THE GENEVA ASSOCIATION

INSURANCE FOR A BETTER WORLD

CYBER RISK ACCUMULATION:

Fully tackling the insurability challenge

Research summary
November 2023

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

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.

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.

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 in cloud-based services.

Large and persistent cyber protection gap

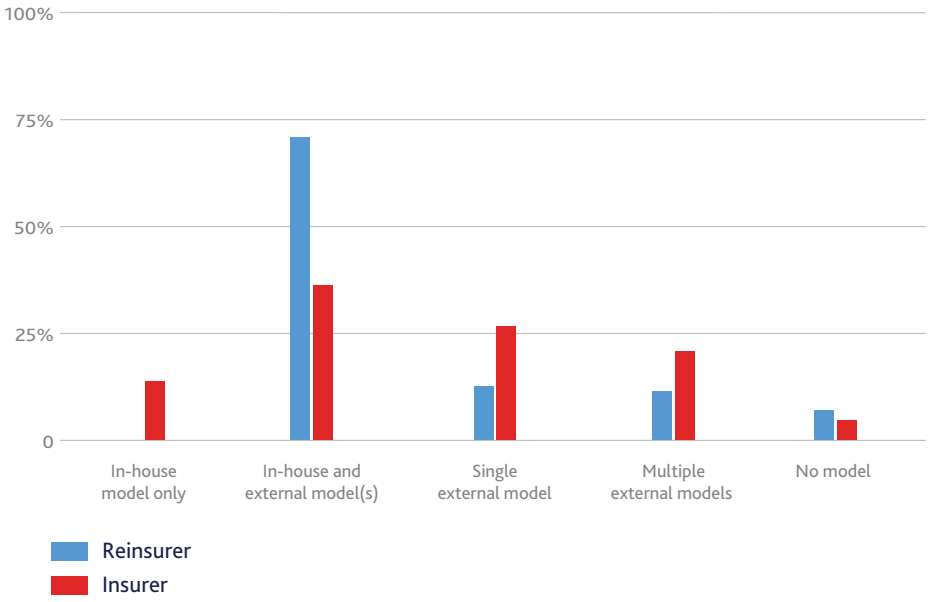
The more hostile cyber environment has only served to highlight the actuarial challenges that cyber risks pose. In particular, the factors that drive the frequency and severity of cyber losses are not always well-understood and typically cannot be modelled with standard statistical approaches. Cyber 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.

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, suggesting a sizeable chunk of cyber-related losses are uninsured.

Actuarial progress

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. As the cyber insurance market has grown and matured, underwriting practices for managing accumulation risks have evolved. 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. Similarly, 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.

FIGURE 1: 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

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. 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 1). 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.

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, also 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 (Table 1).

TABLE 1: 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

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.

Beyond better models

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.

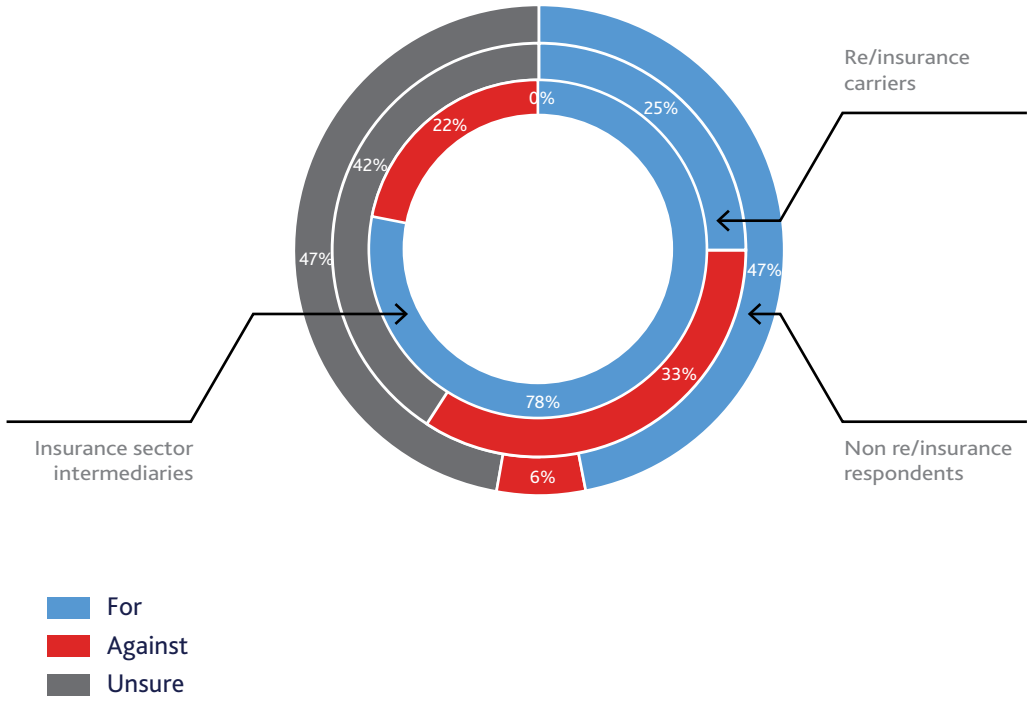
Ultimately, to address the significant cyber protection gap, government financing to backstop extreme re/insurance losses might also be needed. This could encourage and support the re/insurance sector to take on more cyber exposures, knowing that their downside losses are capped. Responses to a recent U.S. Treasury public consultation exercise suggest some support for a federal insurance programme for catastrophic cyber incidents 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 2).

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. 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. 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.

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. 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.

FIGURE 2: 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