



# HOWDEN

## Cyber insurance

Risk, resilience and relevance

# Key takeaways

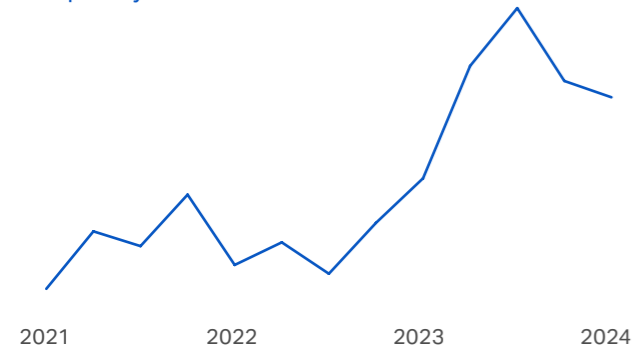
Cyber continues to live up to its dynamic reputation. With no sign of the risk landscape abating – as demonstrated by ransomware, geopolitical instability and the proliferation of Gen AI – market conditions offer businesses an opportunity to secure insurance cover at favourable terms.

## Fluid threat environment

### Ransomware frequency and severity: a mixed picture

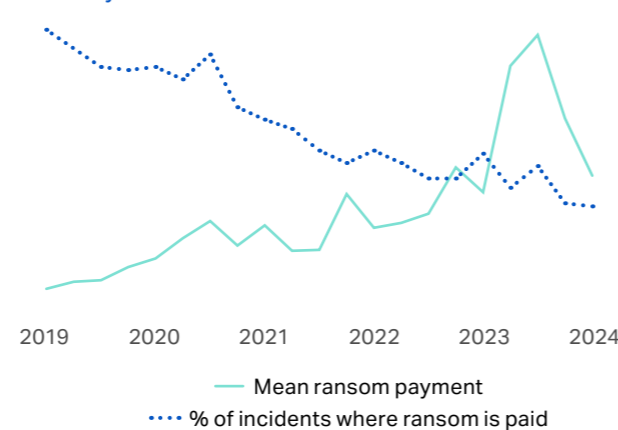
Source: Howden, NCC Group

#### Frequency



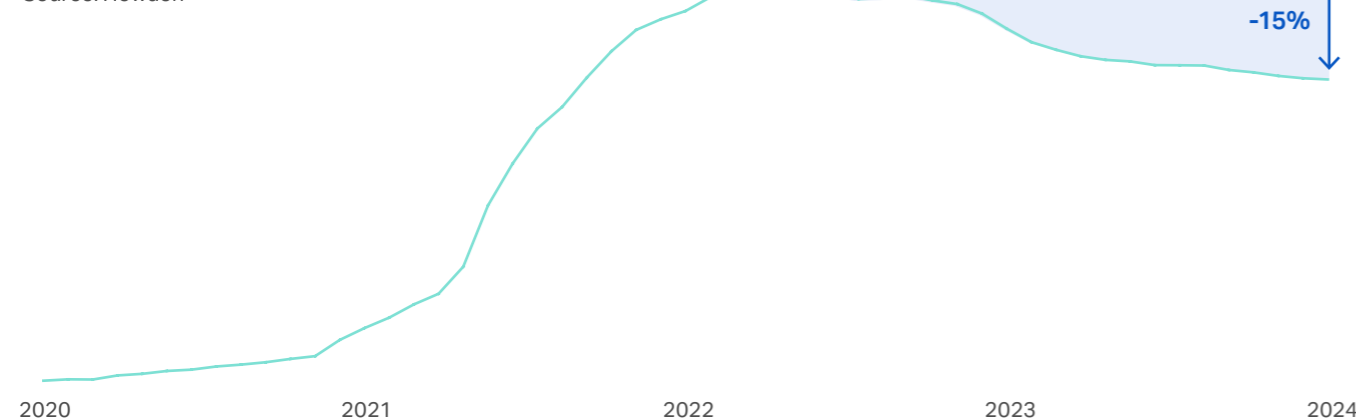
Source: Howden, Coveware

#### Severity



### Cyber insurance pricing down 15% from peak

Source: Howden

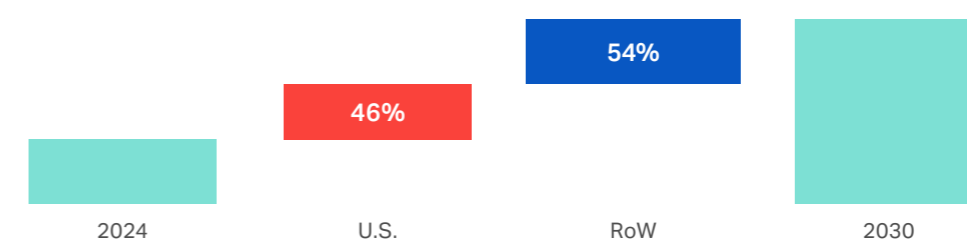


The foundations are now in place for the next phase of development, with opportunities in international geographies and other underserved areas poised to drive growth. Increased insurance penetration is the path to resilience and relevance.

## Untapped potential

### Share of projected premium growth up to 2030

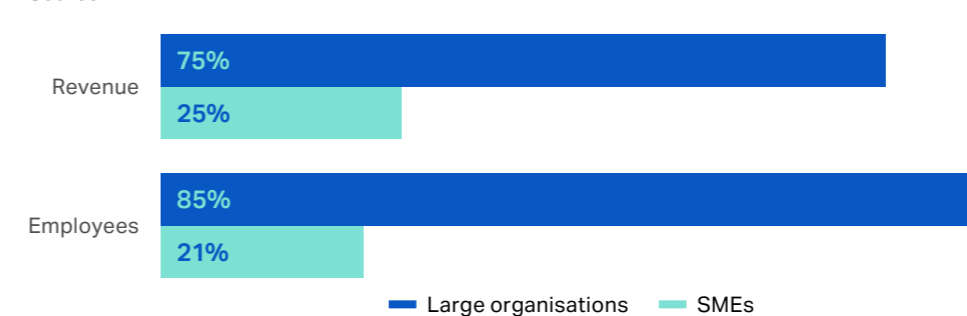
Source: Howden



Major economies in Europe, Asia and LatAm have considerable growth potential given current penetration levels.

### Existing share of organisations with cyber insurance globally; SMEs underserved

Source: WEF



SMEs are the backbone of economic activity in advanced economies and rely heavily on technology.

Innovation is key to growth, requiring a new approach to broking that is cycle-savvy, innovative, entrepreneurial, global and home to the sector's strongest talent. This is what Howden brings to the table and more. Come and talk to us.

# The implications



Welcome to Howden's fourth annual report on the cyber insurance market. The themes for this year's edition are risk, resilience and relevance.

At no other point has the market experienced the current mix of conditions: a heightened threat landscape combined with a stable insurance market underpinned by robust risk controls.

The implications are clear. Current conditions offer an opportunity for buyers to secure protection at favourable terms. For insurers, the opportunity is to lean into a class with clear potential for steady exposure-led growth, ongoing profitability and innovation.

are clear.

## Risk and resilience

Ransomware continues to stalk the threat landscape as the costliest form of cyber attack. The past 12 months have seen the splintering of ransomware groups, increased collaboration between hackers and tacit support from hostile governments. These trends have sustained the heightened threat, with data from NCC Group showing attacks increasing by 85% last year relative to 2022 (when activity dipped due to Russia's invasion of Ukraine) and by 30% from 1Q23 to 1Q24.

Data presents a more nuanced picture on the severity front. Recovery costs from ransomware are once again increasing after a temporary decline in 2022. In addition, multiple high-profile attacks have recently struck the healthcare sector, causing widespread disruption and major economic losses. Investments in cyber security and insurance coverage are paying dividends in this environment, with insured companies now less vulnerable to prolonged disruption in the event of an attack. This is reflected by a marked fall in the proportion of victims compelled to pay a ransom over the last year.

Staying one step ahead of attackers not only makes organisations more resilient to financially motivated cyber attacks, but it also means that they are better prepared to navigate any larger scale incidents. The recent MOVEit, Change Healthcare and NHS hacks have demonstrated how attacks on a single point of failure (SPoF) can radiate across the targeted organisation's customer base or IT network, ultimately affecting thousands of indirect victims. Insured losses are nevertheless expected to be manageable and these events provide valuable lessons around the potential for loss aggregation in any future attack(s).

The rise of Gen AI is the major new development since Howden's previous assessment of the threat landscape. Technologists, cyber security experts and the insurance market broadly agree that this new technology will transform offensive and defensive capabilities. Our research brings the debate forward by drawing out the specific ways in which Gen AI is most likely to increase the frequency, severity and aggregation of claims but also how the technology, along with existing risk controls, can be deployed to repel threat actors.

## Relevance

Over the past few years, carriers and brokers have undertaken important steps to enhance price stability, coverage clarity and the consistency of terms and conditions. Taken together, these actions present solid foundations for a new phase of development for the market.

Against this backdrop, the market has two stand out opportunities to preserve market leading annual growth and secure long-term relevance: expansion beyond the U.S. and serving a broader client base amongst small and medium-sized enterprises (SMEs) across all regions.

Analysis in this report reveals that more than half of premium growth is likely to emanate from non-U.S. territories. In the major European economies of Germany, France, Italy and Spain alone, the premium uplift potential in just replicating penetration levels recorded in more mature markets can be measured in the (high) hundreds of millions of euros.

The SME space, which accounts for close to half of GDP in advanced economies, also offers huge opportunity as brokers and insurers find better ways to bring this currently underserved demographic into the cyber market.

Considerable progress has been made in a short space of time, but our research shows that more work needs to be done to meet demand globally. Innovation is crucial to tapping into new pools of capital and penetrating currently underserved markets.

Howden exists to do just that. We look forward to supporting clients (new and old) in finding the best risk transfer solutions and building cyber resilience in what remains a highly fluid threat landscape.

