Swiss Re Institute

November 2022

Cyber insurance: strengthening resilience for the digital transformation

Executive summary

Cyber risks have risen with geopolitical and economic instability, and with society's increased reliance on digital technologies.

The world of today is one of increasing geopolitical and economic instability. This has many drivers, most prominently the war in Ukraine and simmering tensions between the US and China. With many facets of life going increasingly digital contemporaneously, the spectre of cyberattacks looms large. The prospect of a state-sponsored or private attack on another country/region with catastrophic fallout is very real. It could take the form of an attack on infrastructure facilities such as power grids or key communication systems, among others. The resulting losses from a systemic cyber event could be very large, impacting companies, the broader economy and society at large.

The cyber risk landscape is evolving fast and the associated attack threats are becoming ever more sophisticated.

So far there has not been such a systemic incident. Nevertheless, the cyber risk landscape is evolving fast, with ransomware incidents and cybersecurity worries from businesses and governments at an all time high. McAfee estimates global monetary losses from cyber crime in 2020 at around USD 945 billion. Attacks have become more sophisticated. Hackers now use "triple extortion" techniques, and ransomware-as-a-service has lowered entry barriers to rogue actors. Small and medium-sized enterprises (SME) with little defence capacity have become easy targets for cyber criminals, while digitalisation of industries including the healthcare and critical infrastructure sectors, has increased vulnerabilities across entire supply chains.

Risk management efforts have increased in response, with insurance playing a key role and the market growing quickly...

Before the NotPetya attack of 2017, cyber risks centred around data breaches and third-party liability. For re/insurers, the proliferation of data privacy regulations opens the door to litigation procedures and increases long-tail risk exposures. In the last two years, first-party claims have become dominant, with ransomware incidents from organised crime shifting damages to core business. Firms, insurers and public authorities have redoubled risk management efforts, and industry associations and insurers have worked together to address the related issue of "silent cyber" by clarifying the scope of traditional policies. Insurance plays a key role, providing not just for risk transfer but incentivising risk mitigation, supporting monitoring and aiding responses to cyberattacks.

... but the market remains small compared to economic losses.

But the cyber protection gap remains large, with premiums amounting to just a fraction of total losses from cyberattacks. Most firms are uninsured or significantly under-insured for cyber risks. In a recent survey, only 55% of businesses reported having cyber cover and less than one in five have cover limits above the median ransomware demand. We estimate that the total claim arising from a cyber-incident targeting an SME is in relative terms three times more than for large corporations, with forensic costs typically ranging from USD 20 000 to USD 100 000 for a firm with turnover of less than USD 50 million.

Insurers have addressed the surge in ransomware losses and must now deal with catastrophic events.

The surge in ransomware attacks drove loss ratios higher in 2020. Insurers responded by increasing prices, improving underwriting discipline, introducing sub-limits and coinsurance, clarifying terms and conditions, and excluding – or explicitly pricing for – cyber exposures in other property and liability policies. These actions had a degree of success: loss ratios plateaued in 2021.

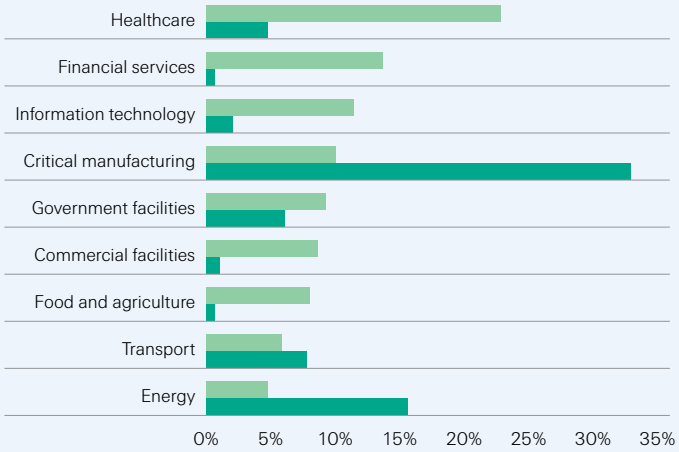
Cyber risk does not meet all the characteristics of insurability, limiting the potential growth of the market.

Some of today's cyber risks do not fully meet the typical characteristics of insurability. Most notably, the aggregation of losses could quickly and significantly impair diversification and/or challenge market capacity. The risk is hard to quantify because of immature data and a lack of model consensus. Limited insurability restrains capacity despite growing demand, creating challenges for market growth in the longer term. To address these limitations, more cyber talent, standardised data, better modelling, greater contract consistency and new sources of capital are needed. Likewise, there is scope to consider opportunities for new types of public-private risk sharing mechanisms. These measures can help mitigate overall exposures, improve risk understanding and help make society more resilient to attacks with devastating and potentially systemic consequences. The human and networked nature of cyber means the risk will continually evolve and require a coordinated response. Enhancing resilience will require collaboration between corporations, insurers and governments.

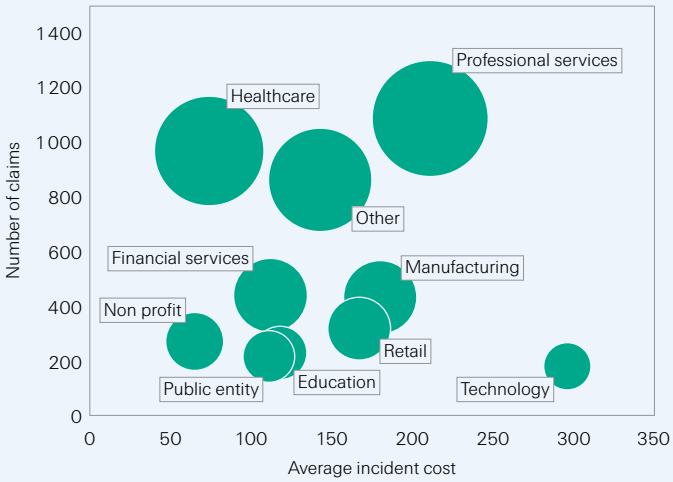
Key takeaways

The digital shift accelerated by COVID-19 has created new cyber vulnerabilities

Reported ransomware incidents and their severity have skyrocketed in recent years, with monetary estimates of global 2020 cyberattack losses at around USD 945 billion. The types of attacks and targeted sectors have also evolved. Cyber criminals have small and medium enterprises on their radar, particularly in the healthcare, professional and financial services sectors. Digitalisation of industries, including the healthcare and critical infrastructure sectors have increased cyber-vulnerabilities across entire supply chains.



Percentage of ransomware attacks per critical infrastructure sectors reported in the US

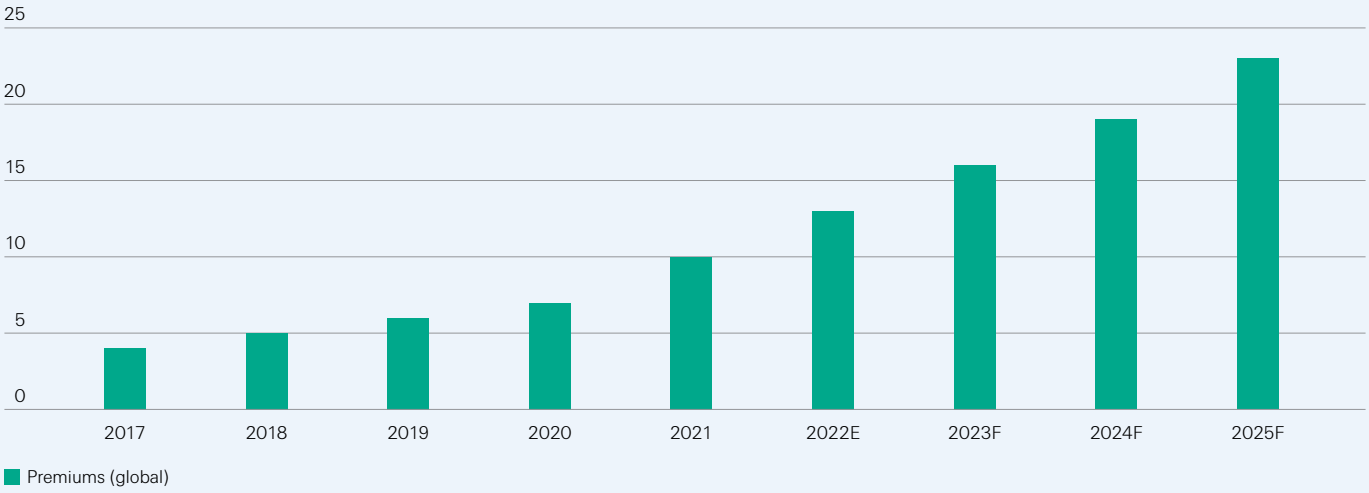


Source: (Left) *DHS NCCIC/ICS-CERT Year in Review*, Department of Homeland Security, 2015; *Internet Crime Complaint Center* Federal Bureau of Investigation, Swiss Re Institute estimates; (Right) *Cyber claims study report*, NetDiligence, 2021; Swiss Re Institute estimates

[A] Source: Computer security firm McAfee *(The Hidden Costs of Cybercrime (mcafee.com).*

Meanwhile, the cyber insurance market has been growing fast

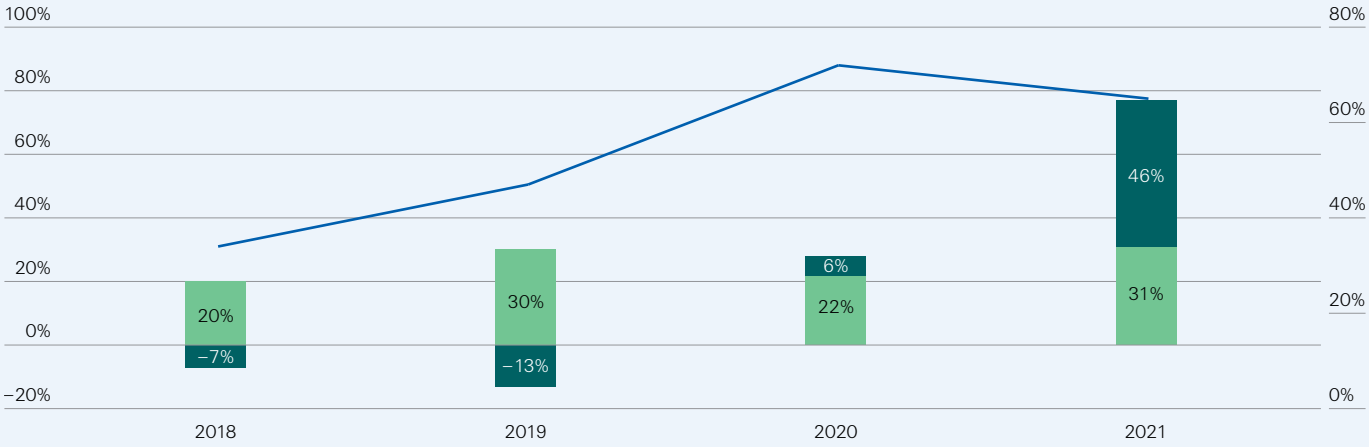
Risk management efforts and cyber insurance premiums have expanded in response to the surge in incidents, with USD 10 billion premiums written globally in 2021. Cyber risks originally centred around data breaches and third-party liability, but ransomware attacks have shifted damages to the core business and first-party liabilities. We expect premiums to grow to USD 23 billion by 2025 but even so, the market remains small relative to a fast-evolving risk.



Note: E = estimates, F = forecasts. Swiss Re estimates/forecasts comprise standalone and packaged cyber policies
Source: Swiss Re Institute

Cyber insurance profitability deteriorated as ransomware attacks skyrocketed and stabilised as underwriting actions took effect

Loss ratios for US standalone cyber insurance policies spiked in 2020 before improving slightly in 2021 as a result of price increases, stricter underwriting standards such as requirements for multi-factor authentication, and tighter terms and conditions including sub-limits and coinsurance. But they remain elevated, especially considering the necessary catastrophe load for a potentially systemic loss.



Source: National Association of Insurance Commissioners, S&P Global, Swiss Re Institute calculations

Undiversifiable aggregation risk and the fast-changing nature of cyber bring increased uncertainty, and a call for new solutions

These solutions include coordinated industry efforts to standardise data and policy languages. Improved modeling capacity (both scenario-driven and data analytics-based) and upgraded cyber skills would help address quantification shortcomings. Altogether, this would help reduce uncertainty, lay the foundation to attract new sources of capital and thereby activate a market for cyber insurance-linked securities (ILS).

