THE GENEVA ASSOCIATION

INSURANCE FOR A BETTER WORLD

CYBER RISK ACCUMULATION:
Fully tackling the insurability challenge

November 2023

THE GENEVA ASSOCIATION

INSURANCE FOR A BETTER WORLD

CYBER RISK ACCUMULATION:

Fully tackling the insurability challenge

Darren Pain, Director Cyber | Evolving Liability,
The Geneva Association

The Geneva Association

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

Photo credits:
Cover page – Pratchaya on iStock

Geneva Association publications:
Pamela Corn, Director Communications
Hannah Dean, Editor and Content Manager
Kelly Gailey, Communications & Events Manager

Suggested citation: The Geneva Association. 2023.
Cyber Risk Accumulation: Fully tackling the insurability challenge.
Author: Darren Pain. November.

www.genevaassociation.org

Contents

ACKNOWLEDGEMENTS

This report has benefitted significantly from inputs and comments from the members and affiliates of The Geneva Association's (GA's) Cyber Working Group. Special thanks go to:

- Sabrina Sexton and Marek Stanislawski (Allianz Commercial)
- Hélène Chauveau, Amine Merchergui and Xavier Servel (AXA)
- Stephen Gibson (AXIS Capital)
- Aidan Flynn (Beazley)
- Anika Stehr (Hannover Re)
- Ramneek Goyal (ICICI Lombard)
- Mary Bieker (Intact)
- Oscar Taboada (MAPFRE)
- Cyrus Delarami and Stephan Brunner (Munich Re)
- Simon Dejung and Téodore Iazykoff (SCOR)
- Eric Durand and Stephan von Watzdorf (Swiss Re)
- Daljitt Barn and Andreas Kempe (Tokio Marine)

In addition, we would like to thank a number of external interlocutors who kindly agreed to share their insights as background to the report and/or for the session on cyber accumulation risks at the GA's inaugural cyber conference in November 2022. In particular:

- Rory Egan (Aon)
- Eric Dallal (Arch, formerly Verisk)
- Pamela Eck (Blue Vouyant, formerly Verisk)
- Charlotte Anderson (Crowdstrike, formerly CyberCube)
- Jon Laux (CyberCube)
- Peter Hacker (Distinction.Global)
- Jennifer Braney, Simon Heather, Theo Norris and Justyna Pikinska (Gallagher Re)
- Matt Harrison (Gallagher Re, formerly RMS)
- Doug Stronberg (GuidewireCyence)
- Jamie Pocock (Guy Carpenter)
- Tom Johansmeyer (Inver Re, formerly PCS)
- Yakir Golan (Kovrr)
- Professor Kerstin Awiszus (Leibniz University Hannover)
- Matt Silley (Lockton Re, formerly AXIS Capital)
- Darren Thomson (One Indentity, formerly CyberCube)
- Gordon Woo (RMS)
- Alan Frith (Verisk)
- Professor Matthias Scherer and Gabriela Zeller (Technical University of Munich)
- Professor Martin Eling (University of St. Gallen)

Foreword

With the digitalisation of society, the cyber problem has only grown in magnitude. Cyberattacks can simultaneously impact so many people and businesses around the world, causing catastrophic economic losses and a high accumulation of insured losses.

How did cyber threats evolve to be such a pressing concern for society, businesses, and the insurance industry in particular? It is worth reflecting.

With the rise of the internet and increase in digitalisation since the 1990s, cyberattacks have become more organised and profit-oriented. Also, nation-state-sponsored campaigns aimed at espionage or disruption are growing more prevalent. Today, the increasingly hostile geopolitical landscape, the targeting of critical infrastructure, and the proliferation of previously unknown ('zero-day') digital vulnerabilities in software and hardware are driving more sophisticated, devastating and potentially far-reaching cyberattacks.

One extreme risk scenario recently published by Lloyd's finds that a major attack on a financial services payment system could cost the global economy USD 3.5 trillion. This extraordinary amount of potential losses, as well as the high degree of uncertainty around them, makes effectively tackling this still-evolving threat one that transcends re/insurers alone.

This report is a full examination of the challenges to insuring extreme cyber risks, with proposed steps to increase insurability. Improving cyber-risk modelling approaches is important in helping insurers make informed decisions about – and potentially increase – their appetite to underwrite cyber risks, but it will not be sufficient. Risk sharing with governments in the form of a government backstop – as part of broader efforts to achieve optimal risk sharing – would be a further impetus for re/insurers to increase the scale and scope of cyber coverage.

Governments, along with critical infrastructure providers and technology companies, also have data and knowledge they could share with re/insurers to help them better understand cyber threats, enabling them to expand insurance protection. Finally, the consequences of poor cybersecurity should be shifted away from the most vulnerable, to those better equipped to prevent risks in the first place: providers of IT products and services. This could be achieved, for example, via enhanced liability regimes for IT firms.

In this era of continued digital transformation, insurers are constantly re-evaluating related risks and working to calibrate the protection they offer. Forming fruitful collaborations with other stakeholders will only strengthen the role they can play in safeguarding people and organisations from extreme cyber risks.

Jad Ariss
Managing Director

Executive summary

Cyber perils have the potential to cause catastrophic damage and result in large accumulated losses for insurers, perhaps across multiple policies.

Cyber perils – malicious or accidental acts that compromise the confidentiality, availability or integrity of data or IT services – can cause harm to many people and organisations, perhaps simultaneously and across different geographies. This potential for significant aggregate losses is particularly problematic for insurers that assume cyber-related risks from their customers, either as part of regular property and liability policies or through dedicated cyber cover. Carriers may find that they face multiple claims, perhaps under different insurance policies, leading to major loss accumulations in their underwriting portfolios. This includes some policies for which coverage was never intended or priced for, which has prompted re/insurers to seek to clarify the scope of protection available.

Worries about potential cyber loss accumulation are not new. Rising geopolitical tensions over recent years, however, have materially worsened the cyber threat landscape and heightened fears about a serious cyber incident. Global cyberattacks increased by 38% in 2022 compared with 2021, with ransomware attacks a continuing menace. Nation-state threat actors have become ever more aggressive in cyberspace, even beyond the ongoing Russia-Ukraine conflict, including using cyber weapons for destructive purposes. In 2022 alone, the number of new wiperware variants (designed to delete files and immobilise computer systems) exceeded those recorded throughout the previous 10 years combined.

Against that background, it is perhaps unsurprising that prudent insurance companies underwrite cyber risks with tightly defined contract wordings and limited risk-absorbing capacity. Yet as firms, individuals and governments become ever more reliant on digital technology, the overall costs from a major cyber incident or campaign of attacks continue to grow. Guesstimates of the annual cost of cybercrime range widely from around USD 1 trillion to as much as USD 8 trillion, yet relative to global cyber premiums of USD 12–14 billion, this suggests a sizeable chunk of cyber-related losses are uninsured.

Improved methods to quantify extreme cyber risks will be crucial in further expanding the size and scope of cyber insurance and helping to close the implied protection gap. However, the more hostile cyber environment has only served to highlight the actuarial challenges that cyber risks pose. In particular, the factors that drive the frequency and severity of cyber losses are not always well-understood and typically cannot be modelled with standard statistical approaches. Cyber is an anthropogenic peril and the extent of any harm depends on the interplay between the incentives, motives and resources of both victims and attackers, which often involve complex, non-linear relationships among multiple factors.

Although we have yet to witness a truly catastrophic cyber incident, adversaries are increasingly targeting critical infrastructure and digital supply chains – key pathways through which economic losses could escalate. This includes executing mega-scale attacks, exploiting previously unknown vulnerabilities in widely used corporate software or weak legacy cybersecurity protocols to encrypt critical computer systems and data across multiple victims, as well as disruptions to cloud-based services. To the extent that large numbers of people could be affected by a data breach this also opens up the potential for mass privacy claims against companies, the cost of which might fall to insurers under dedicated cyber policies and, where relevant, other third-party liability insurance policies.

A truly catastrophic event has yet to occur, but the increasingly hostile threat landscape has heightened fears about potential loss accumulations and the insurability of extreme cyber risks.

Despite the insurability challenges, there are tangible signs that re/insurers' knowledge and understanding of potential aggregate cyber losses is advancing. New approaches to modelling and quantifying catastrophic cyber risks are progressing alongside a general understanding of the factors that might lead to accumulated losses as well as those that limit extreme cyber exposure. These risk quantification efforts have been led not only by re/insurers themselves but also by a growing body of ancillary service providers including cybersecurity and risk modelling vendors, as well as academics.

The insurance industry is making progress in quantifying cyber accumulation risks, although models remain immature and their results can be volatile and inconsistent.

However, cyber models remain immature and their results can be volatile and inconsistent. Some simulations suggest a rare, industry-wide cyber incident could generate insured losses broadly comparable to some natural catastrophes, although the estimates are very sensitive to the assumptions employed. Other deterministic scenario analyses, which capture broader cyber-related claims, indicate potentially much larger catastrophic losses, with re/insurers especially alert to the sizeable threat from a malware attack that indiscriminately affects many firms or disrupts key internet architecture. On balance, this suggests caution in placing too much faith in risk metrics from any one or even multiple models. It also explains why cyber accumulation models, although widely used to inform risk assessment, are so far only partially integrated within re/insurers' underwriting and capital management.

Moreover, better risk modelling, while necessary, will likely not be sufficient to attract significant additional risk-absorbing capital. Residual cyber uncertainties remain that constrain what is knowable and can be reliably modelled, which reduce re/insurers' appetite to take on greater cyber risks. Other institutional innovations may therefore be required to foster a larger, sustainable cyber re/insurance market capable of addressing the future protection needs of policyholders. These include initiatives that:

- Capture standardised claims data and coordinate information sharing and knowledge exchange about cyber risks and exposures. This could involve increased cooperation with key stakeholders such as government security agencies and major technology companies who may have unique insights on evolving threats and vulnerabilities. A number of recent partnerships between cloud service providers and re/insurers illustrate the potential benefits of such collaboration.

- Foster mechanisms to pool cyber exposures among risk carriers as well as transfer cyber risks to capital markets through innovative instruments that match investor appetite better and allow greater transfer of peak cyber risks. Recent developments illustrate that the cyber insurance-linked securities (ILS) market, though small, is maturing and investor interest is growing.

- Create enhanced legal liability regimes to incentivise IT firms to develop secure hardware and software that are more robust to cyberattacks. Such an approach is a core pillar of the U.S. national cybersecurity strategy, which aims to reduce cyber risk and shift the consequences of poor cybersecurity away from the most vulnerable.

Improved risk modelling will help boost insurability, but other innovations will also be required to create a larger, sustainable cyber re/insurance market that meets future protection needs.

Ultimately, to address the significant cyber protection gap, government financing to backstop extreme re/insurance losses might also be needed. This could encourage and support the re/insurance sector to take on more cyber exposures, knowing that their downside losses are capped. Some commentators may be nervous about the unintended consequences of state involvement and look to the primacy of private-sector solutions, especially while the cyber insurance market is still developing. Yet with taxpayers in the end likely to be called upon to absorb a significant share of what could amount to large, uninsured losses from a cyber catastrophe, it seems only sensible to look at measures that could promote re/insurance market functioning rather than deal with the fallout in the midst of a major incident.

1 Introduction

Introduction

The potential for significant accumulated losses due to a major cybersecurity failure constrains re/insurers' capacity to absorb extreme cyber risks.

Cyber perils – malicious or accidental acts that compromise the confidentiality, availability or integrity of data or IT services – have the potential to cause harm to many people and organisations, perhaps simultaneously and across different geographies. For the most part, the resulting damage is small and contained. For example, an isolated data privacy breach is problematic for those impacted but likely has limited broader effects. However, depending on the nature of an incident – especially the number and type of targeted victims and how the breach subsequently affects other entities – cybersecurity failures could give rise to serious and widespread damage and disruption. Critical impacts can include events that completely disrupt organisations' ability to carry out their operations as well as affect the health and safety of individuals, which ultimately may lead to catastrophic losses for society, both physical and financial.[1]

This potential for significant aggregate losses is particularly problematic for insurers that assume cyber-related risks from their customers, either as part of regular property and liability policies or through dedicated cyber cover. Carriers may find that they face multiple claims from different policyholders across various lines of business, leading to major loss accumulations in their underwriting portfolios. Since re/insurers must hold capital to be able to meet unexpected claims, this serious loss potential inevitably constrains their capacity to absorb cyber risks.

Insurers' worries about potential cyber loss accumulation are not new. However, rising geopolitical tensions over recent years – most obviously, but not exclusively, illustrated by the outbreak of the Russian-Ukraine war in February 2022 – have materially worsened the cyber threat landscape. At the same time, deepening digitalisation of societies is widening the attack/vulnerability surface and increasing the cyber risk exposures of firms and individuals. If those risks crystallise, severe economic losses and insurance claims could result, not least because large loss accumulations can arise from the intended targets but also from collateral damage to other parties.

1.1 Increasingly hostile threat landscape

Overall, global cyberattacks increased by 38% in 2022 compared to 2021.[2] Ransomware, a type of malware that prevents or limits users from accessing their system or exfiltrates valuable data, has become the most significant threat to businesses, in terms of the sophistication of attacks and the damage that they cause.[3] The ransom-ware-as-a-service model has lowered the barrier to entry for would-be ransomware actors while also enabling adversaries to specialise in different stages of an attack.[4] Aside from the costs of extortion, victim firms often incur recovery/remediation expenses, legal fees and business interruption costs, as well as harm to their reputation and brand from any associated data breach.

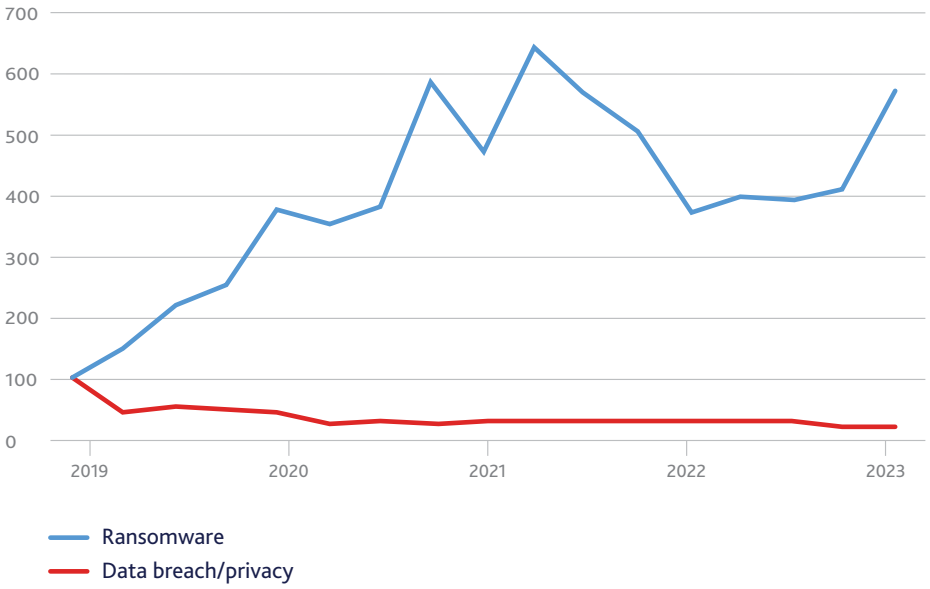
Ransomware has been a major source of cyber insurance claims over recent years and prompted a major reset in underwriting terms and conditions (see Box 1). After a decline in the frequency of attacks during the first half of 2022, in part linked to the Ukraine-Russia conflict as certain criminal gangs diverted their activities towards the war effort, ransomware activity has picked up again. In the first quarter of 2023, the number of cyber claims rose by close

1 Definitions of a catastrophic cyber incident differ depending on the scale and scope of impact considered – for example, purely financial losses, bodily injury, loss of life, impairment of business function etc. Such incidents may also arise from different sources, including an attack on or failure at a specific firm that plays a crucial role in society or disruption to multiple firms at scale at the same time. See the discussion in Tatar et al. 2023.
2 Checkpoint 2023a.
3 Checkpoint 2023b.
4 For a fuller discussion of recent ransom trends and their implications for policyholders and their re/insurers, see The Geneva Association 2022a.

to 50% and stands 473% higher than at the beginning of 2019 (Figure 1).[5] And more recent data suggests the threat from ransomware remains elevated – in six of the first seven months of 2023, the count of new victims outpaced levels during the comparable period in both 2022 and 2021.[6]

FIGURE 1: GLOBAL CYBER INCIDENT RATES

Q1 2019 = 100



Based on Aon's proprietary database of cyber and errors and omissions (E&O) insurance claims

Source: Aon[7]

Box 1: Recent developments in the cyber insurance market

Affirmative cyber insurance, either in the form of standalone policies (offering only cyber coverage) or as part of package policies (offering coverages for several classes), has expanded rapidly since it first emerged in the mid-to-late 1990s. Though still small relative to the overall commercial property and casualty (P&C) insurance market, global cyber premiums have increased more than ten-fold in the last 10 years alone to reach USD 12–14 billion in 2022.[8] The scope of cover has also broadened to include a range of financial losses connected to a cyber incident such as costs for data recovery, IT forensics, non-damage business interruption as well as liabilities for damages incurred by third parties.

For most of its three-decade life, cyber insurance was a highly profitable line. However, in 2020 and 2021, underwriting performance deteriorated significantly on the back of heightened claims activity. According to Munich Re, from the beginning of 2020 until the end of March 2023, ransomware was, by far, the leading cause of cyber insurance losses. While business and professional services accounted for the highest number of overall claims, the costliest impact was on the financial industry.[9]

Beyond elevated claims, re/insurer appetite for assuming cyber exposures has also been dented by fears about the sheer scale of losses that could arise from a cyber incident, including the potential for a single event or campaign of attacks to spread across sectors and affect multiple insureds simultaneously. This prompted a withdrawal of underwriting capacity, a sharp rise in the cost of protection and stricter contract terms and conditions.

5 Aon 2023.
6 Corvus 2023.
7 Aon 2023.
8 The U.S. accounts for the majority of cyber insurance premiums written globally although the market in Europe and Asia has reportedly also grown rapidly. See, for example, Howden 2022.
9 Munich Re 2023.

