability, malicious activities and human errors (Tsohou et al (2023)). First-party coverage protects the insured against direct losses, such as costs related to incident response, cyber extortion, business interruption and data restoration. Third-party liability coverage protects against claims made by third parties affected by the cyber incident, including regulatory sanctions and fines where insurable (see Table 1). While the specifics of coverage may vary across insurers and jurisdictions, most policies offer coverage against both first- and third-party costs.

Common coverage components of cyber policies — Table 1

Coverages	Description	Nature of the costs
Incident response	Costs for incident response services, which include forensics, notification, public relations, and credit monitoring and call centre costs.	First-party
Business interruption	Business income loss and extra expense incurred during period of restoration or business income loss caused by the incident. Contingent business interruption includes cover for business income loss and extra expense resulting from a supplier being unable to deliver services or products as a result of a cyber incident.	First-party
Cyber extortion	Response costs as well as ransoms paid to hackers to decrypt or regain access to data or systems. Box A describes ransomware in greater detail.	First-party
Data restoration	Costs to restore or replace lost or damaged data or software.	First-party
Regulatory defences and fines	Defence costs for regulatory actions and coverage for fines and penalties, where insurable by law.	Third-party
Network security liability	Losses arising from claims brought by a third-party for a security breach to an insured's system, including legal defence costs.	Third-party
Privacy liability	Losses arising from claims brought by a third-party for a data privacy incident, including legal defence costs. Such incidents can also originate from a security breach.	Third-party
Payment card liability	Fines, expenses and costs for any compromises of payment card data.	Third-party
Media liability	Costs that relate to the infringement of intellectual property rights and distribution of materials.	Third-party

Source: FSI-IAIS staff. Adapted from Swiss Re, "Cyber insurance: strengthening resilience for the digital transformation", 7 November 2022.

Box A

Ransomware – the main drivers of cyber insurance claims

Ransomware is a type of malicious software used by cybercriminals to block access to a victim's computer systems or encrypt data, demanding payment (a ransom) in exchange for restoring access or preventing the public release of stolen data. Early ransomware attacks typically focused on encrypting files, but modern ransomware has evolved into a multistage criminal business model. Attackers often combine data encryption with data exfiltration (double extortion), threatening to leak sensitive information if the ransom is not paid. Some groups also employ triple extortion, where they threaten customers, suppliers or employees of the victim organisation to increase pressure to pay.①

Ransomware has become one of the most financially damaging forms of cybercrime and a dominant source of cyber insurance claims. Although estimates may vary depending on the insurer, Coalition (2026) shows that ransomware remained the most expensive category of cyber claim in 2025, with an average loss of USD 269,000 per claim. Similarly, Munich Re (2025a; 2026) report that ransomware was the leading cause of cyber insurance losses with business interruption (BI) accounting for the largest share of costs (51%) among all cost components, increasing by 50% in 2025. German mobile phone insurer Einhaus Group filed for insolvency in August 2025 following a 2023 ransomware attack that infiltrated its information technology (IT) system and encrypted critical data, including contracts and billing. The insurer reportedly paid EUR 200,00 ransom in bitcoin to regain access.

Because ransomware incidents can affect many organisations simultaneously – particularly when attacks exploit widely used software vulnerabilities – they contribute to accumulation risk in cyber insurance portfolios. The sharp rise in ransomware losses in recent years led many insurers to significantly tighten underwriting standards, introduce sub-limits on ransomware coverage, increase premiums and require stronger cyber security controls, such as multifactor authentication, endpoint detection and network segmentation. Policy concerns related to ransomware include whether cyber insurance could inadvertently incentivise ransom payments and whether the resulting accumulation risk may pose solvency threats to insurers. Moreover, there are active discussion on whether firms should be banned from paying ransoms, which may have implications on cyber insurance availability (GOV.UK (2025)). Coalition (2026) notes that although the number of ransomware demands has increased significantly, a record 86% of affected businesses refused to pay ransoms. The use of cryptocurrencies for ransom payment is another area of concern.②

Although ransomware attacks seem to be declining thanks to improving cyber security measures, many victims have suffered multiple attacks and ransom payment rates are increasing. Moreover, some victims that paid the ransom failed to receive decryption keys, and the data of some victims were still published or illegally used after the ransom payment (Semperis (2025)).

① See "What is multi-extortion ransomware?", Palo Alto Networks. ② Chainanalysis (2026) reported USD 820 million on-chain payments in 2025.

14. **Certain forms of cyber losses are not consistently covered across policies, leading to potential coverage gaps or ambiguity.** In some cases, the coverage gap is deliberate because the risks involved may be beyond the risk appetite of insurers, especially if they contribute to accumulation risk. The literature frequently highlights two areas: (i) contingent business interruption (CBI) and (ii) cyber theft or fraud.

- **CBI coverage is not standard in all cyber policies and often applies only to specific categories of service providers** (Munich Re (2020)). CBI coverage extends business interruption protection to losses resulting from cyber incidents affecting third-party service providers, such as cloud infrastructure or information technology (IT) service providers. However, the scope of protection is often limited to specific named suppliers (Geneva Association (2026b)). Some insurers have offered specific endorsement to cyber policies for business interruption arising from cloud service disruptions.[22]

[22] For example, the Google Risk protection programme, with partnerships with Beazley, Chubb and Munich Re, offers a customised cyber insurance protection for Google Cloud customers.

- **Losses arising from cyber theft and fraud, including business email compromise or social engineering attacks, may not always be covered in cyber policies.** Where financial losses occur without direct system compromise, coverage may fall under crime policies rather than cyber insurance. Conversely, where fraudulent activities lead to network intrusion, data breaches or ransomware, such losses may be covered by cyber policies. Some cyber insurers include cybercrime as an endorsement within cyber policies.[23] Only a few cyber insurers offer direct coverage of cybercrime losses under cyber policies, and it is typically subject to sub-limits and high retentions (see Aon (2023); Garlick (2026)).

15. **Cyber insurance policies contain certain exclusions that limit insurers' exposure.** As in any non-life insurance policy, cyber insurance policies may exclude certain risks, particularly those considered difficult to model or insure or those associated with catastrophic losses.[24] Common exclusions include war,[25] terrorism or hostile acts by nation-states, where attribution challenges may complicate claims determination (American Academy of Actuaries (2023)). Cyber policies also generally exclude losses arising out of physical damage or for bodily injury, which are traditionally covered under property and casualty insurance (Munich Re (2025c)).[26] In addition, cyber policies often exclude disruptions affecting defined infrastructure, such as electricity grids or undersea cables. Infrastructure exclusions are among the least well understood elements of cyber insurance policies (FERMA et al (2025)). Losses from power outages, for example, are typically excluded unless the outage is directly caused by a cyber incident affecting the insured's system. Additional exclusions may apply to patent infringement, deliberate criminal acts by the insured or gross negligence in cyber security practices (Tsohou et al (2023)).

16. **Cyber incidents may trigger claims under multiple insurance policies, creating potential overlaps across policies.** The Organisation for Economic Co-operation and Development describes how certain risks covered by cyber insurance policies may overlap with property, liability, crime, and kidnap and ransom insurance policies ((OECD (2020)). Crime policies typically cover financial losses arising from fraud or theft, which may include those arising from a cyber incident (FERMA et al (2025)). In some cases, such as social engineering fraud, coverage in insurance policies like cyber insurance, crime insurance and D&O insurance can overlap (Marsh (2017)). Such overlaps can contribute to accumulation risks, as a single and widespread cyber incident may trigger claims across multiple insurance policies simultaneously (see Graph 5).

[23] See, for example, Axa XL CyberRiskConnect.

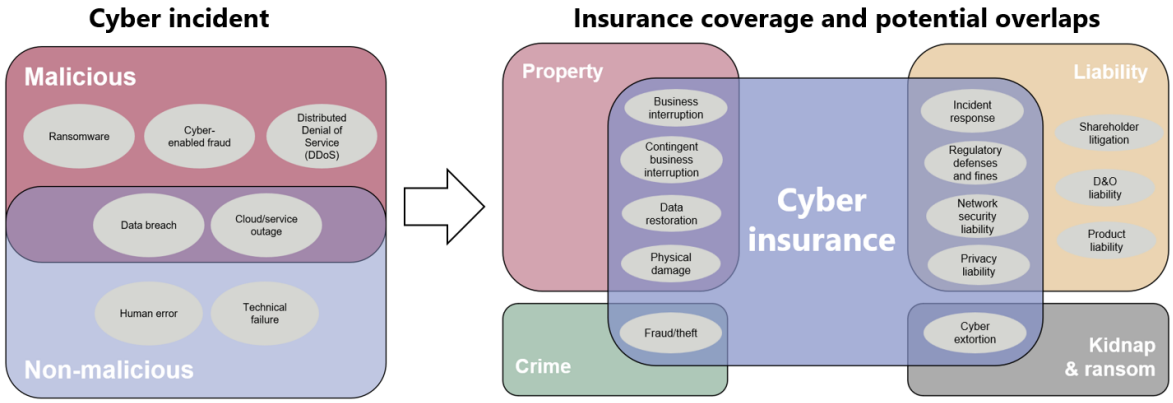
[24] Modelling correlated and tail risks such as widespread cloud outages, systemic software vulnerabilities or large-scale nation-state cyber attacks is very challenging and subject to significant uncertainties (see CyberCube and Munich Re (2025)).

[25] Some products covering war-related cyber attacks exist in the market: for example, Canopius Cyber War Insurance.

[26] However, exclusion clauses LMA 5400 and LMA 5401 were introduced to explicitly exclude cyber risks from property policies and control the risk of "silent cyber". In response to the exclusions, specific products, such as cyber physical damage (cyber PD or CZ), have been developed to address this gap (FERMA et al (2025)).

Illustration of how a cyber incident can trigger insurance claims under different policies and potential overlaps

Graph 5



The list of cyber incidents and insurance coverage is not exhaustive. Other liabilities, mentioned in Table 1, include payment card liability and media liability.

Source: FSI-IAIS staff. Adapted from Organisation for Economic Co-operation and Development, Encouraging clarity in cyber insurance coverage*: the role of public policy and regulation*, February 2020.

Non-affirmative coverage

17. **Non-affirmative cyber exposure (also called "silent cyber") refers to instances where cyber coverage is neither explicitly included nor explicitly excluded within an insurance policy (EIOPA (2022)).** Non-affirmative cover has been the main regulatory/supervisory concern over the years, as it could lead to significant losses for insurers despite not intending to provide cyber coverage.[27] The Bank of England (BoE (2024)) and the European Insurance and Occupational Pensions Authority (EIOPA (2022)) have highlighted that non-affirmative cyber risk can obscure where cyber risk is being underwritten and whether it falls within board-approved risk limits. EIOPA (2022) notes that unclear wordings can lead to unintended risk taking, mispricing and breaches of underwriting risk appetite. The New York Department of Financial Services (NYDFS) states that even non-life insurers that do not explicitly offer cyber insurance may be exposed to non-affirmative risk and therefore they should also evaluate and take steps to reduce their exposures (NYDFS (2021)). Property, liability and specialty insurance policies that are silent on cyber coverage may lead to losses from cyber incidents under non-cyber lines without having been explicitly underwritten or priced, such as from ransomware-induced business interruption or data-driven liability claims. A defining moment was the 2017 NotPetya attack (see Annex 1). Even though the NotPetya attack was a cyber attack, around 85% of insured losses were reported through property claims that did not explicitly include or exclude cyber attacks (Swiss Re (2022)).[28]

18. **Non-affirmative coverage is not a new issue, and over recent years both the industry and the regulators have taken steps to address it.** The IAIS's 2023 and 2025 *Global Insurance Market Reports* noted that insurers have been addressing non-affirmative coverage through exclusions of some cyber risks from all-risk property and casualty policies, while affirmatively covering specific forms of cyber risks by endorsement and/or by offering standalone cyber insurance policies (see IAIS (2023b); IAIS (2025)). To address prudential risks arising from non-affirmative cover, regulators may require clearer policy wording, explicit inclusion or exclusion of cyber risk, and stronger board-level accountability for cyber exposure

[27] Chubb (2024) points out that, with respect to systemic risk (defined as an event that could inflict widespread harm to many customers due to shared commonalities), the lack of a clear definition could lead to costly litigation in claims disputes.