	Insurability Criteria		Current state	Changes to improve insurability
Actuarial criteria	Frequency and severity of risk need to be reasonably quantifiable		Evolving risk; historical data limited Victims of cyber attacks, governments, security firms etc may withhold details for security purposes Wilful act, nature of attacks is continuously changing to escape analysis and mitigation Models remain in their infancy	Initiatives to create collective (pooled) data bases, improve standardization for modeling and analysis, and clear definitions of what constitutes a cyberattack (Recommendation 1)
	Independence of loss occurrences		Coordinated attacks can cause losses to be correlated; large-scale attacks can affect multiple lines of business	Cyber is fundamentally a human risk, but clarity of intent around state-backed acts of war and other exclusions, such as the actions described earlier can help
	Maximum loss needs to be manageable within industry capacity		Catastrophic loss potential hampers diversification	Separate catastrophic risk from cover for attritional losses
	Mutuality: moderate average loss amounts per event and a sufficiently high number of similar loss events per annum		The basis of the cyber insurance market is well established	Increase insurance take-up rate across sectors and firm sizes. Separate catastrophic risk from attritional losses
	No excessive information asymmetry problems (i.e. moral hazard, adverse selection)		Experience and standards regarding data sharing and mitigation are evolving	Coinsurance, mitigation standards, data sharing, crisis management resources
Market criteria	Insurance premium needs to be risk-adequate for a sustainable insurance market		Strong increase in insured losses, loss ratios in recent years	Improve modeling for risk-adequate pricing; separate catastrophic risk from attritional losses
	Sufficient industry capacity		Sufficient capacity to support strong growth in attritional market; not sufficient capacity to fully insure catastrophic risks	Clarity around what constitutes a catastrophe can attract re/insurer capacity (Recommendation 2)

Source: C. Biener, M. Eling, J.H Wirfs, *Insurability of Cyber Risk – An Empirical Analysis*, University of St. Gallen, 2015; C. Christophe, P. Liedtke, "Insurability, its limits and extensions", Insurance Research and Practice, vol 18 (2), 2002; B. Berliner, *Limits of Insurability of Risks*, 1985

Cyber risk landscape

Cyber incidents: getting more severe and sophisticated

As digital footprints deepen, exposures to cyber risks increase.

The digital shift accelerated by the pandemic is anticipated to change how society functions over the coming decades: the way we work, do business, consume, educate our children, manage and source energy, entertain and seek medical support. But as digitalisation proliferates, so too do exposures to cyber-threats. The pace of technological change, the rising awareness of cyber risk and the adoption of cyber hygiene practices to keep data and networks secure, are not synchronised. Rather, it seems as if a legacy of outdated security protocols, IT systems and regulatory frameworks are only slowly catching up with technological realities. This opens the door to rogue actors seeking to exploit digital vulnerabilities for financial, reputational or geopolitical gain.

Cyber threats are increasing in scope and frequency. Ransomware is the predominant risk for business.

The scope and frequency of cyberattacks are increasing, and today ransomware is seen as the predominant risk for businesses. In 2022, cyber incidents top Allianz's risk barometer for the first time, ahead of business interruption and natural catastrophes risks.[1] Computer security firm McAfee estimated the total annual cost of cybercrime at USD 945 billion in 2020,[2] two-thirds of which was attributable to intellectual property theft and financial crime, while the direct costs[3] associated with the four most common types of cyber-incidents in the US quadrupled to an average of USD 100 000 per incident since 2016.[4] Looking at ransomware alone, NetDiligence finds that 70% of ransom attacks conducted since 2017 have occurred in the last two years, with severity at an all-time high in 2021 (average ransom of USD 750 000, more than twice the 2020 figure).[5] In a recent survey of the world's top cyber leaders, 50% indicated that ransomware attacks on their organisation are among their greatest cyber risk concerns, followed by social-engineering attacks and malicious insider[6] activity (see Table 1).[7]

Ransomware attacks are becoming more sophisticated.

With the advance of technology, the sophistication of ransomware attacks has grown considerably. The emergence of cryptocurrencies has provided an easy, but hard-to-trace method of receiving payments from victims, while advances in artificial intelligence (AI) analytics is expanding both attack and defence capabilities.[8] Ransomware actors now employ up to three extortion techniques. They encrypt and extract a company's data against two separate ransoms – the first to unblock the firm's system and the second to not disclose the data (double extortion).[9] Hackers can then leverage the stolen data to extract a third ransom from its primary owner (triple extortion).[10] Sometimes hackers continue their attack until the company has fixed its security protocols (re-extortions).[11]

1 *Allianz Risk Barometer 2022*, Allianz Global Corporate & Specialty, January 2022.
2 Z. Smith, E. Lostri, *The Hidden Costs of Cybercrime*, McAfee, December 2020.
3 The direct cost does not include estimates of lost business, time, wages, files or equipment, or third-party remediation services used by the victim.
4 D. Garcia-Diaz, K. Walsh, *Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks*, Government Accountability Office, June 2022.
5 *Ransomware 2022 Spotlight Report*, NetDiligence, 2022.
6 A malicious insider is defined as an organisation's current or former employees, contractors or trusted business partners, who misuse their authorised access to critical assets in a manner that negatively affects the organisation.
7 In the report, cyber leaders are the senior-most executives from private and public sectors across 20 countries. See *Global Cybersecurity Outlook 2022*, World Economic Forum, January 2022.
8 K. Ramachandran, *Cybersecurity issues in the AI world – Using AI to address AI-driven cyber attacks*, Deloitte, September 2019.
9 If the victim does not pay the ransom, the attacker could leak the victim's data online on the dark web or use the stolen data to exploit vulnerabilities.
10 For example, this occurred at Finnish psychotherapy practice firm Vastaamo in 2020, when hackers stole the data, required a ransom from the firm and also emailed patients with the threat to expose their mental health records unless the victim paid a ransom of EUR 200 in bitcoins. See R. Sen, "Opinion: Hacking and data theft are mostly about making a buck not espionage", *Houston Chronicle*, May 2021.
11 For example, three distinct ransomware groups managed to breach German engineering conglomerate ThyssenKrupp's systems between August and December 2020. See "ThyssenKrupp suffers ransomware attack for the third time", *Security Report*, 1 February 2021.

Financial losses from data breach incidents are expanding beyond third-party risks to also impact core business.

The types of financial loss associated with these attacks have also evolved. Whereas traditional risks confronting businesses were concentrated around third-party data protection and privacy liability, in recent years claims have been largely dominated by ransomware attacks and there has been a shift towards the insured core business. Companies hit by a ransomware attack face several first-party loss elements such as the ransom itself, forensic and data restoration costs, and the business interruption (BI) suffered as a result of disruption to operations. Firms can also suffer reputational harm, undermining their relationship with customers[12] and also their market capitalisation.

Table 1
Description of selected malicious types of cyberattacks

Types	Definition
Ransomware	Ransomware is a type of malicious software ("malware") attack designed to block access to a computer system until a ransom is paid. This attack takes the form of a network intrusion (theft of credentials, installation of backdoors and malware, lateral movement through the network, exfiltration of data, ransom demand). Hackers often spend months spying on a compromised network to plan an attack and maximize their profits.
Malware	Malicious software which infects a computer and that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.
Distributed Denial of Service (DDoS)	In a DDoS attack, hackers attempt to take down a target network by flooding it with traffic from multiple sources (including internet calls) to a point that the system freezes and cannot function properly. The goal is often to sabotage web properties, damage brand reputations or prompt financial loss by making a website or network resource inaccessible.
Phishing	Phishing attacks occur when hackers exploit peoples' vulnerabilities by sending an email from a seemingly trusted source. By clicking on a link in the email and entering a password, the victim allows the hackers to get into the system, access data and/or send emails on their behalf. The term "spear-phishing" refers to cases where hackers take the time to research one intended target and approach the victim with a personally relevant message that appears legitimate and is more difficult to identify.
Social-engineering	Social-engineering is a method hackers use to exploit a person's trust in order to obtain money directly or obtain confidential information to enable a subsequent crime. This risk is often executed by tricking employees of a company into transferring funds to a fraudulent scammer on the other end.

Source: NetDiligence, Splunk, Swiss Re Institute

Cyber criminals are commercialising ransomware services.

Ransomware-as-a-service is becoming the business model of cyber-crime organisations. Increasingly, cyber-mercenaries are selling their hacking services to state and non-state actors. They are primarily motivated by financial gain and conduct their attacks on behalf of other actors, themselves motivated by monetary or geopolitical gains. For instance, the Italian mafia has reported the hiring of hackers to support its criminal activities.[13] Some of these cyber groups are highly technical and well-funded, developing novel attack tactics for their sponsors. The war in Ukraine has intensified the risk of seeing cyber tactics being adopted as a non-kinetic warfare response against allies supporting Ukraine and against economic sanctions.[14]

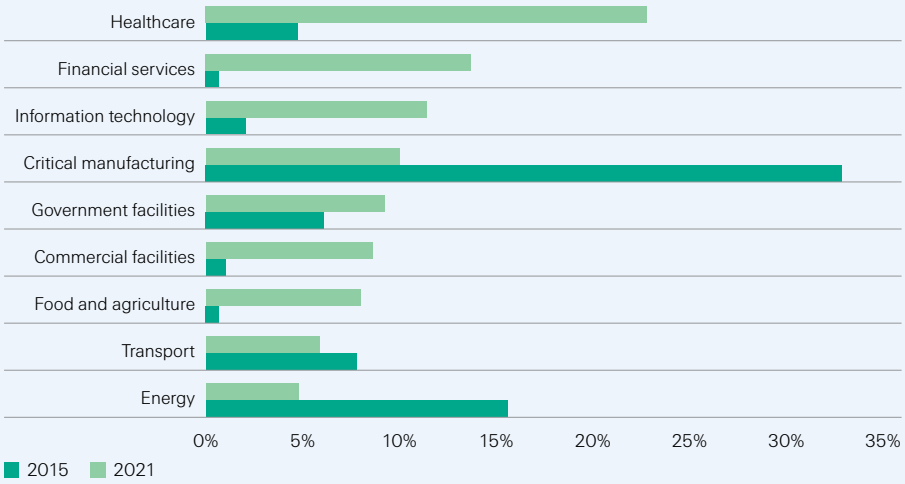
Cyber incidents by sector

With digitisation, all sectors are exposed to cyber threats.

As cyber criminals deploy new tactics that make it harder for organisations to protect themselves, the exposure to attacks has grown considerably across every aspect of the economy. Comparison of ransomware incidents targeting critical infrastructure sectors in 2015 and 2021 show that the number of attacks has jumped 120%, while their distribution has shifted toward the healthcare, financial services and IT sectors (see Figure 1).[15] Likewise, smaller entities are more exposed to cyber threats. In the aforementioned survey, 88% of respondents indicated that they are concerned about the cyber resilience of SME and the associated threat to supply chains.[16]

[12] According to Hiscox's Cyber Readiness Report 2022, 29% of US companies faced increased difficulty to attract new customers after an attack.
[13] How the Mafia Is Pivoting to Cybercrime" *vice.com*, 22 September 2021.
[14] *Pathways to Russian Escalation Against NATO from the Ukraine War.* Rand Corp, July 2022.
[15] In June 2021, the Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center started tracking reported ransomware incidents in which the victim was a member of a critical infrastructure sector. We compared this data with malware incidents reported to federal agencies in 2015. See *2015 NCCIC/ICS-CERT Year in Review,* Homeland Security, 2015 and *Internet Crime Report 2021*, FBI, 2021.
[16] *Global Cybersecurity Outlook 2022,* World Economic Forum, January 2022.