FIGURE 2: CYBER INSURANCE MARKET INDICATORS

[a] Refers to both U.S. standalone and package policies. 2022 estimate based on estimates from Aon
[b] Howden Global index (June 2014=100)

Source: The Geneva Association, based on data from NAIC, Howden and Aon

Though capacity pressures lessened through the second half of 2022 and into 2023 as underwriting profitability improved – preliminary data show a sharp fall in U.S. cyber loss ratios in 2022 – cyber insurance pricing remains higher than in earlier periods, reflecting the heightened risk environment and potential for a catastrophic incident (Figure 2). More restrictive coverage terms, including sub-limits, higher retentions, coinsurance and exclusions, have also remained prevalent, underscoring a hard reset in underwriting standards.[10]

Many insurers have also introduced cyber-specific war exclusions and tighter policy language to rule out coverage for state-sponsored cyberattacks, or at least those that lead to massive damage and financial losses. While the details of individual carriers' cyber war exclusion clauses vary and no consensus in the market has yet emerged, there are a number of common features. In particular, the new contract terms often:

- Exempt hostile cyberattacks where the perpetrators are acting under the control/direction, or at least on behalf of, a nation state.
- Set out a robust basis by which any state-backed cyberattack will be attributed to one or more nation states, and the required evidential burden of proof.
- Apply only if the attack(s) significantly impairs either the ability of a state to function or its security capabilities.[11]

Source: The Geneva Association

10 According to a recent survey of IT leaders, 74% faced increased cyber insurance premiums in 2022 while 43% saw increased deductibles and 10% saw coverage benefits reduced. See Veeam 2023.
11 For a discussion of the new war exclusions for cyber policies see Miller 2023.

So far, ransomware incidents have largely amounted to attritional rather than catastrophic losses for insurers. While the size of some ransom payments has been high, leading to an almost doubling in the average extortion payment in 2022 to USD 1.5 million, the majority of attacks involved relatively small ransoms and remediation costs.[12] However, some established ransomware gangs have begun to execute mega-scale attacks, exploiting vulnerabilities in widely used corporate software to infect multiple victims.[13] To boost their earnings, cybercriminals are targeting larger companies and making ever larger initial extortion demands, which is sustaining the upward trend in ransom payments.[14] Some experts also report a shift towards data destruction rather than solely encryption.[15] Coupled with the growing role of artificial intelligence in enabling and accelerating cyberattacks and malicious activities, this is increasing the prospects of not only more frequent but also more costly claims.

Growing AI-led capabilities of cyber adversaries and the pursuit of large-scale attacks is increasing the prospect of more frequent and costly insurance claims.

Moreover, state-sponsored attackers have increasingly been implicated in targeted and coordinated cyber intrusions, not least given the level of sophistication, capabilities and resources needed to launch and maintain such offensives. This includes ransomware gangs as well as hacktivist groups who select their targets based on nationalistic and political motivations, often with the explicit or at least tacit approval of a government. According to threat intelligence from Microsoft, nation-state actors have become more aggressive in cyberspace, even beyond the Russia-Ukraine conflict, including using cyber weapons for both disruptive and destructive purposes.[16] In 2022 alone, the number of new wiperware variants (designed to permanently erase files and immobilise computer systems) exceeded the combined number recorded throughout the previous 10 years.[17]

1.2 Large and persistent protection gap

Against that background, it is perhaps unsurprising that prudent insurance companies underwrite cyber risks with tightly defined contract wordings and limited risk-absorbing capacity. Individual policy limits – both per incident and cumulative over a policy period – on dedicated cyber insurance are low, even for large companies. And certain coverages such as business interruption may be sub-limited to a fraction of the overall total. According to the insurance brokerage firm Woodruff Sawyer, many carriers offer a maximum policy limit of USD 5 million.[18] As a result, companies often collate coverage from multiple carriers – to form a risk or loss tower – to reach their desired level of cyber insurance coverage.

Yet as firms, individuals and governments become ever more reliant on digital technology, especially the criticality of network connectivity – which has only been reinforced by the post-pandemic shift to remote working – the overall costs from a major cyber incident or campaign of attacks continue to magnify. Guesstimates of the annual cost of cybercrime range widely from around USD 1 trillion to as much as USD 8 trillion.[19] Relative to the global cyber insurance market, which is worth around USD 12–14 billion in premiums, this suggests a sizeable chunk of cyber-related losses are uninsured. Some commentators estimate an overall implied cyber protection gap of perhaps more than 99% of potential losses.[20]

Insurers are employing stricter contract wording and maintaining low policy limits, but with potential cyber exposures only set to grow, this implies a huge and persistent protection gap.

12 Sophos 2023.
13 Checkpoint 2023b.
14 If the recent resurgence in ransomware attacks continues apace, according to some commentators, ransomware could extort USD 898.6 million from victims in 2023, trailing only the USD 939.9 million extorted in 2021. See Chainalysis 2023.
15 Munich Re 2023.
16 Microsoft 2022.
17 Howden 2023.
18 Woodruff Sawyer 2023.
19 The wide dispersion in estimates for the economic costs of cybercrime reflects the breadth of costs that are included. Some studies (e.g. McAffee 2020) only consider the immediate financial costs of a cyber incident, such as damage and destruction of data and systems, ransom and extortion, business interruption, regulatory fines as well as legal defence and incident response. Other studies (e.g. Cybersecurity Ventures 2022) employ broader definitions which also include follow-on costs associated with reputational damage and lost future business opportunities.
20 See, for example, GFIA (2023), although any such point estimates must be treated with caution. Not only are the total economic costs of cyber incidents highly uncertain but publicly available data on insurance coverage against all cyber-related perils, including through traditional P&C policies, are lacking.

Even if industry predictions for continued, rapid, near-term growth in cyber insurance premiums are realised, driven by increased take-up rates and/or a further broadening of coverage rather than simply increased premium rates, it is not clear that will make a large dent in the degree of underinsurance. The frequency and severity of cyberattacks seem only likely to grow further. On some forecasts, the annual costs of cybercrime could triple by 2027, dwarfing the projected increase to over USD 33 billion in global cyber insurance premiums over the same period.[21]

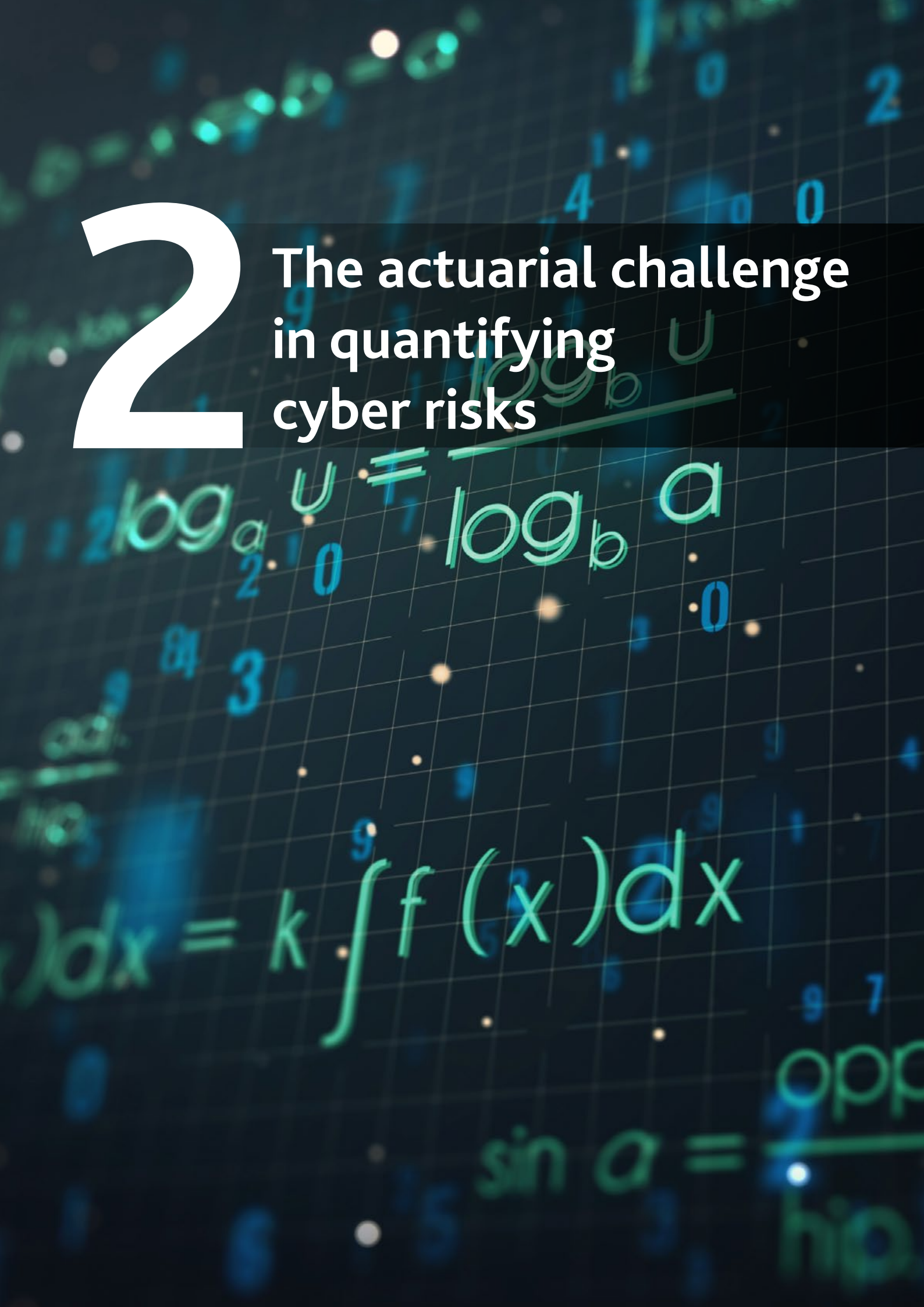
Advances in quantifying potential aggregate cyber losses will be vital in expanding cyber re/insurance capacity and helping to close the protection gap. In particular, improved ways to assess how cyber incidents could create large accumulated claims across their portfolios will help re/insurers better navigate the boundaries of insurability while also developing viable cyber risk solutions for policyholders with broader coverage and larger limits. The rest of the report therefore explores how far the re/insurance industry is getting its arms around possible cyber loss accumulations and the ongoing challenges they pose.

Narrowing this gap through enhanced cyber coverage will, at a minimum, require advances in quantifying the potential for accumulated losses across insurance portfolios.

1.3 Structure of the report

Section 2 provides some analytical context by briefly reviewing the actuarial challenges that cyber poses for conventional risk quantification. This is followed in section 3 by a discussion of the key pathways to loss accumulation. Section 4 describes the latest modelling approaches that re/insurers are developing to understand and quantify their cumulative cyber exposures. Given the residual ambiguities surrounding cyber exposures that will likely persist, section 5 considers what steps, beyond improved modelling, might be taken to progress more optimal sharing of extreme cyber risks across society. The final section offers some concluding remarks.

21 Munich Re 2023.



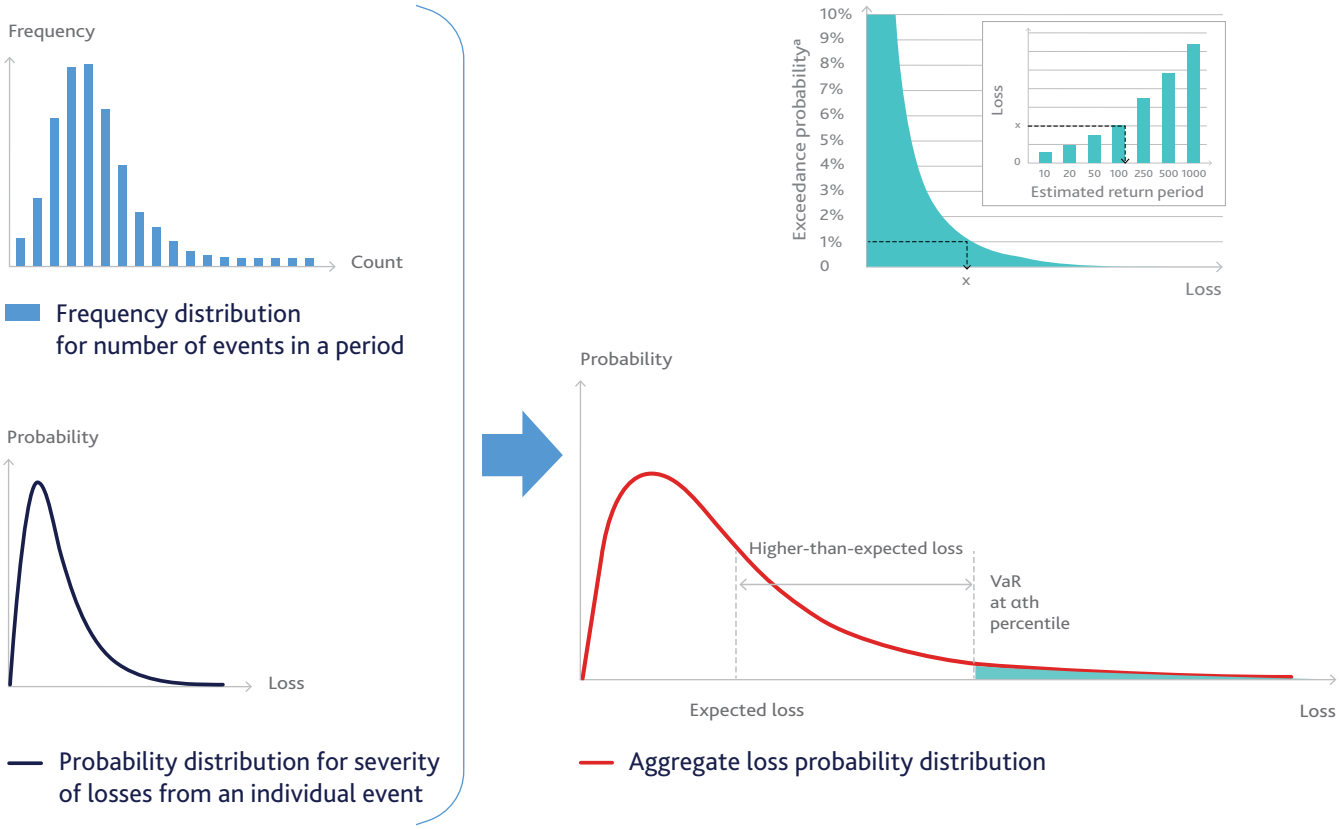
2 The actuarial challenge in quantifying cyber risks

The actuarial challenge in quantifying cyber risks

A lack of historical loss data and the dynamic nature of the cyber threat landscape mean conventional actuarial methods face significant hurdles when applied to rare and severe cyber risks.

The traditional actuarial approach to measuring risk is to use information on both the number and magnitude of past losses to infer probability distributions for the frequency and severity of future losses over a particular horizon. Combining these two distributions gives an aggregate loss probability distribution, which provides a forward-looking view of the full range of possible losses that might arise and their associated likelihood over a given period of time (Figure 3).[22]

FIGURE 3: STYLISED REPRESENTATION OF THE TRADITIONAL ACTUARIAL APPROACH TO RISK QUANTIFICATION



[a] The exceedance probability (EP) refers to the likelihood that a loss of any given size or greater will occur in a given year. A return period (r) is another way to express the annual EP probability, and describes an estimated likelihood of a loss of a given size occurring within a given time frame (i.e. r = 1/EP)

Source: The Geneva Association, based on Swiss Re and Verisk[23]

22 Deriving an aggregate loss distribution from empirical frequency and severity distributions can be generally achieved in two ways. An analytical solution may be used to calculate the compound loss distribution from the frequency and severity distributions. Alternatively, Monte Carlo techniques can be used to construct the aggregate loss distribution by simulating the many possible different combinations of loss frequencies and magnitudes. See, for example, Shevchenko 2020.

23 Swiss Re 2017; Verisk 2017.

From the estimated aggregate loss distribution, the actuary can construct various metrics about the riskiness of an insurance portfolio. For example, the value-at-risk (VaR) indicates the minimum insured loss that is likely to be met or exceeded in a given year for a given level of probability. VaRs at different assumed percentiles of the loss distribution trace out the so-called exceedance probability loss curve or, equivalently, the likely time period over which a given minimum loss amount might occur on average (i.e. the so-called return period). Armed with such information, an insurer can assess probabilistically the size of cumulative claims across its policies and compare that with its willingness and ability to bear losses that might turn out much larger than expected.

Such loss metrics are the modern-day language in which risk is typically communicated. However, these conventional actuarial methods face significant hurdles when applied to risks such as cyber. In practice, the aggregate loss distribution is often not well-defined nor reliably estimated. Consequently, calibrating risk appetite for cyber exposure is not as simple as reading off from estimated curves the level of aggregate losses that might be exceeded with a particular probability.

2.1 Lack of meaningful historical loss data

For many perils, the factors that drive claims frequency/severity are well-understood and can be modelled with standard statistical approaches. The novelty of cyber risks and the absence of an established terminology for cyber incidents, however, makes it difficult for insurers to curate a meaningful database about losses. From a statistical perspective, too, actual history is just one realisation of what might have happened. For routinely occurring cyber events, the actual history of losses is often large enough to encompass most realistic possibilities. But for rare and severe risks, relying on historical information may be misleading because it may encourage perception biases about these sorts of tail events.[24]

Moreover, even with richer and more standardised loss data, it is not clear that the past is a reliable guide to the future. Cyber risks are highly dynamic with new threat actors, attack methods and technologies coming into play, making it extremely difficult for insurers to understand and monitor exposures. This includes changes in laws and regulation that may significantly alter corporate risk management strategies and the losses insured under a policy, thus posing additional risk to insurers.[25] The potential for 'unknown-unknown' cyber threats creates significant ambiguity around the underlying sources of exposure, especially since these may be different for regular data/IT security breaches compared with business interruption events. A victim may also be compromised for an extended period of time and not even realise it – only for damage to occur suddenly and unexpectedly.

A lack of meaningful historical loss data and the dynamic nature of cyber threats make it difficult for insurers to understand and predict extreme exposures.

2.2 Anthropogenic features

The human element complicates the modelling of cyber risks, through its influence on the scope for accidental and malicious disruption both from insider and external attacks. Hackers' motivations and methods will respond to the latest security measures and their effectiveness in exploiting vulnerabilities. Low-level attacks are often not isolated events but continuous and widespread, not least because of easy access to malware via Darkweb markets and more generally the whole cybercrime-as-a-service business model. By the same token, the actions taken by firms to detect and counter threats can go a long way to thwart and mitigate the impact of cyber intrusions.