[28] It is worth mentioning that the insurers being sued were property insurers and not cyber insurers. Some property insurers had to pay the claims, even though they never underwrote the cyber risks.

management. Insurers' underwriting policies and portfolio monitoring need to make explicit how cyber risk – affirmative or non-affirmative – is captured, constrained and reported against cyber and non-cyber underwriting limits. For example, in Bermuda, insurers are expected to ensure clear, contract-certain treatment of cyber risk across all policies by explicitly affirming or excluding cyber coverage. This supervisory expectation is intended to reduce ambiguity and ensure that cyber exposures, whether affirmative or non-affirmative, are appropriately identified, measured and managed (BMA (2025b)). In practice, this has led to a greater use of explicit cyber endorsements and standalone cyber products, although insurers may continue to offer packaged policies where cyber coverage is clearly defined and consistent with their underwriting risk appetite and governance frameworks. Bank of England expects insurers to assess and actively manage their non-affirmative cyber risk exposures and introduce measures to reduce unintended exposure to this risk (BoE (2024)).[29] Where insurers decide to offer cyber cover at no extra premium, the authority expects the insurer's board to confirm that they have properly assessed potential resulting loses and that the non-affirmative cyber exposure is within the stated risk appetite.

19. **Lloyd's of London has played an important role in addressing non-affirmative coverage.** It introduced a series of market bulletins requiring insurers to clearly state whether cyber risks are covered or excluded in all policies underwritten in the Lloyd's market. For example, market Bulletin Y5258 required all policies to clearly affirm or exclude cyber coverage (Lloyd's (2019)). This was followed by further guidance (Y5381) on state-backed cyber attack exclusions in affirmative cyber policies (Lloyd's (2024)). The exclusion applies to liability for losses resulting both from war and from potentially state-backed cyber attacks outside of war. This exclusion is due to the potential damage these attacks can cause and their ability to spread, posing a systemic risk to insurers. However, the IAIS' 2025 *Global Insurance Market Report* noted that the exclusionary language may not have yet been tested in the courts (IAIS (2025)). Other measures that insurers can take to address silent cyber include transferring the risk to reinsurers and imposing policy or coverage limits.

20. **Although insurers and regulators have made significant progress in clarifying cyber coverage, non-affirmative cyber exposure remains present.** The Prudential Regulation Authority (PRA) general insurance stress test of 2022 found that non-affirmative coverage accounted for around 7% of the total gross losses for each of the scenarios (ie cloud outage, mass data exfiltration and systemic ransomware). This is a significant reduction compared with their previous 2019 stress test, with most losses coming from liability lines and professional indemnity policies (BoE-PRA (2020); BoE-PRA (2023)). The Bermuda Monetary Authority (BMA) reported that 50% of Bermudian groups and 37% of commercial insurers still had some silent cyber exposure ((BMA (2025b)). Given the dynamic nature of cyber risk, exposure needs to be constantly measured and monitored. Box B describes an emerging issue relating to coverage of AI-related losses.

Box B

Are we seeing the emergence of silent AI?

The growing use of AI, including generative AI (gen AI), is transforming the cyber threat landscape and introducing new potential sources of insurance losses. A report by the House of Commons Treasury Committee emphasised how AI can heighten cyber security vulnerabilities, increasing the volume and scale of cyber attacks in the financial sector (House of Commons (2026)). The report also called for the financial authorities in the UK to jointly conduct a stress test on AI. AI systems are increasingly used by threat actors to scale and automate cyber attacks, including phishing campaigns, deepfake impersonation, AI-enabled malware and automated social engineering. According to the European Union Agency for Cybersecurity, over 80% of all phishing emails identified between September 2024 and February 2025 used AI to some extent (ENISA (2025). In addition, AI models can be used to significantly improve

[29] To meet these supervisory expectations, insurers could, for example, make adequate capital provisions, adjust premiums to reflect the additional risk and offer explicit cover, introduce exclusion wordings or attach specific limits to cover.

detection of cyber vulnerabilities. On the other hand, bad actors may leverage such models to identify and exploit firms with weak cyber postures.①

From an insurance perspective, AI-related incidents may trigger losses across several insurance lines. Depending on the circumstances, claims could arise under cyber liability, errors and omissions (E&O), directors and officers (D&O), property or product liability policies.② However, these policies were not originally designed to address AI-related risks. This has led to growing discussions of "silent AI", referring to situations where losses involving AI may be covered under policies that do not explicitly include or exclude AI-related risks.

So far, AI risks are not yet excluded in most cyber policies. Munich Re has recently stated that "AI risks currently covered under traditional cyber policies are manageable" and does not see a need for broad exclusions at this stage (Amaral (2025)). This perspective aligns with the view that AI, while increasing cyber attacks, is already addressed within the scope of existing cyber insurance policies. Rather than representing an entirely new risk category, AI is generally regarded as amplifying silent cyber and accumulation risk challenges, as AI-related cyber losses may not be intended and yet may trigger claims across multiple policies.

The primary challenge for insurers is not limited to the inclusion or exclusion of AI risks but extends to ensuring that insurance wordings evolve in line with the new risks introduced by using AI. Munich Re (2025a) notes that risks associated with AI adoption are often not explicitly captured in policy terms. These risks include model manipulation, data poisoning, liability arising from hallucinations or wrong output, as well as IP infringement. Yet, clear contract language could be the determining factor when assessing if, for example, a data breach resulting from a sophisticated social engineering attack enabled by gen AI may be covered by the cyber policy (BMA (2025b)). Determining causation and accountability is becoming increasingly complex, particularly in cases involving AI-assisted decisions. An example is accidents arising from autonomous driving of electric vehicles, where it may be unclear whether motor insurance or cyber insurance could cover the loss. Given this complexity, clear policy wordings are essential to avoid silent AI, including from cyber insurance policies.

Although affirmative AI insurance products remain limited, some solutions are beginning to emerge. For example, Munich Re has introduced aiSure solution, which also covers cyber risk. Some cyber insurers are also developing endorsement covering gen AI exposures (eg Axa XL CyberRiskConnect). In Bermuda, the Bermuda Monetary Authority is increasingly emphasising the need for insurers to assess how emerging risks, including AI-enabled losses, are captured within policy wordings and underwriting frameworks (BMA (2025b)). This includes considering whether existing cyber and non-cyber policies appropriately address risks arising from malicious use of AI, system failures or unintended consequences of AI-driven decision-making and ensuring that any material exposures are consistent with the insurer's risk appetite and governance processes, all of which are required to be included in the insurer's ORSA (own risk and solvency assessment) submission.

A recent report by the Geneva Association (2025) suggests that demand for gen AI-related insurance is strong, especially among medium and large enterprises in the technology and finance sectors. The report also noted that the future of gen AI risk transfer remains uncertain, with standalone coverage, cyber add-ons and embedded insurance all potentially viable options.

① In April 2026, financial authorities in the UK engaged with the country's National Cyber Security Centre to identify potential vulnerabilities in key IT systems (including those used by financial institutions) posed by Anthropic's Claude Mythos model (Arnold (2026)). ② For a comprehensive analysis of which policies might respond to a loss caused by an AI model, see Munich Re and HSB (2024). See also the report from Lloyds (LMA 2026) on which lines of business AI could cause losses in.

Section 3 – Underwriting and pricing

Underwriting of cyber insurance

21. **Given data challenges, significant uncertainties on risk drivers and accumulation risk, among other factors, underwriting control is a key measure to contain the insured cyber**

risk.[30] Insurers can articulate an underwriting policy that converts board-approved risk appetite into concrete underwriting risk limits by product, segment, geography and risk driver. The policy can also ensure that underwriting decisions are consistent with solvency objectives. For example, Bank of England (2024) expects firms to define a clear cyber underwriting strategy covering both affirmative and non-affirmative exposures. EIOPA (2022) similarly emphasises that the administrative management and supervisory body should actively oversee cyber underwriting policy and ensure that growth, pricing and coverage decisions remain aligned with stated cyber risk appetite. In Bermuda, insurers are expected to integrate cyber risk into enterprise risk management and capital frameworks (BMA (2025b)). They are required to demonstrate how cyber underwriting risk – including accumulation risk and model uncertainty – is reflected in board-approved risk appetite statements, internal capital models and ORSA (own risk and solvency assessment) processes. This includes assessing tail-risk scenarios, evaluating dependencies on external service providers and ensuring that reinsurance strategies do not substitute for prudent underwriting discipline.

22. **Underwriting approaches typically vary depending on the type of client.** For commercial cyber insurance, underwriting approaches are more involved, combining questionnaires on IT environment and controls with external risk information including cyber risk ratings. More in-depth underwriting may apply to higher risk entities depending on their size and the industry they operate in. The limits can be specified in risk appetite statements by defining the target industries to focus on, specifying rules for line sizes and aggregate limits for specific industries (BoE-PRA (2024)). For more complex entities, close engagement with internal staff is crucial as part of the underwriting process, as they know best the risk drivers and interdependencies.

23. **Underwriting approaches in cyber insurance have undergone significant transformation, moving from traditional static questionnaires to advanced, data-driven and continuous-assessment models.** These modern methods leverage external cyber risk ratings, automated vulnerability scanning and detailed assessments of an organisation's cyber security maturity to provide a more comprehensive evaluation of risk.[31] Additionally, there has been a shift from purely qualitative assessments to hybrid actuarial, scenario-based models (Geneva Association (2023)).[32] This evolution is driven partly by the limited availability of historical loss data in the cyber domain, necessitating more sophisticated and data-informed frameworks to accurately assess cyber risks and support effective decision-making.

24. **Cyber security standards and frameworks play an increasingly important role in cyber insurance underwriting.**[33] They provide insurers with a common, credible baseline for assessing cyber hygiene, control maturity and resilience across policyholders of different sizes and sectors.[34] Insurers can map underwriting questionnaires, minimum security requirements and eligibility thresholds to these standards to compensate for limited claims data and the non-stationary nature of cyber risk, using them as proxies for loss frequency and severity. Close attention to reliance on such standards may be prudent for a number of reasons: the implicit reliance on these standards shapes risk selection, pricing, exclusions

30 Annex 2 lists the type of data typically used in cyber insurance underwriting.

31 Cloud service providers can support underwriting of cyber insurance given the information they have on a firm's IT infrastructure. For example, Google Cloud's Risk Protection Program assesses a firm's cyber risk posture across its cloud network and provides an assessment against the Center for Internet Security's benchmarks that can be transmitted directly to selected cyber insurers for their underwriting purposes.

32 Lloyd's (2026) sets out disaster scenarios that include cyber risk to support stress-testing by its syndicates.

33 In the financial sector, operational resilience requirements such as the EU Digital Operational Resilience Act (DORA) or the New York Department of Financial Services cybersecurity regulations may drive demand for cyber insurance by financial institutions as a risk mitigation tool. In addition, these standards may be referred to when underwriting financial institutions.

34 For example, the NIST Cybersecurity Framework, CIS Critical Security Controls, NCSC cyber insurance guidance, ISO/IEC27000 standards on information security management and CISA best practices. For the financial sector, the Cyber Risk Institute provides a benchmark for self-assessment by financial institutions.

and coverage availability; it may create de facto minimum security expectations for firms; and it can amplify market-wide concentration if many insurers converge on the same control frameworks.

25. **While requiring policyholders to meet certain cyber security standards and providing information on controls are important aspects of underwriting decisions, these measures alone are not sufficient.** Underwriters often rely on a combination of factors, including identifying red flags and assessing how certain controls impact pricing or capacity. A more effective, though more costly, approach involves evaluating an organisation's overall risk culture. For instance, understanding how many employees are aware of cyber risks can provide an outcomes-based signal of resilience, supplementing questions on how frequently systems are patched. This highlights the need to complement standards-based assessments with broader, outcomes-focused indicators to gain a comprehensive view of a firm's cyber risk management maturity.

Third-party risks

26. **A key challenge in underwriting cyber risk is the lack of visibility of risks arising from third parties.** Third-party risks can arise from the dense and often opaque web of digital dependencies linking insured firms to external service providers, software vendors and infrastructure platforms, and further to those providers' own suppliers and subcontractors (Glover (2025)).[35] Cyber incidents may originate outside the insured's perimeter – such as through a compromised cloud provider, managed service provider or widely used software component – yet still trigger first-party losses and liability claims across multiple insureds simultaneously. For pricing and underwriting, these dependencies create significant challenges, as insurers typically have limited visibility into vendor and sub-vendor controls, rely on self-reported or incomplete information and struggle to attribute losses accurately across contractual chains. This can lead to hidden correlations, delayed loss recognition and underestimation of accumulation risk, particularly where third-party exposures are not explicitly captured in underwriting questionnaires or exposure models, complicating risk selection, limit setting and the design of effective accumulation controls.

27. **Against this backdrop, underwriting scrutiny of third-party risk has intensified, with documentation and controls becoming prerequisites for favourable underwriting terms.** Insurers increasingly require a current inventory and tiering of vendors, evidence of periodic vendor risk assessments and use of continuous monitoring tools or external cyber ratings for key suppliers. They may also assess the insured's dependency map: the number and criticality of vendors, single points of failure, regional and provider concentration, resilience measures like multi-cloud or failover arrangements and contractual service level agreements (Munich Re (2020)). Demonstrated oversight of critical vendors (eg validation of backup, recovery, multifactor authentication, segmentation, and endpoint detection and response at service providers) can lead to broader coverage, lower deductibles or pricing credits. Conversely, gaps in third-party risk management may result in higher retentions, stricter sub-limits, exclusions for key providers or premium surcharges.[36] Ultimately, having clear visibility into dependencies and strong vendor governance not only expands insurability but also improves pricing by reducing uncertainty and accumulation potential.