Figure 1
Ransomware attacks in critical infrastructure sectors reported in the US (percentages)



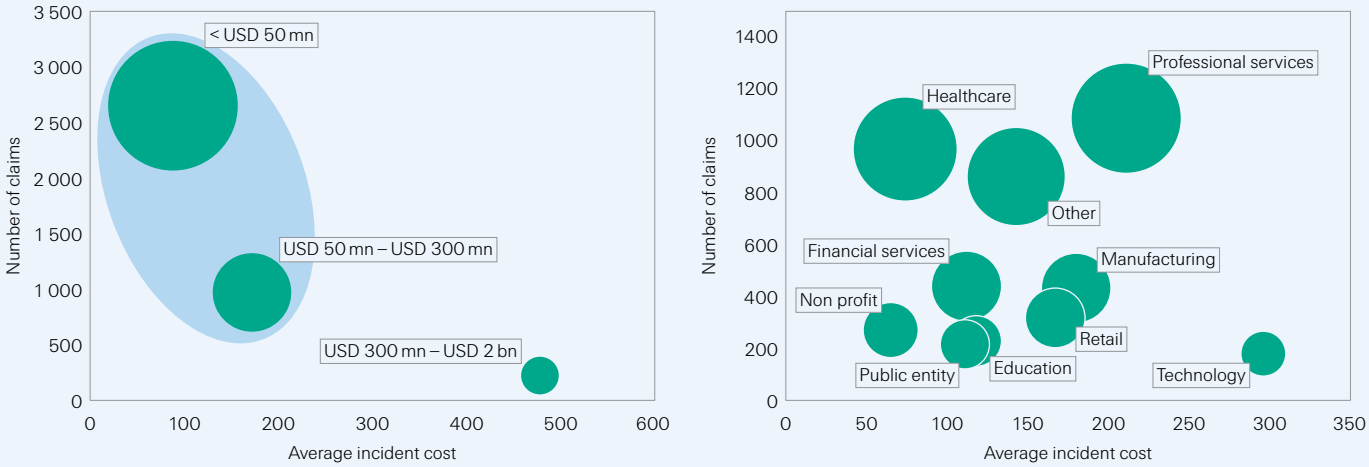
Source: *DHS NCCIC/ICS-CERT Year in Review,* Department of Homeland Security, 2015; *Internet Crime Complaint Center* Federal Bureau of Investigation, Swiss Re Institute estimates

SME are preferred targets for cyber criminals.

SME at risk: targets with limited resilience

Data show that firms with turnover below USD 300 million in the US, UK and Canada made the highest number of cyber-related insurance claims between 2016 to 2020 (Figure 2, left).[17] The attacks reported affected many sectors including predominantly healthcare, professional and financial services, manufacturing and retail (Figure 2, right).[18] The proliferation of entry points brought on by digital practices has increased cyber risk exposures. Prior to the pandemic, cyber security protocols were primarily implemented on premises at corporate locations, a model that has been altered with the surge of remote work, cloud solutions and online retailing. The business ecosystem is likewise changing, with real time collaborations through MS Teams and Zoom, while emails remain an open door for phishing attacks.

Figure 2
Left: SME: Number of cyber-related claims and average incident cost, per company turnover (2016–2020; USD thousands).
Right: SME: Cyber-related claims and average incident costs, per sector (2016–2020; USD thousands)



Source: *Cyber claims study report,* NetDiligence 2021; Swiss Re Institute estimates

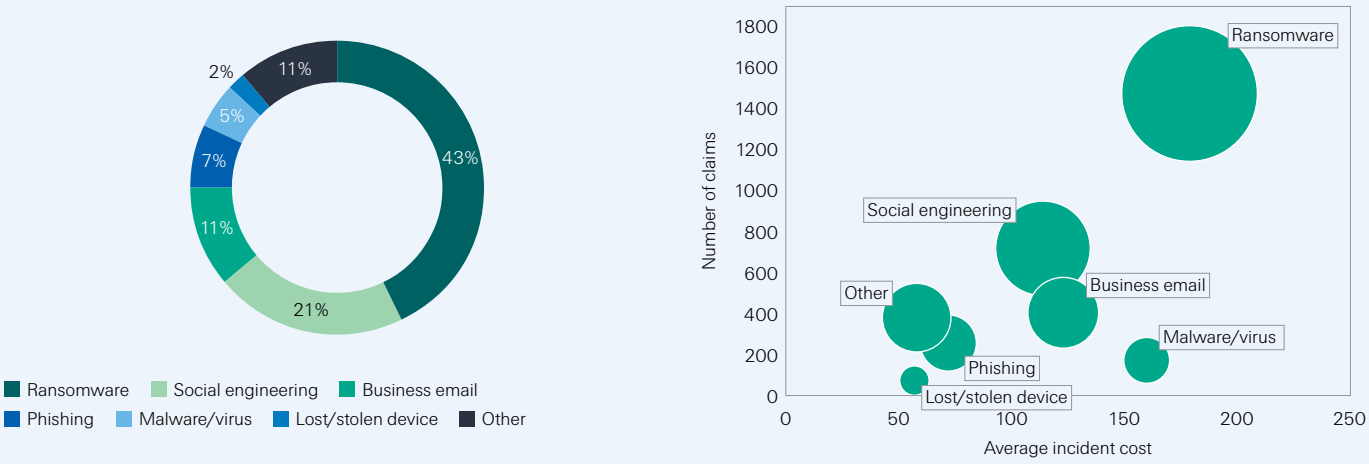
[17] *Cyber claims study 2021 Report,* NetDiligence, 2021.
[18] Ibid.

The average insurance claim of a cyber-incident is in relative terms three times larger for an SME than for larger firms...

Smaller companies with lower cyber-defence capacities have become easy targets for cyber criminals and their loss absorption is more limited than at larger corporations.[19] Analysis of claims data from 2016 to 2020 reveal that ransomware, social engineering and business emails tactics were employed in 3 out of 4 successful cyberattacks on SME (Figure 3, left), costing an average of USD 152 000 (Figure 3, right).[20] Once attacked, the financial resilience of a cyber-entrant is lower than that of a cyber-incumbent.[21] This is because a company without initial cyber capacity generally has little attack preparedness and incident response protocols in place. It will thus take longer for the threat to be detected and resolved and all the while, first-party losses rise. We assess that the total claims arising from a cyber incident suffered by a SME is in relative terms three times larger than that for bigger firms.[22]

Figure 3

Types of cyber-related attacks affecting SME (%, left); average cost of cyberattacks affecting SME (USD thousands, right)



Source: *Cyber claims study 2021 report, NetDiligence*, Swiss Re Institute estimates

... due to the considerable financial, administrative and legal burden for SME.

The financial, administrative and legal burden from a cyberattack targeting an SME is generally considerable. Forensic costs typically range from USD 20 000 to USD 100 000 for companies with turnover of less than USD 50 million,[23] while initial ransom amounts can reach up to USD 25 000 in 75% of cases.[24] If customer data is compromised, the company needs to comply with the notification requirements applicable in the jurisdiction(s) where the customer resides. Court proceedings by customers may also lead to financial compensation obligations. Meanwhile, the company incurs internal costs to get its operations back up and running, and to address the damages it has suffered from the attack (ie, restore systems and data, quantify BI losses, work with a public relations firm to communicate the breach and minimise reputation losses). Cyber policies typically cover most of these elements. They often also offer rapid incident management services that provide step-by-step guidance and swift

[19] Larger corporations with annual turnover above the upper USD 2 billion threshold used by NetDiligence in its classification of SME.

[20] NetDiligence, 2021, op. cit.

[21] We define a cyber-entrant as a firm new to operating online and/or setting up its IT security protocols.

[22] Under the assumption that SME have on average lower cyber defence capacity than larger corporations, we have inferred from NetDiligence's *Cyber claims study 2021 report* that the total cost of handling a cyber incident – including the incident cost and the crisis services cost (ie, breach coach counseling, forensic services, notification, credit/ID monitoring and public relations) – as a percent of annual revenue amounts to 0.33% for SME (average annual revenue of USD 84 million) and 0.11% for large firms (USD 11 billion).

[23] The level of cost will vary depending on how the insured chooses to respond to an incident, how modern the infrastructure was prior to the incident and the number of different/bespoke applications that are operated. For a turnover of USD 50 million to USD 300 million, forensic costs typically range between USD 100 000 –300 000. Over USD 300 million turnover, it ranges from USD 300 000–600 000. Source: Based on Baker Tilly's experience.

[24] Estimation over the period 2018–2020. See *From Kitchenware to Ransomware – A Short Story*, Swiss Re and CyberScout, 2020.

access to a network of specialised service providers along the incident management cycle to facilitate prompt and effective intervention.[25]

Stepping-up cyber-security takes time and resources but delaying this process threatens SME's operations.

Stepping-up cyber-security takes time and resources but delaying this process threatens SME's operations. Estimates found that half of small firms go out of business within six months of a cyberattack.[26] Cyber hygiene and digital capacity are the two main forces at play. First, digitalisation makes the risk landscape more complex, raising the cost of attaining the optimal level of cyber hygiene. In parallel, a company with lower initial cyber hygiene is likely to be less digitalised and therefore less competitive. The resilience of a company with low and stagnant digital capacity is thus threatened by two factors: 1) the loss of competitive advantage within a market environment that is going digital; and 2) the higher investment cost of building the optimal level of cyber hygiene. Both variables impact profitability by lowering revenues and increasing costs. When the profit nears zero, an SME may ultimately exit the market. A cyberattack can accelerate this process. Here insurers can help to bridge the cyber-defence gap for smaller companies by raising risk awareness, establishing cybersecurity requirements and incentivising continuous monitoring/adjustments to risks.

Healthcare data: digital ecosystems on the radar of cyber criminals

The healthcare services sector is becoming increasingly digital.

Healthcare is undergoing a digital shift. IoT devices can monitor patients' health, machine learning algorithms are bringing early-stage cancer detection to new levels, while wearable devices and Health & Wellness apps enable consumers to take an active role managing their health. Likewise, insurers are showing growing interest in leveraging this new health ecosystem for preventive diagnostics, early interventions, and to best tailor coverage to policyholders' needs. For instance, live data analysis possible through new wearable devices, can improve early detection of cardiovascular diseases.[27]

Healthcare digital ecosystems hold very large amounts of personal data.

The healthcare revolution is creating massive amounts of sensitive data. A study from Stanford University estimated that over 2300 exabytes of healthcare data would be produced yearly from 2020.[28, 29] The interconnected nature of this data – centralised in healthcare centres and decentralised in external private devices or insurers' databases – heightens the exposure of healthcare ecosystems to cyberattacks. Data breach incidents among healthcare stakeholders are a concern on account of patient privacy, but also for the continuous provision of healthcare services should they be suspended by a ransom encryption. A recent survey covering the US found that one in four cyber attacks over the previous 24 months resulted in increased mortality by delaying care.[30] Intertwining the financial costs of privacy and mortality litigations raises the bar for insurers grappling with data protection coverages in the healthcare sector.

There have been data breach incidents in the sector.

The number of data breach attacks in the healthcare sector is growing in line with other data-intense sectors with smaller structures emerging as the preferred targets of cyber criminals. In the US, 2021 was a record year for data breaches reported by healthcare entities (see Figure 4, left). As with SME generally, cyberattacks a greater impact on smaller healthcare entities with lower cyber capacities most. Last year, 75% of data breaches were reported by entities with under 30 000 affected individuals per attack. Conversely, the realisation of large data breaches was scarcer, with attacks affecting more than 1.5 million people accounting for less than 1% of the total (see Figure 4, right).

[25] First-party covers include business interruptions and data restoration and third party covers for privacy liability costs. Furthermore, these policies often come with service/assistance costs coverage for IT forensics, notification, crisis management and public relations..

[26] *The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses*, US Securities and Exchange Commission, 19 October 2015.

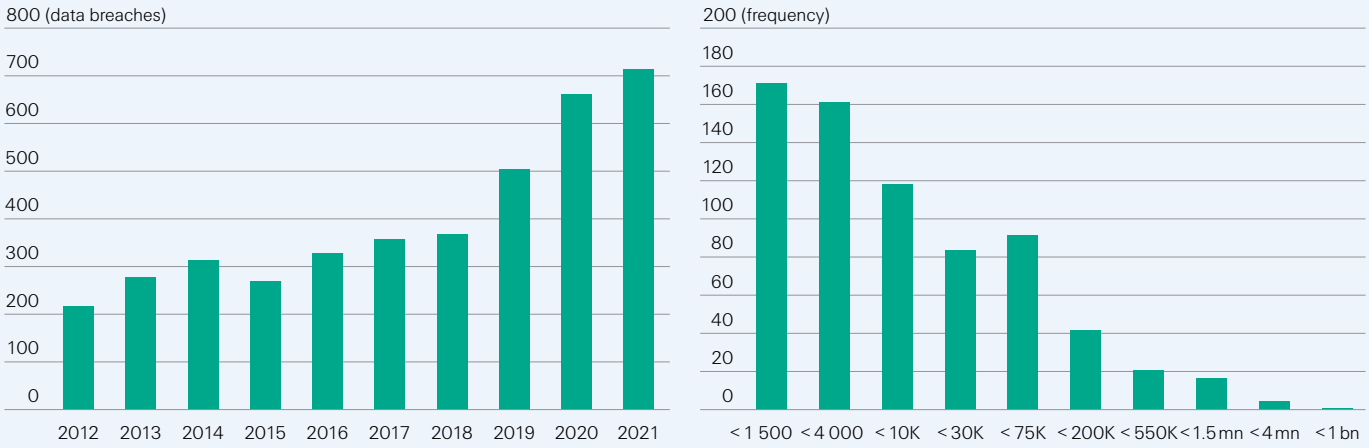
[27] *Healthcare Ecosystem – towards an integrated and seamless patient experience*, Swiss Re Institute, September 2019.