Put another way, cyber is an anthropogenic peril. Losses do not occur in a completely random fashion akin to the outcome of a game against nature in the way that, for example, air and ocean surface temperatures create conditions for weather storms. Instead, the extent of any losses depends on the interplay between the incentives, motives and resources of both victims and attackers. Even a small shift in the balance between the capabilities of hackers and cyber defences could affect the threat landscape and lead to a significant shift in the likelihood and costs of a cyber incident.[26] For instance, the success of a cyberattack in exploiting a known software vulnerability will depend not only on the actions of the hacker but also the speed and agility of users in deploying security patches.

Slight changes in hacker capabilities and cyber defences can alter the cyber threat landscape and thus the likelihood and costs of a cyber incident.

24 Woo 2021.
25 Biener et al. 2015.
26 Harvey 2016.

2.3 Complex interdependencies

Cyber risks are often highly interdependent: one compromised system may infect others both within and across firms, and perhaps across different geographies, although the degree of codependence will vary according to the type of cyber threat (Table 1). A failure of an individual computer due to a hardware problem would probably cause limited damage within the same firm. Similarly, while an insider who abuses his access privileges could affect almost all computers on the internal network and cause significant disruption within a company, the potential for compromising other firms' systems is limited. In contrast, attacks involving user interaction such as phishing or spyware/malware can lead to correlated vulnerabilities across firms if employees in many different firms are targeted. Other types of malware such as worms and viruses can self-propagate across IT networks, leading to correlated damage both within and across firms.[27]

Aggregate loss models must take adequate account of the different dependence structure in arriving at meaningful representations and quantification of cyber risks. This can be challenging, especially allowing for complex, non-linear relationships among multiple risk factors. The types of losses that can occur from a cyber incident and how they interact are also difficult to assess. They often involve intangible assets and liabilities such as data/privacy breaches, intellectual property infringements and reputational harm, the financial costs of which are hard to measure.

2.4 'Silent' cyber

Cyber perils may give rise to losses that extend well beyond the financial costs of network interruptions or data/privacy – the mainstay of dedicated cyber insurance – including physical property damage and bodily injury. A cyber event might therefore lead to multiple claims, perhaps under different insurance policies, including those for which coverage was never intended and therefore priced for (so-called non-affirmative or 'silent' cyber). Many traditional property and liability policies are written on an 'all-risks' basis and may not specifically refer to cyber-related perils.

Cyber events can lead to claims under policies for which cover was not intended and therefore priced for, which can result in coverage disputes.

Silent cyber exposure is a key reason why re/insurers have made determined efforts over recent years to tighten contract language either to expressly include or exclude coverage for cyber risks in commercial property and liability policies. Some exclusions, however, may still be loosely drafted and may not be entirely consistent across policies, creating scope for coverage disputes. For instance, some clauses refer to 'cyber events' while others refer to the use of 'software' or are limited only to 'malicious' cyber incidents. The way the terms are defined in individual contracts complicates the task of assessing potential cyber-related underwriting losses – affirmative or non-affirmative – coming from different insurance classes that may be triggered at the same time and could give rise to significant aggregate losses.

Such disputes and related litigation can lengthen the tail of cyber exposures significantly.

TABLE 1: EXAMPLES OF DIFFERENT KINDS OF CYBER RISK CORRELATION

Within-firm correlation		Across-firm correlation	
		Low	High
	Low	Hardware failure	Spyware/phishing
	High	Insider attack	Worms, viruses and Trojans

Source: The Geneva Association, based on Böhme and Kataria[28]

27 A virus is a type of malware that propagates by inserting a copy of itself into another programme and spreads from one computer to another, leaving infections as it travels. In contrast, worms are standalone software and do not require a host programme or human help to propagate. Trojans do not reproduce by infecting other files; nor do they self-replicate, unlike viruses and worms, but are spread through user interaction such as opening an email attachment or downloading and running a file from the internet. For more information, see Cisco 2018.

28 Böhme and Kataria 2006.

2.5 Reserve development risks

Compared with other commercial insurance such as general or product liability, most standalone cyber insurance policies are written either on a claims-made (for third-party liability) or on a discovery basis (for first-party losses) rather than on an occurrence basis. That is, coverage responds only for claims notified or damage discovered during the current policy period, regardless of when an attack first occurred. This reduces the scope for inadequate reserving, not least because it overcomes the potential for policyholders to combine or 'stack' limits in the event of an occurrence that spans multiple policy years.

Nonetheless, insurance actuaries must still estimate the extent of incurred-but-not-reported losses as well as adverse development on claims that are reported, which can be difficult for incidents that reveal themselves only slowly and/or hit multiple policyholders simultaneously. Further, the possibility that claims are disputed and involve protracted litigation can significantly lengthen the tail of exposures. For example, claims payments from the 2013 data breach at retailer Target that impacted approximately 40 million customers were still being made in 2019.[29] Company executives may also have to defend follow-on liability claims if they made a decision or took a course of action that breached their fiduciary duties – for example, failing to put adequate cybersecurity measures in place – which might trigger Directors and Officers (D&O) insurance.[30]

29 Breg 2023.
30 For a discussion of how cybersecurity breaches may create liability exposure, see The Geneva Association 2023.

3 Key pathways to loss accumulation

Key pathways to loss accumulation

Cyber losses can accumulate in various ways, including through failure of critical infrastructure, supply chain disruption, liability claims and vulnerabilities in widely used software.

In order to evaluate the potential for cyber losses to accumulate, re/insurers need to understand the ways in which multiple policyholders can be negatively impacted by a cyber incident and the resulting harm that might ensue, as well as which insurance policies could be affected. While hostile cyberattacks are often the most significant source of shocks, accidental (i.e. non-malicious) incidents, including system failures, human errors or programming flaws, can also trigger widespread, correlated damages.

3.1 Critical infrastructure failure

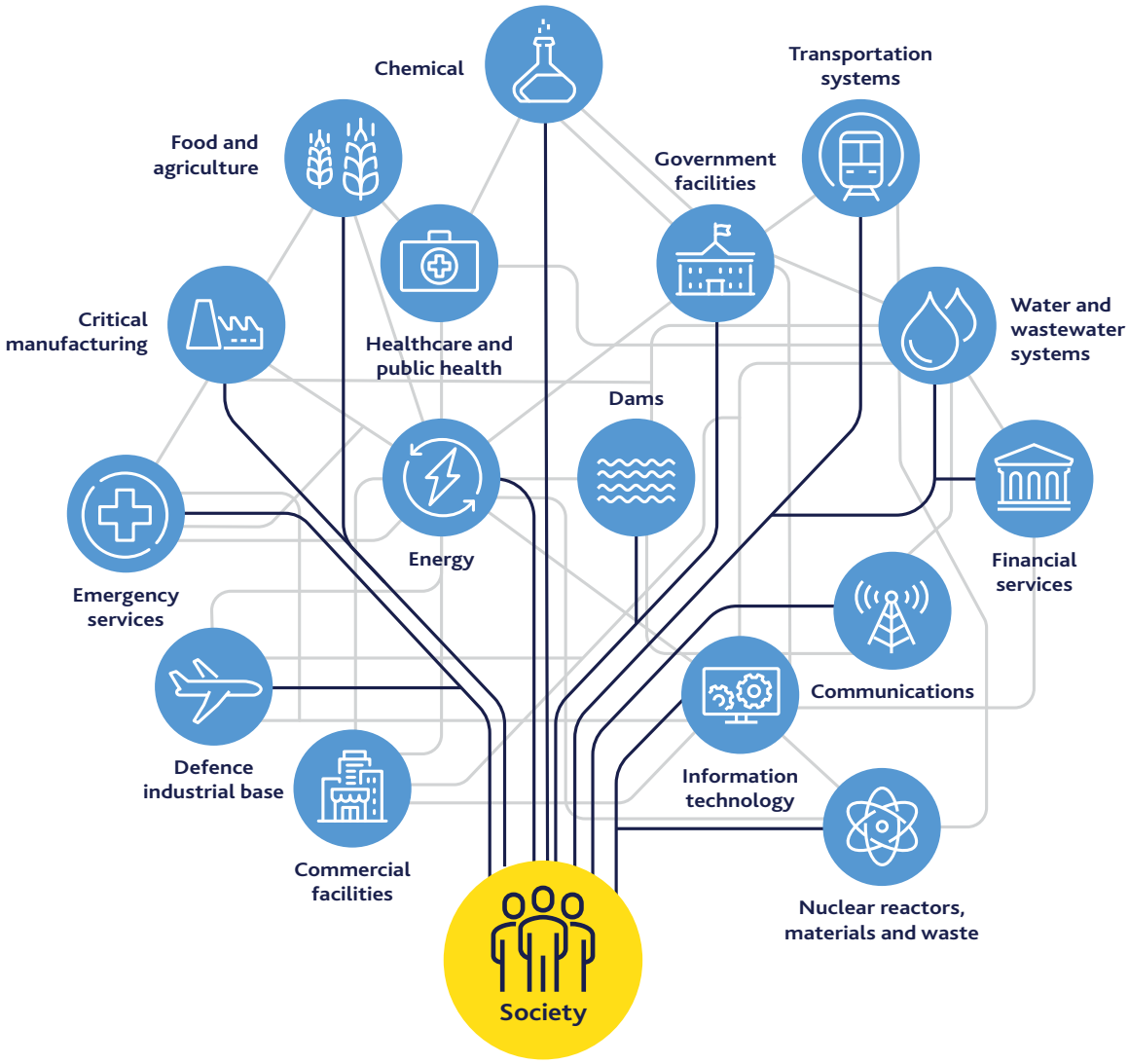
Disruption to critical infrastructure – the body of systems, networks and assets required to ensure the security of a nation, its economy, and the public's health and/or safety – is a key avenue through which losses from a cyber accident or intrusion could escalate. Such entities are increasingly connected both within and to other networks, meaning that a single point of failure could trigger widespread interruption, especially since malicious parties only need to infiltrate one connection to cause potentially massive damage (Figure 4). The shift to remote working and the use of internet-enabled sensors to relay information and perform legitimate maintenance and other actions on industrial control systems (ICS) has increased the attack surface for these companies, leaving them vulnerable to insider threats and opening up ever more opportunities for external hackers to exploit.[31]

The increasing connectedness of critical infrastructure systems means a single point of failure could trigger serious and widespread losses.

Cybercriminals, including those backed by nation states, are increasingly targeting critical infrastructure.[32] The majority of these assaults has been in the form of ransomware, often exploiting weak legacy cybersecurity protocols to encrypt critical computer systems and data across IT networks. However, commentators also highlight a worldwide, sharp pick-up in 2022 in cyberattacks with physical consequences on operational technology (OT) within key ICS.[33] This marks an important departure from the previous decade, where reported attacks were largely aimed at espionage. Several near-misses in core utilities like power and water occurred in 2022, where the ramifications could have been much more serious if the circumstances had been slightly different. Most notably, Ukrainian officials reported in April that they had thwarted a Russian cyberattack on Ukraine's power grid.[34]

31 For a non-technical discussion of the cyber threats and vulnerabilities facing critical infrastructure, see Confederation of European Security Services 2023.
32 According to Microsoft, the proportion of nation-state attacks – i.e., those with technological, financial or other support from a sovereign state – against critical infrastructure doubled from 20% to 40% between July 2021 and June 2022. See Microsoft 2022.
33 Waterfall/ICSSTRIVE state that there were 57 reported cyberattacks with physical consequences to OT in discrete manufacturing and process industries worldwide in 2022, an increase of more than 150% over the preceding year. See Waterfall 2023.
34 Waterfall 2023.

FIGURE 4: CONNECTIVITY ACROSS CRITICAL INFRASTRUCTURE SECTORS



Source: Gartner[35]

As explained in Box 2, not all losses arising from the failure of critical infrastructure can be insured. Standalone cyber insurance typically excludes losses incurred by firms due to the disruption of key utilities or organisations vital to the functioning of the financial sector or the internet. Such policies will usually extend cover for claims resulting from temporary outages to key internet-dependent services such as a cloud service provider (CSP), which are becoming ever more crucial as businesses migrate their core operations to the cloud. Given the potential for a single outage to trigger widespread disruption, however, coverage typically applies only after a minimum downtime and for proven profit shortfalls or loss mitigation expenses. Parametric insurance solutions have therefore emerged – from both incumbent insurers and start-ups – to offer additional, complementary cover against disruption costs arising from internet outages.[36]

35 Gartner 2022.

36 For example, backed by Lloyd's of London underwriters, Parametrix offers insurance for IT downtime and business interruption based on agreed parameters for cloud outages, network failures, third-party system crashes and other hazards which exceed pre-agreed thresholds. See Cohen 2020.

Box 2: Critical infrastructure and cyber insurance

Most cyber insurance policies will reimburse policyholders for financial losses incurred as a direct result of an incident, as well as legal costs stemming from third-party claims, including any compensation damages. However, it is common practice to exclude from standalone policies costs arising from the failures of major critical infrastructure, except for the first-party financial losses of a policyholder who is the provider of infrastructure services.[37]

Critical infrastructure is not universally defined and the scope of coverage will vary depending on the precise policy terms. At a minimum, cyber insurance will exclude losses resulting from disruptions in vital utilities such as power, water and telecommunications, at least where such essential services are not under the control, operation or ownership of the insured. Policy exclusions will also usually extend to the architecture behind the internet, including domain name system (DNS) service providers and trust service providers/certificate authorities, without which online networks could not function. Likewise, coverage will sometimes be excluded for disruption to core entities that facilitate financial markets and securities trading.

As a general rule, dedicated cyber insurance policies exclude both bodily injury and property damage. Any cyberattack or cyber-related incident that causes physical damage to critical infrastructure would therefore not be covered, even for the infrastructure provider, although it might be under traditional P&C policies (depending on any cyber exclusion wording). Financial losses incurred by third-party users of certain key digital services are nonetheless typically insurable. For instance, policies often provide affirmative coverage in the event of a temporary, isolated interruption to key internet-dependent entities such as Internet Service Providers (ISPs), which facilitate access to the World Wide Web, or CSPs (e.g. Google Cloud or Amazon Web Services (AWS)), albeit coverage will usually respond after a minimum waiting period and for provable costs.[38]

Source: The Geneva Association

To the extent that a cyber incident at a major critical infrastructure provider caused material physical damage and/or operational disruption, this might also prompt substantial claims under traditional P&C policies, at least where such affirmative cover is provided. A ransomware attack on a hospital's network, for example, may threaten the lives of patients by interrupting critical medical treatments, which could trigger liability claims.[39] Recent incidents suggest that even an isolated cyberattack can have ripple effects that impact healthcare delivery across an entire region, significantly increasing the number of victims.[40]

3.2 Supply chain disruption

Catastrophic cyber incidents can arise not only from failure of critical infrastructure. Structural features in the way business activity is organised allow a cybersecurity breach or accident at a single firm to propagate widely. Production supply chains increasingly rely on third-party organisations that deliver not only physical inputs but also digital services. In particular, so-called managed service providers (MSPs) typically provide a portfolio of IT services to business customers including software engineering, data storage, network security and disaster recovery management.[41]

The adoption of managed services can be an efficient and cost-effective way to stay up to date with rapid technological change, access in-demand skills or expertise, and have flexible, scalable and high-quality IT services. This is especially true for small and medium-sized enterprises (SMEs) who may not have the in-house resources or expertise. However, the firm's data and files can be compromised via the hacking of a third-party supplier with legitimate access to multiple customers' systems.[42] According to Verizon, 62% of system intrusion incidents recorded in 2021 came through an organisation's partner.[43]

37 According to a recent survey by the European Union Agency for Cybersecurity (ENISA), however, 74% of Operators of Essential Services (OES) do not have a dedicated cyber insurance policy while more than half do not have cyber coverage within their other insurance policies. See ENISA 2023.
38 Beazley 2023.
39 Lloyd's 2022.
40 One recent study investigated the fallout from a ransomware attack on a single hospital in 2021 and found that emergency rooms at adjacent hospitals had more ambulances arrive, saw more patients than normal and had longer wait times for all patients seeking care. See Darneff 2023.
41 For a fuller discussion of the role of MSPs see Acronis 2022.
42 Digital supply chain attacks amplify the impact of cyberattacks in at least two ways. First, by compromising a common supplier, the attacker has the opportunity to impact many companies at once. Second, they enable so-called 'backdoor' attacks, where cybercriminals target vendor companies as a way to infiltrate other, often larger, organisations. See Morot and Héon 2022.
43 Verizon 2022.

Firms that adopt managed IT services may increase their vulnerability to attack via the hacking of a third-party supplier that has access to their systems.

Over recent years, third-party software vendors have been a favoured exploit of cyber adversaries. Recent prominent attacks include:

- SolarWinds (December 2020) – Suspected nation-state hackers targeted SolarWinds, a major software company that provides network management tools. By planting malicious code into regular software updates, the attackers were able to gain access to the data and networks of thousands of SolarWind's customers and partners, including U.S. government agencies.[44]
- Kayesa (July 2021) – A criminal group exploited a vulnerability in Kayesa's Virtual System Administrator software used to distribute ransomware to various MSPs and their clients. This resulted in significant disruptions and financial losses for as many as 2,000 businesses across 17 countries.[45]
- 3CX (March 2023) – An employee of desktop phone developer 3CX inadvertently downloaded malware via the X_Trader app maintained by the financial software firm Trading Technologies, which itself had earlier been hacked. The infected app allowed the hackers to corrupt a 3CX installer application, thereby spreading malware to a broad swath of its customers.[46]
- MOVEit (May 2023) – A mass hack breached Progress Software's MOVEit file transfer app, which is used to move sensitive files such as employee addresses or bank accounts. The attack has thus far impacted more than 2,000 organisations, breaching data from over 60 million individuals worldwide.[47]

Financial losses arising from cyber intrusions at third-party providers – for example, lost business income or remediation expenses incurred to deal with the contagion as well as follow-on liability to customers or vendors impacted by an incident – are usually covered in cyber as well as specific non-damage business interruption insurance policies. However, the scope of coverage varies depending on specific restrictions/exclusions and policy limits. This often reflects the challenges insurers face in gaining a comprehensive overview of the supply and service chains and the potential spillover effects from a disruption to a particular entity.

The scope of coverage for business interruption losses from cyberattacks at third-party vendors varies across policies.