Beyond risk transfer

28. **In addition to offering risk transfer, insurers may play a role in improving cyber resilience of insured firms.** By requiring firms to meet a minimum level of security standard as part of underwriting conditions, insurers can incentivise improved cyber risk management of those firms. Offering premium

[35] The attack on Marquis, a fintech firm serving more than 700 banks and credit unions, highlights a threat to banks' supply chains: it targeted not only of third-party suppliers but also the additional services they rely on ("vendors of the vendors" or "n-th party risks").

[36] AMWINS describes how exclusions and limits are used to mitigate widespread cloud outages such as the Amazon Web Service outage in 2025.

discounts for firms that meet higher security standards is another incentive.[37, 38] By doing so, insurers can drive the adoption of minimum security standards by linking these measures to insurability and pricing.[39] Such standards include multifactor authentication, endpoint detection and response, robust backup systems and oversight of third-party providers. It is important these minimum hygiene standards are effective and avoid unintended moral hazard behaviour. Firms may, in some cases, rely excessively on insurance coverage rather than proactively enhance their cyber security posture, which could undermine overall resilience. A fine balance exists between whether cyber insurance acts as a substitute for or a complement to firms' investments in resilience measures.

29. **Cyber insurers are increasingly offering cyber-related services.** The Geneva Association (2018) explains how cyber insurers are expanding their role across the cyber value chain, providing both pre- and post-breach services. Pre-breach services include not only those mentioned in Table 1 but also consulting services to train and assist firms to prevent and limit the damage from cyber incidence. Post-breach services include response and recovery measures that are now included as part of standard coverage in cyber insurance policies. These services, usually offered through third parties, are particularly helpful for smaller firms that may not have in-house expertise or resources for their own cyber defence or response measures. These services can be complementary to insurers' underwriting, reducing the risk exposure. Nevertheless, cyber insurers may need to be mindful of conflicts of interest that may arise: for example, avoiding recommending a specific third-party provider for pre-breach consulting that may not necessarily be the best or most cost-effective option.

Pricing of cyber insurance

30. **The pricing of cyber insurance is of interest to insurance supervisors because it may have prudential and protection gap implications.** On the one hand, underpricing of any insurance product can lead to solvency and potentially liquidity problems. On the other hand, overpricing may exacerbate the protection gap and become a concern from the perspective of conduct supervision. Given this, supervisors generally expect insurers to adopt a risk-based approach when pricing any insurance product. Nevertheless, risk-based pricing of cyber insurance can be challenging because of the unique nature of cyber risk.

31. **Actuarial methodologies to price cyber insurance policies need to consider the unique nature of cyber risk.** Classical actuarial methodologies based on the frequency and severity of insured risks are challenged by the unique characteristics of cyber risk. In particular, ENISA (2024) highlights unique characteristics of cyber risk (compared with other more "traditional" risks), such as the lack of data, non-stationarity and risk interdependencies. Though this list of challenges is not exhaustive, it provides an idea of how classical actuarial methodologies need to be adjusted to cater to unique features of cyber risk. We discuss each element in subsequent paragraphs.

32. **Insurers underwriting cyber insurance face scarce, fragmented and opaque incident and loss data.**[40] There are few publicly available data sources on cyber losses. This is because many cyber

[37] The UK National Cyber Security Centre mentions that certain insurers in the UK offer premium discounts for firms with recognised cyber security defences in plans such as those certified by its Cyber Essentials standard (NCSC (2020)).

[38] For example, the US Cybersecurity and Infrastructure Security Agency, in partnership with the academia, seeks to correlate data with cyber security controls to understand their effectiveness (see Natarajan (2023)).

[39] The Geneva Association (2026b) cites studies that have found empirical evidence of how cyber insurance can have a positive impact on policyholders' cyber hygiene.

[40] The Geneva Association (2023) highlights the actuarial challenge in quantifying cyber risks: lack of meaningful historical loss data, anthropogenic features, complex interdependencies, silent cyber and reserve development risks. The American Academy of Actuaries (2021) notes that cyber insurers have historically had a lack of in-house data for evaluating cyber risk. This is unlike most other property/casualty insurance lines of business, where insurers typically have relied on vast amounts of premium, exposure and claims data collected over many years to develop tools based on statistically significant results.

incidents are underreported due to reputational concerns, legal uncertainty or regulatory thresholds. Where available, these data sources may not be directly relevant or comparable for insurers' pricing purposes, as the product coverage may be different, the causes of a loss may be different or the definitions may be different, among other reasons. Detection and reporting lags – sometimes extending months after initial compromise – further distort loss timing and severity estimates. As a result, insurers rely on proprietary or closed claims databases, which can limit transparency and pose challenges in validating the pricing models. Nevertheless, various international, national and industry efforts are underway to improve cyber incident data availability.[41]

33. **From a prudential perspective, it is unclear whether the lack of relevant pricing data is leading to underpricing or overpricing.** Both viewpoints appear in the public domain: some argue that the risk is overestimated because insurers are prudent due to uncertainties over future losses; others claim that the absence of a truly systemic event in the past may lead to underpricing of such risks. What is clear is that the lack of data is a supervisory concern, especially as new technologies increase cyber risk exposures.[42]

34. **A contributing factor to the lack of suitable data is the non-stationary nature of cyber risk, meaning that the nature of cyber risk evolves over time.** Reasons for the risk evolution include rapid technological advancements (eg the increasing potential of AI being used for cyber attacks), which can dramatically alter the frequency and severity of cyber losses. As a result, even where historical loss data is available, they may very quickly become outdated for pricing purposes. From a modelling standpoint, the non-stationarity of cyber losses undermines traditional actuarial approaches that assume stable loss distributions and independence across risks. Exogenous factors such as technological innovation, attacker capabilities and digital interconnectedness can also alter the frequency and severity of cyber losses quite significantly over time. In addition, insurers struggle to model correlated and systemic events, such as widespread ransomware campaigns, zero-day exploits[43] or software vulnerabilities affecting thousands of insureds simultaneously.

35. **Human factors further amplify the instability of cyber risk exposures and are especially hard to model.** Errors such as misconfigurations (often propagated through common templates or infrastructure-as-code[44]), delayed patching, credential reuse, weak privilege hygiene and susceptibility to phishing or social engineering can drive large loss swings with little warning. These behaviours vary with workforce turnover, contractor use, remote work patterns, training quality, fatigue and organisational change (eg mergers and acquisitions, new systems, tool migrations), creating regime shifts that historical data rarely capture. Moreover, near-misses are underreported, and data on human failures is sparse.

36. **Analytically, insurers face significant challenges in mapping complex digital dependencies across supply chains and jurisdictions.** Cross-border contagion is intrinsic to cyber risk, as attacks propagate instantaneously across jurisdictions, legal entities and sectors, challenging geographical diversification assumptions commonly used in other lines. These issues are exacerbated by concentration

41 Examples of this include the Financial Stability Board Format for Incident Reporting Exchange (FIRE) (see FSB (2025)); and the US Securities and Exchange Commission cybersecurity risk management, strategy, governance and disclosure rule (see SEC (2025)). Regulatory initiatives (including beyond the financial sector) to improve cyber-incident reporting can enhance the availability of cyber risk data that can facilitate cyber insurance pricing and underwriting. CyberAcuView, an industry body comprising major cyber insurers, supports cyber data collection and voluntary data information standards. Nevertheless, greater transparency about cyber risk could also have unintended consequences for the cyber insurance protection gap, as insurers could tighten underwriting standards, raise premiums or restrict coverage, potentially leaving some firms unable or unwilling to obtain cyber insurance.

42 BMA (2025b) points out that distributed ledger technology ecosystems, particularly centralised digital asset exchanges, have emerged as high-value targets, representing concentrated "honey pot" vulnerabilities that constitute single points of failure. However, gaps exist in reporting of claims data.

43 See What is a Zero-Day Exploit? | IBM.

44 See Infrastructure as Code: Security Risks and How to Avoid Them | Trend Micro (IT).

risk in cloud and managed service providers,[45] where a single outage or security failure at a dominant provider can generate simultaneous business interruption, data loss and liability claims across a large portion of the portfolio. Many cyber events originate in third-party relationships, where insureds may have limited visibility into their vendors' controls – and even less into vendors' suppliers. This creates delayed and incomplete loss signals, as third-party incidents may surface only after cascading operational disruptions, complicating attribution, coverage determination and accumulation tracking. Supply chain risk also introduces hidden correlations, as multiple insureds may unknowingly rely on the same software libraries, platforms or service providers.

37. **In practice, cyber insurance pricing by insurers is still evolving.**[46] Pricing methodologies typically combine classical actuarial methodologies with advanced statistical techniques and expert judgment to address the unique nature of cyber risk and the modelling challenges.[47] The methodologies and models that insurers use vary and are improving over time.[48] Academic literature provides examples of actuarial methodologies that insurers can use to price cyber insurance policies.[49] Table 2 provides a non-exhaustive list of pricing methodologies for cyber insurance:

Pricing methodologies for cyber insurance

Selected examples Table 2

No	Methodology	Description
1	Frequency-severity /aggregate loss model[1]	Model frequency and severity of losses to derive aggregate losses; premiums set based on expected loss plus loadings. Likely to underestimate risk dependencies.
2	Copula-based dependence model[2]	Model the joint distribution of multiple risk components (eg frequency and severity, correlated sources of risk) to capture risk dependencies.
3	Network models[3]	Model cyber risk as interconnected events (where losses at one node increase the likelihood of losses elsewhere) to capture risk dependencies and contagion.
4	Scenario analysis[4]	Model scenarios of possible future cyber events based on threat intelligence and expert judgment and simulate losses across portfolios to price premiums.

[1] See J Bardopoulos, "Cyber-insurance pricing models", *British Actuarial Journal*, vol 30 (2025), e6.

[2] See H Herath and T Herath, "Copula based actuarial model for pricing cyber-insurance policies", *Insurance Markets and Companies: Analyses and Actuarial Computations, Forthcoming* (February 2011).

[3] See J Jang and R Oh, "A bivariate compound dynamic contagion process for cyber insurance", SSRN (June 2020).

[4] See Societies of Actuaries, *Cybersecurity insurance: modeling and pricing*, March 2017.

Source: FSI-IAIS staff.

[45] The US Department of the Treasury (2023) highlights that adoption of public cloud services has increased rapidly over the last decade but that models of adoption continue to vary across the financial sector in the United States and the cloud services market is concentrated around a small number of service providers. The concentration could expose many financial services clients to the same set of physical or cyber risks (eg from a region-wide outage).

[46] The survey of central banks in Doerr, S, L Gambacorta, T Leach, B Legros and D Whyte, "Cyber risk in central banking", BIS Working Papers, no 1039, September, BIS (2022) found that the vast majority of respondents regarded insurance markets as not yet sufficiently mature to effectively price and cover losses in the event of a cyber attack.

[47] Dacorogna and Kratz (2023) compare cyber risk models with other types of risk models.

[48] The Geneva Association (2023) provides an overview of cyber risk models used by selected (re)insurers in practice, highlighting that despite progress in cyber risk modelling, uncertainties around future losses remain a major challenge. Increasingly, insurers are working with service providers (such as cyber security and risk modelling vendors) and the academia to combine forensic data about threats and vulnerabilities with risk analytics frameworks to quantify potential cyber losses.

[49] Awiszus et al (2023) provide an overview of pricing models for cyber insurance, distinguishing between models that cover idiosyncratic, systematic and "systemic" cyber risk.

38. **Scenario analysis is often used in practice to model cyber insurance exposures because the methodology is well-suited to assess extreme, correlated and systemic events without historical precedence.** Commercial cyber catastrophe modelling firms offer stochastic models that simulate large numbers of potential cyber events to estimate the probability distribution of portfolio losses. These models typically combine narrative cyber attack scenarios with probabilistic modelling techniques, allowing insurers to generate simulated loss distributions for events such as cloud service outages, ransomware outbreaks or software supply chain compromises. Such stochastic analysis can be used to assess accumulation risk, inform underwriting and support pricing and capital modelling decisions. In contrast, deterministic scenario analysis defines a specific but plausible cyber event – such as a cyber attack on critical infrastructure or a large-scale cloud service outage – with fixed assumptions about the attack vector, affected systems, duration and economic impact.[50] Counterfactual analysis is another approach that complements stochastic or deterministic scenario analysis. Such approach starts from a real event and examines how losses might have evolved if key parameters such as duration of disruption or number of affected systems had differed (Gallagher Re (2024)). Ultimately, assessing the plausibility of these scenario analyses requires expert judgment.