# A pervasive threat

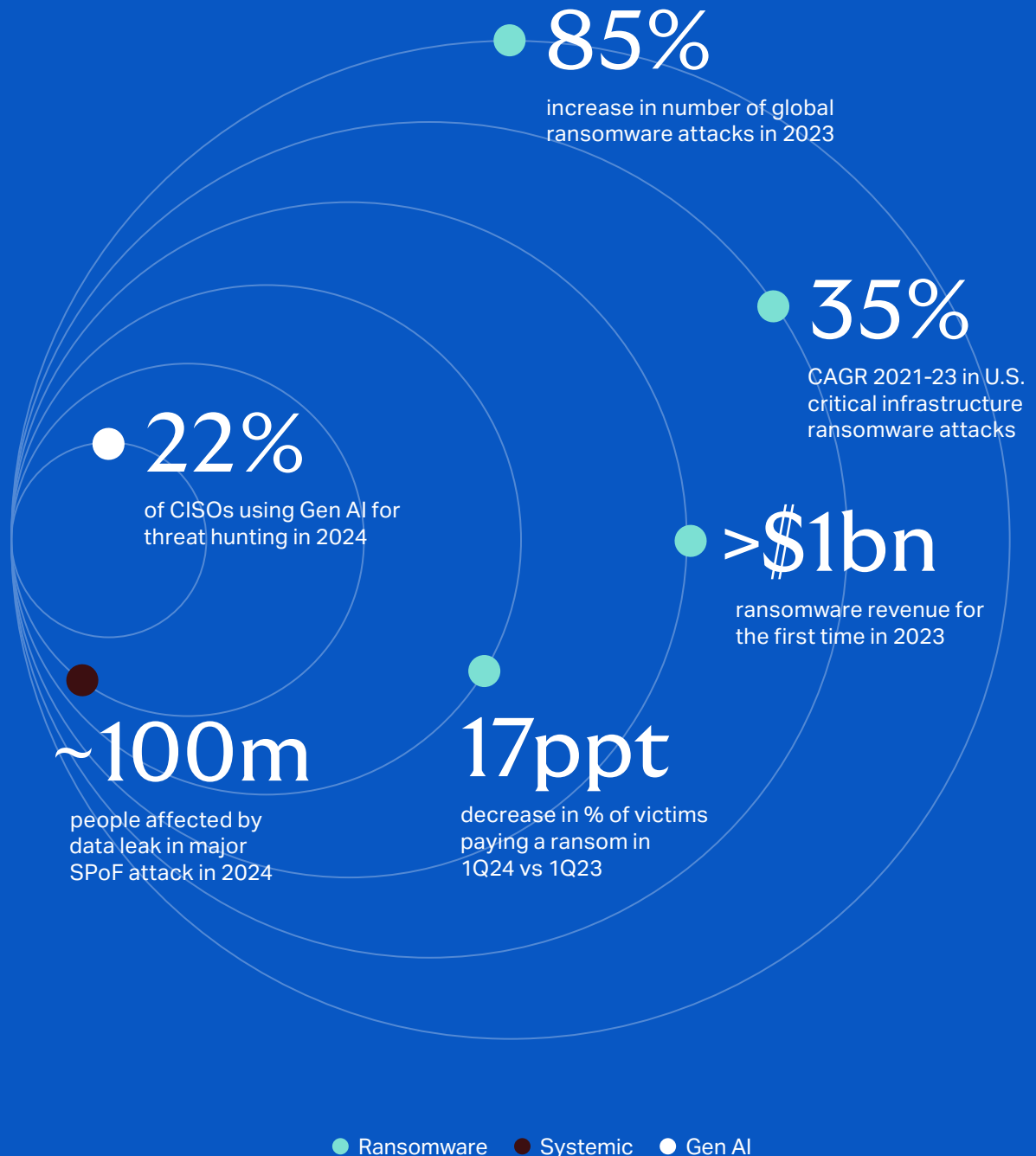
After a prolonged run of market leading growth, cyber insurance is entering a new phase in its journey to maturity.

Having navigated the early stages of development that often come with new, fast growing lines of business, competition is now increasing as insurers look to grow in a space that has huge potential and is relevant to businesses worldwide.

With little sign of the threat environment abating any time soon – the last 12 months have brought resurgent ransomware activity (including a number of high-profile attacks on healthcare entities), persistent geopolitical instability and the proliferation of generative artificial intelligence (Gen AI) – current market conditions offer clients and prospects an opportunity to secure protection at favourable terms.

**Figure 1: Cyber threat landscape in 2024**

(Source: Howden analysis using data from Coveware, NCC Group, Chainalysis, Splunk, House Committee on Energy and Commerce, FBI)



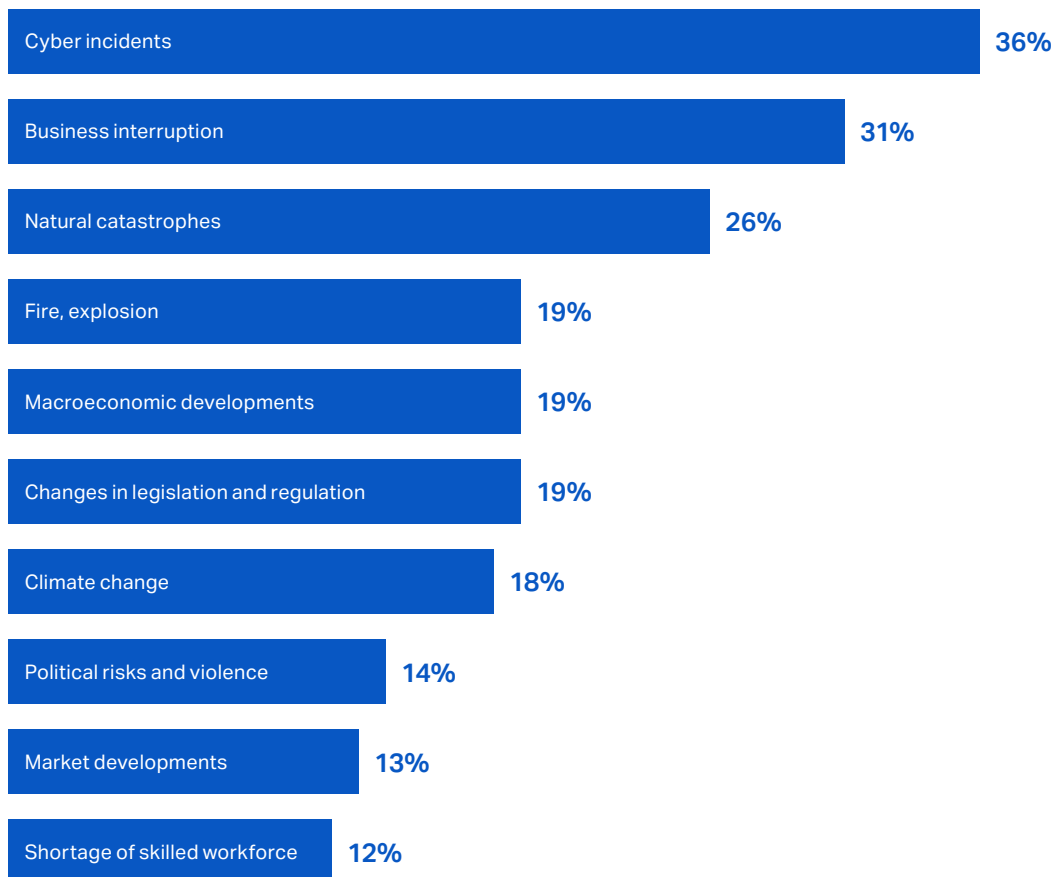


Strengthened cyber resilience is paying dividends for policyholders now attacks are reverting to the long run upward trend. After a temporary lull in 2022 due to Russia’s invasion of Ukraine, ransomware activity has returned to historic high levels. There has also been a steady increase in U.S. privacy claims due to increased biometric breaches and pixel litigation following some high-profile settlements whilst the resurfacing of aggregation risk continues to hang over the market. Recent developments in both of these areas serve to talk to the tail-risk associated with cyber insurance.

All of which has led cyber to increasing its lead as the top global risk in this year’s Allianz Risk Barometer (see Figure 2). Reflecting the pervasive threat landscape, respondents ranked data breaches as the cyber exposure of most concern (59%), followed by attacks on critical infrastructure and physical assets (53%) and the increase in ransomware attacks (53%).<sup>1</sup>

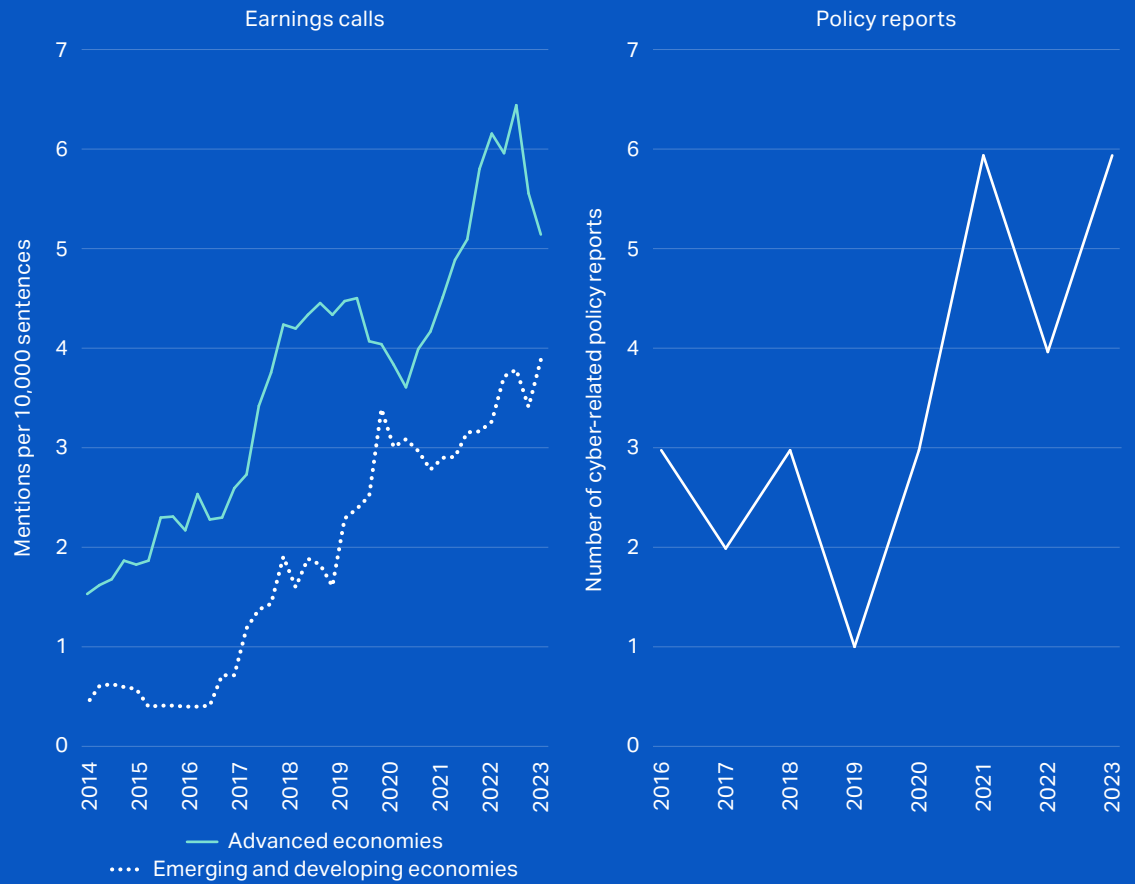
This elevated awareness of risk tallies with the release of several cyber-related policymaking publications in recent years, alongside growing references to cyber risk in corporates’ earnings calls (see Figure 3).