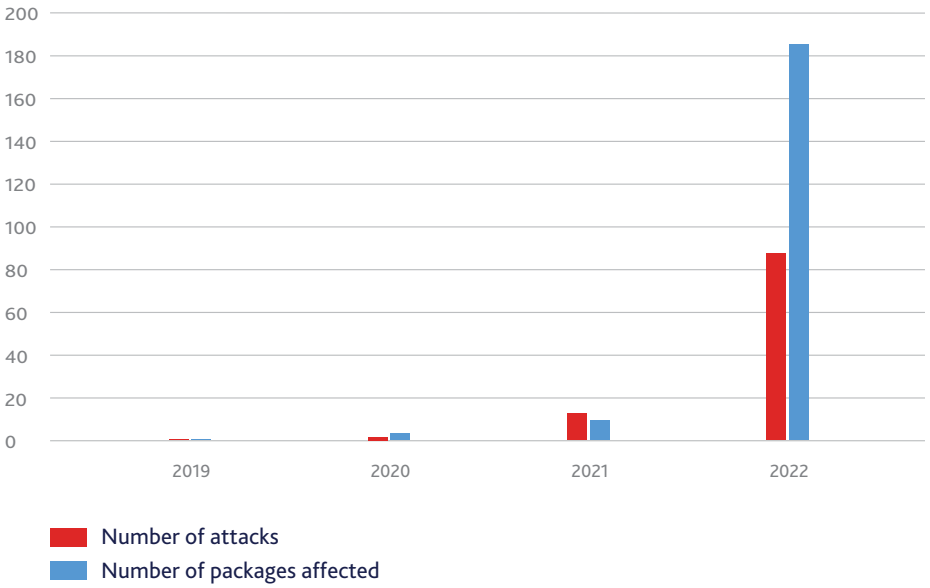
3.3 Zero-day and open-source software vulnerabilities

The nature of software and hardware development in modern economies means that bugs or flaws almost inevitably occur and are unwittingly built into distributed products. Such zero-day vulnerabilities – so called because they are unknown to the manufacturer or vendor at the time the software/hardware is released – can exist for months and sometimes years before being detected. During that time, attackers may steal or copy data and/or damage sensitive systems until a programme fix or security patch is implemented. Since many organisations tend to use similar software, security programmes and other IT infrastructure, multiple organisations are often vulnerable to the same successful zero-day attack.

Multiple organisations are often exposed to common zero-day (i.e. unknown) vulnerabilities as they use the same or similar software provided by third parties.

44 Oladimeji and Kerner 2023.
45 Kost 2023.
46 Greenberg 2023.
47 Simas 2023.

FIGURE 5: SOFTWARE SUPPLY CHAIN ATTACKS



Source: Comparitech and Sonatype[48]

It is not just contaminated proprietary software provided by third-party providers that can trigger widespread cyber-related losses. Firms, including MSPs themselves, tend to rely on open-source software (OSS) in developing their own IT solutions.[49] Indeed, a whole software supply chain model has emerged composed of libraries, tools and processes used to develop, build and disseminate software. This empowers developers to make use of their preferred tools and ship functional software quickly, but it also exposes organisations and their customers to vulnerabilities introduced by changes outside of their direct control.[50]

According to commentators, software supply chain attacks have exploded over the past couple of years as bad actors have targeted OSS ecosystems (Figure 5).[51] While OSS may be no more intrinsically error-prone than other computer code, the distributed development model brings new operational risks.[52] One study found that in 2022, nearly two thirds (63%) of the source-code repositories contained unpatched vulnerabilities rated high or critical, with 51% of those at least two years old.[53] Another investigation uncovered that 95% of all OSS vulnerabilities were not expressly implemented by developers, but indirectly and automatically incorporated through existing software packages.[54]

Perhaps the most high-profile recent OSS vulnerability relates to the bug, known as Log4Shell, which in late 2021 was found in the open-source logging library Log4j commonly used by apps and services across the internet. If left unfixed, attackers can exploit the bug to break into systems, steal passwords and logins, extract data, and infect networks with malware. Fortunately, many users quickly reacted to news about Log4jShell and downloaded a patched version of the software within a few weeks. Security experts highlight, however, that about 25–30% of the world is still using the vulnerable versions of Log4j – perhaps because they have no idea whether Log4j is part of their software supply chain – and so could yet be exploited by associated malicious attacks.[55]

Attacks on open-source software can also trigger widespread cyber-related losses and have spiked sharply in recent years.

48 See comparitech's worldwide software supply chain attacks tracker and Sonatype 2022.
49 A survey by the Linux Foundation found that 98% of organisations surveyed use OSS. See Linux Foundation 2022.
50 Schmitt 2023.
51 According to one study, on their current trajectory, cyberattacks on software supply chains will cost the world economy an estimated USD 80.6 billion in lost revenue and damages annually by 2026. See Juniper Research 2023.
52 Distribution often occurs through software updates, ultimately giving the attacker access to protected networks, user accounts or sensitive information. See Hell (n.d).
53 Hill 2023.
54 Endor Labs 2022.
55 Fox 2023.

3.4 Mass liability claims

The bulk of cyber insurance claims over recent years have been first-party losses such as business interruption and remediation expenses. However, almost any cyber incident can lead to claims for compensation from affected customers, suppliers and other stakeholders whose data may have been compromised. Moreover, the large numbers of people affected by a common data breach opens up the potential for mass privacy claims, the cost of which might fall to insurers not only under dedicated cyber policies but also, where relevant, other third-party liability insurance policies.

Common data breaches affect large numbers of people and can thus trigger mass privacy claims. The costs may fall to insurers under cyber as well as third-party liability insurance policies.

The frequency and scale of liability claims are likely to be boosted by increased regulatory oversight and stricter cybersecurity governance requirements. Data breach and privacy regulations continue to expand, following the introduction of tough rules in Europe under the General Data Protection Regulation (GDPR) and more stringent regulations in places such as California, Brazil, China and India. This includes in some jurisdictions potential collective consumer actions on an 'opt-out' basis – where the action is brought on behalf of every individual falling within a class unless they expressly opt out – which expands the pool of claimants and potentially the size of settlements.[56]

Jurisprudence is also developing which could catalyse civil litigation for data breach claims, including through class actions. In some jurisdictions, firms could face lawsuits even if plaintiffs suffer no concrete harm but the incident substantially increases the risk of future ID theft or other harm.[57] The latest revelations over the use of pixel tracking technology (sometimes called web beacons) on company websites, which resulted in the unauthorised collection and sharing of users' private and personal information, only underscore the potential third-party cyber liability exposure connected to privacy breaches.[58]

3.5 Disaggregating factors – Important caveats

Alongside ways in which cyber-related insurance losses accumulate, there may be important factors that limit the potential for aggregation. Perhaps most obviously, many firms invest in cybersecurity to protect themselves and prevent any escalation in losses. This may include reducing reliance on any single vendor or at least having back-up procedures in place. According to one survey, for instance, 87% of firms globally adopt a multi-cloud strategy, with more than half making use of multiple public CSPs.[59]

Insurers can encourage good cyber hygiene among their policyholders via their underwriting practices as well as the terms and conditions of coverage.[60] Likewise, governments through their law enforcement and national security agencies deploy diplomatic and technical resources to pursue cybercriminals, disrupt their business models and limit the spread of attacks, through, for example, sharing ransomware encryption keys.

Within the IT sector, too, structural mechanisms can work to mitigate cyber threats and localise any disruptive threats. Major CSPs invest heavily to maintain their reliability and resilience, including segmenting their services to prevent a failure of one element spilling over to another. CSPs – at least the top tier firms who collectively account for a large market share – usually organise their cloud infrastructure into different geographical regions, known as cloud regions, each of which has multiple availability zones (AZs) hosting one or more data centres.[61] This physical separation should in principle ensure that a failure or disruption in one AZ does not impact the availability or performance of other AZs in the region, although spillover effects cannot be ruled out entirely.[62] Technology vendors also proactively seek to identify and remedy vulnerabilities before they are exploited, including using internet connectivity to distribute protective software code quickly, disable malware and implement security patches.

There may be important factors that limit the potential for loss aggregation by reducing the geographical and sectoral footprint of a cyber incident.

56 In April 2022, the EU Court of Justice ruled that consumer groups can autonomously bring legal proceedings for alleged breaches of data protection rules as long as national law allows it. See Bertuzzi 2022.
57 Dempsey 2022.
58 Numerous class action lawsuits alleging improper tracking and sharing of website users' data have been filed against many companies, especially healthcare organisations and video content providers. See Breg 2023.
59 Flexera 2023.
60 In the wake of the ransomware outbreak, many insurers required policyholders to tighten cybersecurity protocols as a condition of coverage, especially around user authentication and access privilege rights of MSPs.
61 According to one recent study, the top three CSPs account for 66% of the worldwide market for cloud infrastructure. The dominance of the major cloud providers is even more pronounced with public cloud services, where the top three account for 73% of the market. See Synergy 2023.
62 Zhang 2023.

These disaggregating factors, collectively and individually, can work to reduce the geographical and sectoral footprint of a cyber incident as well as lower the associated interruption costs or damage to assets. Indeed, they were probably influential in limiting the scale of impact of recent major cyber events such as SolarWinds and the Log4j vulnerability.[63] Equally, past near misses illustrate that good fortune also often plays a part in the overall loss impact, underlining the empirical challenges in assessing and calibrating the pathways through which catastrophic cyber losses can occur.[64]

63 For example, estimated insured losses from the SolarWinds attack amounted to only USD 90 million, even though 18,000 companies may have been affected by the malware. See discussion in Shah 2021 and Gallagher Re 2022a.

64 For example, in May 2017 the fortuitous discovery of a 'kill switch' ended the self-propagating nature of the Wannacry ransomware (see MalwareTech 2017). Later that year, the NotPetya attack impacted only a small number of multinational companies, in part due to an accidental calendar mismatch with a government deadline for tax filing in Ukraine where the malware was first deployed. By another stroke of luck, one of the main affected firms, Maersk, was able to restore its systems from a subsidiary that was offline at the time of the initial intrusion. See Box 2 in The Geneva Association 2022b.

4 Latest advances in accumulation risk assessment

Latest advances in accumulation risk assessment

Re/insurers' ability to assess and model cyber risks is advancing, and will likely only improve as time goes on. However, not all of the uncertainty around future losses can be resolved with more information, enhanced knowledge and better modelling.

Despite the relative immaturity of cyber as a peril and associated insurance solutions, incremental progress has been made in better understanding and modelling the emerging risk.[65] In general, the latest initiatives seek to combine forensic data about threats and vulnerabilities with cyber domain expertise and advanced risk analytic frameworks in order to craft metrics of potential cyber losses. In doing so, they aim to address, although they do not entirely overcome, some of the empirical actuarial challenges outlined above. These risk quantification efforts have been led not only by re/insurers themselves but also by a growing body of ancillary service providers, including cybersecurity and risk modelling vendors, as well as academics.

4.1 Innovations in data capture and analytics

Early cyber models had to be built almost entirely on expert judgement, conjecture and speculation due to a scarcity of data and an incomplete understanding of the risk.[66] Knowledge gaps still persist, especially when the root cause of any loss is hard to establish and/or third-party involvement (i.e. incident response firms, lawyers etc.) in responding to claims can complicate information sharing with insurers. But more and better quality data and insights can now be gathered from a variety of sources that together help build a picture of the cyber risk landscape. This includes information about the different threat actors, their resources, motivations and habits that can throw light not only on the prospects of attacks but also the potential for multiple victims and the severity of incidents.

Better quality data and analytics are enabling a more detailed picture of the cyber risk landscape, as well as firms' cybersecurity postures.

Three key types of information play an important role in contemporary cyber threat assessment:

- **Historical incidents.** Although inevitably incomplete and subject to potential bias – not least because firms may have incentives not to reveal they have been breached, perhaps on account of reputational or legal concerns – the anatomy of past cyber incidents can still be useful. Correlating historic data across attacks helps identify patterns, detect intrusions and reduce potential risks.[67]

- **Firmographics.** Information about an entity such as its size, industry location and organisational structure may provide pointers as to its possible cybersecurity vulnerabilities and corporate linkages that might widen the footprint of an incident. For example, firmographic data can sometimes inform about the potential spread of a zero-day vulnerability within a particular piece of hardware or software.

- **Technographics.** These data provide information about the cybersecurity stance and posture of an organisation and come in two main flavours: inside-out and outside-in.

  - Inside-out data document the hardware and software that companies use to operate their business, including their reliance on MSPs. With a company's consent, data can be collected by an application or device installed on the firm's network to provide continuous monitoring of its digital infrastructure.

  - Outside-in data refers to information about a company's externally facing IT infrastructure which can be scanned 'from the outside'. These data are often gathered by specialised technology firms with the goal to detect, for example, potential openings for attackers such as open Remote Desktop

65 For an early review of cyber risk modelling advances, see The Geneva Association 2018.
66 Gallagher Re 2022c.
67 Stransky 2021.

Protocol (RDP) ports, unpatched vulnerabilities and poorly configured web services.[68] This may include building 'honeypots' to lure hackers and extract information on their strategies and possible weaknesses in cybersecurity.[69]

Some vendors combine past incident data, firmographics and outside-in technographic data to develop cybersecurity ratings for individual companies. These ratings help re/insurers in screening insureds and in assessing the overall risk profile of their cyber insurance portfolios, including the potential for common vulnerabilities and contagion. Similarly, defensive AI/machine learning algorithms can help spot and alert users to suspicious behaviour and even highlight ways to prevent intrusions from happening in the first place.[70]

4.2 Probabilistic models

Even with richer data and analytics, re/insurers still need ways to convert those insights into quantifiable indicators that provide a guide to both the scale and likelihood of future cyber losses. Nascent actuarial approaches differ, but often amount to variations and combinations of three main types: extended frequency-severity models, network propagation models and expert-led scenario analysis.

New actuarial techniques seek to combine forensic data with cyber domain expertise and advanced risk analytic frameworks in order to craft probabilistic models of extreme cyber losses.

Extended frequency-severity models

Based on actual claims data, actuaries use regression analysis to fit standard statistical distributions for the frequency and severity of cyber incidents based on observable data such as firm size, industrial sector and cybersecurity maturity. Importantly, compared with traditional approaches such models make allowance for more complex dependence structures between the incidents. This includes correlation across sources of loss (e.g. business interruption and data privacy breaches), between affected policyholders (e.g. due to commonly used software, such as Windows or MacOS) and between the severity of damage (e.g. due to commonly used IT security measures).[71]

A major obstacle with such models stems from having to extrapolate from actual claims the full extent of possible cyber losses. The estimated parameters are not always robust (or at least are subject to considerable uncertainty) and the implied overall loss distributions may not be well defined.[72]

Some models look to inform about tail risks by extrapolating from historical claims frequency and severity data, although implied loss distributions may not always be well defined.

Network propagation models

Borrowing from the epidemiological literature on the spread of infectious diseases, these models investigate the extent to which cyber 'infections' can spread via entities' physical or social interactions in a network. The typical cyber context is the propagation of malware across IT systems or devices, but contagion may arise from the breaking of supply chains and subsequent escalation in business interruption.

As well as the topology of how firms are linked, network models also rely on processes that capture how contagion occurs.[73] The extent of any disruption will depend, for example, on whether a firm that is suddenly hit has adequate measures in place (e.g. up-to-date software patches or the ability to switch suppliers) to stop the disruption spreading further. Some modellers also allow for behavioural shifts by individual actors (both attackers and defenders) that influence the likelihood of attacks or how firms decide to interact.[74]

A number of studies have demonstrated that network-based approaches can generate improved estimates for the frequency and dependence of cyber threats compared with standard actuarial approaches.[75] However, such models are often computationally challenging to implement and parameterise reliably.

68 Gallagher Re 2022b.
69 Crowdstrike 2022.
70 For a review of the application of AI and machine learning in cybersecurity, see Daryanani 2023.
71 Awiszus et al. 2023.
72 For example, in some studies that deploy extreme value theory (EVT) methods to extrapolate for missing data, the mean and/or variance of the aggregate loss distribution may not be computable, inhibiting statistical inference. See Dacorogna et al. (2023) for a discussion of empirical EVT studies applied to cyber.
73 Such models were widely used by policymakers to analyse the spread of the COVID-19 pandemic. Specifically, versions of the Susceptible - Infected - Recovered (SIR) model were deployed to split the population into three groups: the number of susceptible individuals that could be infected, the number of infected people that could spread infections and the number who recovered from infection.
74 See, for example, Benomar et al. 2022.
75 See, for example, Hillairet et al. 2022.

Others apply formal models used for infectious diseases to understand how cyber losses can spread. While sometimes offering improved predictive accuracy, these models can be challenging to implement.

Expert-led scenario analysis

In the absence of historical data about extreme cyber incidents, re/insurers often turn to the knowledge of experts, both within their organisations and outside, to help calibrate their cyber risk models. Specifically, cyber scenarios are posited and expert judgement is used to inform about the probability and impact of particular disturbances. Rather than modelling individual events, sometimes events are grouped together into event families; for example, the failure and/or outage of a CSP regardless of the precise reason for the interruption.

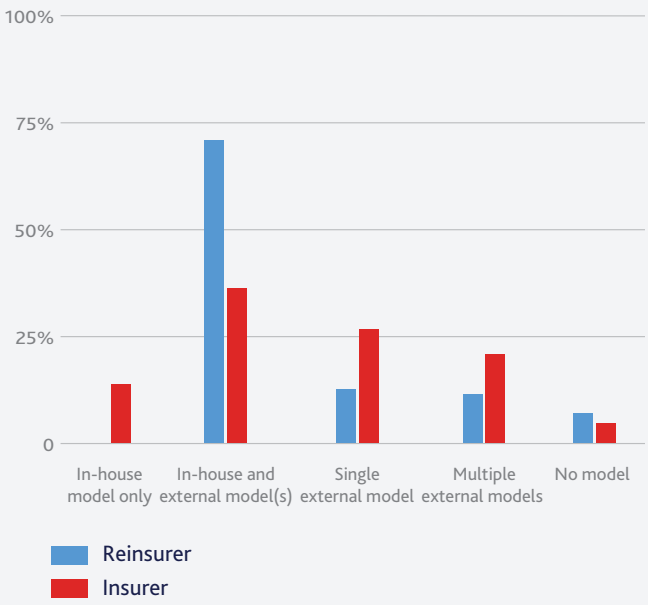
Such expert-led scenario approaches are the mainstay of a small but influential group of specialist cyber modelling firms that have developed over recent years. Leveraging experience in modelling losses for other extreme perils, most notably natural catastrophes such as hurricanes and earthquakes, combined with detailed cybersecurity intelligence, these vendors construct risk metrics for multiple adverse scenarios. Many cyber re/insurers use these vendors' models to assess exposures within their underwriting portfolios (at least for cyber insurance), sometimes as a complement to their own in-house models (see Box 3).