[28] "How Big Data Will Unlock the Potential of Healthcare", *visualcapitalist.com*, 26 July 2018.

[29] For comparison, the data information created every day on the internet in 2012 was estimated to be 1 exabyte. See "What is an exabyte?" *techtarget.com*.

[30] *The Insecurity of Connected Devices in Healthcare 2022*, Cynerio and Ponemon Institute, 2022.

Figure 4
US healthcare industry: number of reported data breaches (left); individuals affected per data breach event (logarithmic scale, right)



Source: US Department of Health & Human Services' data breach portal, Swiss Re Institute estimates

Critical infrastructure is the backbone of national economies.

Critical infrastructure: potential for systemic fallout

Major security breaches have highlighted the vulnerability of critical infrastructure to cyber threats,[31] a risk that is gaining scrutiny among policymakers and chief executives around the world. Should a cyberattack discontinue the provision of clean water, energy or internet services for an extended period of time, the consequences on the broader economy could be disastrous. When Colonial Pipeline in the US was hit by a ransomware attack in 2021, the company stopped its gas supply operations for six consecutive days, impacting downstream customers and consumers (see Appendix 1).[32] Recent geopolitical turmoil increases the potential for a large-scale attack on critical infrastructure. A recent survey finds that infrastructure breakdowns due to a cyberattack is the top personal cybersecurity concerns of cyber leaders, with 42% saying so.[33]

Given high digital interconnectivity, cyberattacks on critical infrastructure could lead to huge systemic losses.

Throughout the years, critical infrastructure has become reliant on operational and information technologies (OT/IT) that make them vulnerable to cyber threats. From renewable energy generation to water management systems and energy distribution networks, critical infrastructure is composed and operated through networks of industrial control systems and enterprise information technology systems. For instance, Singapore governs its water supply management and water quality system through AI analysis of real time data collected by IoT devices, themselves monitoring quality parameters and consumption patterns.[34] Further, the interconnected nature of critical infrastructure means the failure of one system is likely to impact others. With the digitalisation of operations and adoption of remote technologies, cyber targets have thus evolved beyond traditional IT systems, towards those OT used to manage entire industrial systems.[35] These are all new entry points for rogue actors seeking to disrupt critical assets.

[31] The US Critical Infrastructure Protection Act defines critical infrastructures as those physical or virtual systems and assets, so vital to the country that their incapacity or destruction would have a debilitating impact on security, national economic security, national public health or safety, or any combination of these. See *42 U.S. Code § 5195c – Critical infrastructures protection | U.S. Code | US Law | LII / Legal Information Institute*, Cornell Law School, 26 October 2001.
[32] "Cyberattack Forces a Shutdown of a Top US Pipeline", *New York Times*, 8 May 2021.
[33] WEF, January2022, op. cit.
[34] C. Banerjee, A. Bhaduri, C Saraswat, "Digitalization in Urban Water Governance: Case Study of Bengaluru and Singapore", *Frontiers in Environmental Science*, 24 March 2022.
[35] *Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks*, US Government Accountability Office, 21 June 2022.

Legacy infrastructure assets are more vulnerable to cyberattacks.

Old infrastructure assets face additional risks, as they are often run on inadequately protected legacy systems. Hence system components must be taken offline to apply the latest cybersecurity updates. Today's new critical infrastructure can be designed more efficiently with the latest technologies and in ways that enable real-time maintenance and rapid breach detections without disrupting the provision of critical services (See *Critical infrastructure in China: threats and opportunities).*

Critical infrastructure in China: threats and opportunities

The digital economy in China is growing, covering also critical infrastructure.

China is undergoing a transition towards a digital-driven economy,[36] with a GDP share expected to reach 50% by 2030 [37] from 40% currently.[38] Digital expansion will impact many traditional industries and critical infrastructure, and take shape through investment in "new digital infrastructure" (eg, AI technologies,[39] 5G base stations).[40] Investments in new infrastructure projects have been planned and are expected to reach CNY 15 trillion (USD 2.2 trillion) over 2020–2025.[41] This means more critical infrastructure exposures to cyber risks. According to the China Information Security Assessment Center, in 2021 "new infrastructure" assets including 5G, IoT, Industrial Internet, AI and Blockchain were targets of cyberattacks.[42] This new trend has triggered a growing demand for cyber risk protection solutions in China.

New infrastructures equipped with the latest technologies are more resilient to cyberattacks.

A positive development is that critical infrastructure based on emerging technologies could reduce exposure to cyberattacks. For example, digital critical infrastructure, especially associated with 5G and AI, can adopt upgraded security standards and architecture to defend against cyber threats. Advances in data analytics are effective tools to combat cyberattacks but may also increase attack surface. One report says that around 70% of organisations would have not been able to identify or respond to cyber threats without AI.[43] Likewise, cloud technologies may offer a greater degree of resilience, while also constituting an additional single point of failure if their operating security does not adapt to the latest threats.

Supply chain vulnerabilities

Supply chains exposed to cyberattacks through multiple entry points.

Supply chains have multiple entry points for hackers. The interconnected nature of supply chain networks across digital and physical borders makes participating companies vulnerable to shocks that can propagate through the entire system. The more digitally integrated the network, the faster the propagation of the shock and the less clustered the impacts. The NotPetya attack of 2017, during which hackers embedded malware in accounting software used by companies in Ukraine for tax reporting purposes, is one example of such a shockwave event. It propagated horizontally by discontinuing the operations of infected companies and had vertical spill-over effects across multiple supply chains and borders. It is estimated that affected downstream companies experienced a loss of USD 7.3 billion, a fourfold increase from the losses reported by the firms upstream hit directly.[44] Losses were found to be higher among companies with an undiversified pool of suppliers, and infected suppliers were more likely to be cut out of the supply chain after an attack.

[36] The digital economy refers to a broad range of economic activities, including using digitised information and knowledge as a key factor of production, and also modern information networks. See *China's Digital Economy: Opportunities and Risks*, IMF working paper, 17 January 2019.
[37] See *China Academy of Information and Communication Technology* (CAICT).
[38] China spurs digital economy as new driver of growth, *Xinhunet*, 4 August 2022.
[39] "China to build AI-powered 3D printed hydroelectric dam in Tibet", *3D Printing Industry*, 9 May 2022.
[40] According to official definitions, new infrastructure that exploits emerging technologies include AI technologies, 5G base stations, industrial IoT applications, data processing & storage centres, Ultra High Voltage (UHV) capacities, intercity high-speed railways (HSR) and charging stations to support the electric vehicle network expansion.
[41] *New Infrastructure Investment Will Reach CNY 15 Trillion Within Five Years*, Equal Ocean, 15 Oct. 2020.
[42] See China Cyber Security Assessment and Overview, 30 December 2021.
[43] *Reinventing Cybersecurity with Artificial Intelligence*, Capgemini Research Institute, 11 July 2019.
[44] M. Crosignani, M. Macchiavelli, A.F. Silva, *Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains"*, Federal Reserve Bank of New York, Staff Report No. 937, July 2020 (rev July 2021).

The further up the chain an attack, the more widespread its consequences.

If the shock targets firms at the very top of the supply chain, the fallout can span the entire network. One such example is the targeting of supply chain-enabling companies such as SolarWinds.[45, 46] In 2020, hackers introduced a malware to the company's software system that spread to 30 000 customers over seven months. The nation state actor (see Appendix 1) was then able to select targets of interest from this large pool, including US government agencies. The attack raised awareness on the cyber vulnerability of entire supply chains through third-party providers. It remains a major concern today as cybersecurity vulnerabilities can be exploited by different agents, including those working on behalf of governments. Stringent scanning of third-party vendors is one avenue to mitigate upstream cyber risks.

Downstream attacks have more local consequences.

Conversely, downstream attacks have a more local impact. Today's business models are digitalising across supply chains; they operate across national borders; and are composed of sizes of companies with different degrees of cyber hygiene. These multiple entry points for cyber criminals threaten sub-network operations, especially in cases where a firm cannot easily substitute for an intermediate input provider that is hit by a shock.[47] In a recent survey, 40% of CEOs said their organisation had been negatively affected by a supply chain cybersecurity incident in the last year, with close to 60% questioning the cyber resilience of their partners and suppliers.[48] To ensure resilience to direct and indirect cyberattacks, it is essential that companies of all sizes proactively map out their supply network and strategically diversify suppliers.

Data privacy regulations: increasing long tail risks for insurers

Data privacy laws inspired by Europe's GDPR are proliferating globally.

Europe has been a leader in establishing data privacy regulations, and many other regions are following. Since the General Data Protection Regulation (GDPR) came into force in 2018, not less than 60 countries have either enacted or considered enacting new data privacy laws, with many adopting similar concepts to the ones enshrined in the GDPR. In Asia, last year saw the introduction of new privacy laws in Japan, Singapore and China. In the US, while there is no federal privacy law yet, California introduced a first state-based privacy legislation in 2018.[49] Since then, Colorado and Virginia among others, have implemented their own data privacy and security legislations.

Stronger data privacy rights incentivise litigation and grow exposures to regulatory fines and financial losses.

Stronger data privacy rights expose firms and insurers to consumer-led litigation and regulatory sanctions that can result in huge financial losses. New privacy and security laws provide additional rights for consumers and reinforce those already in place. For instance, the California regime provides for statutory damages on a per-person basis and has seen increasing claims settlement values for state residents. And in Europe, reporting a security and/or privacy breach to regulators and consumers is mandatory.[50] Failure to do so, or to have the wrong security measures in place, can result in fines being levied under the GDPR, of up to 4% of a company's global turnover or EUR 20 million, whichever is greater.[51] The GDPR also rules that any person who has suffered material and non-material damages (ie, emotional distress) as a result of an infringement of the regulation has right to compensation for the damage suffered. Litigations in Europe post GDPR, either via individual lawsuits or EU-style class actions, show that consumers are now using this right to obtain compensation in cases of data/privacy breach.

Litigation procedures resulting in large third-party claims increase insurers' long tail risks.

Lengthy litigation procedures resulting in hefty third-party claims are growing insurers' long-tail risk exposures. In the US, large third-party claims settlements with regulators and/or consumers were obtained following data privacy and security violations (see Table 2). The legal fees incurred to defend third-party claims (most of the time in the form of class actions lawsuits) are very expensive and often come on top of indemnities.

[45] The Austin-based company SolarWinds develops software for businesses to help manage their networks, systems and IT infrastructure. It operates in the US and many other countries.
[46] "Supply chain attacks show why you should be wary of third-party providers", *csoonline.com*, 27 Dec 2021.
[47] M. Elliott, B. Golub, M. V. Leduc. 2020. "Supply Network Formation and Fragility." *American Economic Review,* 12 January 2020 (rev. 18 April 2022).
[48] WEF, January 2022 op. cit.
[49] Referred to as the California Consumer Privacy Act (CCPA).
[50] In other regions, we are seeing a growing number of new privacy laws making reporting mandatory.
[51] In 2020, Marriott and British Airways were fined by the UK Information Commissioner's Office GBP 18.4 million and GBP 20 million, respectively, to that effect.

Consequently, these litigations impact the long tail part of cyber losses as it often takes several years until they are resolved (see the year of the breach vs the year of the settlement) as opposed to the first-party losses, where costs are known usually within a year of the incident (short tail risks).

Table 2
High-profile data breaches

Breached entities	Impacted individuals	Year of the breach	Year of the settlement	Amount (in USD millions)
Deutsche Telekom - T Mobile	76.6 million	2021	2022	350
Morgan Stanley	15 million	2016/19	2022	60
OPM	22 million	2015	2022	63
Capital One	106 million	2019	2021	190
Yahoo	500 million	2013/16	2020	117.5
Equifax	163 million	2017	2020	575
Home Depot	56 million	2014	2020	200
Uber	57 million	2016	2018	148
Target	110 million	2013	2017	18.5
Anthem	80 million	2014	2015	115

Source: Based on Swiss Re Institute research

Third-party claims are just one of many components in losses resulting from data breach incidents.

Third-party claims are just one of several elements constituting a data-breach related loss. In addition, there can also be legal fees, crisis management costs (first party) and potential fines. Breaches become even costlier when they involve many jurisdictions because of the international regulatory implications and potential lawsuits that may be filed by aggrieved parties in different countries. Table 3 details the losses resulting from the Capital One data breach in 2019, when data from citizens in the US and Canada were compromised. In some cases, all the losses added together can surpass the value of the entire cyber insurance programme bought by the policyholder.