Figure 2: Allianz Risk Barometer 2024<sup>1</sup> (Source: Allianz Commercial)



<sup>1</sup> Figures represent how often a risk was selected as a percentage of all survey responses. Figures do not add up to 100%, as respondents were asked to name up to three risks they saw as most important.

Figure 3: Growing profile of cyber risk amongst corporations and policymakers  
 (Source: Howden analysis using IMF data)



“  
 Strengthened  
 cyber resilience is  
 paying dividends for  
 policyholders now attacks  
 are reverting to the long  
 run upward trend.

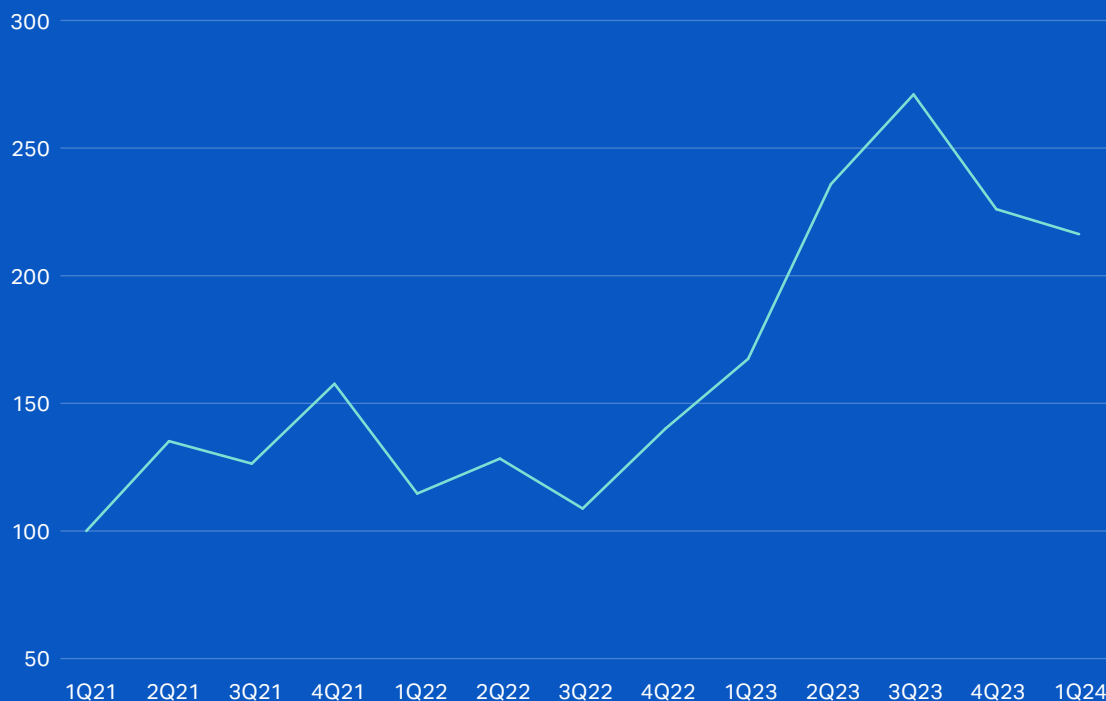
## Ransomware frequency

Ransomware continues to dominate the cyber loss environment. Given current levels of frequency and severity, ransomware looks set to be a source of significant losses for businesses for some time to come.

Figure 4 shows how the frequency of global ransomware attacks has trended since 2021. The availability of accessible (and low cost) ransomware kits, otherwise known as ransomware-as-a-service (RaaS), combined with the ongoing profitability of attacks, have been important factors in driving the proliferation of ransomware during this timeframe.

**Figure 4: Frequency index for ransomware – 1Q21 to 1Q24<sup>2</sup>**

(Source: Howden analysis based on data from NCC Group)



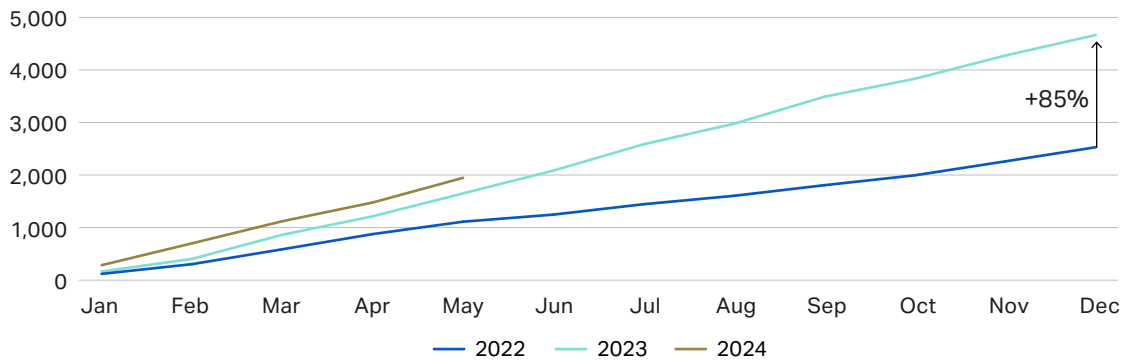
Fears that Russia's invasion of Ukraine in early 2022 would fuel activity proved to be unfounded as both warring sides, host to some of the worst offending ransomware groups, focused their efforts and resources on kinetic warfare.

Ransomware activity has picked up significantly since then, however. Established gangs, facing depleted funds following a drop in revenues in 2022, along with the emergence of new groups, drove a marked acceleration in frequency last year. Figure 5 compares cumulative ransomware activity by month between 2022 and early 2024, with data from NCC Group showing frequency up 85% in FY23 compared to FY22.

Whilst increased pressure on gangs from law enforcement agencies (including efforts to take down Russian groups such as LockBit and BlackCat) has played a part in driving activity down from peak levels recorded in 3Q23, it does not appear to have had a decisive impact. Recorded incidents in the first five months of this year were up 18% on already elevated 2023 levels.

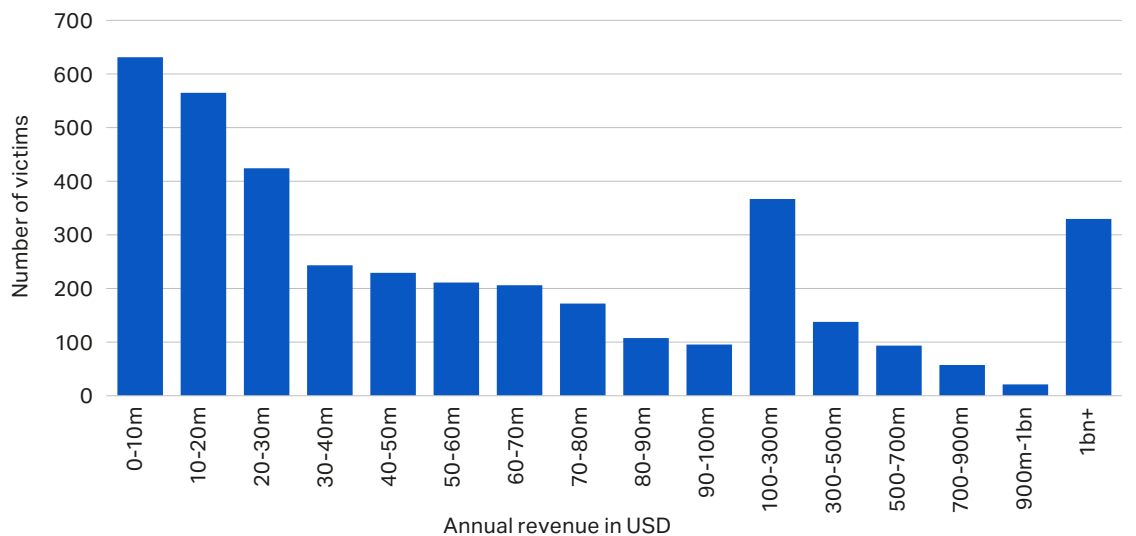
Law enforcement action has also emboldened cybercriminals to hit back at critical infrastructure, with U.S. healthcare providers Change Healthcare and Ascension falling victim to ransomware attacks in February and May this year. These attacks caused significant disruption to both companies and have triggered substantial first-party (in the case of Ascension) and third-party claims. A number of UK hospitals also suffered serious disruption in June following a ransomware attack on Synnovis, a provider of pathology services for the NHS.

**Figure 5: Cumulative global ransomware activity by month – 2022 to 2Q24<sup>2</sup>**  
(Source: Howden analysis based on data from NCC Group)



Companies of all sizes continue to be targeted, with a noticeable bias towards the upper and lower bands of the revenue range (see Figure 6). Attackers' tactics are predicated on maximising financial gain whilst minimising risks, with gangs weighing up victims' ability to pay against security measures in place without provoking a response from law enforcement agencies.

**Figure 6: Distribution of ransomware attacks by companies' annual revenue in 2023/24**  
(Source: Howden analysis based on Black Kite data)



<sup>2</sup> NCC Group tracks ransomware groups operating the hack and leak double extortion tactic by monitoring leak sites and scraping victims' details as they are released.