Expert-led scenario analysis, which integrates the knowledge of experts within regular statistical frameworks, is the favoured approach among insurance practitioners and specialist cyber modelling firms.

Box 3: Re/insurers' use of cyber accumulation models

As the cyber insurance market has grown and matured, underwriting practices for managing accumulation risks have evolved. Many re/insurers now use formal models to support their assessment of cyber risks and help steer their exposure management. Primary insurers tend to rely more on external vendors than re/insurers, who have their own in-house models (Figure 6). This includes comparing insights from multiple external models, although in practice different model setups make that challenging, while strict licencing arrangements mean it can become prohibitively expensive.

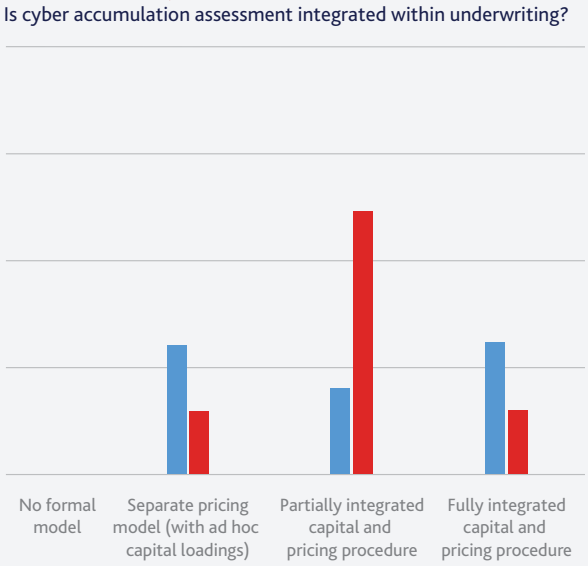
FIGURE 6: USE OF CYBER RISK MODELS BY RE/INSURERS (% OF FIRMS)



Based on 52 re/insurers who have in-house or licence external models, weighted by cyber insurance premiums

Source: The Geneva Association, based on data from Gallagher Re

FIGURE 7: ROLE OF CYBER MODELS IN UNDERWRITING (% OF RESPONDENT RE/INSURERS)



Based on a poll of 11 GA member cyber re/insurers, weighted by relative size of cyber insurance premiums

Source: The Geneva Association

Despite progress in modelling extreme cyber risks, cyber accumulation issues are not fully integrated within re/insurers' underwriting procedures and capital management. According to a poll of 11 GA member firms – which account for around 35% of global cyber re/insurance premiums – most re/insurers rely on ad hoc or partial methods to account for aggregate exposures (across insureds, regions, lines of business etc.) in their pricing/costing of cyber risks and allocation of capital (Figure 7). Of the surveyed re/insurers, more than three quarters employ deterministic or partially probabilistic scenarios – whereby expert judgement is applied to benchmark the return period on associated projected losses – in order to calibrate their risk appetite for cyber exposures.

Source: The Geneva Association

Given the bespoke features of vendors' scenario frameworks and calibrations, it is not straightforward to compare results across models, especially isolating the crucial assumptions underpinning loss estimates. To the extent that a meaningful comparison can be made, one recent analysis, based on a synthetic market-wide portfolio of cyber insurance policies, indicated a 1-in-200 year global industry event loss in the range of USD 15.6–33.4 billion (Table 2).[76] Unsurprisingly, the bulk of those projected claims arise from U.S. risks given the size of the U.S. cyber insurance market relative to other regions.

The variation in methods used to predict extreme cyber losses makes comparing the results from different empirical models difficult.

At face value, such peak losses appear well below estimates of the insurance sector's aggregate cyber exposure limit.[77] Though material, they would be also comparable with insured losses from some natural catastrophes and, in fact, much less than recent extreme weather events. For instance, industry estimates put insurance sector losses from Hurricane Ian in 2022 at USD 50–65 billion.[78] However, the projected peak losses are highly sensitive to the assumptions and judgement applied, especially about the pathways to aggregation such as the use of common technologies and suppliers as well as variations in scope of insurance coverage. They also do not capture the full extent of claims from non-cyber insurance policies.

TABLE 2: POTENTIAL LOSSES FROM AN INDUSTRY-WIDE CYBER EVENT, FROM DIFFERENT CYBER MODEL VENDORS (USD BILLION)

Return period	CyberCube	Guidewire-Cyence	Moody's RMS
Global			
1-in-50 years	24	10	6
1-in-200 years	33	26	16
U.S.			
1-in-50 years	17	7	4
1-in-200 years	23	18	10

Source: Guy Carpenter[79]

76 Broadly similar risk metrics for the tail of the industry-wide cyber loss probability distribution are reported by specialist cyber insurer Coalition, albeit focused solely on the U.S. Specifically, by extrapolating simulations from a representative sample of cyber insurance policies to approximate potential insured losses across the U.S. economy as a whole, Coalition's analysis suggests a 1-in-250 year estimated loss of around USD 30 billion. See Coalition 2023.

77 Data on re/insurers' overall cyber exposure limits are not publicly available. But bottom-up analysis based on discussions with individual re/insurers suggests an industry-wide limit of somewhere in the region of USD 360–500 billion across both packaged and standalone policies. See Johansmeyer 2023.

78 Figures from Reinsurance News (n.d.).

79 Guy Carpenter 2023.

On some estimates, projected peak cyber losses may be similar to those from a major natural catastrophe, but the results are highly sensitive to the assumptions and judgement applied.

Underscoring the sensitivity point, some model vendors highlight that counterfactual analyses of recent cyber events suggest far larger losses are plausible and a major cyberattack could be much more damaging than anything seen to date. If, for example, the threat actors behind the SolarWinds compromise had focused on sabotage rather than espionage, the outcome would have been materially different. Similarly, the 2017 NotPetya attack – the largest cyber insurance loss event recorded so far – could have been much worse if the attackers had exploited a zero-day vulnerability for which no patch was readily available.[80]

Even if such conjectures can help assess the extra loss severity, attaching a probability to alternative outcomes is difficult. More broadly, as discussed in Box 4, the immaturity of cyber models suggests caution in placing too much faith in risk metrics from any one or even multiple models. We have yet to witness a cyber incident generating extreme insurance losses – NotPetya being the arguable exception and even then, losses largely hit traditional P&C rather than cyber policies.[81] It is therefore impossible to validate the accuracy of both in-house and external vendor models.

Box 4: Challenges of validating cyber catastrophe models

Experience with other nascent lines of business suggests that credible risk quantification is vital to achieving sustainable growth and cyber insurance is no different. Formal cyber risk models have therefore been developed by both re/insurers and specialist analytics vendors. Such cyber models have often gone through rapid updates, improving and rebuilding to reflect the evolving threat landscape, understanding of the risk as well as the coverages offered by insurers.

Although models are used to inform accumulation risk management and they rarely dictate pricing, some re/insurers are beginning, or at least are considering, to incorporate model outputs into their economic and regulatory capital setting. Unfortunately, most statistical validation tools are ineffective or unsuitable due to the lack of historical catastrophic events to use as test data, unpredictable threat actor behaviour and the oftentimes rapidly changing nature of cyber risks. Evaluation of cyber models, whereby re/insurers assess the suitability of a model by comparing the outputs against their own view of the risk, is somewhat more achievable. But comparison of outputs across external vendors can be frustrated by differing model specifications and the prevalent use of subjective expert judgement.

Variations in model methodologies

Unlike modelling natural catastrophes, where empirical frameworks have mostly converged over time, there are large variations in the methods used to quantify cyber risk. Among the main external vendors' models, the key differences relate to:

- **Event simulation.** Some cyber model vendors rely on standard statistical methods to describe the frequency of future attacks, while others appeal to causal analyses. The latter seek to replicate each stage of a cyber event from infiltration, defence through to loss, in order to simulate how attacks might unfold.
- **Scenario definition.** The sequence of events that make up a scenario typically detail the type of attack, how it propagates across companies and its impact. Modelled incidents often include ransomware, service-provider outage or a data breach, although these may not necessarily be distinct events. For instance, a ransomware attack on a service provider may also involve a data breach, so considered scenarios can vary significantly.
- **Coverage and loss components.** Cyber policies differ widely in terms of coverage. Vendors have to decide the scope of losses they model and the different cost elements included under each coverage, which can differ markedly.[82]
- **Utilisation of technographic data.** Most model vendors use technographic data from outside-in scanning exercises to parameterise their models but the approaches vary in sophistication. The more technical methods seek to match technographic data against companies within their portfolio, but potential errors in matching processes mean this does not always translate into improved model reliability.

80 CyberCube 2023.

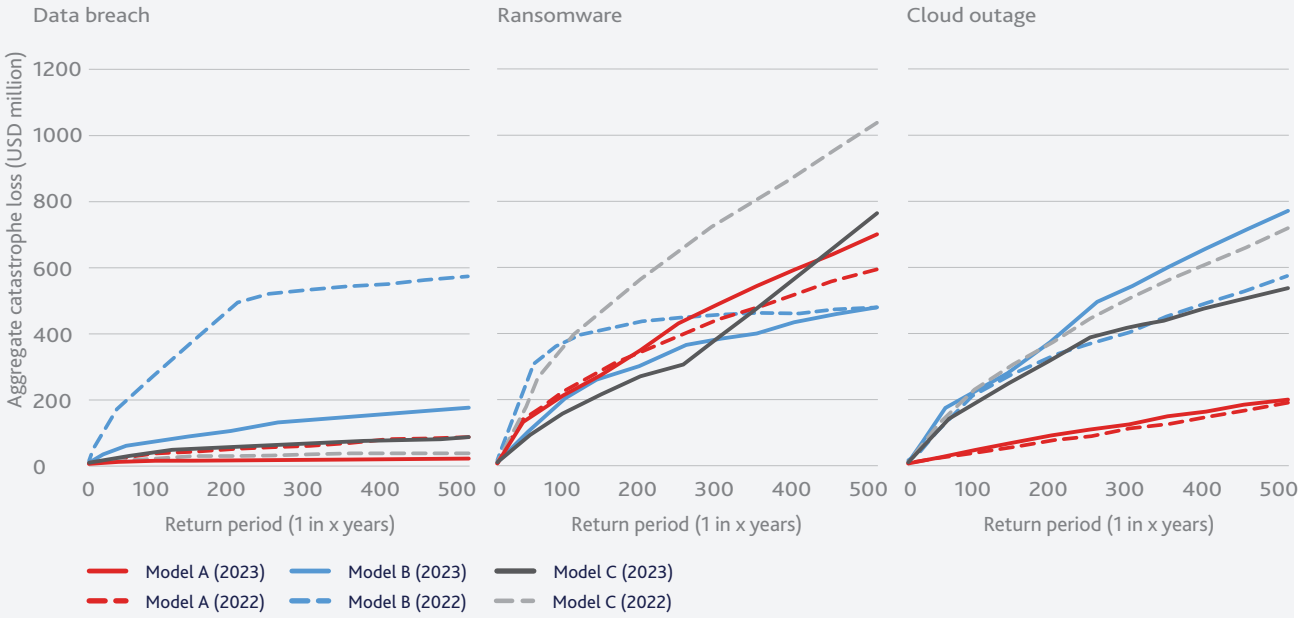
81 Economic losses from the NotPetya attack are estimated at more than USD 10 billion, of which around USD 3 billion were covered by insurance. See Howden 2022.

82 For example, all of the main external cyber models include losses from event forensics, notification, credit monitoring and event management under 'data breach coverage'. One model also includes costs associated with third-party class action lawsuits, while another model includes regulatory fines; these cost components are included in the other models but under separate coverage options.

Divergence of model outputs

Estimated cyber losses differ significantly across models. The divergence is most noticeable when looking at the far tail of the loss probability distributions, especially for a cloud outage or ransomware scenario (Figure 8).

FIGURE 8: MODELLED LOSSES FOR SELECTED SCENARIOS, BY MAJOR CYBER CATASTROPHE VENDOR[a]



[a] *The y-axis refers to annual loss estimates for a sample insurance portfolio for each model. The x-axis shows the associated return period – the likelihood of the estimated loss occurring on average within a given timeframe*

Source: Gallagher Re calculations

A large driver of the differences in modelled losses reflects sensitivities to key input data. Variations in even simple firmographic information – such as revenue, company name, industry or domiciled country – can have a significant impact on the loss estimates. Understanding how data quality drives model difference is therefore a key consideration of re/insurers when they compare model outputs. However, due to the lack of transparency about the models and their calibration processes, it is not possible to account fully for the divergent model estimates.

Over the years, estimated risk metrics for extreme cyber scenarios, though volatile, have converged across the main vendors as new model versions have been released. This is due in part to vendors relying on external feedback to recalibrate their models in line with re/insurance market views.[83] As a result, the convergence may not necessarily reflect a better grasp of the underlying drivers of catastrophic cyber risks and hence more accurate estimates of the 'true' aggregate loss distribution.

While understanding of cyber risks continues to evolve, and until cyber insurance policies become more standardised, we should expect to see the loss models undergoing frequent and possibly significant updates before they reach maturity. The downside of frequent model revisions, however, is the burden they place on re/insurers that make use of cyber models to judge capital calculations as regulators require them to re-evaluate the models and reconcile the output each time. Vendors must therefore navigate a tricky path between model inertia and volatility, although in the absence of empirical data with which to independently calibrate the models, convergence across them should be avoided if it is driven by market sentiment alone.

Source: Contributed by Simon Heather, Gallagher Re

83 One vendor explicitly states in their documentation that they use feedback from a panel of market experts to calibrate their loss outputs while another has indicated that directional changes in tail losses between previous and the latest versions of their model were driven by market sentiment.

4.3 Deterministic scenarios

In light of the difficulties in quantifying cyber risks, most re/insurers augment formal probabilistic models with deterministic scenarios to gauge the size of possible extreme cyber losses. These 'what-if' type exercises look to investigate the full scale of potential losses without necessarily attempting to enumerate the chances of such scenarios occurring. By careful selection, construction and analyses of different scenarios, re/insurers hope to gain increased visibility on the possible size and shape of the tail of the aggregate loss distribution. The scenarios may be informed by external vendor models, although re/insurers tend to develop their own narratives and estimates of realistic extreme losses, drawing on a wide variety of expertise across their business units (Figure 9).

Most re/insurers supplement probabilistic cyber models with deterministic scenarios to gain a fuller picture of the scale of potential peak losses.

A serious malware or ransomware attack or a major outage of a key internet service provider which prompted widespread business interruption is currently top of mind for cyber re/insurers.

Among the many possible adverse scenarios, the prospect of widespread business interruption – triggered by, for example, a malware or ransomware attack that indiscriminately affects multiple businesses or targets key internet intermediaries with resulting spillovers on other sectors' operations – is currently of most concern to cyber re/insurers (Table 3). Previous empirical studies have shown that the economic costs of such a concerted cyberattack might rise to as much as USD 193 billion.[84] And the losses borne by society could be many multiples of that if an attack disrupted or destroyed major critical infrastructure (such as a power plant), most of the associated costs of which would not be covered by cyber insurance given prevailing insurance coverage and exclusions.[85]

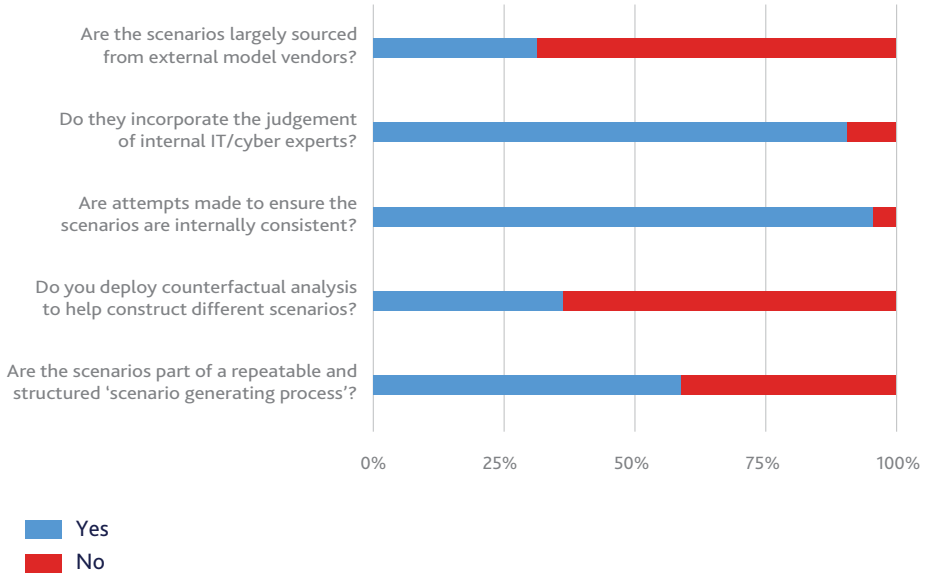


FIGURE 9: SCENARIO DEVELOPMENT BY RE/INSURERS (% OF RESPONDENT FIRMS)

Based on the results from a poll of 11 GA member cyber re/insurers, weighted by relative size of cyber insurance premiums

Source: The Geneva Association

84 Lloyd's and the University of Cambridge 2019.
85 Lloyd's and the University of Cambridge 2015.

TABLE 3: RE/INSURERS' RANKING OF EXTREME CYBER SCENARIOS

Extreme cyber scenarios	Average ranking of scenario
Denial of service/interruption of operations	
Worm-like malware epidemic	1
Widespread ransomware attack	2
Mass data breach	
Exfiltration of sensitive information (PII, encrypted passwords, etc.) at key organisation/institution which has widespread effects on customers/suppliers	4
Disruption to critical infrastructure	
An extortion of supervisory control and data acquisition (SCADA) networks of industrial control systems	4
A cyberattack on a crucial participant in an industry/sector (e.g. hospital, food manufacturer/distributor, etc.)	5
A cyberattack on a key utility provider (power, water etc.)	2
A compromise of state/municipal services	5
Cross-sector IT failure	2

Refers to median ranking score assigned by survey respondents (1 being the highest-ranked scenario). Based on the results from a poll of 11 GA member cyber re/insurers

Source: The Geneva Association

A major drawback of pure deterministic scenario analysis, however, is the difficulty of establishing the credibility of associated loss estimates. The level of potential losses could be high yet so uncertain that even experts struggle to assess the different scenarios with any confidence. It may simply be too challenging to identify the full set of dependencies among risk factors, define scenario footprints and assess the impact of an event on the many companies that could be affected.[86] Notaly, shifts in key assumptions about the degree of permanent destruction of both tangible and intangible assets (i.e. the extent of reversibility of an attack or non-malicious IT failure), the length of any outage in production as well as the time to recover or replace key inputs could all have a significant bearing on overall losses.