39. **Supervisors may expect insurers to demonstrate how stress tests influence not only capital planning but also cyber pricing discipline and decisions to expand, restrict or withdraw underwriting capacity.** The NYDFS (2021) expects insurers to conduct cyber stress tests based on unlikely but realistic catastrophic cyber events that account for both affirmative and non-affirmative cover. It also expects insurers to have a formal strategy for measuring cyber insurance risk that is directed and approved by their senior management and board. In the UK, the PRA's general insurance stress test 2022 covered general insurers' cyber insurance underwriting risk by assessing the impact of three cyber scenarios: cloud outage, mass data exfiltration and systemic ransomware. Findings from such stress tests are useful to highlight to firms where they may need to improve.[51] The BMA (2025a) requires insurers writing cyber risk to incorporate severe but plausible cyber scenarios into their stress testing and capital adequacy assessments, including systemic events such as large-scale ransomware attacks or cloud service provider outages. These exercises are intended to support a forward-looking assessment of solvency resilience and to inform underwriting limits, pricing discipline and reinsurance strategies.

40. **Insurers typically rely on cyber catastrophe models provided by specialist cyber risk quantification firms.** These models can be used to price low frequency, high severity accumulation (tail-risk) events such as a major cloud outages or widespread malware. These models typically combine exposure data (eg firmographics, sector, technology stack), incident scenarios and probabilistic simulations to estimate expected losses across all policies (Hervé-Mignucci (2023)). Three major vendors provide such cyber catastrophe models, which suggests some concentration in the market. The results across the models may vary for a given portfolio of cyber insurance policies, highlighting the need to carefully evaluate and calibrate the assumptions underlying the models (Guy Carpenter (2023)). Some insurers may use or complement vendor models with deterministic, in-house models.

41. **While actuarial models provide an estimate of the technical or "risk-adequate" premium based on expected losses and uncertainty, this actuarially determined price is only one input into the final market price of a cyber insurance policy.** In practice, premiums are also shaped by a range of factor such as supply–demand dynamics, insurers' risk appetite and capacity constraints, reinsurance availability and cost, as well as competitive pressures. Additional adjustments reflect underwriting judgment, uncertainty margins arising from data scarcity and risk interdependencies. Policy conditions

[50] For example, see Lloyd's and the University of Cambridge Centre for Risk Studies (2015), which modelled a cyber attack on the US electricity grid.

[51] For example, in its general insurance stress test of 2022, the PRA called for the general insurance market to develop consensus on the likelihood of tail cyber insurance risk under the prescribed scenarios. It also urged boards to understand the risks of unclear policy language and potential contract uncertainty and to ensure these risks align with their firm's risk tolerance (BoE-PRA (2023)).

such as deductibles, limits, exclusions and cost-sharing also play a factor, and these conditions themselves may change over time, depending on loss trends such as frequency and severity of ransomware losses. As a result, cyber insurance pricing is not purely model-driven but emerges from the interaction between technical risk assessment and market forces. This means that premiums can move sharply in response to shifts in loss experience, capital conditions or perceived threat levels.

42. **From a regulatory perspective, the continued monitoring of the cyber insurance market can help identify potential regulatory concerns.** In a soft market (when premium rates are low), an overly intense competition could lead to a downward pricing spiral, to the detriment of all players if policies are underpriced (IAIS (2025)). In a hard market (when premium rates are high), overpricing or stricter underwriting conditions may exacerbate the protection gap.

Accumulation risk

43. **A major concern around the pricing of cyber insurance relates to accumulation risk, which refers to the possibility that a single cyber event or vulnerability triggers losses across many policyholders simultaneously, leading to large aggregate claims for insurers.**[52] In traditional insurance lines, losses are typically independent. In contrast, cyber incidents may spread across multiple firms, sectors or even countries at the same time due to the interconnected nature of digital systems and shared technology platforms. As a result, insurers may face multiple claims arising from a single underlying event, sometimes across several insurance policies or lines of business. From a systemic risk perspective, a single event may impact multiple insurers across multiple policies simultaneously. Moreover, IAIS (2020) highlighted that non-affirmative cyber cover as well as overlapping cyber coverage may accentuate accumulation risk.

44. **Cyber accumulation risk arises primarily because digital infrastructure and software ecosystems are highly interconnected** (IAIS (2020)). Many organisations increasingly rely on the same cloud providers[53] (including AI service providers), software systems or managed service providers. If a vulnerability or cyber operation affects one of these shared components, the disruption can cascade across numerous companies simultaneously. For example, a single point of disruption such as widespread malware infection or cloud outage could trigger widespread losses from multiple policyholders and from multiple policies (CyberCube and Munich Re (2025); Beazley et al (2024)). The Geneva Association (2022) lays out the following pathways through which cyber losses may accumulate:

- **Critical infrastructure failure:** Systems, networks and assets required to ensure the security of a nation, its economy and the public's health or safety can be disrupted (eg attack on power grids).
- **Supply chain disruption:** Reliance on third parties to deliver IT services such as software engineering, data storage or network security can be compromised.
- **Zero-day and open-source software vulnerabilities:** Software bugs may not be detected for some time, allowing attackers to steal/copy data and/or damage sensitive systems.
- **Mass liability claims:** Almost any cyber incident can lead to claims for compensation from affected customers, suppliers and other stakeholders (eg a major data breach affecting millions of customers).

45. **Cyber incidents may trigger property damage losses, which can accentuate accumulation risk.** As various economic sectors become more digitalised, the line between cyber and property risks is becoming more blurred. In addition, the growing use of the Internet-of-Things (IoT), including in

[52] The IAIS (2020) quoted the CRO Forum's definition of "accumulation risk" as risk that arises from concentration of insured risks that may be affected by events that cause substantial losses under several insurance policies, potentially over multiple years and geographies.

[53] Koh and Prenio (2023) outline potential oversight frameworks for cloud service providers.

manufacturing processes, is increasing the link between digital and physical systems.[54] The German Federal Office for Information Security (2014) has cited an example where attackers used spear phishing[55] e-mails to compromise a steel mill's IT network, allowing the attackers to control the plant's operating system, which led to the uncontrolled shutdown of a blast furnace and resulted in massive damage.

46. **These characteristics make cyber accumulation risk a major concern for both insurers and supervisors in the context of cyber insurance underwriting.** For insurers, large correlated losses may lead to underpricing, potentially threatening solvency or capital adequacy. To manage accumulation risk, insurers typically rely on scenario-based stress testing, exposure caps, sub-limits, exclusions, coinsurance and tight policy wording as imperfect accumulation controls. From a supervisory perspective, accumulation risk raises concerns about the potential systemic impact of a large cyber event on the insurance sector.[56] Despite the use of stress tests, limits, exclusions and reinsurance, cyber accumulation risk remains subject to significant uncertainty and may not be fully controlled, particularly for correlated and cross-business line events. Supervisors therefore emphasise the importance of monitoring cyber exposures of insurers, improving data collection and stress testing insurers against severe but plausible cyber scenarios. Supervisors may also expect insurers to demonstrate how underwriting limits, pricing, exclusions and reinsurance structures collectively constrain cyber accumulation risk given increasing reliance on third-party service providers.

47. **For markets dominated by reinsurance, such as Bermuda, accumulation risk is further amplified by global aggregation across cedants and lines of business, where a single cyber event may trigger losses across multiple counterparties and geographies.** This creates additional complexity in measuring exposures, particularly where dependencies on common technology providers or shared vulnerabilities are not fully visible, reinforcing the need for robust aggregation controls and scenario-based analysis. In response to this, the BMA (2025b) requires insurers to undertake cyber worst-case scenario analyses, focusing on systemic cyber events (including global ransomware campaigns and major cloud service provider failures) as key drivers of accumulation risk. These exercises underscore the importance of integrating accumulation considerations across underwriting, capital modelling and reinsurance arrangements, particularly given the global and interconnected nature of cyber exposures. Box C provides a high-level overview of how frontier AI models may significantly transform the cyber threat and defence landscape.

Box C

Glasswing and Mythos – the transparent butterfly that is no longer a myth①

On 7 April 2026, Anthropic (2026) announced Claude Mythos Preview – a general-purpose AI model that it judged too dangerous to release to the public. Mythos is, on its surface, the latest in a line of increasingly capable large language models. It operates like a senior software engineer, spotting bugs and self-correcting its mistakes. But what has set Mythos apart is its remarkable ability to find and exploit previously unknown software vulnerabilities at a scale and speed that no human team could match. Previous AI tools could assist skilled human security researchers in finding vulnerabilities. Mythos can conduct the full attack chain – from identifying the flaw to developing and chaining working exploits – without human expertise in the loop.

54 Munich Re (2025c) cites more than 16.6 billion IoT devices being networked around the globe and more than 60% of manufacturers integrating IoT technologies into their production and assembly processes.

55 See What is spear phishing? | IBM.

56 EIOPA (2022) highlights increasing accumulation and concentration risks arising from common technologies and service providers. NAIC (2025) highlights that mitigating third-party-driven cyber incidents with widespread consequences, even non-malicious events such as the July 2024 CrowdStrike incident, will only increase in importance as companies continue to integrate more third-party solutions.

In the weeks before its announcement, Anthropic used Mythos to scan critical software infrastructure and found thousands of zero-day vulnerabilities – previously unknown flaws – across every major operating system and every major web browser.② Ninety-nine percent of those vulnerabilities remain unpatched. The UK's AI Security Institute, which was granted early access to the model, found that it succeeded in expert-level hacking tasks 73% of the time. Prior to April 2026, no AI model could complete those tasks (AISI (2026)).

Anthropic's own benchmarks illustrate the advancement. Its previous frontier model, Opus 4.6, had a near-zero success rate at autonomous exploit development – turning a known vulnerability into a working attack. Mythos Preview, presented with the same set of Firefox JavaScript engine vulnerabilities that Opus 4.6 had identified, developed working exploits 181 times compared with Opus 4.6's two successes out of several hundred attempts. Each exploit was written completely autonomously, without human intervention after an initial prompt. This is the critical distinction.

Anthropic launched Project Glasswing: a restricted-access programme under which Mythos Preview is made available to a small group of organisations for defensive security work.③ The logic of Glasswing is to use the model's capabilities to close vulnerabilities before less responsible actors – nation-state adversaries, criminal ransomware groups, hacktivists – independently develop equivalent capabilities or gain access to Mythos or a comparable model. Anthropic's CEO Dario Amodei said, "The dangers of getting this wrong are obvious, but if we get it right, there is a real opportunity to create a fundamentally more secure internet and world".④

Implications for the cyber insurance market

For the cyber insurance industry, frontier AI models with capabilities like Mythos present both a structural threat to the existing risk environment and a potential opportunity to close cyber vulnerabilities:

- The attacker-defender asymmetry: If AI dramatically lowers the cost, expertise and time required to exploit a known vulnerability, the increasing frequency and severity of successful attacks may challenge the industry's underwriting and pricing models. Cyber insurers may raise the bar on underwriting requirements related to insured firms' cyber readiness, especially considering potential increases in the velocity of attacks. On the other hand, Pollard et al (2026) mention that traditional penetration testing – currently priced at USD 20,000–120,000 per engagement, with pricing anchored to the scarcity of human expertise – faces repricing to near-zero for AI-automated equivalents, which may counter-balance the potential increasing losses. Nevertheless, if offensive capability is similarly democratised, cyber insurers' loss ratios will deteriorate.
- Accumulation risk: If frontier cyber AI models materially lower the cost of finding exploitable weaknesses, they could increase the frequency and speed of attacks, especially where many insureds depend on common software, cloud environments or service providers. If a future model is used to exploit vulnerabilities that are identified but remain unpatched in widely used software, the resulting incident could trigger simultaneous losses across thousands of insured organisations.
- Improved cyber defence capabilities: Used defensively, frontier cyber AI models may improve patching, security testing and risk assessments.⑤ For cyber insurers, such models may improve underwriting: insureds that use AI-enabled code review, red-teaming and patch management may become more attractive risks, while firms that are not able to fix those vulnerabilities may become less insurable. If Project Glasswing succeeds in its stated purpose, the global attack surface available to threat actors may actually shrink – thus supporting the insurability of cyber risk.⑥

Regulatory considerations

The regulatory response to Mythos has been rapid.⑦ For insurance regulators specifically, several considerations are immediate:

- Risk reassessment: Existing prudential risk assessment tools including scenario analysis or stress testing may not adequately capture a scenario in which a single AI model simultaneously surfaces and exploits thousands of vulnerabilities across interdependent infrastructure. Underwriting approaches may need to transform from a point-in-time to continuous assessment in a world where a new critical vulnerability can be exploited and weaponised in hours (Motta (2026)).
- Competition: A frontier model that can help find and exploit vulnerabilities could create an uneven competitive situation in which well-resourced firms obtain defensive tools first, while smaller firms without access to such models may lag.