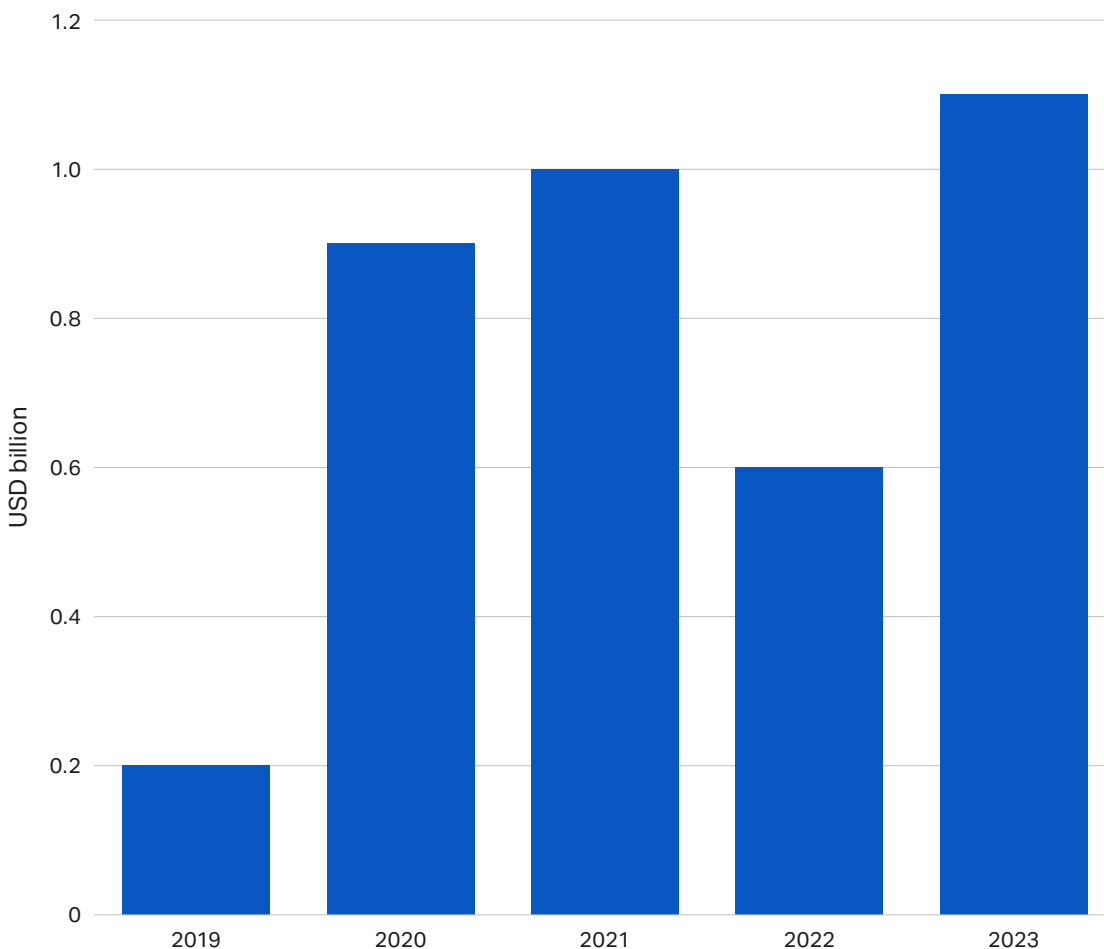
## Mixed severity

Ransomware frequency only tells part of the story from a loss perspective. The severity side of the equation is primarily made up of downtime costs (business interruption and lost productivity), ransom payments and other expenses. These can be more challenging to measure, particularly when factoring in intangible impacts such as reputational damage. Available data presents a nuanced picture, with recent large-scale attacks underlining how the ransom payment (if there is one) can be only the tip of the iceberg.

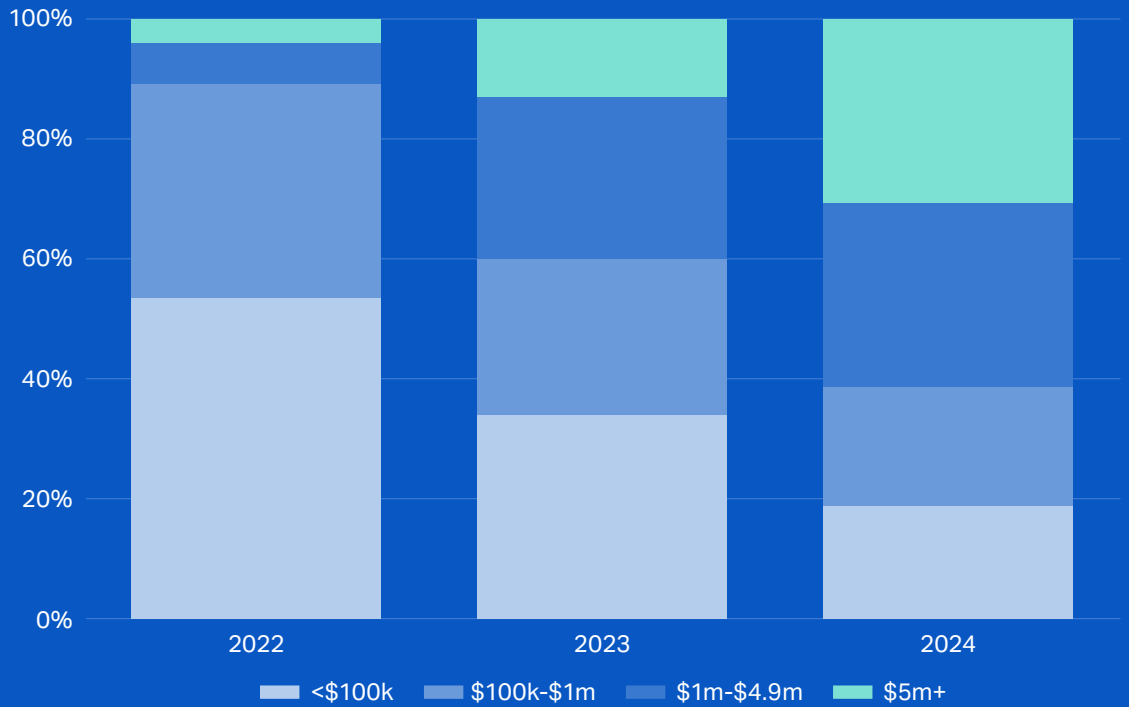
Whilst data from Chainalysis and Sophos shown in Figures 7 and 8 reveal how paid ransoms in dollars have increased in recent years, they mask an equally important trend away from payment. Coveware data in Figure 9 shows a marked decline in the proportion of companies paying ransoms between 2019 and early 2024, falling to 28% in 1Q24 compared to an average of 70% in 2020.

Companies that have invested in risk controls and crisis management are now less susceptible to material impacts, rebalancing cost-benefit considerations for some firms over whether to pay ransoms. Furthermore, the increasing prevalence of double and even triple extortion has undermined the assumption that paying a ransom will put a stop to the hack.

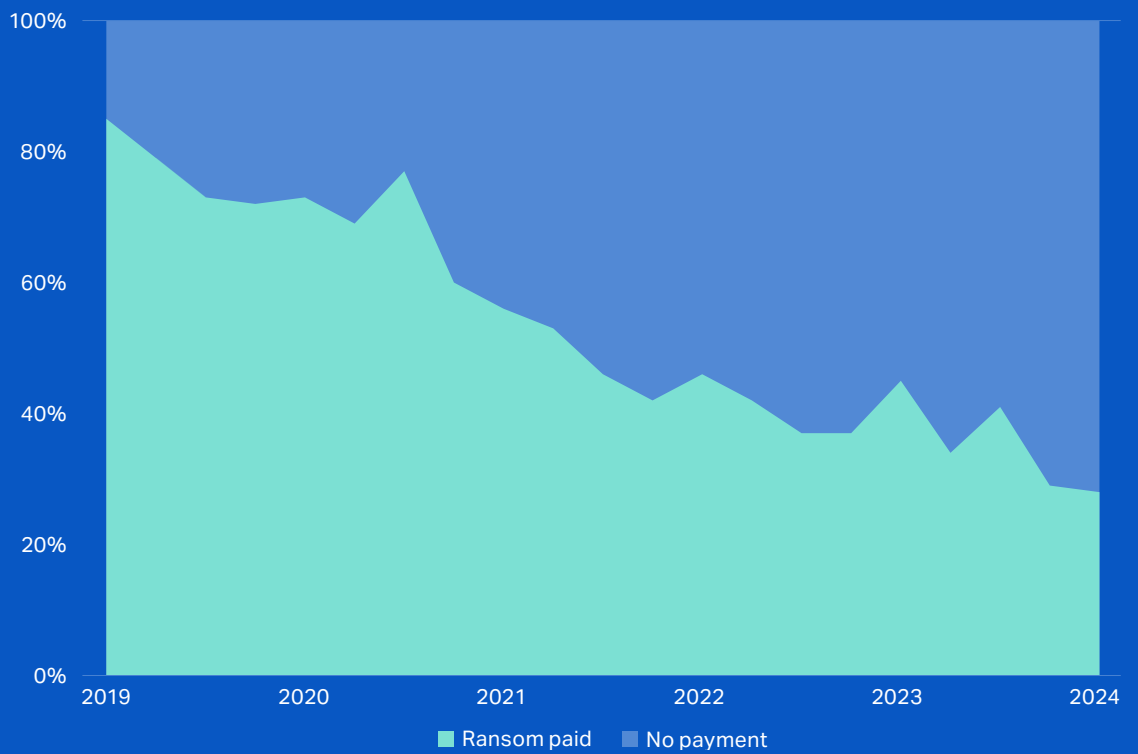
**Figure 7: Revenue received by ransomware attacks – 2019 to 2023** (Source: Chainalysis)