4.4 Irreducible uncertainty

Over time, some of the uncertainty around possible extreme cyber losses will no doubt be reduced. Better data collection and analysis, claims experience from different cyber incidents and increased understanding of the underlying threats and vulnerabilities will increase re/insurers' ability to assess and model cyber risks, not only attritional claims but also catastrophic losses.

Not all of the uncertainty around future cyber losses, however, can be resolved with increased information, enhanced knowledge and better modelling. Almost inevitably, a residual amount of irreducible uncertainty will persist, reflecting the impossibility to conceive clearly and exhaustively all the possible outcomes that could occur and the ambiguity over the probability of specific events and/or the magnitude of any consequences.[87] In assuming risks from others, re/insurers need to be adequately compensated for the uncertainty surrounding future insured losses, including those that cannot be reliably modelled or quantified.

This situation is not unique to cyber. Even natural perils for which extensive historical information and the laws of physics provide significant insights about the likelihood and scale of possible losses are affected by structural change, the precise implications of which cannot be completely mapped. More formally, the world is subject to non-stationary forces – i.e. is not governed by unchanging scientific or behavioural laws – which can give rise to unprecedented and profound uncertainties. Climate change provides a classic example of such a shift that is leading to extreme weather events far outside the historical envelope of uncertainties that frame most natural catastrophe modellers' views of such risks.[88]

86 The Geneva Association 2022b.
87 For a discussion of irreducible or radical uncertainty, see Kay and King 2020.
88 Energetics et al. 2022.

As data and understanding about cyber threats expand, cyber risk quantification will improve. However, some elements of cyber exposures extend beyond the reach of probabilistic reasoning, suggesting caution in relying solely on formal risk models.

Cast in this light, it is misguided to think that quantitative models will provide a definitive guide to cyber exposure management and/or underwriting. Instead, the value of such models is in thinking through simplified thought experiments about what is an ultimately complex, unknowable system. Put differently, some elements of cyber exposures extend beyond the reach of probabilistic reasoning, in the sense that we cannot attach meaningful numerical probabilities to all future outcomes or scenarios. Re/insurers therefore need to use model-derived estimates judiciously in order to avoid misplaced precision.

5 Towards more optimal risk sharing

Towards more optimal risk sharing

While some cyber exposures will remain out of scope for re/insurers due to the scale of potential accumulated losses, cyber risk will almost certainly become more insurable over time.

That ultimately there are limits to how far the frequency and severity of extreme cyber losses can be precisely quantified does not mean that such risks are completely uninsurable. The history of insurance is replete with examples where cover has been provided for new classes of exposure with limited relevant historical data and only partial understanding of the underlying risk drivers. The earliest insurance policies for the maritime sector, for example, were written without the benefit of full and detailed actuarial assessments.[89]

Some cyber exposures will almost certainly remain out of scope for re/insurers on grounds that possible accumulated losses far outstrip what the re/insurance sector can safely and sensibly underwrite. Most obviously, in line with other insurance lines, war-related cyber risks will continue to be excluded from standalone and packaged policies, even if market preferences over contract language have yet to reach a consensus. In the same vein, potential losses arising from disruption to major critical infrastructure may be so large, uncertain or too highly correlated that they bump up against and even overstep the boundaries of insurability.

But the perimeter of the set of insurable risks is not immutable. It shifts as the structure of information, knowledge and expertise as well as incentives influence ambiguities around potential tail events and attitudes towards them.[90] In this way, societies over time can move closer to optimal risk sharing, which in the absence of ambiguity would allocate risks to those most willing and able to absorb them.[91] In the case of cyber, the amount of achievable risk exchange will depend not only on the actions of those seeking to shed exposures and those willing to assume them. It is also affected by actions of governments that may end up bearing the bulk of losses from a catastrophic cyber incident as well as IT developers whose products and services individuals and firms have come to rely on but who may not fully bear the hidden costs they impose on others.

5.1 Broader re/insurance participation

The dedicated cyber insurance market remains relatively concentrated. According to Insuramore, the top five re/insurance groups account for close to a third of premiums worldwide, a market share that rises to over 70% for the top 20 groups.[92] Expanding the number of market participants could therefore boost overall risk-absorbing capacity for cyber exposures. As well as spreading the risks across more balance sheets, additional carriers might choose to locate at different attachment points (i.e. the thresholds at which insurance policies begin to provide cover) in the loss tower, depending on the relative likelihoods they attach to cyber perils and/or their risk appetite.

Expanding the number of participants in the cyber re/insurance market will help boost risk-absorbing capacity.

In fact, participation in cyber insurance markets has increased over time. Insuramore's research shows that over 220 insurer groups were underwriting cyber risks on a

89 For a discussion of the analytical foundations of early insurance policies, see Minto 2008.

90 Ambiguity describes situations in which probabilities surrounding future events are defined only imprecisely. Ambiguity aversion refers to a preference for known (relative to unknown) probability distributions over future outcomes. Both agents' perceptions over ambiguity and their degree of ambiguity aversion will influence the amount of risk that is willingly exchanged and on what terms.

91 In a frictionless world where uncertainty can be represented by objective probabilities that are known to all parties, aggregate (i.e. undiversifiable) risk is optimally distributed between individuals according to their preferences and initial endowments. In this stylised world, a risk-neutral insurer would fully insure all other agents. However, if the insurer is risk averse or there are administrative costs in settling claims or there is asymmetric information (which creates conditions for moral hazard or adverse selection) full insurance is no longer optimal. Instead, the insurer will offer coinsurance above a deductible amount that is retained by the policyholder. See Aase 2008.

92 Insuramore 2023.

direct basis by the end of 2022, an increase from over 180 in 2021. But reinsurance remains constrained, with limited options for re/insurers to lay off some of their exposure through retrocession. The majority of cessions are concentrated among the largest global reinsurers and the Lloyd's market.[93] As primary insurers grow more comfortable managing attritional losses, this might permit a shift away from proportional reinsurance to other structures (such as excess-of-loss) which might free up reinsurance capacity.[94,95]

New institutional mechanisms to spread and share cyber risks have been created, although the incremental increase in overall capacity is modest. For example, a new syndicated cyber facility was launched in the London Market at the beginning of 2023 which provides up to GBP 50 million of excess layer capacity through Lloyd's A-rated insurers.[96] Similarly, leading European multinational industrial companies from different sectors recently formed a mutual insurance company to underwrite direct cyber insurance on behalf of its owner-members, albeit up to an initial capacity limit of EUR 25 million per member.[97]

Discussions are also ongoing in certain jurisdictions about the potential to create or extend formal private-sector re/insurance pools to allow carriers to mutualise cyber risks, at least for certain types of exposure. In particular, press reports suggest that the U.K.'s Pool Re, originally created to share terrorism risks, is exploring how to expand its cover to state-sponsored or war-related cyberattacks.[98] Likewise, ideas are reportedly being mooted in the Australian market that might eventually lead to a standalone cyber reinsurance pool focused on insuring commercial SME cyber risk.[99]

Enhanced ways to share information and experiences in underwriting cyber risks may encourage more re/insurers to offer cyber insurance. And again there are recent examples which suggest the industry is making progress in that direction. For example, in early 2023 the Oasis Loss Modelling Framework announced the launch of its new Open Exposure Data standard for cyber to promote consistency and efficiency in the capture and transfer of exposure data.[100] Similarly, CyberAcuview, an industry consortium set up in 2021 by a number of leading cyber insurers, provides a coordinating framework to collate claims data for the U.S. market and share insights about the fundamental drivers of cyber losses, including possible systemic risks.[101]

5.2 Capital markets involvement

Attracting additional risk-absorbing capacity from capital markets will be essential in creating a sustainable cyber insurance market; the size of possible extreme losses are too large and/or uncertain for the re/insurance sector to carry alone. The pool of investable funds from financial markets is much larger than the total insurance capital base, which is around USD 2 trillion.[102] In 2022, global fixed income markets outstanding was USD 129.8 trillion, while global equity market capitalisation was USD 101.2 trillion.[103]

As explained in Box 5, there are signs of growing investor interest in cyber insurance-linked securities (ILS), although a number of hurdles must still be overcome. Potential lengthy coverage disputes over whether policy criteria have been satisfied and protracted negotiations over settlements do not sit well with end-investors who typically have a preference for short-duration financial securities and want ready access to the invested collateral upon maturity of the contract.[104] Instruments with parametric triggers as well as moves to set up an independent body to categorise cyber catastrophe events might help boost investor interest in cyber ILS, although such initiatives are still nascent.[105] Securities that look to tranche out first-party losses, which are likely to be shorter-tail than third-party liability claims, might also better match investors' preferences.[106]

93 Fitch 2023.
94 According to Guy Carpenter, primary insurers cede more of their cyber exposure to reinsurers compared with other classes of business, with a median cession rate of around 50%. The bulk of cessions are transacted through proportional reinsurance arrangements. See Guy Carpenter 2023.
95 Howden 2023.
96 Insurance Journal 2023.
97 Mutual Insurance and Reinsurance for Information Systems (MIRIS) is a capitalised mutual – membership is only granted after payment of the capital – and issued its first policy on 1 January 2023. Domiciled in Belgium, MIRIS writes insurance to cover the activities of its members worldwide albeit through policies issued in Europe. See https://www.miris-insurance.com/
98 Pool Re currently provides cover for insurers of 'remote digital interference', which relates to terrorist attacks with a cyber trigger, but specifically only those resulting in physical damage and not financial losses from cyber assaults. For more on recent discussions about extending the scope of coverage by Pool Re, see Smith 2023.
99 See, for example, Marshall 2023 and Wood 2023.
100 Sheehan 2023.
101 See https://cyberacuview.com/
102 Evans 2019.
103 SIFMA 2023.
104 In an empirical analysis based on a small sample of specialist ILS investors, Braun et al. (2023) show that maturity is ranked the most important attribute of a cyber ILS. This is followed by the multiple-over-expected-loss (i.e. projected return on the security) and then investor confidence in the empirical model used to calibrate cyber risks.
105 London market specialist cyber insurer CFC has announced plans to establish an independent committee of experts in the U.K. that would define whether a cyber event was an attritional or a catastrophic event. See Spoerry 2022.
106 Instech 2023.

Interest in cyber ILS is growing, but the prospect of long-tail claims, immature risk models and the limited potential for resale options can be off-putting to capital market investors.

Limited liquidity is also an impediment to further expansion in cyber ILS. Compared with natural catastrophe bonds, for which there is an active secondary market, investors are more restricted in how they can sell-on or trade their cyber ILS positions. In part at least, this reflects the way transactions have been structured, and in particular doubts that the cyber securities can be easily traded. To the extent that new instruments could be designed to allow wider resale opportunities, this would in turn boost primary issuance of cyber ILS. Secondary market trading would also help illuminate investors' views about extreme cyber uncertainties and, in turn, aid price discovery about the underlying risks and rewards.

Richer, more reliable models will foster engagement with cyber ILS market participants, especially if a new breed of more tech-led investors emerges with greater appetite for cyber risks. Arguably more important however, is enhanced disclosure by sponsors of securities that will enable ILS funds to become more comfortable with the exposure. Just like re/insurers, specialist ILS investors recognise the limitations of model-based risk metrics, especially for extreme cyber incidents for which historical benchmarks are limited. Since they are at least one step further removed from the underlying policyholders, ILS investors often look for a forensic understanding of how a cedent manages its underwriting in order to avoid major loss surprises in the transferred portfolio.[107]

Box 5: Cyber ILS – Developing a strong and sustainable market

Re/insurers have discussed transferring cyber risks to capital market investors for years, with little obvious progress to show for it apart from a few small, bespoke deals. Recent developments, though, illustrate that the nascent cyber ILS market is maturing and investor interest is growing, with a notable pick up in both public and private transactions. While cause for optimism, the latest deal activity nonetheless also highlights the need for further innovation to overcome structural barriers.

In the spotlight

Two high-profile transactions in 2023 offered proofs of concept for future ILS trades that ultimately could attract additional capital to absorb extreme cyber risks.

- **Beazley's Cairney cyber catastrophe bond series.** Issued over three tranches, these securities raised USD 81.5 million in fresh capital. They indemnify the re/insurer on an all-perils basis against losses from a catastrophic cyber event, including tech errors & omissions (E&O) risks, over a roughly one-year term.[108] The transactions mark both the first formal securitisation of cyber risks – albeit structured as a short-maturity, privately placed security rather than a traditional cat bond – and the first follow-on issuance to a cyber bond via an existing structure.

- **Hannover Re's collateralised reinsurance agreement with Stone Ridge.** The quota share structure was similar to the majority of cyber reinsurance transactions. But at USD 100 million in limit, this was the largest publicly revealed cyber ILS transaction so far, exceeding the USD 70 million deal announced by Hudson Structured Capital Management in 2020.[109]

In the shadows

Beyond these headline deals, the private cyber ILS market has grown rapidly if unevenly over recent years. Interviews with market participants reveal that more than 10 ILS managers have actively engaged in cyber ILS transactions since at least 2016, up from seven in 2021.[110] Several trades of around USD 100 million have been completed, including quota share, aggregate stop loss, and excess of loss transactions. ILS fund managers have also reportedly completed a handful of small parametric-based deals over the past five years. From the beginning of 2022 alone, as much as USD 1 billion (possibly more) cyber ILS may have been placed, doubling the size of the market according to some estimates.

107 Instech 2023.
108 Artemis 2023.
109 Evans 2020; Gallin 2023.
110 Johansmeyer and Mican 2022.

Nevertheless, the cyber ILS market remains small – it represents less than 1% of all ILS – and fragile. A small number of ILS fund managers are responsible for the bulk of the deployed capital and cyber is not the main focus of any of them. Modest changes in investment philosophy, market conditions or the loss environment could therefore prompt a sharp reduction in overall cyber ILS capacity.

The missing ingredients

Liquidity was a recurring theme mentioned by almost three quarters of interviewed ILS managers as vital for cyber ILS. Somewhat ironically, small deals can be a deterrent for some prospective investors. Size allows them to deploy meaningful amounts of capital, build and manage portfolios, and take comfort in the fact that they are not alone in the deal. Further, size not only shields investors from reputational risk – if the deal is spread over multiple investors – but it also provides the scale necessary to dull the impact of frictional costs. Securitisation is more expensive than traditional forms of reinsurance, and larger transactions make more sense in this regard.

To execute larger deals, many ILS managers suggest that improved modelling and quantification of systemic cyber risks will be necessary. Several managers expressed frustration with the wide divergence in modelled losses for similar scenarios. Some differentiation makes sense, but the current differences make the conversation with end investors extremely difficult.

Increased standardisation and more precise event definitions – perils included, temporal limits, damages covered etc. – will also help. ILS managers interviewed believe that those in place are too loose for adoption in more rigorously structured instruments, although many note recent improvements in contract terms and recognise that more are on the way.

In terms of secondary trading, the private cyber transactions completed so far are among the least liquid instruments in the catastrophe bond space. Alternatives with more liquidity are typically issued under Rule 144A of the U.S. Securities Act, which simplifies the resale process between sophisticated investors and makes it easier and less costly to trade. Despite the Cairney cyber bonds being marketed as fully tradable under Rule 144A resale, many market participants remain cautious. ILS managers note the discipline and transparency afforded by the 144A format.

Market outlook

The recent deal flow in cyber ILS shows that financial market investors are interested in taking on risks that re/insurers are eager to hedge. That represents a profound improvement from only a few years ago when transactions were perceived as small, infrequent and opaque.[111] The investor community has appetite to commit even more capital, especially if instruments with more features that support liquidity can be developed. Cyber ILS has come a long way, and the next billion dollars should come far faster than the first billion.

Source: Contributed by Tom Johansmeyer, Inver Re

5.3 Collaboration with critical infrastructure providers and government security agencies

Given the potential for cyber intrusions to spread via online connectivity, one way for re/insurers to gain increased understanding of the potential for widespread losses is by collaborating with organisations that provide critical functionality of the internet. This could be especially important in expanding business interruption coverage for cyber perils. Companies such as the major CSPs have a unique vantage point to assess the cyber vulnerabilities of their users and the geographical/industrial footprint of attacks.

A number of partnerships have already been initiated between CSPs and re/insurers, albeit these remain nascent. For instance, Munich Re and Allianz partnered with Google to offer bigger policy limits for large U.S. customers of Google Cloud.[112] By leveraging the internet giant's cybersecurity expertise, including tools that scan workloads on the cloud and provide proactive security recommendations, the re/insurers benefit from insightful data about policyholders' security posture. A similar collaboration is in place between AWS, Swiss Re and insurtech Cowbell to enhance the cyber insurance underwriting process for U.S. SMEs.[113]

Cooperation with government security agencies can also help to boost the governance role of cyber insurance in helping to identify and mitigate the financial impact of cybersecurity incidents. Enhanced threat intelligence could enable re/insurers to provide targeted alerts and risk-management suggestions for insureds, thereby improving policyholders' cyber resilience.

111 The Geneva Association 2022b.
112 Munich Re 2021.
113 Cowbell 2022.

Collaborations between re/insurers and key internet infrastructure will improve cyber risk monitoring, allowing coverage and policy limits to expand.