Table 3
Data breach event costs example

Coverages	Capital One data breach	Nature of the costs
Crisis management costs 1. Forensics costs 2. Notification, credit monitoring and call centres 3. Breach counsel costs 4. Public relation costs 5. Legal fees	Estimated USD 100 million	First party
Regulatory fine	USD 80 million	Third party
Network Security Liability / Privacy liability (litigation will be filed where the affected consumers reside so if the data breach compromises the data of individuals residing in different countries, there could be as many litigations ensuing)	US: USD 190 million Canada: pending (a USD 636 mn equivalent class action was certified in June 2022)	Third party
Legal fees to defend legal actions	Estimated tens of USD mn	Third party
Total event costs	> USD 400 million	

Source: Capital One, Office of the Comptroller of the Currency, Global Data Review, Insurance Insider

China has established a data protection regulatory framework with similar standards to GDPR.

In China, the Personal Information Protection Law (PIPL) was enacted in November 2021. It outlines the legal framework of data privacy protection, with similar scope to the GDPR, adding more ways that organisations from which information has leaked can be punished (eg, suspensions). Since taking effect, data privacy breach incidents have exposed companies to higher business and regulatory risks. These could in part be covered by insurance, and Chinese insurers expect to be more engaged in the data breach sector.

Risk management with cyber insurance

Cyber risk management helps companies determine whether to mitigate, transfer, avoid or accept certain exposures.

Risk management is the process of identifying, assessing and responding to/mitigating risk events.[52] Organisations must understand the probability and potential severity of loss events to determine their acceptable level of risk. Based on their tolerance, they can choose to avoid or accept certain risks, and take steps to mitigate or transfer the resulting exposures. In the cyber context, organisations must manage the vulnerabilities of their computer and network systems. They must also train employees to identify threats, stay abreast of privacy laws and navigate a risky geopolitical environment.

Private and public sector cyber risk management efforts have intensified.

Efforts to manage the risks emanating from third-party liability, ransomware claims and supply chain/critical infrastructure threats have been ongoing since the 1990s.[53] Since then, the scope of cyber threats has reached new levels and overall awareness has increased. The private and public sectors have responded with more risk management efforts and investment in cyber security, and by growing the cyber insurance market.

The cyber insurance market is growing fast.

Companies retain a greater share of cyber risk than property and other liability risks. This partly reflects the relative novelty of the digital economy. In 2022, only 16.6% of digital and other intangible assets were insured, compared to 58% of tangible assets.[54] But the cyber insurance market grew rapidly in 2021, driven by the rise in ransomware and first-party losses, while at the same time also seeing increased third-party claims. We expect strong growth will continue in the coming years as cyber risks are better understood.

Insurance is a valuable component of cyber security efforts by transferring risk and incentivising mitigation actions.

Insurance plays a key role in improving cyber security beyond its core function of risk transfer. Following the recent spike in malware attacks, the industry has tightened underwriting standards, contributing to a temporary decrease in the frequency and severity of ransomware attacks and claims in 2022.[55] Beyond creating financial incentives to improve security protocols and mitigate vulnerabilities before the policy period, cyber insurance is a valuable input to the risk management process by pricing the risk, which provides a financial basis for framing decisions; monitoring,[56] which can reduce vulnerabilities during the policy period;[57] and claims payments and response support, which improve resilience and can mitigate losses following a cyberattack.

Cyber: outpacing growth in other insurance lines

The first cyber insurance covers were for liability (data-breach related) exposures.

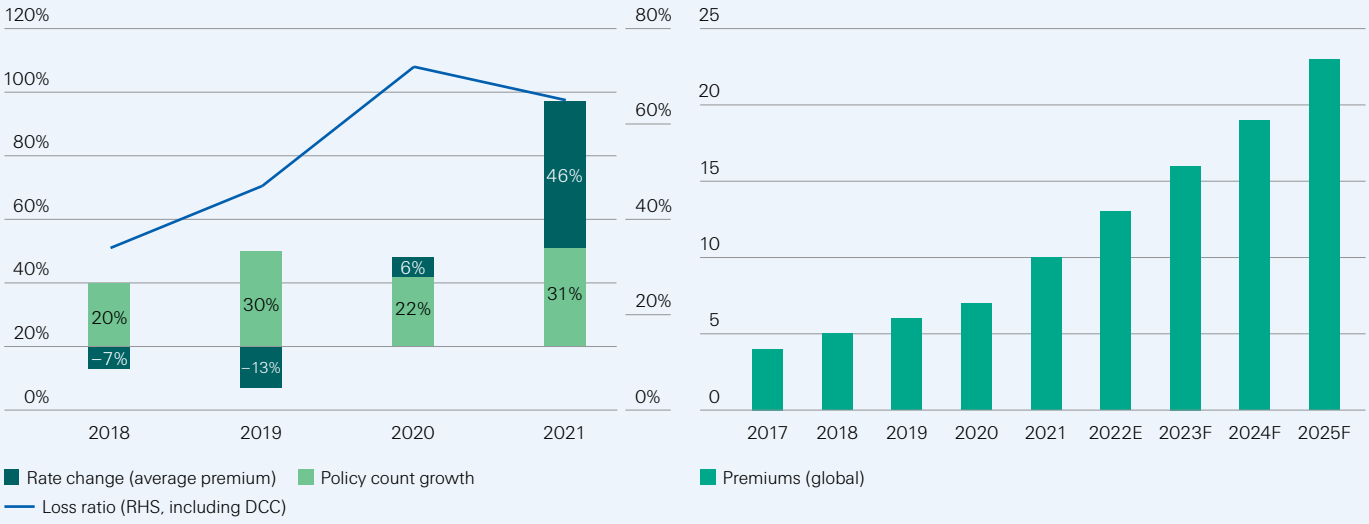
The cyber insurance market has grown with the digitalisation of the economy. Cyber insurance originated in the mid/late 1990s in the US, evolving from professional liability policies such as E&O.[58] The policies indemnified companies for third-party privacy/security claims post data breaches that affected customers, employees, investors and/or business partners. Coverage for first-party losses was introduced in the mid-2000s but given US data privacy regulations, third-party liability remained the main catalyst for product innovation. By the 2010s, the cyber insurance market expanded beyond the US. Developments such as the implementation of GDPR in the EU in 2018, increased investments in digital infrastructure and rising awareness of cyber threats have helped spur global market growth.[59]

[52] *Framework for Improving Critical Infrastructure Cybersecurity: Version 1.1,* National Institute of Standards and Technology, 6 April 2018.
[53] Eg, cyber threats to critical infrastructure were analysed in *Critical Foundations: Protecting America's Infrastructures*, Report of the President's Commission on Critical Infrastructure Protection, 1997.
[54] *2022 Intangible Assets Financial Statement Impact Comparison Report*, Aon/Ponemon, April 2022.
[55] *Mid-Year Update: 2022 SonicWall Cyber Threat Report*, Sonicwall, July 2022.
[56] For example, Coalition, a cyber managing general agent, which includes Swiss Re among its partners, monitors IP addresses for clients. See *Active Monitoring.*
[57] For example, Coalition states that it scans 4.5 billion IP addresses every month to actively monitor cyber exposures and catch vulnerabilities before they escalate. See Ibid.
[58] The first cyber standalone policy was written in 1997 (see *Cyber Claims: A Guide to Calculating Business Interruption,* JS Held, 2022) although there were instances of first-party information system business interruption coverages in the 1980s.
[59] For a summary of the state of the market and historical developments as of that year, and risk management principles that remain relevant, see *sigma* 1/2017: Cyber: getting to grips with a complex risk, Swiss Re.

Claims and premiums have grown quickly in recent years, but the protection gap remains large.

A main driver of cyber insurance market growth has been rising frequency and severity of cyberattacks, which in turn have raised awareness of the risk. In the US, the largest cyber market, premiums grew by 74% in 2021.[60] Standalone policy premiums increased 92%, driven by rate increases after ransomware incidents led to a spike in loss ratios in 2020 (see Figure 5, left).[61] We estimate that global cyber insurance premiums reached USD 10 billion in 2021 and we forecast 20% annual growth to 2025, with total premiums rising to USD 23 billion (see Figure 5, right). That said the market has significant growth potential beyond these projections. Given estimates of annual global cyber losses at USD 945 billion,[62] nearly all of the risk remains uninsured. One estimate puts the protection gap at 90%.[63] According to a recent study, only 55% of polled businesses have insurance, and less than one-fifth have ransomware cover limits above USD 600 000, the median of the losses resulting from such attacks.[64]

Figure 5
Left: US standalone loss ratio and rate and exposure growth
Right: Global cyber insurance premiums, USD bn, Swiss Re estimates



Source: National Association of Insurance Commissioners, S&P Global, Swiss Re Institute calculations

Cyber insurance market: evolution and structure

The US has a high share of global cyber insurance premiums, and a relatively competitive market.

We estimate that two-thirds of current global cyber-insurance covers are written for US clients, and the majority of those by US-domiciled insurers. The top 10 direct cyber insurers account for 57% of the US market.[65] The market is less concentrated than personal lines such as auto and homeowners, but more concentrated than large commercial lines like workers' compensation and general liability.[66] For insurers with sufficient capacity to increase market share and knowledge of the risk, cyber insurance offers a compelling growth opportunity.

[60] Based on data from the cyber insurance supplement filed by US insurers with the National Association of Insurance Commissioners.
[61] In Figure 5 (left), policy growth is a proxy for exposure growth. If policies are written with tighter terms and conditions such as lower limits, new sub-limits, coinsurance or exclusions, the effective exposure increase is lower and rate increase higher than suggested in the chart. The loss ratio includes defence and cost containment expenses.
[62] McAfee. op. cit.
[63] This compares to a Geneva Association estimate of 90% based on Lloyd's economic loss scenarios rather than McAfee's annual loss estimate. See *Understanding and Addressing Global Insurance Protection Gaps, The Geneva Association,* April 2018.
[64] G. Davis, *The Cyber Insurance Gap: What Is It, and How Can We Close It?*, BlackBerry, 10 August 2022.
[65] Swiss Re Institute analysis of NAIC cyber supplement data.
[66] Based on a comparison of Herfindahl-Hirschman Indexes of premium revenues.

Table 4
Largest US cyber insurers, by direct premiums written (USD million, based on NAIC cyber supplement data)

	Company	2021 DPW	2020 DPW	Growth	Cumul. share
1	Chubb	473	404	17%	10%
2	Fairfax Financial	436	109	302%	19%
3	AXA SA	421	293	44%	28%
4	Tokio Marine	250	86	189%	33%
5	AIG	241	228	5%	38%
6	Travelers	232	207	12%	43%
7	Beazley	201	178	13%	47%
8	CNA (Loews)	181	120	52%	50%
9	Arch Capital	171	16	967%	54%
10	AXIS Capital	159	134	19%	57%
	Industry	**4 827**	**2 774**	**74%**	**100%**

Source: NAIC cyber insurance supplement, S&P Global, Swiss Re Institute

Up to 50% of cyber insurance premiums are ceded.

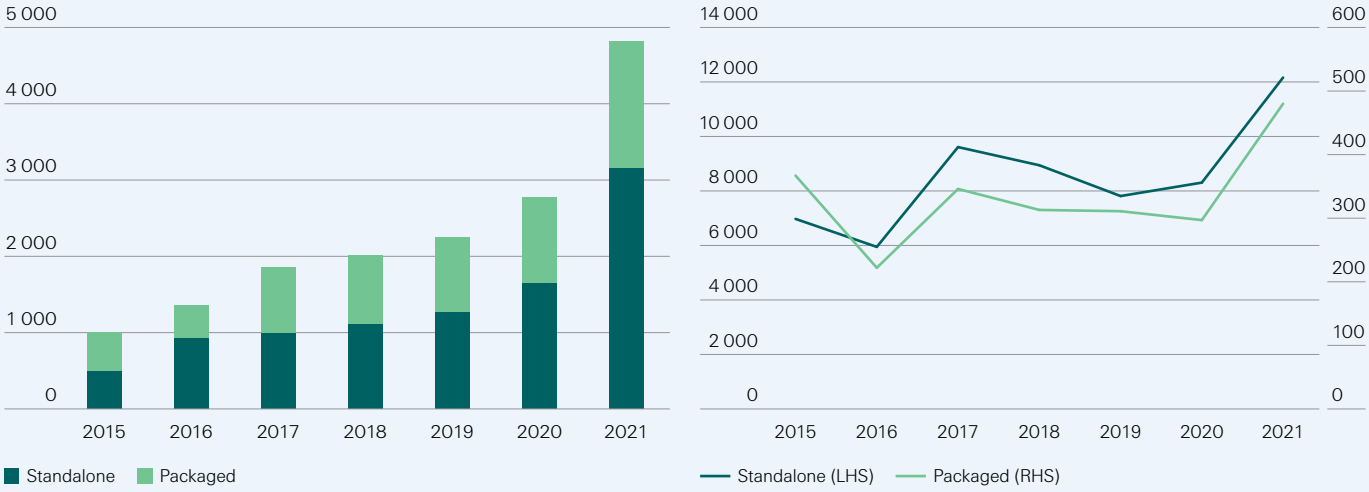
The competitive landscape comprises direct writers, managing general agents (MGAs) and managing general underwriters (MGUs). We estimate that 40-50% of global cyber insurance premiums are ceded, well above the 15% commercial lines average. This provides potential for new entrants to gain a foothold in the market. Even with that, however, capacity at the industry-wide level remains constrained primarily due to the potential for large systemic loss events.