- Non-affirmative cyber cover: Frontier models may accentuate the need to urgently clarify if new categories of AI-augmented attack fall into coverage ambiguity – ie are not clearly included or excluded – in current policy wordings. Insurers may need to consider how AI-enabled autonomous exploitation is treated in cyber insurance.

Conclusion

Claude Mythos Preview is a real and significant development. Whether it represents a sudden break in the cyber security landscape or an anticipated step along a trajectory that was already clear, the practical consequence is the same: the development of AI-automated vulnerability discovery and exploit has crossed into a capability range previously reserved for human specialists. All the capabilities identified within Mythos may have been observed previously; however, what sets it apart is the accelerated pace of these capabilities, driven by enhanced coordination and a centralised effort from the software and security communities to identify and address vulnerabilities. Rather than being an outlier, Mythos represents an early example of a capability that is poised to grow and scale over time.

For the cyber insurance market, the implications run in two directions simultaneously. On the loss side, the prospect of AI-democratised offensive capability points to higher claims frequency and potential accumulation scenarios that current models may not fully capture. On the risk-reduction side, if defensive deployment of Mythos-class tools proceeds at scale, the underlying attack surface may shrink faster than at any previous point in the market's history. It remains to be seen which way the transparent butterfly may tip this scale.

① The glasswing butterfly is so-called because of its transparent wings – beautiful, fragile and extraordinarily difficult to see when it is moving, reflecting how much of the world's software has been transparent to sophisticated attackers all along. ② For example, a 27-year-old vulnerability was found in OpenBSD, an open-source operating system used to run critical firewall infrastructure. A 16-year-old flaw was identified in FFmpeg (a code library embedded in common consumer and enterprise applications) in a line of code that automated testing tools had executed five million times without catching it. ③ See Anthropic - Project Glasswing. Initial launch partners include Microsoft, Google, Apple, Amazon Web Services, JP Morgan Chase, Cisco and Nvidia. A further group of over 50 organisations that build or maintain critical software infrastructure has received access to scan and secure both proprietary and open-source systems. In June 2026, the project was further expanded to 150 new organisations in more than 15 countries. ④ See Dario Amodei on X. ⑤ *Wire*d reported that Mozilla used early access to Mythos to identify and fix 271 vulnerabilities in Firefox 150, illustrating the possibility that advanced models could help defenders clear long-standing vulnerability backlogs faster than before (see Newman (2026)). ⑥ National Cyber Security Centre (NCSC (2026)) describes how frontier AI models can strengthen cyber defence. ⑦ Financial authorities across the globe have raised urgent concerns about the governance, risks and unequal access implications of Mythos, with calls for immediate regulatory assessments. See Annex 3 for a list of actions taken.

Section 4 – Protection gap

Size of the gap and the trend

48. **The cyber protection gap is significant, exposing large sections of the global economy.** Coverage in emerging market and developing economies (EMDEs) is particularly low.[57] For instance, while Asia Pacific accounts for 10% of cyber insurance GWPs, IBM (2025) estimates that it experiences 34% of global cyber attacks. While estimates of the gap vary, all of them acknowledge the large gap, which means economies are significantly exposed to cyber risk. Munich Re (2025a) estimates that the total market for cyber insurance is more than USD 15.3 billion against total economic losses from cyber incidents, which range from an estimated USD 1 to 10 trillion.[58] Large attacks or non-malicious disruptions could have significant economic impacts to individual firms, sectors or broader economic output. For instance, in the UK, the cyber attack on Jaguar Land Rover, which is now the costliest cyber attack in the UK, is estimated to have cost USD 2.5 billion (Stewart (2025)).

[57] See paragraph 9 on the geographical concentration of cyber insurance markets.

[58] See footnote 5.

49. **Large corporates represent the vast majority of cyber insurance coverage.**[59] Swiss Re (2025) estimates that in North America and Europe between 60% and 70% of large corporates purchase cyber cover, compared with 40% to 50% for mid-market firms and 10% to 20% for small and medium enterprises (SMEs). A number of factors account for this difference, not least that large corporates are better resourced to put in place the necessary cyber risk management measures to reduce their cyber exposure and meet underwriting requirements. Given these governance structures, large corporates are more likely to consider insurance to protect against cyber risk, and they are therefore a more attractive risk proposition for insurers. Their purchasing power and use of brokers increase their ability to secure cover.

50. **Nevertheless, even large corporates may find coverage is insufficient for the risks they face.** Cyber underwriters are managing their risk by setting limits on cover. This makes sense from a prudential perspective, but it means that cover for large corporates could be limited and at significantly lower limits for SMEs.[60] While a study by IBM (2025) estimates that the average cost of a data breach globally for a large corporate is USD 4.4 million, this is dwarfed by the costs of some of the larger attacks,[61] which exceed the limit of the largest available cyber insurance cover.

Reasons for the gap

51. **Given limited cyber cover and the increasing number of cyber incidents, the cyber protection gap is likely to grow.** Cyber attacks will increase because of a combination of heightened threat capabilities, geopolitical tensions, growing digitalisation, concentrated digital dependencies and supply chain vulnerabilities. The growth in economic losses may be particularly big if attackers are able to take advantage of AI to mount attacks quicker than cyber security teams are able to use AI to protect IT networks. Estimates suggest that attacks increased by more than 160% between 2020 and 2025 (see Total Assure (2025)).

52. **Unless the dynamics of supply and demand change significantly in the market, the protection gap will continue to increase.** Both supply and demand factors impact the protection gap, though current market conditions suggest that the demand-side factors are more significant.[62] While insurers report the capacity to increase underwriting, the demand for cover is not increasing in line with the growing risk. Attacks are increasing significantly, but the level of insurance cover is increasing only a mid-single digit. According to Swiss Re (2025), the compound annual growth in the market has slowed from 31% between 2017 and 2022 to 5% from 2022 onwards.

53. **A number of factors drive a lack of demand for cover**:

- **Awareness of insurance availability**: Some corporates may not know that these risks can be insured (see Graph 6).[63]
- **Product complexity**: Smaller businesses, especially those that do not use brokers, may be confused by the cover available and the complexities of insurance contract exclusions.[64]

[59] As regards financial institutions, most central bank respondents in a BIS survey (Doerr et al (2022)) stated that less than half of financial institutions in their jurisdictions hold cyber insurance policies.

[60] An anecdotal source estimated that limits for large corporates could be around USD 750 million.

[61] For instance, the UnitedHealth Group estimated an attack as costing USD 2.87 billion in 2024.

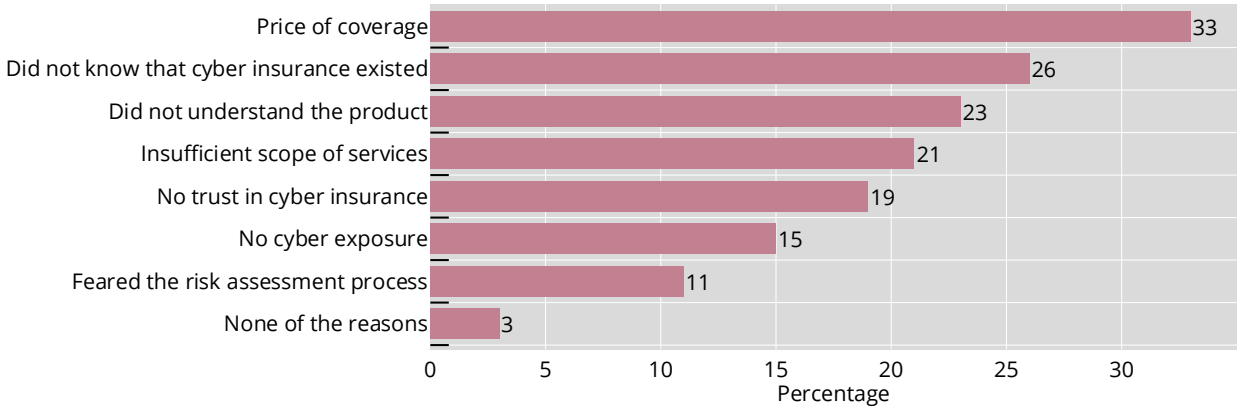
[62] Despite premium rates falling, demand has not increased significantly.

[63] In a 2024 survey, Munich Re (2024) found that 34% of executives of businesses with revenue of less than USD 1 million did not know that cyber insurance existed. This reduced to 5% for executives from businesses with more than USD 5 billion of revenue.

[64] In the UK, SMEs struggle to understand cyber insurance policy details due to complex policy language. SMEs also often overestimate their ability to self-insure (see US Department for Science, Innovation and Technology and GrantThornton (2025)).

- **Trust**: A lack of trust on the part of prospective policyholders is likely to contribute to the lack of demand for cyber coverage.[65] This can be attributed to policyholders not wanting to provide the necessary information to insurers for loss adjustment to preserve confidential commercially sensitive data. Firms may perceive that coverage is unreliable because of opaque and ambiguous policy wordings (Geneva Association (2026b)).
- **Affordability**: The cost of cyber insurance could be prohibitive, especially for SMEs. The cost includes not only the premiums for cyber insurance policies but also the cost to build and maintain operational resilience at a level that satisfies the underwriting requirements of cyber insurers (BoE (2025)).[66]

Reasons for not taking cyber insurance[1] Graph 6



[1] The 2024 Munich Re Global Cyber Risk and Insurance Survey included over 7,500 participants from 15 countries, covering all industries and company sizes.

Source: FSI-IAIS staff. Adapted from Munich Re, Munich Re global cyber risk and insurance survey 2024: bridging the gap in cyber protection, April 2024.

Addressing the protection gap

54. **In addressing the protection gap, it is important to consider which cyber risks are insurable and which are uninsurable.** Risks are insurable where they are measurable or quantifiable and where insurers may apply limits to coverage. For those cyber risks that are insurable, a multistakeholder approach is needed to support the growth of the market by working together. This will mean increasing both demand and supply. Cyber risks may be uninsurable for risks such as state-sponsored cyber attacks, terrorism and systemic vulnerabilities (eg a breakdown of critical infrastructure) (Eling and Wirfs (2016)). These are difficult to insure because they cannot easily be diversified and the potentially large cost may exceed insurers' risk-bearing capacity.

55. **A combination of factors could over time drive demand:**

- **Research**: More research about risk perceptions and drivers for increasing cover could be useful to understand how to reduce the protection gap. For instance, a 2018 study by Marsh found that in a survey of 1,300 risk professionals and other senior executives globally, representing 26 industry

65 Of all respondents to the Munich Re survey, 19% stated they have "no trust" in cyber insurance (see Munich Re (2024)).

66 Munich Re (2025b) reports that among corporates, the price of coverage was the reason for the protection gap in a third of cases.

sectors, two thirds of respondents list cyber security as a top five risk while only 30% have adopted a plan to address the risk (Marsh (2018)). Such research will, over time, help to understand risk perceptions and the steps that can be taken to increase demand for cover.

- **Education**: Governments can take steps to promote the importance of effective cyber hygiene in reducing cyber exposure not only to corporates but also to SMEs and individuals.[67] Equally, the insurance industry can collectively consider how it can highlight the benefits of coverage. It is important that businesses understand the economic losses that could arise from a cyber attack on their business. Smaller organisations may not have the resources to understand the risks to which they are exposed. Or this might be because senior management and boards are not fully engaged with the risks businesses are exposed to.
- **Product design**: A number of steps could be taken to make cyber solutions more appealing for the SME market, including designing dedicated products that are simple, affordable and modular. Focusing on essential coverage and offering technical support may make it possible to increase penetration (Swiss Re (2025)).
- **Policy coverage**: Perceptions about the complexity of coverage and exclusions may be a factor in the lower take up of cyber insurance. For overly complex products, a prospective policyholder may be worried about their ability to claim on a policy if they needed to.
- **Linking cover to cyber hygiene**: Pricing can be an effective signal for policyholders to improve their cyber hygiene. Interviews undertaken for this paper suggested that while insurers expect a minimum cyber hygiene to cover cyber risks, over a certain threshold policyholders do not gain the benefits of increased cyber hygiene. Insurers may need to find a better way to send these price signals given the benefits provided to policyholders and the risk reduction it will provide for insurers.