5.4 Government backstops

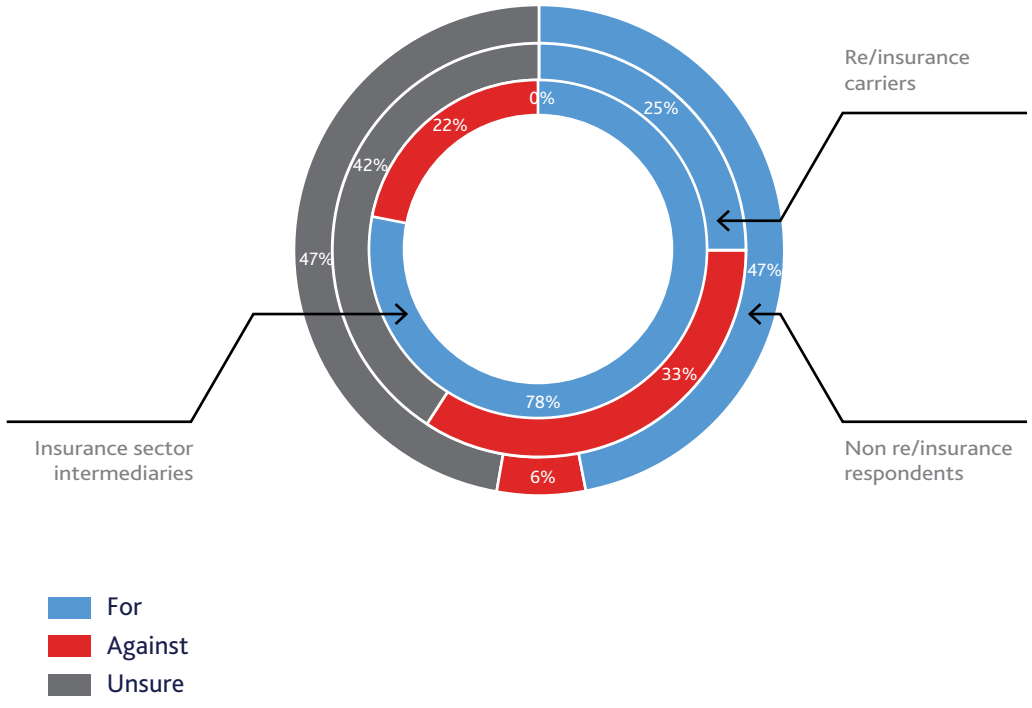
Even with additional capacity from capital markets, there may be limits to the amount of cyber risk transfer that the private re/insurance sector can sensibly undertake. As government balance sheets might ultimately be called upon to absorb outsized uninsured losses should a major incident occur, it is rational to think about whether some form of government backstop facility could contribute to more efficient risk sharing. In principle, by cutting the size of catastrophic losses borne by private re/insurers and investors, such a backstop might encourage re/insurers to extend coverage and offer extra capacity. And to the extent that increased take-up of cyber insurance catalysed improved cyber hygiene and overall risk management, this might even make societies more resilient – decreasing the chances that a government facility would ultimately be called upon.

In this context, towards the end of 2022, the U.S. Treasury undertook a public consultation to solicit views about the potential benefits of a federal insurance programme for catastrophic cyber incidents.[114] The sample of respondents was not entirely representative – notably, none of the major, global reinsurance companies submitted individual replies to the consultation. Nevertheless, at face value, the responses suggest some support for such a risk transfer mechanism or at least for exploring further the potential, both within and outside the re/insurance sector. At the same time, a significant proportion of respondents, including among insurance carriers, remain unconvinced that a public-private insurance arrangement for cyber is appropriate at the present time (Figure 10).

The sheer scale and/or uncertainty surrounding extreme potential accumulated cyber losses, however, may ultimately call for government backstops to limit the downside risks assumed by private sector re/insurers and investors.

FIGURE 10: INDUSTRY VIEWS ON A U.S. FEDERAL INSURANCE FACILITY FOR CYBER RISKS

A potential federal insurance for catastrophic cyber incidents?



Based on 55 unique individual responses. Joint responses submitted on behalf of discrete organisations were counted separately. Carriers also include responses from industry bodies representing re/insurers while intermediaries refers to responses from brokers, rating agencies and model vendors

Source: The Geneva Association analysis of published responses to the U.S. Treasury consultation exercise

114 U.S. Treasury 2022.

From the written consultation responses, a common theme among doubters (as well as some of those who are unsure) is a concern that any government backstop might have unintended consequences.[115] This includes the potential for it to encourage lax cybersecurity among policyholders as well as weaken the incentives of insurers to promote good cyber hygiene and develop innovative insurance solutions. The cyber threat landscape itself could be influenced by the existence of a backstop to the extent that it encourages cyber adversaries – especially state-sponsored threat actors not solely motivated by financial gains – to exploit vulnerabilities that cause large and widespread losses knowing that a government may ultimately pick up the tab.[116] Some market participants also worry that a government backstop would go hand in hand with a mandate for insurers to offer protection for all cyber perils, even those that are currently uninsurable.

These are legitimate reservations, although they arise for other public-sector coinsurance mechanisms that already exist for perils besides cyber, such as government-backed reinsurance schemes to protect against extreme losses from floods or terrorism attacks.[117] They must also be balanced against the benefits such facilities provide. Suitably designed, calibrated and implemented, a cyber backstop could ensure that governments assume responsibility only for extreme losses beyond some agreed threshold while also aligning incentives to promote continued development and take-up of cyber insurance to boost societal resilience. This includes premiums to cover the cost of any government guarantee as well as procedures to claw back taxpayer-funded losses after a major cyber event.

Suitably designed, state-sponsored backstops could encourage re/insurers to extend coverage, promote good cyber hygiene and ensure that governments only face extreme losses above an agreed threshold.

Designing any backstop inevitably involves fine judgements, especially about the calibration of features such as deductibles and aggregate retention levels, as well as any scope for co-operative international solutions. There is no unique blueprint, although existing schemes offer clues as to what might work and what to avoid.[118] As with other peak perils, any such facilities for cyber would need to be routinely reviewed and adapted to reflect the evolution in the understanding of cyber accumulation risks and who is best placed to absorb them.

Moreover, a government-sponsored backstop would not operate in isolation; accompanying public policy initiatives should aim to promote increased cyber resilience and/or reduce cyber threats. Governments can encourage minimum cybersecurity standards among firms, at least for entities with which they enter into commercial contracts, but more generally through sector- or industry-wide regulations. For example, in the U.S., The National Institute of Standards and Technology of the U.S. Department of Commerce has developed a voluntary framework for reducing cyber risks to critical infrastructure that could become a de facto legal standard through the operation of fiduciary and other legal duties of care.[119]

5.5 Enhanced IT-sector liability

State involvement in standard-setting also extends to third parties whose conduct may create cybersecurity vulnerabilities for others but who may not bear the full consequences of their actions. Specifically, legislators and regulators could create tougher liability regimes for both IT hardware and software manufacturers as well as vendors who provide associated services. In the scramble to introduce new products, IT firms all too often pay scant regard to cybersecurity during the design phases, choosing to remediate flaws and bugs as they come to light in operation. By imposing higher duties of care or limiting liability indemnities, legislators could incentivise vendor companies to develop secure hardware and software that are more robust to cyberattacks.[120]

115 The detailed written responses to the U.S. Treasury consultation exercise are published at https://www.regulations.gov/docket/TREAS-DO-2022-0019/comments

116 Some researchers have dubbed this an example of third-party moral hazard, whereby the presence of insurance can influence the behaviour of those not party to the insurance contract. See, for example, Parchomovsky and Siegelman 2022.

117 For example, Pool Re is a mutual insurance company set up by U.K. insurers to provide terrorism insurance. It is underpinned by a U.K. HM Treasury commitment to support Pool Re if ever it has insufficient funds to pay a legitimate claim.

118 For a discussion of some of the design issues surrounding public-private partnerships in the context of cyber, see The Geneva Association 2022b.

119 Baker and Shortland 2022.

120 Cybersecurity vendors, for example, often include a limitation clause that caps the monetary liability they can be held responsible for at the amount of the services a company pays for them. Similarly, legal claims alleging negligence for a data breach, for example, can also be difficult to prove. See Jones 2023.

Stricter liability regimes for IT manufacturers and third-party vendors could also incentivise the development of secure hardware and software that are more robust to cyberattacks.

Such an approach is a core pillar of the recently announced U.S. national cybersecurity strategy, which aims to reduce overall cyber risk and shift the consequences of poor cybersecurity away from the most vulnerable.[121] Details of any prospective legislation are yet to emerge, but some commentators highlight prospective new rules to:

- Limit software manufacturers from using contracts to shift liability to end-users
- Establish higher standards of care for software in specific high-risk scenarios
- Implement an adaptable 'safe harbour framework' to shield providers who securely develop and maintain their software products and services.[122]

As with government coinsurance, enhanced liability rules also have possible drawbacks. Notably, policymakers must navigate important trade-offs. Increased developer responsibility for cybersecurity could stifle or at least impede technical innovation while at the same time reduce competition if the fixed costs of compliance favour large firms over small ones.[123] The cost of software upgrades might become prohibitively expensive for some users meaning known security vulnerabilities remain unpatched for longer. There are also practical challenges in crafting new liability rules and standards. For example, who decides when software is robust enough or how far to allocate responsibility if the underlying flaw was linked to OSS?

Despite these implementation challenges, attempts to ensure that the costs of externalities are borne by those who create them ought in principle to drive the IT market to produce safer products and services. In doing so, that will enable re/insurers to become more comfortable in assuming some of the aggregate tail risks associated with cyber incidents and in turn deploy more risk-absorbing capacity.

121 The White House 2023.
122 Finch et al. 2023.
123 Ellis 2023.

6 Concluding remarks

Concluding remarks

Improved risk modelling, partnerships with government security agencies and technology companies, enhanced liability regimes, and potentially even government backstops, will be key to making extreme cyber losses more insurable.

Cyber is a complex risk. It challenges many of the traditional actuarial assumptions normally applied in insurance to quantify the potential losses that might arise from an incident. In particular, worries persist that the scale of possible accumulated claims arising from some cyber perils – across policyholders, geographies, insurance lines etc. – are simply too large and/or uncertain for re/insurers to underwrite. Such fears have been heightened by the increasingly hostile cyber threat landscape, especially in light of the ongoing ransomware menace and the outbreak of the Ukraine-Russia war, which have highlighted important cybersecurity vulnerabilities within physical and digital supply chains as well as critical infrastructure.

So far we have (thankfully) yet to witness a truly catastrophic cyber incident. Nevertheless, it is hardly surprising and indeed entirely sensible for re/insurers to recalibrate the cost and availability of cyber protection to reflect the new risk landscape. This includes tightening contract language to rule out coverage for state-sponsored cyberattacks that give rise to outsized losses, maintaining prudently low policy limits to guard against remote but still sizeable claims, as well as reducing silent cyber exposure for which coverage was never intended nor priced for. Over-stretching re/insurers' balance sheets would only undermine their ability to make good on their promises to policyholders to cover the bulk of cyber-related claims for which insurance is an appropriate form of protection.

However, with elevated threats to cybersecurity unlikely to recede anytime soon and the costs of cybercrime seemingly set on an inexorable rise, society faces a large and persistent cyber protection gap. Re/insurers have an important part to play in helping to narrow that gap by increasing the take-up of cyber insurance and broadening the scale and scope of available cover. The standalone cyber insurance market is relatively young and has already expanded rapidly to meet the needs of insureds but it must adapt and mature still further if it is to stay relevant. In pushing out the frontiers of insurable cyber risks while adequately compensating their capital providers for bearing potential unexpected losses, re/insurance can incentivise improved cyber hygiene and risk prevention, boost policyholders' robustness to cope with cyber incidents and enhance their abilities to restore and recover afterwards.

Progress in risk modelling and quantification of potential loss accumulation is an important element in making cyber exposures more insurable. And there are tangible signs that knowledge and understanding on this front are advancing as information and expertise about the drivers of extreme cyber losses continue to develop. However, current approaches remain immature and their results can be volatile and inconsistent, suggesting caution in relying solely on the insights from the latest vintage of cyber models.

Re/insurers have an important role to play in narrowing the cyber protection gap by increasing the take-up of cyber insurance and broadening the scale and scope of available cover.

Moreover, better risk models, while necessary, will likely not be sufficient to attract significant additional risk-absorbing capital; residual cyber uncertainties remain that constrain what is knowable and can be modelled with any reliable degree of precision. Other institutional innovations may therefore also be required in order to foster a larger, sustainable cyber re/insurance market capable of addressing the future protection needs of policyholders.

Recent re/insurer initiatives that seek to coordinate information sharing and knowledge exchange about the nature and size of cyber risks, including involving key technology companies with unique insights on evolving threats and vulnerabilities, are a positive move in that direction. Likewise, building on the success of recent cyber ILS transactions, cultivating broader financial market interest through the design of instruments that

better match investor appetite will be very important in spreading and transferring peak cyber risks to those best placed to absorb them. Equally, pursuing ideas to create mechanisms to pool cyber exposures among risk carriers could be helpful in broadening participation and adding capacity to the re/insurance market.

Governments are also pivotal. They already play a role through encouraging information capture and dissemination about cyber threats as well as setting and enforcing laws and regulations that establish liability and impose sanctions on those who cause harm to others. Yet there is scope to go further and establish enhanced responsibilities for the IT sector to promote more robust cybersecurity protocols in software and hardware. Ultimately, too, government financing to backstop extreme losses might encourage the private re/insurance sector to take on more cyber exposures knowing that their downside losses are capped.

Doing so will require an approach that combines the development of better cyber risk models, enhanced information sharing, and greater participation from capital market investors and governments.

Some may be nervous about the unintended consequences of further state involvement and look to the primacy of private-sector solutions. Yet with taxpayers in the end likely to be called upon to absorb a significant share of uninsured losses from a cyber catastrophe, it is sensible to look at measures that could promote re/insurance market functioning. Rather than wait for a catastrophic event to occur and figure out how to cope with the losses ex post, it is better to look at measures that anticipate such an eventuality and can be appropriately designed and executed to encourage better ex ante risk sharing.

References

Aase, K. 2008. Optimal Risk-Sharing and Deductibles in Insurance. *Encyclopedia of Quantitative Risk Analysis and Assessment.* https://onlinelibrary.wiley.com/doi/abs/10.1002/9780470061596.risk0361

Acronis. 2023. What is a Managed Service Provider (MSP)? 16 May. https://www.acronis.com/en-eu/blog/posts/msp/

Aon. 2023. Buyer-Friendly Cyber and E&O Market: How to take advantage.
https://www.aon.com/insights/articles/2023/buyer-friendly-cyber-and-e-and-o-market-how-to-take-advantage

Artemis. 2023. *Beazley Sponsors Third Cyber Catastrophe Bond, $16.5m Cairney III.*
https://www.artemis.bm/news/beazley-sponsors-third-cyber-catastrophe-bond-16-5m-cairney-iii/

Awiszus, K., T. Knispel, I. Penner, G. Svindland, A. Voss, and S. Weber. 2023. Modeling and Pricing Cyber Insurance. *European Actuarial Journal* 13: 1–53. https://doi.org/10.1007/s13385-023-00341-9

Baker, T., and A. Shortland. 2022. The Government Behind Insurance Governance: Lessons for ransomware. *Regulation and Governance.* https://onlinelibrary.wiley.com/doi/full/10.1111/rego.12505

Benomar, Z., C. Ghribi, E. Cali, A. Hinsen, and B. Jahne. 2022. Agent-based Modeling and Simulation for Malware Spreading in D2D Networks. https://arxiv.org/pdf/2201.12230.pdf

Beazley. 2023. *Catastrophic Cyber Risks – External FAQs.*
https://www.beazley.com/globalassets/documents/external-faq-for-catastrophic-discussion-updated.pdf

Bertuzzi, L. 2022. EU Top Court: Consumer groups can bring class actions for data protection infringements. *EURACTIV.* 28 April.
https://www.euractiv.com/section/data-protection/news/eu-top-court-consumer-groups-can-bring-class-actions-for-data-protection-infringements/

Biener, C., M. Eling, and J. Wirfs. 2015. Insurability of Cyber Risk: An empirical analysis. *The Geneva Papers on Risk and Insurance – Issues and Practice* 40: 131–158. https://link.springer.com/article/10.1057/gpp.2014.19

Böhme, R., and G. Kataria. 2006. Models and Measures for Correlation in Cyber Insurance. Workshop on the Economics of Information Security.
https://www.semanticscholar.org/paper/Models-and-Measures-for-Correlation-in-B%C3%B6hme-Kataria/24af7e7832277628c9fa108e31c31d75d3c494bc

Braun, A., M. Eling, and C Jaenicke. 2023. Cyber Insurance-linked Securities. *ASTIN Bulletin* 53 (3).
https://www.cambridge.org/core/journals/astin-bulletin-journal-of-the-iaa/article/cyber-insurancelinked-securities/69986C0DCA02746A0FBD678042A44D67

Breg, D. 2023. Quarterly Cyber Insurance Update. *Wall Street Journal.* 26 May.
https://www.wsj.com/articles/quarterly-cyber-insurance-update-may-2023-2f9ecc68

Cambridge Centre for Risk Studies and RMS. 2018. *Managing Cyber Insurance Accumulation Risk.*
https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-rms-managing-cyber-insurance-accumulation-risk.pdf

Confederation of European Security Services (in collaboration with International Security Ligue).
2023. Cyber-Physical Security and Critical Infrastructure. https://www.coess.org/newsroom.php?news=Critical-Infrastructure-under-attack-New-CoESS-White-Paper-details-emerging-cyber-physical-security-risks

Conger, K. 2022. Ukraine Says It Thwarted a Sophisticated Russian Cyberattack on Its Power Grid. *The New York Times.* 12 April. https://www.nytimes.com/2022/04/12/us/politics/ukraine-russian-cyberattack.html

Checkpoint. 2023a. *2023 Cyber Security Report*.
https://resources.checkpoint.com/report/2023-check-point-cyber-security-report

Checkpoint. 2023b. *2023 Mid-year Cyber Security Report*.
https://pages.checkpoint.com/2023-mid-year-cyber-security-report.html

Chainalysis. 2023. *Crypto Crime Mid-year Update*.
https://blog.chainalysis.com/reports/crypto-crime-midyear-2023-update-ransomware-scams/

Cisco. 2018. *What Is the Difference: Viruses, worms, Trojans, and bots?*
https://sec.cloudapps.cisco.com/security/center/resources/virus_differences

Coalition. 2023. *Introducing Coalition's Active Cyber Risk Model*.
https://info.coalitioninc.com/download-active-cyber-risk-model-2023-03-21.html