**Figure 8: Distribution of ransom payment amounts – 2022 to 2024**  
 (Source: Howden analysis using Sophos data)



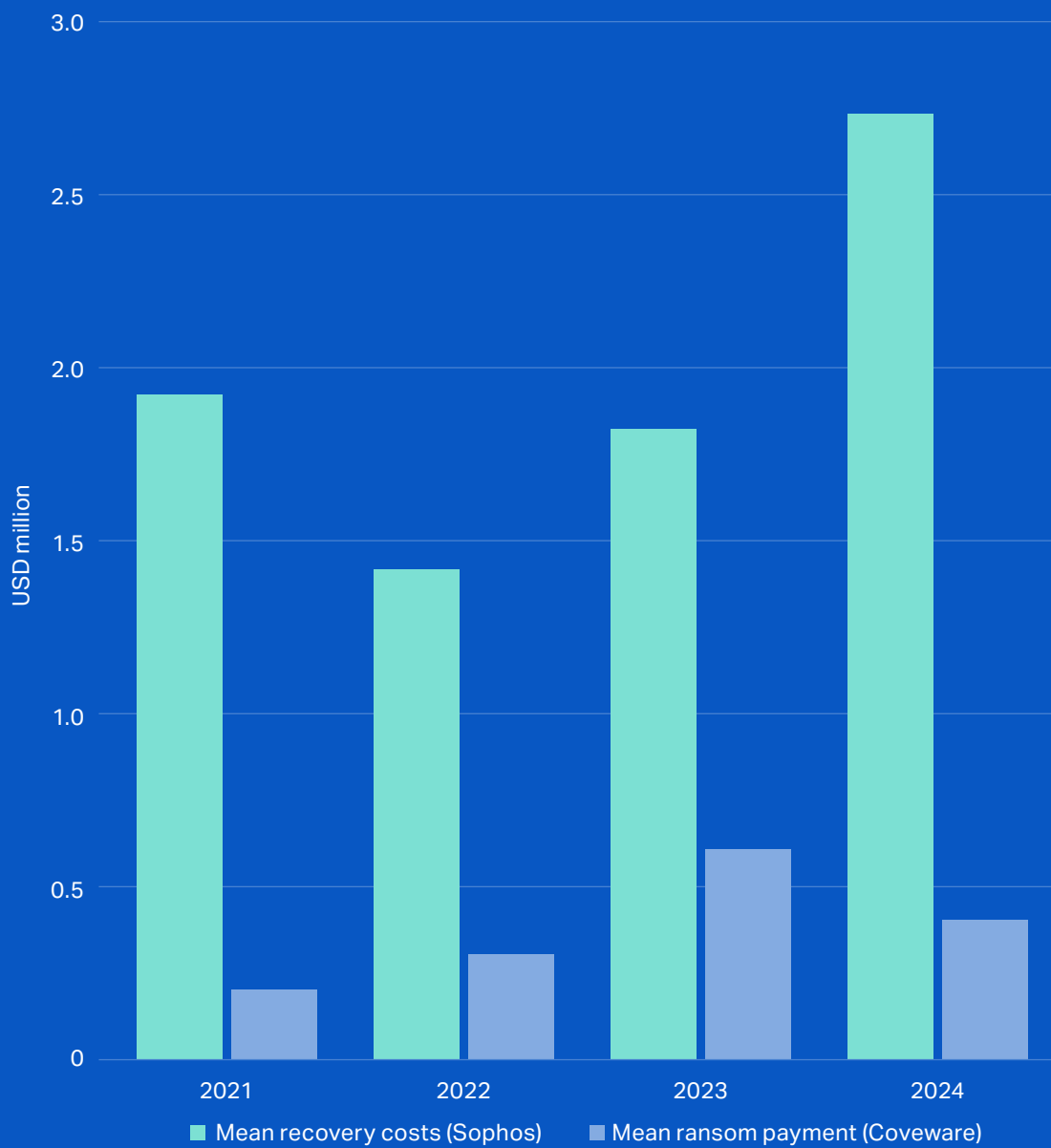
**Figure 9: Proportion of ransomware victims paying a ransom – 1Q19 to 1Q24**  
 (Source: Howden analysis based on Coveware data)



Ransom payments are just one input into losses sustained by companies. Data from Sophos and Coveware in Figure 10 compare mean ransom payments to mean recovery costs, with the latter accounting for the lion's share of total costs through the timeframe.

According to S-RM, business interruption is typically the biggest cost component of a significant event, making up to 70% of claims costs where a firm is heavily reliant on the availability of critical systems in sectors such as manufacturing and financial services. Other ancillary costs can aggregate when there is significant regulatory exposure, or where multi-jurisdictional exposure brings the need to address various regulatory obligations.

**Figure 10: Mean ransom payments and recovery costs from ransomware attacks – 2021 to 2024<sup>3</sup>** (Source: Howden analysis based on Coveware and Sophos data)

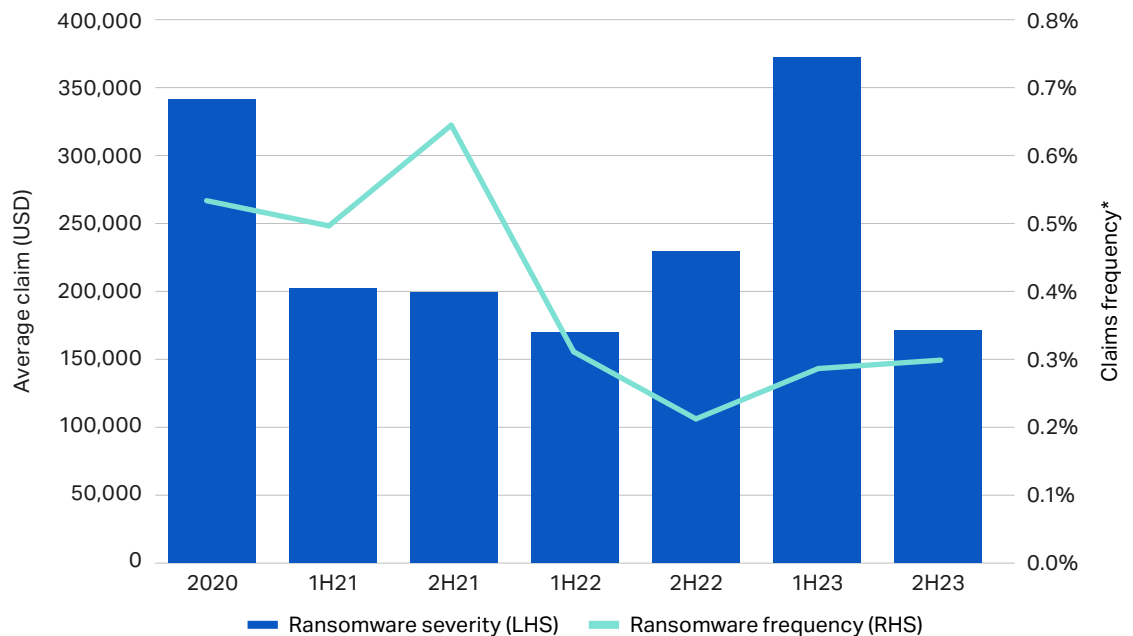


## Building resilience

An increasing number of ransomware attacks now involve the theft of sensitive personal or commercial data for extortion purposes (i.e. threatening to leak data into the public domain), which not only increases the complexity of incidents but also brings a greater risk of reputational damage. Hardened cyber defences and secure backups have helped to mitigate business interruption losses, thereby insulating insured companies from prolonged disruption or outsized losses.

These conflicting dynamics continue to play out in the market, with peaks and troughs in ransomware frequency and severity indicative of fast-moving developments (see Figure 11 for data recorded by Coalition based on its own book of business since 2020).

**Figure 11: Ransomware claims frequency and severity for Coalition policyholders – 2020 to 2023** (Source: Howden analysis based on Coalition Claims Report)



\* Frequency is the average number of claims per earned insurance policy, without reflecting policy limits and / or retention.

Disclosures in 2023 and early 2024 nevertheless continue to show strong profitability for cyber insurance, reflecting price adequacy for a wide range of incidents, the success of risk controls in mitigating losses and the ability to adapt terms quickly given the short-tail nature of the business.

All of which portends runway for favourable market conditions more generally. As cyber lives up to its dynamic reputation, the value of insurance is being brought into even sharper focus as it incentivises (and helps to implement) better cyber hygiene, strengthens resilience and indemnifies losses.

<sup>3</sup> Recovery costs include downtime, people time, device costs, network costs and lost opportunities. 2024 for average ransom payment from Coveware represents data available at 1Q24.



# Systemic cyber: the known unknown

Prevention, preparedness and protection are critical layers of defence in such a heightened threat environment. Improved risk management not only makes organisations more resilient to ransomware and other financially motivated cyber attacks, but it also means that they are better equipped to navigate a highly volatile geopolitical climate that increases the potential for larger-scale incidents.

“

# The uncertainty around aggregation continues to hang over the market.

Risks associated with cyber warfare and systemic events more generally – scenarios where single attacks trigger widespread failures across multiple organisations – remain a concern but worst-case scenarios have not yet come to pass. The risk of and uncertainty around aggregation continues to hang over the market by impeding capital inflows and tempering risk appetite, but loss data to date shows that the most pervasive threat comes from targeted (and lower level) attacks carried out by criminal gangs rather than state actors.

Indeed, much of state-level cyber activity connected to current warzones has been integrated and contained to the kinetic campaign. This is indicative of shifting priorities during conflicts: cyber tactics and tools deemed most effective in supporting military goals (e.g. sabotage and / or disruption) are likely to take priority in certain phases.

Hostile governments nevertheless continue to shield criminal actors in their respective countries, allowing them to operate with near impunity when attacking Western companies and critical infrastructure (see the contribution from XCyber on pages 28-31). Healthcare has been a prime target for a number of years now, likely reflecting the prevalence of legacy (and interconnected) systems, large volumes of sensitive data and a relatively high willingness to pay ransoms to restore operations quickly and protect life.

Figure 12 on page 20 shows that the number of ransomware attacks on U.S. critical infrastructure increased by a CAGR of 35% between 2021 and 2023.

**Figure 12: Reported ransomware attacks on U.S. critical infrastructure – 2021 to 2023**  
 (Source: Howden analysis on FBI data)



“

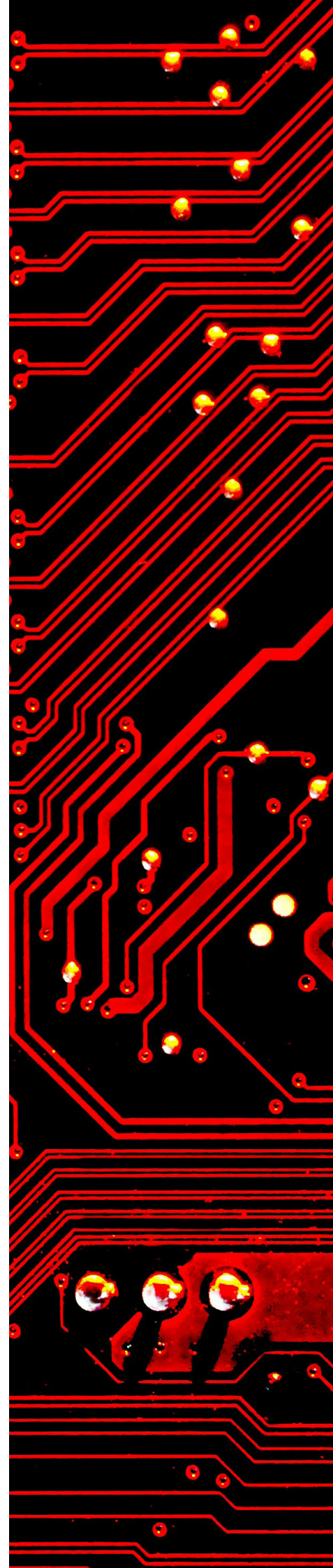
Hostile governments continue to shield criminal actors in their respective countries, allowing them to operate with near impunity when attacking Western companies and critical infrastructure.

## Warning shots

Systemic cyber attacks are highly uncertain in terms of trigger, likelihood and size. On the one hand, the potential for loss is clear – the proliferation of attack surfaces from rapid digitalisation, limited understanding of where and how technologies are vulnerable and a dearth of historical data on cyber catastrophes – but it is also true that only a small number of nation state actors or highly sophisticated groups have the capabilities, expertise and resources to execute such attacks. These actors also need to balance the attendant risk of escalation and reprisals associated with a large-scale cyber attack.