Cyber insurance is provided either as a standalone product or packaged within another insurance policy.

Cyber insurance coverage can be provided on a standalone basis or packaged within an existing commercial multi-peril policy.[67] The standalone market developed in response to the introduction of cyber exclusions in other policies and, in terms of direct premiums written, has grown to nearly twice the size of the packaged cyber market. These covers can include: 1) all losses resulting from a cyberattack; 2) liability related to data breaches; and 3) losses related to data restoration.[68] Standalone policies are typically purchased by larger firms with more data and financial resources at risk. Based on the cyber supplement filed with the NAIC, the average premium for standalone policies written in 2021 increased to USD 12 161, compared with an increase to USD 480 for the cyber component of packaged policies (standalone shown in Figure 6, right), such as financial (D&O) or professional lines (tech and miscellaneous E&O). Around 259 000 standalone policies were reported in force at year-end 2021 compared with 3.5 million packaged policies. Ninety-four percent of the standalone policies were classified as claims-made rather than occurrence.[69] There was a near even split in packaged policies.

[67] Cyber premiums within packaged policies are either explicitly quantified or estimated for purposes of the NAIC cyber supplement.
[68] Cyber Risk Task Force, "Cyber Risk Toolkit", *American Academy of Actuaries*, August 2021, updated February 2022.
[69] Claims-made policies cover incidents that occur and are reported within the policy time frame, while occurrence policies offer lifetime coverage for incidents that occur during the policy period.

Figure 6
Total DPW (USD million) reported in the cyber supplement filed with the US National Association of Insurance Commissioners (left); average premium (USD) by policy type (right)



Source: NAIC

First-party coverage has grown fast in recent years as malware attacks have proliferated.

Product trends: strong demand for first- and third-party coverages
As ransomware attacks have increased, so too have first-party coverages, with corporations focused on protecting data and preventing business interruption. The NotPetya attack in 2017 marks the start of the shift from third- to first-party as the dominant coverage. In contrast to earlier class action lawsuits, claims filed for the NotPetya attack were not for data breach losses but the financial and operational harm caused by the malware attack.[70] By 2019, with the proliferation of ransomware-as-a-service and the increased sophistication of criminal hacking groups, companies faced significant exposure to first-party losses.

Don't forget third-party claims: recent privacy rulings will likely create demand for more cyber liability coverage.

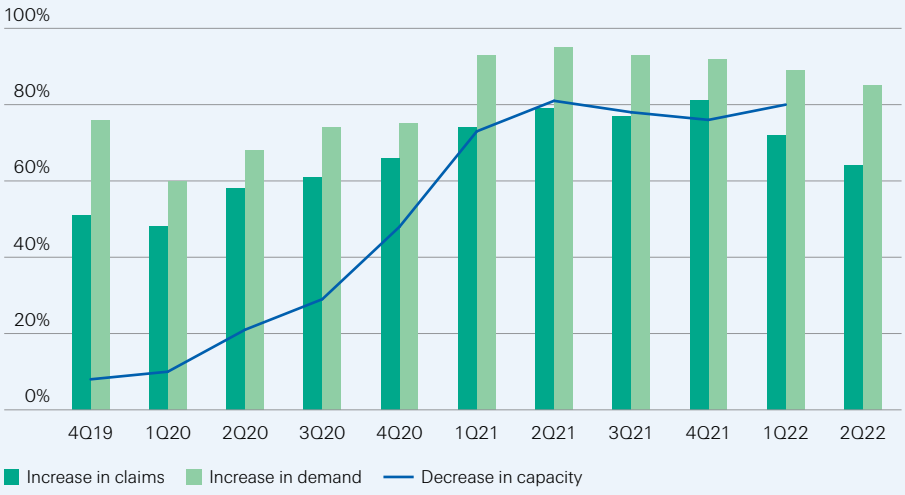
Alongside the surge in ransomware claims and associated measures, recent privacy rules and rulings could also provide a renewed catalyst for demand for third-party covers such as fines, legal fees and privacy and network security liability. The outcomes of existing cases will set precedents for corporate and insurer exposures under data protection rules such as the EU's GDPR, the California Consumer Privacy Act, the Illinois Biometric Information Privacy Act, and the China Personal Information Protection Law. In addition, companies must monitor new rules and understand their potential exposures. For example, under the American Data and Privacy Protection Act, introduced in the US House of Representatives in June 2022, firms will need to implement security practices to protect and secure personal data against unauthorised access, and individuals will be able to bring civil actions for violations of the Act.[71]

These incidents and more awareness of a heightened risk have driven large increases in the price of cyber insurance.

Claims trends: systemic risks drive strong rate increases
The upshot is increased demand for cyber insurance and heightened awareness of the potential for systemic losses. This surge in demand has met with restricted capacity, pushing prices higher, with some brokers reporting triple-digit year-over-year increases in 2021. [72] The momentum has continued into 2022, but with some deceleration. In the Council of Insurance Agents and Brokers' second quarter 2022 survey, 85% of respondents reported an increase in demand for cyber coverage, and 64% reported an increase in claims.[73] These numbers are less than in 2021 but indicate persistent elevated demand and adverse loss experience. Supply remains constrained, with nearly 80% of survey respondents reporting a decrease in capacity in the first quarter of 2022.[74] In addition to double-digit rate increases since late 2020, underwriters have included sub-limits for ransomware covers, co-insurance of up to 50% for ransom payments, and a revamped application process.

[70] For an example, "FedEx Hit with Cyber Attack-Related Securities Suit", *The D&O Diary*, 28 June 2019.
[71] *American Data Privacy and Protection Act*, Library of Congress, accessed 22 August 2022.
[72] "BRIEF-U.S. Q4 cyber insurance rates soar 130%, UK up 92%-Marsh", *Reuters*, 2 February 2022.
[73] *Commercial Property/Casualty Market Index: Q2/2022*, Council of Insurance Agents and Brokers (CIAB), August 2022.
[74] *Commercial Property/Casualty Market Index: Q1/2022*, CAIB, May 2022.

Figure 7
Percentage of respondents indicating an increase in claims demand vs decrease in capacity



Source: Council of Insurance Agents and Brokers, Swiss Re Institute

Standards for loss mitigation become a prerequisite to underwriting risks

The recent increase in ransomware events has resulted in targeted underwriting updates.

Clients in the US and globally now need to showcase their preparedness for a ransomware attack. Insurers or associated analytics firms review exposure with scanning technology, emphasising business continuity/disaster recovery planning, privileged access controls, multi-factor authentication and pro-active scanning/testing. Typically, a supplemental ransomware application is required as a part of the application or renewal process, and if the answers are unsatisfactory the policy is either not written or non-renewed.

The underwriting process can incentivise risk mitigation measures.

For insureds, the expenses of implementing required security measures to meet the baseline level of cyber hygiene can be more than offset by premium savings. The application and underwriting process can therefore motivate a business to focus on risk assessment, ultimately incentivising implementation of risk-based security measures to minimise insurance costs. Coverage encourages greater precaution and thus reduces the probability of loss.[75]

Underwriting standards can reflect externalities and help achieve cyber deterrence objectives.

The American Property Casualty Insurance Association has described cyber resilience as "a societal obligation."[76] Because of the borderless nature of the cyberspace, companies that lack appropriate digital defences put themselves and the broader economy at risk. After high-profile cyberattacks such as the one on Colonial Pipeline's IT systems, policymakers have started to push for increased mandates. The new strategy in the US includes rules mandating that organisations meet minimum cybersecurity standards, partnering with the private sector and stricter enforcement of any new rules.[77] To the extent that cyber insurance provides financial incentives aligned with market and public authority cyber deterrence objectives, it can limit the need for mandates and promote productive cooperation between the private and public sectors.

[75] I. Ehrlich and G. Becker, "Market Insurance, Self-Insurance, and Self-Protection," *Journal of Political Economy,* Vol. 80, No. 4, July–August 1972.
[76] E. Gilligan, "APCIA Announces Strong Cyber Extortion/Ransomware Guiding Principles", *American Property Casualty Insurance Association,* 1 July 2021.
[77] For example, in early 2022 US national cyber director Chris Inglis stated that "when critical functions that serve the needs of society are at issue, some things are just not discretionary." See "Inside the plan to fix America's never-ending cybersecurity failures" *MIT Technology Review,* 18 March 2022.

Figure 8
Underwriting criteria and data sources

Source: Swiss Re, *CyberCube*

The public and private sectors can also collaborate to improve cybersecurity standards.

Public and private entities can also improve cybersecurity by coordinating on processes such as "design and testing". Similar to building codes for earthquake or fire and crash-tests for cars, hardware and software could be tested and officially validated before release. One example is a recent initiative in the US modelled after Energy Star, a labeling program used to promote energy efficiency.[78]

Insurance clients can also benefit from ancillary services

Cybersecurity companies play an important role in the insurance function by providing technical expertise and supporting services.

Re/insurers often work with cybersecurity companies to develop customised products for clients, especially in the critical infrastructure sector. The cybersecurity companies have teams with strong technical capabilities and can either steer the project or act as service providers and risk consultants. The engagement of cybersecurity companies expands the capacity to undertake pre-underwriting examinations and offer holistic cyber solutions, including ongoing cyber risk monitoring.

Re/insurers need to establish a unique value proposition in cooperation with cyber companies.

Cyber insurers can extend beyond their risk mitigation and transfer function when an attack occurs. The insurer may provide claims services and loss compensation, while the cybersecurity company evaluates the losses. Emergency assistance, loss control and data recovery are also available to clients. In some countries, re/insurers and cybersecurity companies work with the public sector to develop a more holistic picture of the risk. These forms of cooperation can expand the scope of business for re/insurers but also require investment to develop the necessary skills and partnerships.

Table 5
Cyber insurance process in a typical cooperation model

Before underwriting	Before incidents	After incidents
Risk specialists interview	Monitor possible risks and minimise the losses	24/7 emergency hotline
Cyber security examination	Educate clients to better understand laws, regulations, and claim trends	Optional emergency response vendor
Claims cases review	System testing to optimise loss-prevention measures	Incidents Investigation Report
Cyber solution design and pricing		

Source: Swiss Re Institute

[78] "White House to unveil ambitious cybersecurity labeling effort modeled after Energy Star" *Cyberscoop,* 11 October, 2022.

Addressing aggregation risk and other limitations to insurability

Addressing challenges to insurability can boost the potential growth of the cyber insurance market.

In response to uncertainty around cyber risk, insurance providers have become more selective in their underwriting through better risk selection, lower limits, co-insurance and tighter policy terms.[79] As insurers reduce portfolio sizes and exposures, market growth might face upper bounds. This could leave the economy more exposed to cyber threats and affect societal resilience. By reducing uncertainties, risk carriers can increase the insurability of cyber exposures and improve the growth potential of the cyber insurance market. In this section, we focus on enhancing insurability by improving risk knowledge through data and modelling, and increasing clarity around catastrophic losses.