Cohen, O. 2020. *What Is Parametric Insurance? Parametrix*. 2 December.
https://parametrixinsurance.com/what-is-parametric-insurance/

Corvus. 2023. Record Ransomware Attacks: 6 month upward trend continues in July.
https://www.corvusinsurance.com/blog/record-ransomware-attacks-6-month-upward-trend-continues-in-july

Cowbell. 2022. *Prime Cloud. Frequently asked questions for businesses seeking coverage*.
https://cowbell.insure/wp-content/uploads/2022/07/Cowbell-Prime-Cloud-FAQ.pdf

Crowdstrike. 2022. *Honeypots in Cybersecurity Explained*.
https://www.crowdstrike.com/cybersecurity-101/honeypots-in-cybersecurity-explained/

CyberCube 2023. *Cyber Attack Event Analysis Reflecting Trends in CyberCube's Portfolio Manager Version 5*.
https://insights.cybcube.com/pmv5-report-cyber-attack-event-analysis

Cybersecurity Ventures. 2022. *Cybercrime To Cost The World 8 Trillion Annually In 2023*.
https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

Darneff, C., J. Tully, T. Chan, E. Castillo, S. Savage, P. Maysent, T. Hemmen, B. Clay, and C. Longhurst. 2023. Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US. *JAMA Network Open* 6 (5): e2312270.
https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2804585?resultClick=3

Dempsey, J. 2022. Third Circuit Shows how to Establish Standing in Data Breach Cases. *IAPP*.
https://iapp.org/news/a/third-circuit-shows-how-to-establish-standing-in-data-breach-cases/

Dacorogna, M., N. Debbabi, and M. Kratz. 2023. Building Up Cyber Resilience by Better Grasping Cyber Risk via a New Algorithm for Modelling Heavy-tailed Data. *European Journal of Operational Research* 311 (2).
https://www.sciencedirect.com/science/article/abs/pii/S0377221723003466

Daryanani, M. 2023. How AI influences cybersecurity. *LPMG*.
https://kpmg.com/ch/en/blogs/home/posts/2023/04/ai-influences-cybersecurity.html

ENISA. 2023. *Demand Side of Cyber Insurance in the EU: Analysis of challenges and perspectives of OESs*.
https://www.enisa.europa.eu/publications/demand-side-of-cyber-insurance-in-the-eu

Ellis, A. 2023. Software Liability Reform is Liable to Push Us Off a Cliff. CSO. March
https://www.csoonline.com/article/574671/software-liability-reform-is-liable-to-push-us-off-a-cliff.html

Endor Labs. 2022. *The State of Dependency Management.*
https://www.endorlabs.com/state-of-dependency-management

Energetics, Swiss Re and ARC Centre of Excellence for Climate Extremes. 2022. *Treating Climate Uncertainties as Knowable Risks – A recipe for greenwash?* https://www.energetics.com.au/media/2668/20220210-treating-climate-uncertainties-as-knowable-risks-a-recipe-for-greenwash.pdf

Evans, S. 2019. Alternative Capital Now 4% of $2 Trillion Non-life Insurance Market: Swiss Re. *Artemis.* 11 April.
https://www.artemis.bm/news/alternative-capital-now-4-of-2-trillion-non-life-insurance-market-swiss-re/

Evans, S. 2020. Hudson Structured & Aon Team Up for $70mn Cyber Catastrophe Product. *Artemis.* 19 November.
https://www.artemis.bm/news/Hudson-structured-aon-team-up-for-70m-cyber-catastrophe-product

Flexera. 2023. 2023 *State of the Cloud Report.*
https://info.flexera.com/CM-REPORT-State-of-the-Cloud-2023-Thanks#multicloud-1

Finch, B., A. Ghosh, and A. Heffez. 2023. New Biden Administration Cyber Strategy Proposes Dramatic Shift in Order to Hold Software Developers Liable for "Insecure" Software. *Pillsbury Winthrop Shaw Pittman LLP.* March.
https://www.jdsupra.com/legalnews/new-biden-administration-cyber-strategy-4400077/

Fitch. 2023. *Recent ILS Cyber Bond Issuance Encouraging for (Re)Insurers.*
https://www.fitchratings.com/research/insurance/recent-ils-cyber-bond-issuance-encouraging-for-re-insurers-31-01-2023

Fox, B. 2023. The Shifting Landscape of Open Source Supply Chain Attacks - Part 2. *Sonatype.* January.
https://blog.sonatype.com/the-shifting-landscape-of-open-source-supply-chain-attacks-part-2

Gallagher Re. 2022a. *CY–FI: The Future of Cyber (Re)insurance.*
https://www.ajg.com/gallagherre/-/media/files/gallagher/gallagherre/future-of-cyber-reinsurance.pdf

Gallagher Re. 2022b. *Looking from the Outside-In: Can taking the threat actors' viewpoint help insurers?*
https://www.ajg.com/gallagherre/-/media/files/gallagher/gallagherre/gallagher-re-cyberiq-outside-in-data.pdf

Gallagher Re. 2022c. *Evaluation of Cyber Models.*
https://www.ajg.com/gallagherre/news-and-insights/2022/november/evaluating-cyber-models/

Gallin, L. 2023. Hannover Re and Stone Ridge in $100m Retrocession Cyber Quota Share. *Reinsurance News.* 19 January.
https://www.reinsurancene.ws/hannover-re-and-stone-ridge-in-100m-retrocession-cyber-quota-share/

Gartner. 2022. 3 *Planning Assumptions for Securing Cyber-Physical Systems of Critical Infrastructure.* February.
https://www.gartner.com/en/articles/3-planning-assumptions-for-securing-cyber-physical-systems-of-critical-infrastructure

GFIA. 2023. Global protection gaps and recommendations for bridging them. March

Greenberg. 2023. The Huge 3CX Breach Was Actually 2 Linked Supply Chain Attacks. *Wired.* 28 April.
https://www.wired.com/story/3cx-supply-chain-attack-times-two/

GuyCarpenter. 2023. *Through the Looking Glass: Interrogating the key numbers behind today's cyber market.*
https://www.guycarp.com/content/dam/guycarp-rebrand/pdf/Insights/2023/Guy_Carpenter_Cyber_(Re)insurance_Market_Report_Publish_rev%20.pdf

Harvey, T. 2016. Prudential Regulation Authority on the Challenges Facing Cyber Insurers. *Moody's RMS.* 22 November.
http://www.rms.com/blog/tag/cyber-risk/

Hell, M. How to Close OSS Attack Vectors in Your Supply Chain. *TechBeacon.* https://techbeacon.com/security/how-close-oss-attack-vectors-your-supply-chain

Hill, M. 2023. Weak Credentials, Unpatched Vulnerabilities, Malicious OSS Packages Causing Cloud Security Risks. *CSO Online.* 18 April. https://www.csoonline.com/article/575029/weak-credentials-unpatched-vulnerabilities-malicious-oss-packages-causing-cloud-security-risks.html

Hillairet, C., O. Lopez, L. d'Oultremont, and B. Spoorenberg. 2022. Cyber-contagion Model with Network Structure Applied to Insurance. *Insurance: Mathematics and Economics* 107: 88–101. https://www.sciencedirect.com/science/article/abs/pii/S0167668722000889

Howden. 2022. *Cyber Insurance: A hard reset 2.0.* https://www.howdengroupholdings.com/sites/default/files/2022-12/howden-cyber-insurance-a-hard-reset-2.pdf

Howden 2023. *Cyber Insurance: Coming of age.* https://www.howdengroup.com/sites/g/files/mwfley566/files/2023-07/9100%20Cyber%20Report%20June%2023%20v04.pdf

Instech. 2023. *Four Keys to Unlocking Cyber ILS Capacity in 2023.* https://www.instech.co/insight/four-keys-unlocking-cyber-ils-capacity-2023

Insurance Journal. 2023. Markets/Coverages: WTW launches cyber facility, providing excess capacity globally. 30 January. https://www.insurancejournal.com/news/international/2023/01/30/705125.htm#

Insuramore. 2023. *Cyber: Insurer group global rankings.* https://www.insuramore.com/rankings/insurers/premiums-cyber/

Johansmeyer, T. 2023. How Big Is the Cyber Insurance Market? Can It Keep Growing? 27 June. https://www.lawfaremedia.org/article/how-big-is-the-cyber-insurance-market-can-it-keep-growing

Johansmeyer, T., and A. Mican. 2022. Cyber ILS: How acute demand could drive a scalable retro market. *Journal of Risk Management and Insurance* 26 (1): 40–59. https://jrmi.au.edu/index.php/jrmi/article/view/245

Jones, D. 2023. Who is Liable for Flawed Software? New guidance upends the security standard. *Cybersecurity.* 6 March. https://www.cybersecuritydive.com/news/national-cyber-software-liability/644232/

Juniper Research. 2023. *Vulnerable Software Supply Chains Are a Multi-billion Dollar Problem.* https://www.juniperresearch.com/whitepapers/vulnerable-software-supply-chains-problem

Kay, J., and M. King. 2020. *Radical Uncertainty: Decision-making beyond the numbers.* Norton. https://wwnorton.com/books/9781324004776

Kost, E. 2023. How Did Kaseya Get Hacked? *Upguard.* March. https://www.upguard.com/blog/how-did-kaseya-get-hacked

Linux Foundation. 2022. *Software Bill of Materials (SBOM) and Cybersecurity Readiness.* https://8112310.fs1.hubspotusercontent-na1.net/hubfs/8112310/LF%20Research/State%20of%20Software%20Bill%20of%20Materials%20-%20Report.pdf

Lloyd's and University of Cambridge. 2015. *Business Blackout. Insurance implications of a cyber-attack on the US power grid.* https://www.jbs.cam.ac.uk/faculty-research/centres/risk/publications/technology-and-space/lloydsbusiness-blackout-scenario/

Lloyd's and the University of Cambridge. 2019. *Bashe Attack. Global infection by contagious malware.* https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/crs-cyrim-bashe-attack-scenario.pdf

Lloyd's. 2022. *Shifting Powers: Physical cyber risk in a changing geopolitical landscape.* https://assets.lloyds.com/media/0926f9be-0f3d-49cc-9960-52accc888aad/Lloyds_Shifting_%20Powers_Physical_%20Cyber_Risk_Final_2906.pdf

Mahoney Group. 2023. *Watching for Cyber Insurance Policy Exclusions.* https://www.mahoneygroup.com/cyber-insurance-policy-exclusions/

Marshall, C. 2023. 2023 Young Actuaries' Public Policy Essay Competition Results Announced! *Actuaries Digital.* 5 April. https://www.actuaries.digital/2023/04/05/2023-young-actuaries-public-policy-essay-competition-result-announced/

McAffee. 2020. *The Hidden Costs of Cybercrime.* December. https://companies.mybroadband.co.za/axiz/files/2021/02/eBook-Axiz-McAfee-hidden-costs-of-cybercrime.pdf

Microsoft. 2022. *Microsoft Digital Defense Report 2022.* https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022

Miller, J. 2023. War Exclusions in Cyber Policies: An overview. March. https://www.dacbeachcroft.com/es/gb/articles/2023/march/war-exclusions-in-cyber-policies-an-overview/

Minto, A. 2008. Early Insurance Mechanisms and Their Mathematical Foundations *The Mathematics Enthusiast* 5 (2): 16. https://scholarworks.umt.edu/cgi/viewcontent.cgi?article=1113&context=tme

Morot, A., and S. Héon 2022. Cybersecurity of the Supply Chain. *SCOR.* September. https://www.scor.com/en/news/cybersecurity-supply-chain

Munich Re. 2021. *Pioneering Cyber Insurance: Munich Re partners with Google Cloud and Allianz.* https://www.munichre.com/en/company/media-relations/media-information-and-corporate-news/media-information/2021/pioneering-cyber-insurance.html

Munich Re. 2023. *Cyber Insurance: Risks and trends.* https://www.munichre.com/landingpage/en/cyber-insurance-risks-and-trends-2023.item-738a133628e04cb9ff6114486f1d9964.html

Oladimeji, S., and S. Kerner. 2023. SolarWinds Hack Explained: Everything you need to know. *TechTarget.* June. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know

Parchomovsky, G., and P. Siegelman. 2022. Third Party Moral Hazard and the Problem of Insurance Externalities. *Journal of Legal Studies* 93. https://scholarship.law.upenn.edu/faculty_scholarship/2811/

Reinsurance News. *Significant Insurance Industry Losses, Events & Data.*

Shah, S. 2021. The Financial Impact of SolarWinds Breach. *Bitsight.* 12 January. https://www.bitsight.com/blog/the-financial-impact-of-solarwinds-a-cyber-catastrophe-but-insurance-disaster-avoided

Schmitt, J. 2023. Software Supply Chain: What it is and how to keep it secure. June. https://circleci.com/blog/secure-software-supply-chain/

Shevchenko, P. 2010. Calculation of Aggregate Loss Distributions. *The Journal of Operational Risk* 5 (2). https://arxiv.org/pdf/1008.1108.pdf

Smith, I. 2023. Insurers in Talks on Adding State-backed Cyber to UK Reinsurance Scheme. *Financial Times.* https://www.ft.com/content/84221be3-2beb-4710-9970-5bccac2a98ed

Sheehan, M. 2023. Oasis Develops Open Data Standards for Cyber Exposure. *Reinsurance News.* 10 February. https://www.reinsurancene.ws/oasis-develops-open-data-standards-for-cyber-exposure/

Sifma. 2023. 2023 *Capital Markets Fact Book.* July. https://www.sifma.org/resources/research/fact-book/

Simas, Z. 2023. Unpacking the MOVEit Breach: Statistics and analysis. 18 July. https://www.emsisoft.com/en/blog/44123/unpacking-the-moveit-breach-statistics-and-analysis/

Sonatype. 2022. *8th Annual State of the Software Supply Chain Report.* https://www.sonatype.com/state-of-the-software-supply-chain/introduction

Sophos. 2023. *The State of Ransomware 2023.* https://news.sophos.com/en-us/2023/05/10/the-state-of-ransomware-2023/

Spoerry, L. 2022. CFC Aiming to Set Up Independent Cyber Cat Body by End-2023. *CyberInsurer.com.* https://cyberinsurer.com/articles/cfc-aiming-for-independent-cyber-cat-body-by-end-2023

Stransky, S. 2021. The Cyber Vendor Landscape. *Marsh-McClennan.* https://www.marshmclennan.com/insights/publications/2021/october/cyber-vendor-landscape.html

Swiss Re. 2017. *Cyber: Getting to grips with a complex risk.* Sigma No. 1. https://www.swissre.com/institute/research/sigma-research/sigma-2017-01.html

Synergy. 2023. Cloud Spending Growth Rate Slows But Q4 Still Up By $10 Billion from 2021; Microsoft Gains Market Share. February. https://www.srgresearch.com/articles/cloud-spending-growth-rate-slows-but-q4-still-up-by-10-billion-from-2021-microsoft-gains-market-share

Tatar, U, B. Nussbaum, O. Keskin, E. Dubois, and D. Foti. 2023 Setting the Scene: Framing catastrophic cyber risk – An expert panel discussion (Part 1). *The Society of Actuaries Research Institute.* January. https://www.casact.org/sites/default/files/2023-02/catastrophic_cyber_risk_expert_panel_report_.pdf

The Geneva Association. 2018. *Advancing Accumulation Risk Management in Cyber Insurance: Prerequisites for the development of a sustainable cyber risk insurance market.* Authors: Daniel Hoffmann and Steve Wilson. August. https://www.genevaassociation.org/publication/cyber/advancing-accumulation-risk-management-cyber-insurance

The Geneva Association 2022a. *Ransomware: An insurance market perspective.* Authors: Darren Pain and Dennis Noordhoek. July. https://www.genevaassociation.org/publication/cyber/ransomware-insurance-market-perspective

The Geneva Association 2022b. *Insuring Hostile Cyber Activity: In search of sustainable solutions.* Authors: Rachel Anne Carter, Darren Pain and Julian Enoizi. January. https://www.genevaassociation.org/publication/cyber/insuring-hostile-cyber-activity-search-sustainable-solutions

The Geneva Association 2023. *Forewarned is Forearmed: Emerging commercial liability trends.* Author: Darren Pain. March. https://www.genevaassociation.org/publication/evolving-liability/forewarned-forearmed-emerging-commercial-liability-trends

MalwareTech. 2017. Finding the Kill Switch to Stop the Spread of Ransomware. *U.K. National Cyber Security Centre.* 13 May. https://www.ncsc.gov.uk/blog-post/finding-kill-switch-stop-spread-ransomware-0

U.S. Treasury. 2022. *Potential Federal Insurance Response to Catastrophic Cyber Incidents.* September. https://www.federalregister.gov/documents/2022/09/29/2022-21133/potential-federal-insurance-response-to-catastrophic-cyber-incidents

The White House. 2023. *National Cybersecurity Strategy.* March.
https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

Veeam. 2023. *Ransomware Trends. 2023 global report*.
https://www.veeam.com/ransomware-trends-report-2023?ad=in-text-link

Verisk. 2017. *5 Things About Catastrophe Modeling Every Reinsurer Should Know.* February 14.
https://www.verisk.com/insurance/visualize/5-things-cat-modeling-every-reinsurer-know/

Verizon. 2022. *Data Breach Investigations Report*.
https://www.verizon.com/business/resources/reports/dbir/

Waterfall. 2023. *2023 Threat Report - OT cyberattacks with physical consequences.*
https://waterfall-security.com/scada-security/whitepapers/2023-threat-report/

Woo, G. 2021. Counterfactual Disaster Risk Analysis. *Casualty Actuarial Society*.
https://www.casact.org/sites/default/files/2021-07/Counterfactual-Disaster-Woo.pdf

Wood, D. 2023. Cyber Crisis: Is a reinsurance pool the answer? *Insurance Business.* 5 May.
https://www.insurancebusinessmag.com/au/news/cyber/cyber-crisis-is-a-reinsurance-pool-the-answer-444945.aspx

Woodruff Sawyer. 2023. Looking Ahead – *Cyber insurance trends for 2023*.
https://woodruffsawyer.com/wp-content/uploads/2023/01/Cyber-Looking-Ahead-2023_WEB.pdf

Zhang, M. 2023. Cloud Regions and Availability Zones: Explained. *Dgtl Infra.* 12 October.
https://dgtlinfra.com/cloud-regions-availability-zones/

The Geneva Association
Talstrasse 70
Zurich, Switzerland

www.genevaassociation.org