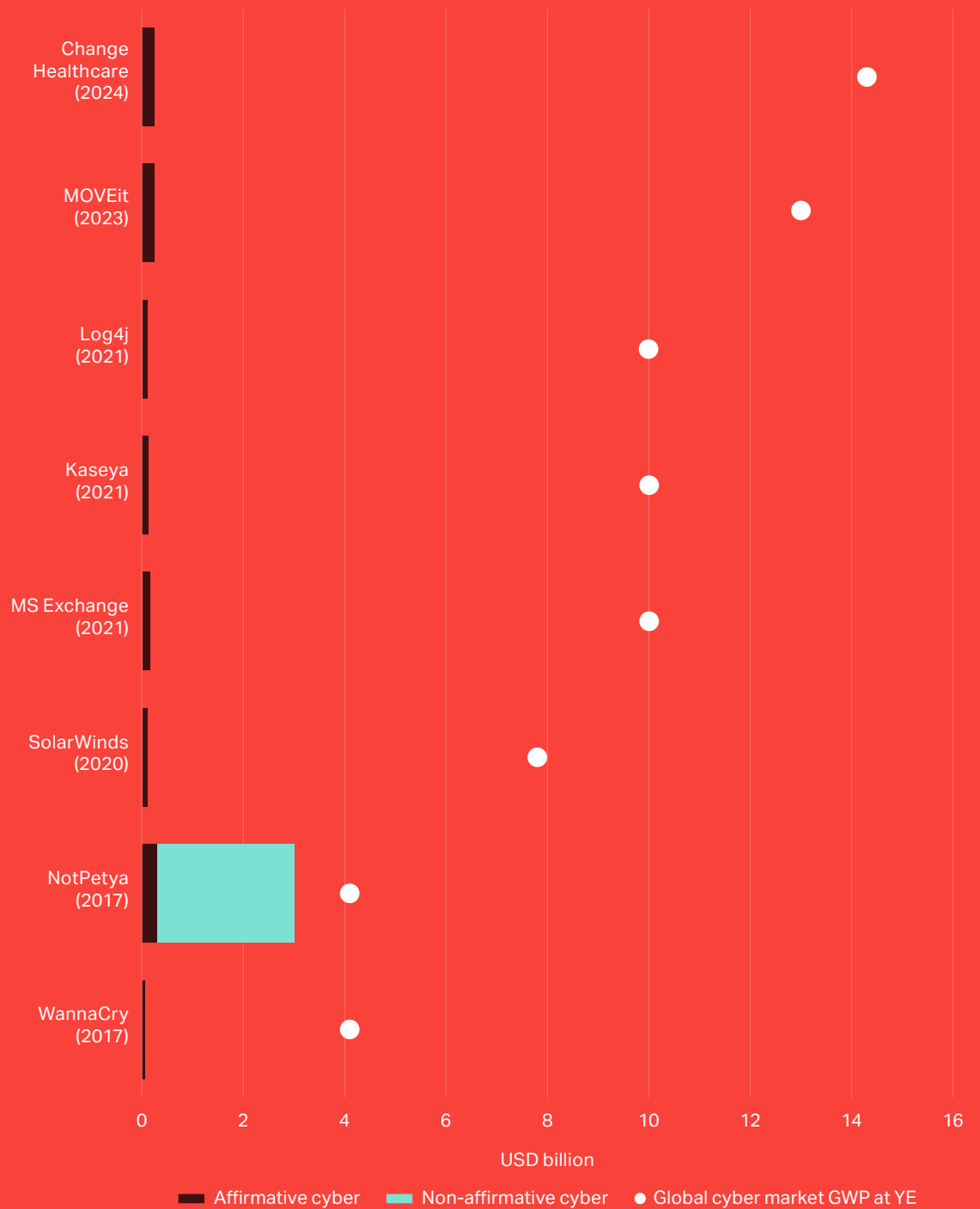
Several incidents in recent years, including SolarWinds, Microsoft Exchange, Kaseya, Log4j and MOVEit, have seen threat actors target software supply chains in an attempt to maximise the fallout across multiple organisations, even if losses have ultimately been manageable for the insurance market (see Figure 13).

Change Healthcare is the latest event to raise questions about the extent of aggregation risk. Whilst it will take some time to know how losses will develop, Verisk's Property Claim Services (PCS), a provider of insurance loss estimates, has designated the event a cyber catastrophe, which points to a market loss in excess of USD 250 million.



The ability of the cyber market to absorb losses of the quantum often associated with large-scale events will grow over time as it approaches the scale of other major P&C lines of business and pricing is sustained at levels commensurate with risks. Clarifications about the applicability of war exclusions to all but the remotest of nation state attacks should also reduce the scope for claims disputes and encourage more capacity to enter the market.

**Figure 13: Insured loss estimates for high-profile cyber events vs GWP for global cyber market (Source: Howden, PCS)**



## Aggregation risk

None of which is intended to minimise the potential for risk aggregation. A large-scale event that resulted in a widespread cloud outage, disrupted global payment platforms or compromised software that underpins global digital systems (see callout opposite for S-RM's view on the latter) would pose a serious risk to the market and broader economies, although this is true of tail events in several other lines of business.

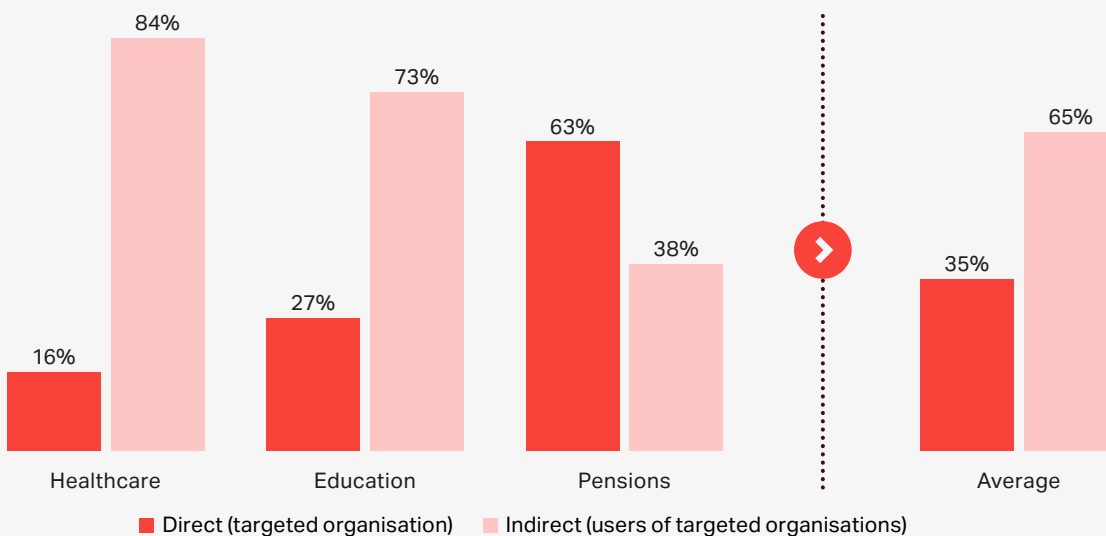
The MOVEit and Change Healthcare incidents help to contextualise the loss potential associated with systemic events. Recent disclosures show that the MOVEit file transfer breach, which began in June 2023, affected approximately 2,800 organisations and 96 million people.

The user base for the Change Healthcare payments and claims platform is made up of 900,000 doctors, 33,000 pharmacies and 5,500 hospitals in the United States. The CEO of parent company UnitedHealth has indicated that up to one-third of the U.S. population has had sensitive data leaked. The scale of these types of attacks underscores how economic costs have the potential to spiral.

The impact of the loss on the cyber insurance market is nevertheless expected to be manageable. Not only has UnitedHealth confirmed it lacked standalone cyber cover at the time of the attack (a major miss for the market given the company booked USD 870 million in costs related to the breach in 1Q24 and estimated they could rise to USD 1.6 billion for the full year), but the support afforded to affected third parties by UnitedHealth has limited the fallout and stemmed claims.

Figure 14 incorporates trends observed during recent systemic ransomware attacks to show how costs sustained by third party companies not directly targeted (including business interruption, clean-up costs and any secondary ransomware payments) can make up the lion's share of economic losses overall. Events underscore the inherent risk of aggregation across multiple organisations via a SPoF and reveal how losses have been concentrated in sector verticals due to reliance on industry specific software and payments / administration platforms.

**Figure 14: Estimated economic distribution from major ransomware attacks in 2023/24**  
 (Source: Howden analysis of public economic and insured cyber loss data)<sup>4</sup>



As more information comes to light around ransomware exposures, data shows that claims from indirect attacks have been (much) lower on average relative to direct claims. Coupled with the inconsistent provision of contingent business interruption cover for cyber attacks and the work businesses are undertaking to reduce supply chain risk, the degree of loss aggregation (or frequency of loss) would need to be multiples of what has been experienced to date to generate losses that threaten the premium base of the global market.

All of which serves to reinforce the importance of securing tailored and comprehensive cyber insurance cover with adequate limits. Access to the best broking advice can make all the difference to achieving this goal in the current marketplace.

## S-RM on risk of digital cornerstone attacks

By Roddy Priestley, Director, Cyber Security and Martijn Hoogesteger, Head of Cyber Security, Benelux

A successful attack on a digital cornerstone carries equivalent catastrophic potential impact to a global cloud outage. Such a scenario would see a malicious actor compromising the software that underpins global digital systems. Given most organisations rely on two operating systems – Windows and Linux – and these in turn rely on open-source libraries developed collaboratively by unknown contributors, a single compromise could have an enormous impact.

An incident earlier this year underscores this systemic risk after a Microsoft engineer identified a malicious backdoor in an open-source library called XZ Utils, which is built into most Linux operating systems. This had been implanted into the code by one of its contributors, in what appears to be a meticulously planned operation over several years. Had the compromise not been identified, the unknown actor behind the operation would have had backdoor access to almost every organisation, as Linux servers are often used to host backup systems, databases, virtualisation hosts, cloud services, web servers and enterprise resource planning systems.

As well as state actors, some criminal groups are known to be investing large amounts of cash into developing a wide-ranging compromise of this nature. Although the likelihood of such an event remains low, requiring a cascade of unfortunate events to occur, the impact could be catastrophic

---

<sup>4</sup> Sources used in Figure 14 are Change Healthcare, Coalition, At-Bay, Pension Benefit Information and National Student Clearinghouse. Analysis is based on reported numbers of entities affected and average costs for first- and third-party ransomware attacks.