Table 6
Main types of cyber loss estimates

	Insurability Criteria		Current state	Changes to improve insurability
Actuarial criteria	Frequency and severity of risk need to be reasonably quantifiable		Evolving risk; historical data limited Victims of cyber attacks, governments, security firms etc may withhold details for security purposes Wilful act, nature of attacks is continuously changing to escape analysis and mitigation Models remain in their infancy	Initiatives to create collective (pooled) data bases, improve standardisation for modeling and analysis, and clear definitions of what constitutes a cyberattack (Recommendation 1)
	Independence of loss occurrences		Coordinated attacks can cause losses to be correlated; large-scale attacks can affect multiple lines of business	Cyber is fundamentally a human risk, but clarity of intent around state-backed acts of war and other exclusions, such as the actions described earlier can help
	Maximum loss needs to be manageable within industry capacity		Catastrophic loss potential hampers diversification	Separate catastrophic risk from cover for attritional losses
	Mutuality: moderate average loss amounts per event and a sufficiently high number of similar loss events per annum		The basis of the cyber insurance market is well established	Increase insurance take-up rate across sectors and firm sizes. Separate catastrophic risk from attritional losses
	No excessive information asymmetry problems (i.e. moral hazard, adverse selection)		Experience and standards regarding data sharing and mitigation are evolving	Coinsurance, mitigation standards, data sharing, crisis management resources
Market criteria	Insurance premium needs to be risk-adequate for a sustainable insurance market		Strong increase in insured losses, loss ratios in recent years	Improve modeling for risk-adequate pricing; separate catastrophic risk from attritional losses
	Sufficient industry capacity		Sufficient capacity to support strong growth in attritional market; not sufficient capacity to fully insure catastrophic risks	Clarity around what constitutes a catastrophe can attract re/insurer capacity (Recommendation 2)

Source: C. Biener, M. Eling, J.H Wirfs, *Insurability of Cyber Risk – An Empirical Analysis*, University of St. Gallen, 2015; C. Christophe, P. Liedtke, "Insurability, its limits and extensions", Insurance Research and Practice, vol 18 (2), 2002; B. Berliner, *Limits of Insurability of Risks*, 1985

Improving risk knowledge to reduce pricing uncertainty

Standardised data and modelling improvements can expand available coverage.

When there is a high degree of uncertainty around average expected losses, insurers tend to restrict coverage. To this end, reducing uncertainty with data and improved modelling capacity can expand the coverage available in the market. Cyber risks are difficult to quantify due to a lack of standardised data and modelling constraints within a shifting risk environment. Actuaries typically infer future risks based on backward-looking data, but this approach is limited in the context of cyber risk for two reasons: 1) a

[79] J. Pendleton, *Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market*, US Government Accountability Office, 20 May 2021.

lack of standardised data; and 2) backward-looking information is less useful in a rapidly changing risk environment. Capturing and analysing better data is critical for probabilistic modelling and developing reliable loss estimates to better understand the dynamics and implications of cyber losses. This requires detailed knowledge of the range of risks, their impacts and the reliability of data.[80] The introduction of cybersecurity standards can also reduce uncertainty about potential losses.

The private and public sectors have started to address data standardisation.

Private-sector attempts to address these shortcomings include the establishment of CyberAcuView, a consortium of leading cyber insurers to collect cyberattack and claims data, and to develop cyber data information standards. In Europe, the insurance and reinsurance federation is taking steps to facilitate access to standardised and anonymous breach data collected under GDPR. [81] There is increasing scope for coordination between the public and private sectors as well. For example, the US Cyber Incident Reporting for Critical Infrastructure Act was signed into law in March 2022, which will require critical infrastructure operators to report "substantial cyber incidents" to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency within 72 hours and ransomware payments within 24 hours.

Quantifying cyber is challenged by the rapidly changing nature of the risk.

Even as the cyber insurance market matures and additional data become available, developing accurate loss estimates will remain challenging given the evolving nature of the risk. New technologies, motives, threat actors and attack methods make the past a weak guide to the future, as underlying loss distributions change faster than those of more traditional lines. These characteristics of cyber risk bring both probabilistic and scenario models into play with limitations for either concept. Data for individual clients will not be sufficient for risk assessment and need to be complemented by larger industry data pools. This requires a modelling landscape that is capable of adopting new analytic methods including artificial intelligence (AI) and machine learning (ML). The dynamic nature of such models also means they require more model governance (ie, performance monitoring, data review and benchmarking).

Scenario-based models can improve confidence in potential cyber exposures.

To date there has not been a true cyber catastrophe event, so scenario estimates are instructive for the purpose of giving a sense of scale, emphasising the potential for risk accumulation and aggregate levels of cyber risk (see Table 7 for the main types of cyber loss estimates), and ultimately giving risk carriers confidence to allocate additional capacity to the sector.[82] Acts of cyber warfare, the disruption of a cloud provider of critical software or the deployment of malware through commonly-used software are examples of scenarios that could generate catastrophic losses. Re/insurers and analytics firms continue to enhance proprietary scenario estimates, which will improve with data standardisation and experience with cyber events.

Shrinking the cybersecurity skills gap at technology firms and re/insurers can help businesses stay on top of a shifting risk.

To remain current on an evolving risk, technology firms and re/insurers must also continually work to develop greater cyber expertise in the work force. As a recent example, in October 2021 Microsoft unveiled an initiative to fill the cybersecurity skills gap by providing access to free a curriculum and teaching tools.[83] Re/insurers can also help to tackle the cyber talent shortage by strengthening partnerships with universities to develop education programmes relevant to their business. This would include cyber risk modelling and forensic analysis to strengthen the actuarial and technical skills needed for the underwriting and claims management cycles.

Decreasing uncertainty around catastrophe risk can increase cyber capacity.

Underwriting actions and data standardisation can help insurers manage attritional losses,[84] but available capacity in cyber is also impacted by potential extreme events that are much more capital-intensive. Greater confidence in cyber catastrophe risk modelling and clarity around what constitutes a catastrophic loss can improve insurability and attract more capacity to the cyber insurance market.

[80] *sigma* 1/2017 op. cit.
[81] See *Insurers' key role in increasing cyber resilience*, Insurance Europe.
[82] *Cost of a Cyber Incident: Systematic Review and Cross-Validation*, CISA, 26 October 2020.
[83] *Closing the cybersecurity skills gap – Microsoft expands efforts to 23 countries*, Microsoft, 23 May 2022.
[84] Attritional losses are all claims not related to major catastrophes or exposures.

Table 7
Main types of cyber loss estimates

Type	Description
Bottom-up analysis	Rely on statistical microdata (eg, individual cyber incident claims data), typically used in actuarial analyses to assess risk.
Aggregate estimates (national/global scale)	Typically used by cybersecurity vendors to show the need for investment in cybersecurity.
Scenario estimates	Emphasise extreme events and the potentially devastating magnitude of the resulting losses.

Source: *Cost of a Cyber Incident: Systematic review and cross-validation*, CISA, Swiss Re Institute

Aggregation risk connects public and private sector concerns.

Some potential cyber scenarios might reduce available capacity. For example, in 2015 Lloyd's estimated that a widespread cyberattack on the US power grid could cause up to USD 1 trillion in economic damage and USD 71 billion in insured losses.[85] The fallout from this type of attack includes a rise in mortality rates, decline in trade, and disruption to supplies and transportation networks. Aggregation risk links national security and critical infrastructure vulnerabilities with private markets. National defence is the government's priority while the private sector typically owns large parts of the critical infrastructure that is vulnerable to attacks. Collaboration between the public and private sectors to address cyber threats to infrastructure can expand insurability by mitigating the risk and reducing uncertainty about the response to cyber catastrophes.

The public sector is working with critical infrastructure providers.

A cyberattack on critical infrastructure could have cascading impacts across the economy. Beyond economic damages, a successful attack could erode public confidence in utilities and the financial system.[86] The public and private sectors are working together to identify critical assets and define responsibilities for maintenance, provision of services and the implementation of response protocols.

Addressing aggregation risk via policy language standardisation

The industry is pushing for standardised policy language to address potentially catastrophic events.

The relative youth of the cyber insurance market and complexity of the risk are reflected in a lack of standardisation around exclusion clauses and terms and conditions. The potential for catastrophic events stemming from state-backed acts of war, hostile cyber acts or critical infrastructure failure – and a lack of clarity regarding the ensuing liability – is an important factor curtailing capacity in cyber insurance. Scenario estimates of cyberattacks with insured losses in the tens of billions of dollars are many multiples of 2021 insurance premiums, and modelled economic losses are much greater. Developing a uniform approach to deal with aggregate losses can support sustainable growth by creating better-understood solutions for corporations and bolstering the risk appetite of insurers.

Policy language shortcomings are being addressed with various approaches but risk leaving the market without a solution for the biggest events.

Associations, individual insurers and think tanks have taken steps to standardise definitions for cyber war, operations and attribution. In November 2021, the Lloyd's Market Association introduced clauses designed to exclude coverage for cyber war and cyber operations,[87] with a requirement that these or similar exclusions are applied from 31 March 2023.[88] The significance of Lloyd's bulletins extends beyond the direct marketplace since the exclusions must fit into any reinsurance tower that Lloyd's syndicates are involved in and thus have implications for all re/insurers in the same programme.

[85] *Business Blackout: The insurance implications of a cyber attack on the US power grid*, Lloyd's, July 2015.
[86] *Critical Infrastructure Protection: Treasury Needs to Improve Tracking of Financial Sector Cybersecurity Risk Mitigation Efforts*, GAO, 27 September 2020.
[87] *Cyber War and Cyber Operation Exclusion Clauses*, Lloyd's Market Association, 25 November 2021.
[88] "State backed cyberattack exclusions", *Lloyd's Market Bulletin*, 16 August 2022.

Attribution is a core problem. Insurers are adopting differing approaches.

But a coordinated approach remains aspirational. A fundamental problem for coverage determinations is that a simple technical process for attributing cyber operations does not exist.[89] Some observers suggest that carriers avoid the Lloyd's exclusions,[90] and a couple of insurers in the US are creating their own exclusions to address catastrophic cyber events. Chubb has created endorsements to tailor coverage for widespread events, ransomware encounters and neglected software vulnerabilities,[91] providing a framework for pricing catastrophic risks and evolving vulnerabilities. And Beazley is updating its exclusions for cyber war and infrastructure failure while placing sub-limits around catastrophic cyber events that have a "major detrimental impact" on the functioning of a state.[92]

Earlier reports provide ideas that remain part of the discussion, including new definitions of cyber events and different types of exclusions.

Earlier reports provide a basis for consideration in moving towards a common language and provide insights to help evolve industry policy language. For example, in 2020 the Geneva Association proposed the term "hostile cyber activity" to describe cyber acts that fall between war and terrorism,[93] while the Carnegie Endowment proposed using two complementary exclusions to deal separately with catastrophic and war-related or state-sponsored cyber risks.[94] Some companies expect to see more of these cat/non-cat rather than war exclusions. [95]

Silent cyber presents a large risk to the industry.

Insurers have taken steps to address silent cyber exposures

The cyber insurance cover described in this report is "affirmative", as perils are explicitly included or excluded. "Silent cyber" is a related topic, encompassing cyber perils that are not explicitly listed in traditional policies, although policy holders may still assert claims. This can lead to significant losses for insurers despite not intending to provide cyber coverage. The best-known example to date is the NotPetya attack in Ukraine. Despite being a cyberattack, approximately 85% of insurance industry loss was reportedly through property claims that did not explicitly include or exclude cyberattacks.[96]

Insurers have responded with stronger policy wording including new exclusions.

Exposure to silent cyber can be mitigated by making cyber exposures explicit – either pricing for cyber in packaged (non-cyber) policies, or shifting the risk into standalone policies. Better risk evaluation and more accurate pricing will improve the sustainability of the market. Insurers have taken steps to address silent cyber risks, updating policies and beginning to standardise wording, exclusions and endorsements. For example, in November 2019, the Lloyd's Market Association (LMA) introduced clauses to address silent cyber exposures in property and marine insurance.[97]

Adding capacity with non-traditional risk-carriers

There is scope to increase capacity through greater capital markets involvement...

One option for addressing part of the protection gap that results from hard-to-model and non-diversifying tail risks is to develop a market for cyber insurance-linked securities (ILS). Currently, it is estimated that alternative capital will provide around USD 95 billion additional catastrophe reinsurance capacity in 2022, supplementing dedicated traditional reinsurance capital of USD 435 billion.[98] There is latent interest in growing alternative capital solutions for cyber risks to support a sustainable cyber market. To date, however, ILS investor interest has been limited, with aggregation risk and model uncertainty acting as main deterrents. True ILS structures (akin to cat bonds) require the

[89] *Guide to Cyber Attribution*, US Office of the Director of National Intelligence, 14 September 2018.
[90] "Lloyd's Cyber Insurance Tweaks Stir Coverage Restriction Concern", *Bloomberg Law*, 26 August 2022.
[91] *Chubb Addresses Growing Cyber Risks with a Flexible and Sustainable Approach*, Chubb, 2021.
[92] "Beazley finalises systemic cyber wordings ahead of phased rollout", *Insurance Insider*, 24 August 2022.
[93] R. Carter, J. Enoizi, *Cyber War and Terrorism: Towards a common language to promote insurability*, Geneva Association, 23 July 2020.
[94] *War, Terrorism, and Catastrophe in Cyber Insurance: Understanding and Reforming Exclusions*, Carnegie Endowment for International Peace, 5 October 2020.
[95] M. Geoghegan, "Episode 122 Dan Trueman: The only way to be in Cyber is to be an expert", *The Voice of Insurance Podcast*, 10 May 2022.
[96] *Could NotPetya's Tail Be Growing?*, PCS, 2019.
[97] *Property and Marine Cyber Clauses*, Lloyd's Market Association, 3 November 2019.
[98] *Dedicated Reinsurance Capital Growth of 2021 May Not Continue*, AM Best Market Segment Report, 22 August 2022.

development of objective triggers, which could present the insured with considerable basis risk. Alternative capital managers are investing in cyber insurtech companies to improve the understanding of the risk and to potentially deploy capital to support it. Meanwhile, indemnity-based third-party capital structures, such as re/insurance sidecars, can bring new capacity to cyber underwriters.[99]

...and public-private partnerships.