56. **Reinsurance capacity plays an important role in supporting the underwriting capacity of cyber insurance by primary insurers.** Over 2022–24, approximately 50% to 75% of global cyber insurance premiums were ceded to reinsurers (Cremer et al (2024); S&P Global (2024)). Howden Re (2025) highlights the concentrated nature of global reinsurance players, with the top five reinsurers accounting for 62% of cyber GWPs in 2025. The National Association of Insurance Commissioners (NAIC) notes the important role that reinsurance plays in expanding capacity of cyber insurance market and improving underwriting controls. Capacity has also increased by transferring risks to capital markets (NAIC (2025)). In 2025, the IAIS noted that insurers have started to transfer some risks with cyber insurance-linked securities. For instance, in 2023, Bermuda-based ILS vehicles issued USD 670 million of aggregate insurance protection. That said, the global market remains a small proportion of cyber limits and a very small part of the total Cat bond market (IAIS (2025)). As these trends develop, it is important for supervisors to continue efforts to understand the emerging risks. While reinsurance expands capacity, it can also concentrate correlated cyber risk among a small number of counterparties. Equally, while the development of capital market participation is welcome, it remains limited and largely untested for systemic cyber events.

57. **In common with other insurance protection gaps, addressing this one will likely require a multi-stakeholder approach.**[68, 69] Insurers, trade associations, consumer groups, supervisors and governments all have important roles to play in addressing the protection gaps (MarshMcLennan and Zurich Insurance (2024)).

[67] For instance, in the UK, Cyber Essentials is a government-backed, industry-supported scheme to help organisations protect themselves against common online threats.

[68] The Bank of England highlights that greater collaboration between insurers and other financial firms can increase the visibility of financial impacts arising from cyber risks and the role of insurance risk transfer (BoE (2025)). Such collaboration can enable informed decision-making around risk, including where risks are not being insured.

[69] The IAIS (2023a) provides a framework for addressing protection gaps more generally.

- **Insurers**: An effective commercial insurance market for covering cyber risks is needed to close the protection gap. Where pricing reflects the measures policyholders have put in place to manage their cyber risk, this also leads to an overall increase in cyber hygiene. Insurers can engage with supervisors as they develop new cyber insurance products and move into new markets.
- **Trade associations**: Trade associations for the insurance sector have a role to play in encouraging the sector to find solutions to address the protection gap. These associations have been some of the leading sources of research in this area. Meanwhile, business trade associations could work to support their commercial members in understanding risks from cyber and the benefits of cover.
- **Supervisors**: Some supervisors with mandates to promote financial inclusion and market development can seek to narrow protection gaps. In cases where supervisors do not have such explicit mandates, insurance supervisors can still contribute to narrowing the protection gap by contributing to financial stability as firms enhance their cyber resilience.

  From a prudential perspective, by requiring insurers to adopt risk-based pricing approaches, insurance supervisors can promote cyber resilience more broadly, as riskier firms will be charged more and vice versa. Insurers that adopt a risk-based underwriting and pricing approach can provide incentives to firms to improve their cyber hygiene.[70] To support sustainable insurance markets, prudential supervisors will want to ensure that insurers are taking a prudent approach to moving into or growing their underwriting in this market. Those supervisors in markets where cyber cover is not offered may wish to consider whether barriers exist to the development of a market.

  Many supervisors are also responsible for supporting consumer financial education, including information about insurance policies. Insurance supervisors can raise awareness on the benefits of risk prevention, inform and encourage policyholders to invest in risk prevention measures and implement supervisory measures to incentivise transparent risk-based pricing by insurers. Additionally, as risk experts, supervisors can provide guidance to governments on the extent to which private and public solutions may help to reduce the protection gap.
- **Governments**: The primary role of governments is to support efforts to reduce cyber risk given broader security and the economic consequences of cyber incidents. They can encourage effective cyber hygiene standards across both businesses and the public more generally, particularly for critical infrastructure (GFIA (2023)). They should also consider if, when and to what extent they can address larger cyber risk. This might be an explicit statement that large risks need to be commercially insured or that the government will support public-private partnerships to address these risks. Key is that governments set clear expectations and that governments facilitate dialogue on these matters. Such clear statements from the government on risk sharing can help the market to better understand and price risk. Equally, given governments' information about cyber attacks, they may have a role to play in sharing non-sensitive assessments on cyber threats (including details on attacks) to improve cyber hygiene and support effective underwriting.

58. **No one-size-fits-all solution is likely to work, as jurisdictions have varying capacities.** For instance, advanced economies are likely to have more fiscal space and access to capital markets, whereas EMDEs may face more constraints on both these points. Graph 7 sets out a stylised approach to segmenting cyber risks as a way to consider how to reduce the protection gap.

- **Cyber hygiene**: Overall exposure could be reduced by concerted efforts to increase cyber hygiene. Governments can set minimum standards, insurers can incentivise action and, most importantly, policyholders can address the risks they face.
- **Insurable market**: Commercial insurance markets should be able to cover quantifiable catastrophic risks to a certain level with increased capacity through reinsurance- and insurance-linked securities.

[70] The NYDFS (2021) encourages insurers to incentivise insured firms to adopt preventive cyber security measures through favourable pricing policies that recognise the reduced risks.

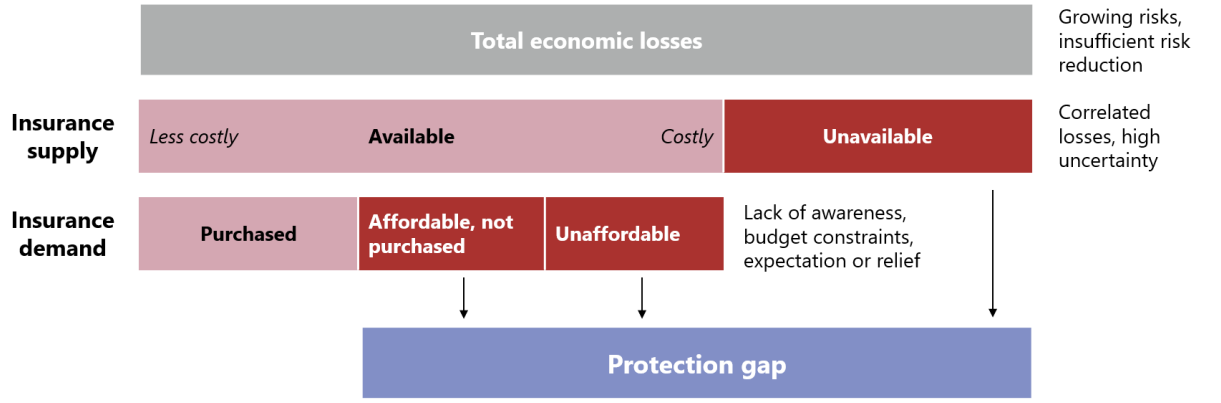
Therefore, supply-side issues could be addressed by: (i) insurers committing to grow their insurance business; (ii) an increased focus on cyber hygiene; and (iii) finding capital market solutions that support the growth of the available cover.

- **Public-private partnerships**: Where cyber risk becomes unquantifiable or uninsurable, public-private partnerships with some commercial cover could allow cover at least up to certain limits, encourage the development of the cyber insurance market and support improvements in cyber hygiene. Equally, governments will be able to ensure that cover is offered only to those that have taken out commercial insurance. Governments may be able to reinsure tranches of the risk or sell the risk in capital markets.

  EMDEs, which may be unable to access capital or reinsurance markets, may have the potential to use the support of development banks or seek other backstop guarantees.

  Where economic losses are higher and securing cover in the capital markets is not possible, governments must be explicit about the level of risk they are willing to take on. Given the different fiscal capacity governments have, they too will likely need to limit their exposure.

Stylised illustration of attribution of cyber risk protection gap — Graph 7



Source: Adapted from Geneva Association, Addressing growing protection gaps through better public-private insurance programmes, February 2026.

59. **For cyber risks that are not commercially insurable, policymakers need to consider whether and how a backstop may work.** Pool schemes, similar to those used for terrorism, can offer some potential to reduce risks for organisations and individuals. A limited number of such schemes currently exist (see Box D). In the UK, Pool Re, established in 1993 to cover terrorism risk, was extended in 2018 to include physical damage to properties in Great Britain from cyber terrorism acts certified by Pool Re and the British government. If governments develop pool schemes, they will need to be clear on the level of coverage and comfortable with the possible fiscal impact of claims. Pool schemes that maintain a risk-based approach to coverage can increase the incentives for risk reduction and remove the chance of governments becoming the insurer of first resort. Developing public-private partnerships can allow for a system where insurers can incentivise risk reduction and where initial losses are assumed by insurance markets and not taxpayers (GFIA (2023)). A wholly government-funded solution ex post will instead lead to moral hazard and reduce the incentives for cyber hygiene.[71]

[71] Lessons can be drawn from public-private partnerships developed to address other protection gaps. Well-established schemes such as France's Caisse Centrale de Reassurance, the US National Flood Insurance Program, the Swiss Pool for Earthquake Insurance, or the various European windstorm pools offer concrete examples of how governments and the private insurance industry have structured risk-sharing arrangements for systemic and hard-to-insure risks.

Box D

Public-private partnerships – cyber terrorism pools

Cyber terrorism pools are public-private risk sharing arrangements to absorb extreme losses arising from cyber terrorism event. Increasing geopolitical conflicts may heighten the use of cyber attacks as a weapon of choice. For example, CyberCube (2026) estimates that 12% of US based companies with revenues over USD 1 billion face the greatest likelihood of being targeted by Iranian cyber threat actors. Cyber attacks as an act of war are usually excluded from cyber insurance policies.① In addition, catastrophic cyber incidents resulting in highly correlated large losses across many entities and/or jurisdictions may exceed private insurance capacity. For these reasons, cyber terrorism pools can become critical to serve as systemic cyber risk absorber. Table 3 provides an overview of a selection of cyber terrorism pools.②

Selected list of cyber terrorism pools

Table D.1

Jurisdiction	Name	Type	Cyber coverage	Additional information
France	Gestion de l'Assurance et de la Reassurance des Risques d'Attentats et Actes de Terrorisme (GAREAT))	Government-backed (re)insurance pool	Cyber physical damage	Terrorism insurance is mandatory extension for all property policies. State provides unlimited backstop. Maximal use of private reinsurance before state intervention.
Germany	Extremus	Government-backed private insurer	Cyber physical and non-physical damage	
Netherlands	Dutch Terrorism Reinsurance Pool		Cyber physical and non-physical damage	
Spain	Consorcio de Compensación de Seguros (CCS)	First-party	Cyber physical damage	
United Kingdom	Pool Re	Government-backed mutual reinsurer	Cyber physical damage	Public-private partnership between insurers and UK government
United States	Terrorism Risk Insurance Program (TRIP)	Government co-insurance backstop	Cover only if cyber attack is certified as terrorism	Mandates insurers to provide coverage for insured losses resulting from terrorism; insurers can claim from the US Treasury, subject to deductible.

Sources: FSI-IAIS staff.

① See Lloyd Market Association's "Cyber war and cyber operation exclusion clauses". ② See OECD (2021) and WTW (2024)).

Section 5 – Conclusion

60. **Cyber risk is becoming a significant threat to financial stability and to economic and operational resilience in an increasingly digitalised and interconnected world.** The rapid evolution of cyber threats driven by advancements in technology (including AI), geopolitical tensions and the interconnected nature of digital ecosystems have amplified the need for robust risk management strategies. Against this backdrop, cyber insurance has the potential to become an important tool for mitigating the financial and operational impacts of cyber risk. However, the market continues to face significant challenges. These include uncertainties over the future trajectory of cyber threats, ambiguities in coverage and growing accumulation risks. A persistent protection gap poses a broader policy challenge in addressing cyber risk more generally.

61. **Uncertainties over future trends of cyber risk underscore the importance of closely monitoring claims development.** Volatile claims experience can be expected to continue. Cyber underwriting policy should reflect the evolving nature of cyber risk and its sensitivity to external and macro conditions. Insurers should consider how underwriting risk may change with the operating environment, the threat landscape, digitalisation trends and geopolitical tensions that may increase incentives for cybercrime or amplify business interruption losses. AI, particularly frontier AI models with autonomous capabilities, has the potential to increase the scale, speed and sophistication of cyber attacks, while the growing reliance on cloud computing and digital interconnectedness can propagate shocks across firms and sectors. Supervisors should closely monitor these trends and their implications for the cyber insurance market, ensuring that insurers' risk management practices remain robust and adaptive.

62. **Both the industry and the regulatory community have come a long way in addressing non-affirmative cyber coverage, but more efforts are needed.** Nevertheless, the dynamic nature of cyber risk and the external environment that shapes it continue to pose challenges. As geopolitical tensions rise, increasing physical property damage could arise from cyber-related policies and cyberterrorism could accelerate, impacting many different business lines. At the same time, technological advancements especially AI, may uncover surprises in terms of claims not intended to be covered in cyber policies. Given these circumstances, both the industry and regulators need to closely monitor the evolution of non-affirmative cyber coverage.