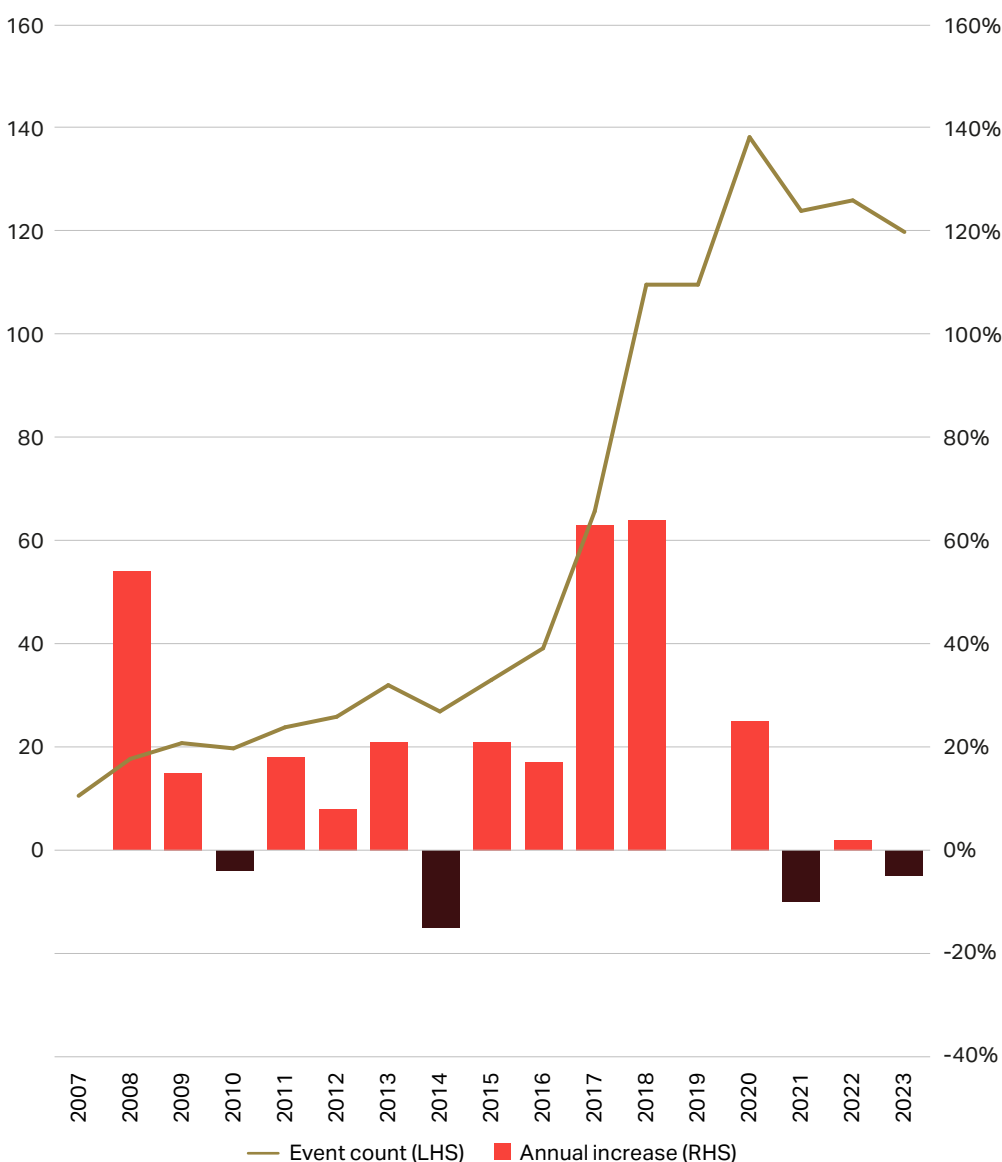


## The geopolitical effect

An increasingly febrile geopolitical environment is adding to the sense of uncertainty. Data from the Centre for Strategic and International Studies (CSIS) shown in Figure 15, which provides a snapshot of state-affiliated activity by charting major cyber attacks against government agencies, defence and high-tech companies, reveals a dramatic increase over the last decade. Russia and China are shown to be the standout perpetrators, accounting for 65% of attacks in the past year (April 2023 to March 2024).

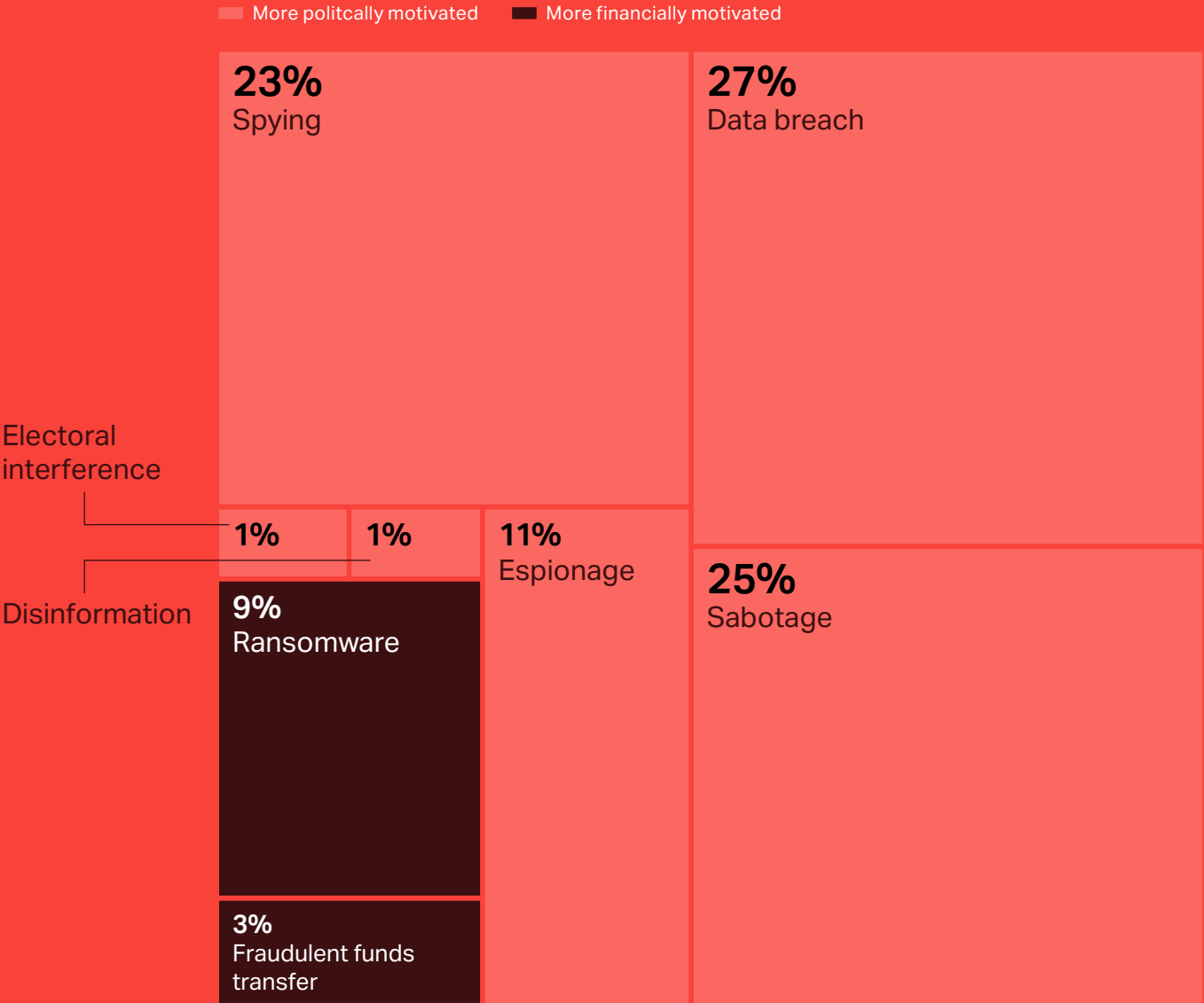
**Figure 15: Number of major state-affiliated cyber attacks – 2007 to 2023**

(Source: Howden analysis of attacks recorded by CSIS)



The breakdown of cyber incidents by type reflects nation states' motivations, with close to 90% of incidents politically motivated (data breaches, sabotage and spying being the most frequent forms of attack).

**Figure 16: Major state-affiliated cyber attacks by type - April 2023 to March 2024**  
 (Source: Howden analysis of attacks recorded by CSIS)



The reach and duration of ongoing wars in Ukraine and the Middle East, alongside lower-level activity aimed to undermine the democratic process in a major election year, are likely to have profound effects on global cyber security.

This reaffirms the important work being done by the market in getting ahead of the cyber warfare issue and determining proactively the scope of cover should any major nation state loss materialise. A recent survey by the World Economic Forum shows that 70% of CISOs reported that geopolitics has influenced their firm’s cyber security strategies.

Nation states are increasingly bolstering their cyber capabilities to seek political, economic and military advantage, thereby blurring distinctions between state-orchestrated attacks and those carried out by affiliate groups. Insights provided by XCyber overleaf provide intelligence-led expertise into what can be expected in relation to the fallout from heightened geopolitical risk.

# Geopolitics and the cyber threat landscape

---

**Milo Wilson**

Lead Intelligence Analyst at XCyber

---

**Bill Jarvis**

Head of Intelligence at XCyber

Amidst rising tensions and shifting priorities between global powers in cyber space, the most important threat to businesses is the growing professionalisation of cybercriminals as they carry out sophisticated attacks with impunity from hostile countries.

## Tensions between nation states heat up in cyber space

Global cyber powers appear to have accepted that concerted state-sponsored, and often aggressive, cyber campaigns have become a norm. The demarcation between the West and the so-called 'big four' of Russia, China, North Korea and Iran (which has become increasingly apparent over the last 12 months) will likely lead to more aggressive cyber campaigns in the future.

Russia specifically has abandoned any pretence of cracking down on cybercriminals operating inside its borders, as demonstrated by the passing of a law last year that provides immunity for crimes committed by hackers 'in the interests of the Russian State'. Russia's protection of cybercriminal groups has

heightened the global threat landscape, especially as sanctions against Russia have left a large amount of un(der)employed skilled IT professionals that could be enticed into lucrative cybercrime.

Russia is ultimately aiming for a contested and unsafe cyber landscape, as it believes this will disproportionately harm Western powers, something seen in the running of disinformation networks targeting global elections. This heightened threat landscape has also arguably led to more aggressive espionage campaigns from Chinese state actors, as well as more pointed responses from their targets.

## Repeat of Ukraine cyber conflict unlikely

It is hard to draw firm conclusions from the war in Ukraine on future conflicts. Ukraine has both an extremely resilient domestic cyber security ecosystem, as a result of years of preparation against Russian attacks, and has been supported by some of the world's largest tech companies. Russia has also been careful to contain the impacts of its cyber efforts in Ukraine to the conflict zone, despite its capability to launch attacks of greater scale and consequence.