Another potential solution to help close the protection gap is to design a type of public-private partnership (PPP) insurance scheme, where the coverage of systemic risks is split between insurers and a government(s)-backed fund. In the US, the Government Accountability Office has recommended that the Cybersecurity and Infrastructure Security Agency and the Federal Insurance Office produce a joint assessment on the extent to which catastrophic cyberattacks on critical infrastructure warrant a federal insurance response.[100] The ultimate form this could take, including structure, funding, participation requirements and scope of coverage remains to be determined and is being assessed by policymakers at the US Treasury[101] and in other jurisdictions.

[99] See, for example, "Coalition launches $300m Ferian Re to provide third-party cyber risk capital", *Artemis,* 13 October 2022.
[100] Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks, GAO, June 2022.
[101] *Potential Federal Insurance Response to Catastrophic Cyber Incidents"*, Federal Register, Department of the Treasury, 29 September 2022.

Conclusion

The global cyber protection gap is estimated to be at around 90%.

The cyber risk landscape is rapidly evolving and, as cyberattacks have increased, so too has awareness of the risk and demand for cyber insurance solutions. However, most businesses and individuals are uninsured or significantly under-insured for cyber exposures, and cyber insurance premiums amount to just a fraction of total losses from cyberattacks. Estimates put the cyber protection gap at 90%. This points to the large growth potential for the insurance market, but there is much work to do to ensure sufficient risk protection is available to make society more resilient to cyber risk. And this effort will require collaboration between businesses, the insurance industry and government.

Data quality and risk modelling need upgrading if society is to be more resilient against cyber exposures.

A first requirement is to improve data quality and modelling. Cyber risks are difficult to quantify due to a lack of standardised data and modelling constraints. Future risks are typically inferred based on backward-looking data, but this approach is of limited value in the rapidly changing environment of cyber risk. Introducing cybersecurity standards will improve data in terms of breadth and transparency to allow meaningful risk insights and enable more accurate pricing and modelling. Re/insurers must also invest in the cyber workforce to help strengthen the actuarial, technical and forensic skills needed for the underwriting and claims management cycles.Meanwhile, the high degree of uncertainty regarding expected losses and the evolving nature of the risk challenges the insurability of peak and accumulation risks.

Insurers can make an important contribution by updating their policy language for clarity and consistency.

Second, re/insurers should update policy language for clarity and consistency. The relative youth of the cyber insurance market and complexity of the risk are reflected in a lack of standardisation around exclusion clauses and terms and conditions. Exposures to hard-to-insure systemic risk scenarios remain a barrier for industry capacity. Stakeholders have taken steps to fix some of these issues, but factors such as attribution of cyber events remain a core problem. By clarifying the scope of coverage, as well as supporting risk analysis and mitigation efforts, contract clarity and consistency can lead to increased cyber capacity.

Public-private insurance schemes could help cover systemic risk events.

Finally, there is also need and scope for new types of public-private risk sharing mechanisms. Public and private sector collaboration is key to mitigating cyber threats to critical infrastructure. A public-private partnership insurance scheme, where coverage of systemic risks is split between insurers and a government(s)-backed fund is one option to address part of the protection gap. Another would be to tap into the market for alternative capital, such as by developing a market for cyber-insurance-linked securities.

Appendix

1. Selected cyberattacks per major economic segment

Part 1/2

Sectors	Name	Description	Implications
Oil and gas	Colonial Pipeline attack	The Colonial Pipeline attack was the largest successful cyberattack on an oil infrastructure target in US history.[A] Colonial Pipeline is the country's largest distribution system for refined oil products and supplies about 45% of all fuel consumed on the East Coast. On 7 May 2021, a ransomware attack forced the company to halt all operations until it paid the ransom. It restored operations eight days later. The shutdown triggered panic buying, fuel shortages, price increases and widespread economic disruptions. In Georgia and South Carolina, the price of regular gasoline climbed 8%, for example.[B]	Geopolitically, it refocused the US political debate on the importance of cyber-security oversight for the nation's critical energy systems.[C] Financially, the company paid a ransom of USD 4.4 million (of which USD 2.3 million was recovered by the US Department of Justice). It also suffered a business interruption loss and a data breach in the attack.
Health, Energy, Multiple	WannaCry	The high-profile WannaCry ransomware cyberattack occurred in May 2017 and targeted a vulnerability in Windows-operating systems by encrypting data until a ransom was paid. It is estimated that the attack infected over 230 000 computers worldwide and caused damages scoring in the billions of dollars across the public and private spheres.[D] The attack also affected the UK's National Health Service (NHS) due to outdated computer systems. It resulted in critical health equipment and systems becoming inoperable or unavailable.[E]	It endangered the functioning of the UK's National Health Service. The Department of Health and Social Care estimated that the attack cost the NHS GBP92 million, including GBP 20 million of lost output because of service disruption and GBP 72 million covering direct IT costs.[F]
Transport, Energy, Supply chains	NotPetya	In June 2017, the malware version NotPetya exploiting the same vulnerabilities as WannaCry started in Ukraine and affected organisations including the government, banks, state power utilities and key public transport systems (airport, metro) and even the radiation monitoring system at Chernobyl.[G] Infected entities included local branches of international groups linked to global supply chain networks such as FedEx or Maersk.	Supply chain network disruptions across multiple industries and borders. Losses for downstream companies are estimated at USD 7.3 billion, four times larger than losses at directly hit companies.[H]
Food	JBS attack	In May 2021, the Brazil-based and world's largest meat processing company JBS was forced to halt its operations due to a ransomware attack. It halted its beef and poultry processing operations at multiple locations in North America and Australia for 3–4 days. Eventually, the attack was resolved with a ransom payment of USD 11 million.[I]	The attack threatened the entire meat supply chain with consumers facing the risks of supply shortages and increases in meat prices.
Water	Tampa water system hack	In February 2021, a water system hack took place in Tampa, Florida as hackers broke into the computer system of a water treatment facility supplying 15 000 people and attempted to poison the city's water supply.[J]	The breach raised concerns over the talent deficit in the cybersecurity industry and the difficulty that smaller cities have in sourcing cybersecurity workers and to maintain up-to-date cyber hygiene.[K]
Oil and gas	ARA attack	Amid a continental energy crisis, a cyberattack on the oil refining hubs of Amsterdam-Rotterdam-Antwerp (ARA) disrupted terminal operations in February 2022. Multiple companies reported being victim of a ransomware attack that affected IT systems and consequently disrupted (largely automated) ports operations and triggered the rerouting of tankers.[L]	Besides the risk of energy supply disruptions, such attacks also prevent companies from fulfilling their supply contracts and lead to legal liabilities.
Supply chains, Multiple	SolarWind hack	In 2020, hackers added a malicious code into SolarWind's software system.[M] The malware spread to over 30 000 customers through regular routine system updates and enabled hackers to penetrate and spy on the IT systems of thousands of companies and organisations, including sensitive US government agencies.[N] The cyberattack constitutes an advanced supply-chain breach that was carried out over a period of 7 months. It was later attributed to nation-state Russian hackers.	The attack raised awareness on the cyber vulnerability of supply chains through third-party providers.

A "'Jugular' of the U.S. fuel pipeline system shuts down after cyberattack", *Politico*, 8 May 2021.
B "The Colonial Pipeline Crisis Is a Taste of Things to Come", *Columbia/SIPA* (subscription service).
C *Why the energy sector's latest cyberattack in Europe matters*, WEF, 4 February 2022.
D "Petya' ransomware attack: what is it and how can it be stopped?" *The Guardian*,28 June 2017.
E See *What is WannaCry Ransomware Attack?* Fortinet.
F "Department of Health and Social Care puts cost of WannaCry to NHS at GBP 92m," *digitalhealth.net*, 12 October 2018.
G The Guardian, op. cit.
H M. Crosignani, M. Macchiavelli, A.F. Silva, op. cit.
I "An Overview of the 2021 JBS Meat Supplier Ransomware Attack" *mitnicksecurity.com*, 3 June 2021.
J "Hackers try to contaminate Florida town's water supply through computer breach", *Reuters*, 8 February 2021.
K "One year after the Oldsmar water breach, some experts question the utility's cybersecurity", *WUSF Public Media*, 4 February 2022.
L "Cyberattack causes chaos at key European oil terminals", *S&P Global Commodity Insights*, 3 February 2022.
M SolarWind is a Texas-based company producing the Orion software widely used by customer companies to manage their IT resources.
N "The US is readying sanctions against Russia over the SolarWinds cyber attack. Here's a simple explanation of how the massive hack happened and why it's such a big deal", *businessinsider.com*, 15 April 2021.

Part 2/2

Sectors	Name	Description	Implications
Aluminum	Norsk Hydro	In 2019, Norwegian-based aluminum producer Norsk Hydro – among the world's largest industry players with factories in 40 countries – was subject to a massive ransomware attack that affected the entire organisation. It was the result of an infected email and forced the company to revert to manual operations to manage its industrial control systems much slower than in normal time.[A]	The year the attack occurred, Norsk Hydro estimated the total cost of the cyberattack to be in the range of NOK 650–750 million (~ USD 65–75 million).[B]
Electrical grids	Ukraine power grid hacks	The Ukrainian power grid has been repeatedly targeted by Russian-linked hackers, with attacks recorded in 2015 and 2016. In December 2015, the power grid of Ukraine was hacked, which resulted in power outages for over 200 000 consumers in Ukraine for several hours. It was later attributed to the Russian cyber hacking group sandworm. One year later, Ukraine's electrical grid was again targeted by hackers who inserted a blackout malware into the power system. Amid the ongoing conflict with Russia this year, Ukraine's national grid operator Ukrenergo pushed a request to integrate with the European Union's electrical grid.[C]	New cyberattacks elevate the risk of geopolitical incidents, especially if considered as attacks against the European Union.[C]

Source: Swiss Re Institute research.
[A] "Norsk Hydro – A Ransomware Case Study" – *cyberbrokers.co.uk*, 17 February 2022.
[B] See *Annual report 2019*, Hydro.
[C] *A Power Struggle over Ukraine's Electrical Grid*, Center for Strategic and International Studies, 9 March 2022.

2. Selected types of cyber policy coverages

Level	Coverages	Description	Nature of the cost
Company	Crisis management costs	1. Forensics costs 2. Notification costs 3. Credit monitoring and call centres costs 4. Public relations costs 5. Legal fees	First party
	Social Engineering	Financial losses arising from social engineering fraud schemes, including the impersonation of a vendor, supplier, executive, or client.	First party
	Extortion	Response costs as well as ransoms paid to hackers to decrypt or regain access to data or systems.	First party
	Data restoration	Data restoration from back-ups or re-creating data.	First party
	Business interruption / Contingent Business Interruption (CBI)	Business income loss and extra expense incurred during period of restoration or business income loss caused by the incident. CBI 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
	Fines	Regulatory fines levied by governmental agencies and/or the Payment Card Industry Data Security Standard (PCI-DSS) fines and penalties assessed by credit card companies or banks under payment card processing agreements.	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
	Legal fees	Legal costs incurred to defend a regulatory investigation or legal action.	Third party

Source: Swiss Re Institute

Published by:
Swiss Re Management Ltd
Swiss Re Institute
P.O. Box
8022 Zurich
Switzerland

Telephone +41 43 285 2551
Email institute@swissre.com

Authors
Elena Jelmini Cellerini
James Finucane
Loic Lanci
Dr Thomas Holzheu

The authors thank Yaxin Chen, Scott Swift and Sunnie Wang for their contributions to this report.

Editor
Paul Ronke

Managing editor
Dr Jerome Jean Haegeli
Swiss Re Group Chief Economist

The editorial deadline for this study was 26 October 2022.

The internet version may contain slightly updated information.

Swiss Re Management Ltd.
Swiss Re Institute
Mythenquai 50/60
P.O. Box
8022 Zurich
Switzerland

Telephone +41 43 285 3095
swissre.com/institute