63. **Accumulation risk, which has the potential to pose systemic risk, is currently the most pressing concern in underwriting cyber insurance.** Widespread ransomware attacks or cloud service outages could trigger simultaneous losses across multiple policyholders and insurers because of the interconnected nature of digital systems and shared dependencies. While the use of limits and exclusions on certain risks can be an effective tool for insurers to manage their accumulation risk and maintain financial stability, it is important to recognise the potential unintended consequences. Such measures, if not carefully designed and communicated, could lead to conduct or reputational risks for insurers. Therefore, while protecting their own risk exposure, insurers need to uphold transparency, fairness and customer trust to mitigate these adverse implications.

64. **The protection gap in cyber insurance remains significant, particularly for SMEs and EMDEs.** While both demand-side and supply-side factors play a role in this, the former appear more significant. Addressing this gap requires a multistakeholder approach, with regulators, insurers and governments working together to promote better cyber hygiene and risk awareness. Regulators can encourage insurers to incentivise improved cyber security practices through risk-based pricing and premium discounts. Nevertheless, insurers should not be compelled to underwrite cyber insurance risk if they are unable to assess, manage and mitigate the underwriting risk.

65. **Governments may need to step in to address the protection gap in cyber insurance by providing backstops for catastrophic accumulation losses from systemic events.** Public-private partnerships, like government-backed insurance pools, can help absorb extreme losses and ensure market

stability. However, this could create moral hazard, where insurers or policyholders rely on public support rather than strengthening risk management. To mitigate this, governments should clearly define their role, ensure private insurers retain some risk exposure and tie backstop access to strong cyber security standards.

66. **Looking ahead, the cyber insurance market can play an important role, to a certain extent, in mitigating the increasing scale and complexity of cyber risks and in contributing to financial stability.** The development of the cyber insurance market needs to be underpinned by risk-based pricing and disciplined underwriting approaches to support broader efforts in increasing risk awareness and the provision of cyber insurance. Nevertheless, cyber insurance should not and cannot replace sound cyber risk management controls. Strengthening resilience across firms, sectors and digital ecosystems will be essential to complement the role of cyber insurance and ensure a more secure and stable digital future. Without collective efforts to strengthen overall cyber resilience, cyber insurance may fall short of serving as a digital safety net – which is increasingly crucial in safeguarding financial and economic stability.

References

AI Security Institute (AISI) (2026): "Our evaluation of Claude Mythos Preview's cyber capabilities", 13 April.

Allianz (2026): *Allianz Risk Barometer: identifying the major business risks for 2026*, January.

Amaral, R (2025): "Cyber insurance market wrestles with AI risk challenge", *Insurance Day*, 17 October.

American Academy of Actuaries (2021): *Silent cyber*, August.

——— (2023): *War, cyberterrorism, and cyber insurance*, February.

——— (2025): *An overview of the global cyber (re)insurance market*, August.

Anthropic (2026): *Assessing Claude Mythos Preview's cybersecurity capabilities*, 7 April.

Aon (2023): "When is a cyber crime not a "cyber-crime"? Social engineering fraud (SEF) and Business email compromise (BEC)", August.

——— (2025): "Findings from Aon's Global Risk Management Survey", October.

Arnold, M (2026): "UK financial regulators rush to assess risks of Anthropic's latest AI model", *Financial Times*, 12 April.

Australian Prudential Regulation Authority (2026): "APRA letter industry on artificial intelligence (AI)", 30 April.

Australian Signals Directorate and Australian Cyber Security Centre (2026): *Frontier models and their impact on cyber security*, April.

Awiszus, K, T Knispel, I Penner, G Svindland, A Voss and S Weber (2023): "Modeling and pricing cyber insurance", *European Actuarial Journal*, vol 13, pp 1–53.Bank of England (BoE) (2025): *Financial Stability Report*, Financial Policy Committee, December.

——— (2026): "The Bank, FCA and HM Treasury joint statement on Frontier AI models and cyber resilience", 15 May.

Bank of England (BoE) and Prudential Regulation Authority (PRA) (2020*): Insurance Stress Test 2019 and Covid-19 stress testing: feedback for general and life insurers*, June.

——— (2023): *Insurance stress test 2022 feedback*, January.

——— (2024): *Cyber insurance underwriting risk*, Supervisory Statement SS4/17, November.

Bank of Spain (2026): *Financial Stability Report Spring 2026*, May.

Bardopoulos, J (2025): "Cyber-insurance pricing models", *British Actuarial Journal*, vol 30, e6.

Beazley Security (2026): *Quarterly Threat Report: First Quarter, 2026*, May.

Beazley, Gallagher Re and Munich Re (2024): *Cyber realistic disaster scenario development and modelling*, Whitepaper, October.

Bermuda Monetary Authority (BMA) (2025a): *2025 capital and solvency return – stress/scenario analysis – class 4, class 3b and insurance groups*, December.

——— (2025b): *Bermuda Cyber Underwriting Report 2025*, December.

Bolton, C (2026): "Average cyber insurance cost (2026 report)", *MoneyGeek*, March, updated 12 May.

Bowman, M (2026): "Artificial intelligence in the financial system", speech at the Financial Stability Oversight Council Artificial Intelligence series roundtable on "Cybersecurity and risk management", Board of Governors of the Federal Reserve System, Washington DC, 1 May.

Chainanalysis (2026): "Total ransomware payments stagnate for second consecutive year, while attacks escalate", 26 February.

Chubb (2022): "Chubb addresses growing cyber risks with a flexible and sustainable approach".

——— (2024): *A better way to define and insure systemic cyber events*, April.

——— (2026): *2026 Cyber Claims Report*.

Coalition (2026): *2026 Cyber Claims Report*, March. Cremer, C, B Sheehan, M Mullins, M Fortmann, S Materne and F Murphy (2024): "Enhancing cyber insurance strategies: exploring reinsurance and alternative risk transfer approaches", *Journal of Cybersecurity*, vol 10, no 1, tyae027.

CrowdStrike (2026): *2026 Global Threat Report – Year of the Evasive Adversary*, February.

CyberCube (2026): "CyberCube identifies 12% of critical US firms at highest risk form Iran cyber threats", 4 March.

CyberCube and Munich Re (2025): "Key insights into systemic cyber risk: findings from CyberCube and Munich Re's joint expert survey", 15 July.

Dacorogna, M and M Kratz (2023): "Managing cyber risk, a science in the making", *Scandinavian Actuarial Journal,* vol 2023, no 10, 1000–1021.

Doerr, S, L Gambacorta, T Leach, B Legros and D Whyte (BIS) (2022): "Cyber risk in central banking", *BIS Working Papers*, no 1039, September.

Eling, M and J Wirfs (2016): "Cyber risk: too big to insure? Risk transfer options for a mercurial risk class", University of St. Gallen, Institute of Insurance Economics, March.

European Central Bank (2026): "Market fragmentation is bank's real constraint", Interview with Frank Elderson, 13 May.

European Insurance and Occupational Pensions Authority (EIOPA) (2022): *Supervisory statement on management of non-affirmative cyber exposures*, August.

European Union Agency for Cybersecurity (ENISA) (2024): *Cyber insurance – models and methods and the use of AI*, February.

——— (2025): *ENISA Threat Landscape 2025*, October.

Federal Financial Supervisory Authority (2026): "Introductory remarks by President Mark Branson at Bafin's annual press conference", Frankfurt, 12 May.

Federal Office for Information Security (2014): *The state of IT security in Germany 2014*, November.

Federation of European Risk Management Associations (FERMA), Marsh and Howden (2025): *Demystifying cyber insurance: today's trends and tomorrow's challenges*, October.

Financial Services Agency (FSA) (2026): "Press Conference by KATAYAMA Satsuki, Minister of Finance and Minister of State for Financial Services", 24 April.

Financial Stability Board (FSB) (2023): *Cyber Lexicon: updated in 2023*, April.

——— (2025): *Format for incident reporting exchange (FIRE): final report*, April.

Finnish Government (2021): "Administrative fine imposed on psychotherapy centre Vastaamo for data protection violations", December.Gallagher Re (2024): *A history of near misses: utilising counterfactual analysis to understand cyber risk*, April.

Garlick, B (2026): "How deepfakes are reshaping cyber insurance, and exposing policy blind spots", *Insurance Business*, 11 February.

Geneva Association (2018): *Cyber insurance as a risk mitigation strategy*, April.

——— (2023): *Cyber risk accumulation: fully tackling the insurability challenge*, November.

——— (2025): *Gen AI risks for businesses: exploring the role for insurance*, October.

——— (2026a): *Addressing growing protection gaps through better public-private insurance programmes*, February.

——— (2026b): *Strengthening cyber resilience through insurance*, March.

Global Federation of Insurance Associations (GFIA) (2023): *Global protection gaps and recommendations for bridging them: Report extract: cyber protection gap*, March.

Glover, T (2025): "Marquis cyber breach exposes 'fourth-party' danger", *The Banker*, 30 December.

Guy Carpenter (2023): *Under the lens: investigating cyber vendor model divergence*, June.

Herath, H and T Herath (2011): "Copula based actuarial model for pricing cyber-insurance policies", *Insurance Markets and Companies: Analyses and Actuarial Computations, Forthcoming*, February.

Hervé-Mignucci, M (2023): "The art (and peril) of modeling catastrophic cyber risk", *Coalition*, 21 June.

House of Commons (2026): *Artificial intelligence in financial services*, Treasury Committee, Fifteenth report of session 2024–26, January.

International Association of Insurance Supervisors (IAIS) (2020): *Cyber risk underwriting: identified challenges and supervisory considerations for sustainable market development*, December.

——— (2023a): *A call to action: the role of insurance supervisors in addressing natural catastrophe protection gaps*, December.

——— (2023b): *Global Insurance Market Report (GIMAR): special topic edition cyber*, April.

——— (2025): *Global Insurance Market Report (GIMAR)*, December.

——— (2026): *Application paper on operational resilience objectives and toolkit*, February.

International Business Machines (IBM) (2025): *Cost of a Data Breach Report 2025*, August.

——— (2026): *X-Force Threat Intelligence Index 2026*, April.

International Monetary Fund (2024): *Global Financial Stability Report*: *The Last Mile: Financial Vulnerabilities and Risks*, April.

Jang, J and R Oh (2020): "A bivariate compound dynamic contagion process for cyber insurance", SSRN, June.

Jones, C (2025): "German phone repair biz collapses following 2023 ransomware attack", *The Register*, 4 August.

Koh, T Y and J Prenio (2023): "Managing cloud risk – some considerations for the oversight of critical cloud service providers in the financial sector", *FSI Insights on policy implementation*, no 53, November.

Lloyd's (2019): "Providing clarity for Lloyd's customers on coverage for cyber exposures", *Market bulletin*, ref Y5258, July.

——— (2024): "State backed cyber attack wordings", *Market bulletin*, ref Y5381, May.

——— (2026): "Realistic Disaster Scenarios (RDS) 2026 Scenario Specification", January.

Lloyd's and the University of Cambridge Centre for Risk Studies (2015): *Business blackout: the insurance implications of a cyber attack on the US power grid*, *Emerging Risk Report*, May.

Lloyd's Market Association (LMA) 2026: *Understanding AI exposures: AI loss scenarios survey results*.

Marsh (2017): "Interaction of coverage under financial lines policies".

——— (2018): *By the numbers: global cyber risk perception survey*, February.

MarshMcLennan and Zurich Insurance (2024): *Closing the cyber risk protection gap*, August.

Motta, J (2026): "After Mythos: what actually changes for cyber risk", *Coalition*, 23 April.

Munich Re (2020): "Contingent business interruptions due to cyber events: a challenging cyber insurance cover component", 14 April.

——— (2024): *Munich Re global cyber risk and insurance survey 2024: bridging the gap in cyber protection*, April.

——— (2025a): "Cyber insurance: risks and trends 2025", 3 April.

——— (2025b): "From gap to gains: protection gap in cyber insurance", 29 September.

——— (2025c): "Physical damage from cyberattacks: an underestimated risk in the age of automation and digitalisation", 15 October.

——— (2026): "Cyber insurance: Risks and trends 2026", 25 March.

Munich Re and Hartford Steam Boiler Inspection and Insurance Company (HSB) (2024): "Mind the gap: a US-focused analysis of AI liability risks and the implications for insurance", Whitepaper.

Murdoch, S and Y Nagi (2026): "Asia regulators monitor Anthropic's Mythos for potential banking risks", *Reuters*, 20 April.

Natarajan, N (2023): "Cybersecurity insurance and data analysis working group re-envisioned to help drive down cyber risk", *Cybersecurity and Infrastructure Security Agency*, 20 November.

National Association of Insurance Commissioners (NAIC) (2025): *Report on the cybersecurity insurance market*, November.

National Cyber Security Centre (NCSC) (2020): "Cyber insurance guidance", August.

——— (2026): "Why cyber defenders need to be ready for frontier AI", March.

Newman, L (2026): "Mozilla used Anthropic's Mythos to find and fix 271 bugs in Firefox", *Wired*, 21 April.

New York Department of Financial Services (NYDFS) (2021): "Insurance Circular Letter No. 2 (2021)", 4 February.

OpenAI (2026): "Scaling trusted access for cyber with GPT-5.5 and GPT-5.5-Cyber", 7 May.

Organisation for Economic Co-operation and Development (OECD) (2020): *Encouraging clarity in cyber insurance coverage: the role of public policy and regulation*, February.

——— (2021): *Enhancing financial protection against catastrophe risks: the role of catastrophe risk insurance programmes*, October.

Pollard, J, A Mellen, J Burn J Blankenship and C Scott (2026): "Project Glasswing: the 10 consequences nobody's writing about yet", *Forrester* 10 April.

Securities and Exchange Commission (SEC) (2025): "Cybersecurity risk management, strategy, governance, and incident disclosure", May.

Semperis (2025): *2025 ransomware risk report*, July.

Societies of Actuaries (SOA) (2017): *Cybersecurity insurance: modeling and pricing*, March.

South African Reserve Bank (2026): "Prudential Authority communication to the financial sector: preparing for frontier AI and AI-accelerated cyber risk", April.

Standard & Poor's Global (S&P Global) (2024): *Cyber insurance market outlook 2025: cycle management will be key to sustaining profits*, November.

Stewart, H (2025): "UK economy grew by just 0.1% in third quarter after hit from JLR cyber-attack", *The Guardian*, 13 November.

Swiss Re (2022): "Cyber insurance: strengthening resilience for the digital transformation", 7 November.

——— (2025): "Shifting cyber insurance growth into the next gear", 3 September.

Total Assure (2025): "Cyber attack statistics by year: 2020–2025 data reveals unprecedented growth in global threats", 21 October.

Tsohou, A, V Diamantopoulou, S Gritzalis and C Lambrinoudakis (2023): "Cyber insurance: state of the art, trends and future directions", *International Journal of Information Security*, vol 22, 737–748.

UK Department for Science, Innovation and Technology and GrantThornton (2025): *Insuring resilience: adoption of cyber insurance by UK small and medium sized enterprises*, April.

US Department of the Treasury (2023): *The financial services sector's adoption of cloud services*.

UK Government (GOV.UK) (2025): "Consultation outcome: Government response to ransomware legislative proposals: reducing payments to cyber criminals and increasing incident reporting (accessible)", 22 July.

US Securities and Exchange Commission (SEC) (2025): "Cybersecurity risk management, strategy, governance, and incident disclosure", May.

Vaziri, A (2023): "One cyber incident away from insolvency", *Lewis Silkin*, 28 September.

Vergara Cobos, E and S Cakir (2024): "A review of the economist costs of cyber incidents", World Bank Group, working paper.

World Economic Forum (WEF) (2026): *Global cybersecurity outlook 2026: Insight report*, January.

WTW (2024): *The terrorism pool index 2024*, April.

Annex 1: Selected list of malicious and non-malicious cyber incidents

List of malicious and non-malicious cyber incidents — Table A.1

Nature	Victims	Date	Description	Consequences
Malicious	Drift Protocol	April 2026	A major decentralised finance derivatives platform built on the Solana blockchain was compromised following a sophisticated cyber intrusion targeting its smart-contact infrastructure.	About $265 millions in digital assets were illicitly transferred out of the platform. The incident triggered a rapid loss of confidence, with the platform's total value locked falling from around $550 million to under $300 million within an hour.
Malicious	Mexican government agencies	February 2026	A single hacker exploited commercial AI coding agents (Anthropic's Claude Code and OpenAI's GPT-4.1) to breach nine Mexican government agencies. It is estimated that 75% of the remote hack activity was generated and executed by Claude Code AI agent.	The breach led to the exfiltration of more than 150 GB of sensitive data. Compromised information reportedly included civil registry, government employee credentials, tax and voter records, potentially exposing data relating to up to 195 million individuals.
Non-malicious	Amazon Web Services (AWS)	October 2025	A major outage in AWS' US-EAST-1 region, triggered by a technical failure in its internal network, disrupted thousands of websites, financial services platforms and applications globally.	The incident affected around 70,000 organisations worldwide. Insured losses are estimated between $38 million and $581 million. Losses for US companies alone are estimated to be between $500 million and $650 million.
Malicious	Collins Aerospace	September 2025	A ransomware attack on Collins Aerospace disrupted airport check-in and baggage-drop services across Europe.	Within the first 48 hours, 37 departures and 33 arrivals were cancelled across the major affected airports. The total industry impact is estimated at potentially exceeding EUR 150 million.
Malicious	Jaguar Land Rover	August 2025	Jaguar Land-Rover suffered a cyber-incident that forced a shutdown of its UK manufacturing and IT systems, halting production across its major UK factories and triggering major disruptions in its supply chain.	The attack is estimated to have cost the UK economy around USD 2.5 billion and even dragged down the quarterly UK GDP growth figures. Production across UK factories was stopped during five weeks and affected an estimated 5,000 businesses.
Non-malicious	CrowdStrike	July 2024	A faulty software update from CrowdStrike's Falcon security platform caused a global IT outage, crashing approximately 8.5 million Windows systems and disrupting critical services worldwide.	The outage affected airlines, hospitals, banks and retailers globally, with Fortune 500 companies alone facing estimated losses of around USD 5.4 billion. The incident is widely described as one of the largest IT outages in history.
Malicious	Change Healthcare	February 2024	Change Healthcare, a major provider of health-data services in the US, was hit by a ransomware attack with intruders disrupting operations and stealing personal	Nation-wide healthcare providers faced cash-flows problems because claims processing was blocked. Pharmacies and hospitals experienced disruption to

			information of over 190 million people.	prescriptions, billing and discharges. Costs are estimated to USD 2.47 billion, with a USD 22 million ransom reportedly paid to the attackers.
Malicious	Arup	January 2024	Fraudsters used AI-generated deepfake video and voice to impersonate Arup's UK CFO and colleagues on a live call, instructing a Hong Kong finance employee to make "confidential" transfers.	Arup lost USD 25.6 million across 15 transfers before the fraud was detected. No internal IT systems were breached, but the case has become a reference point for deepfake fraud risk.
Malicious	SolarWinds	2020	The software vendor SolarWinds was compromised via its Orion update mechanism, enabling attackers to infiltrate thousands of organisations, including US government agencies, via a poisoned software update.	Many clients and agencies had to assume they were breached, triggering investigations, remedial work, software replacements and reputational damage. The supply-chain amplified risks across sectors. SolarWinds reported direct costs of at least approximately USD 18 million. Insured losses for others have been estimated at around USD 90 million. SolarWinds agreed to a USD 26 million settlements with shareholders over a securities class action.
Malicious	Capital One	March 2019	A hacker exploited a misconfigured firewall to access sensitive data from over 100 million Capital One customers. The breach affected around 100 million people in the US and about 6 million people in Canada.	The company expects to incur between USD 100 and 150 million in costs related to the hack (including customer notifications, credit monitoring, tech costs and legal support due to the hack). In 2020, Capital One was fined USD 80 million by the Office of the Comptroller of the Currency.
Malicious	NotPetya	2017	What began as a malware outbreak targeting Ukraine quickly morphed into a global destructive event: NotPetya spread rapidly across corporate networks in many countries, triggering widespread systems failure (rather than classical ransomware).	Massive disruptions to logistics, manufacturing and supply-chains: Maersk's global shipping operations were halted; firms had to rebuild and restore entire IT estates. One estimate places the global damage at over USD 10 billion, of which USD 3 billion has been covered by the insurance sector to date (both affirmatively and non-affirmatively). For example, Maersk lost approximately USD 250–300 million and chemical firm Merck reported USD 870 million losses to shareholders.

Source: FSI-IAIS staff.

Annex 2: Types of data used for cyber insurance underwriting

Table A.2 provides a non-exhaustive list of data typically used for cyber insurance underwriting.

Types of data used for cyber insurance underwriting — Table A.2

Data type	Description	Example
Firmographic data	General characteristics of a firm and its business operations	Industry sector, annual revenue, number of employees, geographical footprint
Technographic data	The IT environment and digital infrastructure of a firm, including dependency/supply-chain data	Software platforms, cloud providers, operating systems, network architecture
Cyber security controls	Risk management controls in place to address cyber risk	Multifactor authentication, patch management, backup procedures, employee training, incident response capabilities
Exposure data	Data that show potential financial consequence of cyber incidents	Value of digital assets, data volumes held
External data	Historical claims data and threat intelligence	Historical cyber incidence and claims data, emerging malware or ransomware campaigns

Sources: FSI-IAIS staff.

Annex 3: Selected supervisory reactions to Mythos

Table A.3 provides a non-exhaustive list of responses by financial authorities to Anthropic's Claude Mythos Preview.

Reactions from financial authorities in response to Anthropic's Claude Mythos Preview

Table A.3

Jurisdiction	Authority	Response
Australia	Australian Prudential Regulation Authority	Issued an industry letter on AI that included a warning that AI models such as Mythos can enhance discovery of vulnerabilities by bad actors and are expected to further increase the probability, speed and scale of cyber attacks.[1] Engaging the financial sector on the potential for increased cyber threats from high capability AI frontier models such as Anthropic Mythos. Pointed regulated entities to the Australian Signals Directorate's advice on frontier models.[2]
European Union	European Central Bank	Requested banks to increase efforts to identify cyber vulnerabilities, even minor ones, using existing AI tools and to update their operational resilience plans to cater for greater likelihood of severe disruptions. Engaging with other authorities and the financial industry to have a good overview of the cyber security situation across the banking system.[3]
Germany	Federal Financial Supervisory Authority	Creating a new supervisory division to carry out targeted inspections, such as "IT spotlight" inspections, that take far less time than fully fledged reviews to respond more effectively to current developments and incidents. Called for supervised entities to accelerate patching process.[4]
Hong Kong SAR	Monetary Authority	Forming a public-private sector taskforce to examine, monitor and respond to AI-driven cyber risk. Will introduce a cyber resilience testing framework to augment banks' response and recovery capabilities.[5]
Japan	Financial Services Agency	Together with the Ministry of Finance and Bank of Japan, convened a public-private liaison meeting to strengthen cybersecurity measures in the financial sector against AI-related threats. Called for acceleration of patching processes and strengthened preparedness for cyber incidents.[6]
South Africa	South Africa Reserve Bank	Issued an industry communication specific on frontier AI and AI-accelerated cyber risk, setting out expectations around cyber risk management including the need for continuous monitoring and the role of boards and senior management.[7]
Spain	Bank of Spain	Called for banks to bolster quality control in the development and deployment of new software solutions and to enhance responsiveness to vulnerabilities. Highlighted importance of international coordination to bolster global resilience.[8]
United Kingdom	Bank of England, Financial Conduct Authority and HM Treasury	Called for firms to take actions across domains (such as governance and strategy, identification and risk management of vulnerabilities) managing risks from third parties, access, network and data protection, and response and recovery.[9]
United States	Board of Governors of the Federal Reserve System	Called for supervisors to continue staying abreast of developments and to coordinate efforts across government; engage in regular communication with banks of all sizes; and review regulatory approaches, taking into account industry feedback.[10]

[1] See Australian Prudential Regulation Authority, "APRA letter industry on artificial intelligence (AI)", 30 April 2026.

[2] See Australian Signals Directorate and Australian Cyber Security Centre, *Frontier models and their impact on cyber security*, April 2026.

[3] See European Central Bank, "Market fragmentation is bank's real constraint", Interview with Frank Elderson, 13 May 2026.

[4] See Federal Financial Supervisory Authority, "Introductory remarks by President Mark Branson at Bafin's annual press conference", Frankfurt, 12 May 2026.

[5] See S Murdoch and Y Nagi, "Asia regulators monitor Anthropic's Mythos for potential banking risks", *Reuters*, 20 April 2026.

[6] See Financial Services Agency, "Press Conference by KATAYAMA Satsuki, Minister of Finance and Minister of State for Financial Services", 24 April 2026.

[7] See South African Reserve Bank, "Prudential Authority communication to the financial sector: preparing for frontier AI and AI-accelerated cyber risk", April 2026.

[8] See Bank of Spain, *Financial Stability Report Spring 2026*, May 2026.

[9] See Bank of England, "The Bank, FCA and HM Treasury joint statement on Frontier AI models and cyber resilience", 15 May 2026.

[10] Bowman, M, "Artificial intelligence in the financial system", speech at the Financial Stability Oversight Council Artificial Intelligence series roundtable on "Cybersecurity and risk management", Board of Governors of the Federal Reserve System, Washington DC, 1 May 2026.

Sources: FSI-IAIS staff.