Future conflicts could differ though, with concerns centred on a war involving aggressive and competent cyber attackers that reveal highly destructive malware or

other techniques to the wider world. China is amongst the most aggressive exploiters of zero-day vulnerabilities. In 2021, the Chinese government passed a law that made the reporting of vulnerabilities to authorities before public release compulsory.

This appears to have significantly boosted China's offensive cyber capabilities (Chinese groups were the most prolific attackers to exploit zero-days in 2023). Criminal groups have a long history of exploiting state-backed hacking techniques once they are revealed publicly, particularly against businesses too slow to adapt to the new vulnerabilities.

## Russia pivots to espionage

Russia's cyber efforts in Ukraine over the last year have shifted away from disruptive and destructive attacks (the deployment of wiper malware specifically) towards espionage and intelligence gathering, with the evolution of tactics reflecting reset expectations around the duration of the war.

The resilience of Ukraine, both militarily and in the cyber sphere, has seen the nature of the war change, which in turn has impacted Russian cyber efforts. Sandworm, the most active Russian-backed group in Ukraine, for example, has pivoted from disruption to intelligence collection, with increasing emphasis on espionage to assist Russia's forces.

The blending of military and cyber goals reflects the nature of warfare in that the objectives of cyber operations can be achieved more efficiently with kinetic warfare. Whereas Russian pre-war cyber attacks against Ukrainian energy infrastructure caused (at most) hour-long blackouts, 80% of its electricity-generating capacity has now been lost in almost 180 aerial attacks.

Operations extend beyond Ukraine. The same actors are also running disinformation campaigns to coincide with a number of high-profile elections this year. Election interference is part of a wider effort from Russia to disrupt Western interests, including the use of mercenaries in Africa and funding fringe political parties, and should therefore not be seen as a 'cyber only' issue.

## Cybercrime remains key threat to business

Cybercrime remains a huge threat to global businesses. Groups continue to favour easy attacks against the worst guarded victims, and a recent IMF report cited growing cyber inequality between organisations that are cyber resilient and those that are not. Around half of all cyber breaches impact businesses with fewer than 1,000 employees and many small companies go out of business soon after falling victim to an attack.

Although many cybercrime groups operate independently from state-backing, the two are still often interlinked. This has been illustrated by the growing levels of cybercrime coming from Russia, as well as the targeting of companies by criminal groups for political reasons. In December 2023, a pro-Palestinian operation claimed dozens of data breaches against Israeli firms, and in the same month a brewery company in the United States was targeted over their use of Israeli-made hardware.


## Cybercrime inc.

The professionalisation of cybercrime has been one of the most marked and important trends in cyber security over the past few years. This has involved the rapid growth of threat actors, with different groups specialising in different parts of the supply chain, and within the groups themselves, leading to a heightened threat environment.

Many criminal groups now operate almost like professional businesses, with recruitment teams and corporate infrastructure. One example of this professionalisation is the Russian group, AlphaLock, which operates a two-part business model designed to both educate cybercriminals and weaponise them for profit against organisations, offering an affiliate programme to join the hacking group.

Criminal groups typically operate to a business model that follows the path of least resistance. The explosion of Malware-as-a-Service (MaaS) and RaaS offerings is testament to that. Other models being adopted include paying specialists to identify easy targets. Larger groups can also offer initial access to a corporate's business infrastructure, such as a remote desktop or a CEO's email account, to less sophisticated gangs who have sufficient knowledge and skills to exploit it for monetary gain.

All of which has created a wider ecosystem of cybercrime, where groups do not need to be highly proficient, or even 'hack a company', to make significant profits.



“  
The professionalisation  
of cybercrime has been  
one of the most marked  
and important trends  
in recent years.”

# Gen AI: a double-edged sword

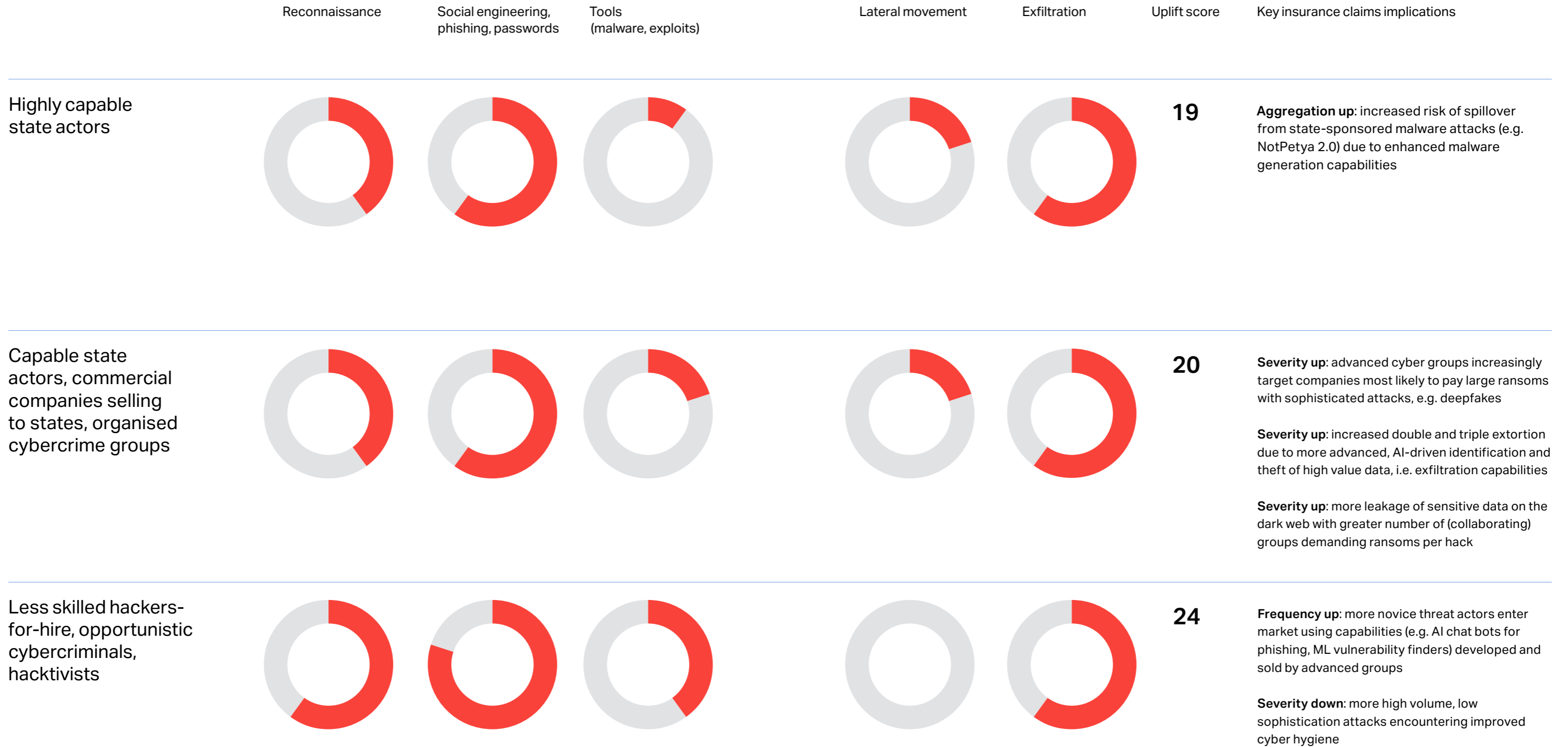
Whilst ransomware and systemic risk continue to dominate the cyber threat landscape, another major and relatively new development has been the explosion of Gen AI.

Despite broad consensus within the cyber security community and insurance market about the transformative potential of this new technology, for both offensive and defensive capabilities, there is far less clarity on which use cases will prove the most important and when they are likely to gain traction.

Nonetheless, two emerging conclusions on how Gen AI will reshape the threat landscape over the next few years are becoming increasingly clear.

**Figure 17: Gen AI uplift to threat actor capabilities – 2024 to 2026**

(Source: Howden analysis using information from the National Cyber Security Council)



Note: uplift scores are none (0), possibility (1), minimal (2), moderate (4), uplift (6) or significant (8)



“

Gen AI will push up the potential aggregation, severity and frequency of claims in predictable areas.

First, given the geopolitical and financial incentives, sophisticated, state-backed threat actors will use Gen AI to sharpen their tactics, techniques and procedures (TTPs) with increasing effectiveness and scale. In February 2024, Microsoft and Open AI disclosed that nation state threat actors have been using ChatGPT to make established hacking activities easier, with one Russian gang, for example, conducting reconnaissance on satellites.

Second, and more importantly for the insurance market, Gen AI will push up the potential aggregation, severity and frequency of claims in predictable areas by enhancing the capabilities of commercial hackers.

Figure 17 scores the degree to which AI will improve threat actors' capabilities between 2024 and 2026 across five key dimensions and draws out the implications for claims. All types of attackers, ranging from highly capable state actors to organised crime groups and less skilled hackers, will see AI enhance their capabilities. Beyond this, the impact will be highly nuanced.

## Less skilled hackers

This group will see the biggest uplift to their capabilities. Most importantly, many novice threat actors will gain access to tools, code and intelligence that will enable them to start hacking. This will be driven by sophisticated hackers with deep expertise in AI monetising their skills by selling capabilities online, a relatively low risk business model. As a result, AI will accelerate the trend of recent years for the democratisation of hacking, which is visible in the rise of outsourced hacking such as RaaS.

The main implication of AI-driven democratisation of hacking will be a rise in the frequency of low-level claims. Novice threat actors will find it easier to carry out phishing, which was the vector used in 84% of UK business attacks in 2023.<sup>5</sup> They will have also access to chatbots to help draft high quality phishing content, akin to ChatGPT without guardrails, AI-generated reconnaissance on which businesses to target (e.g. from machine learning trained to spot patterns in vulnerability) and even AI-generated ransomware code.

## Organised crime groups

Organised and technologically advanced cybercrime groups will see their capabilities enhanced in ways that point to a significant increase in the severity of a small number of claims. These groups will increasingly focus on the most lucrative hacking, i.e. targeting companies most likely to pay big ransoms with sophisticated attacks.

One such vector is social engineering via deepfakes, where AI generates convincing fake voice and even video calls to dupe employees into transferring funds or sharing login details. Furthermore, Gen AI will improve exfiltration capabilities by enhancing the speed and accuracy with which high value data can be identified and stolen.

Over time, large language models (LLMs) will be trained on stolen datasets to learn what to look for. This will in turn lead to more extortion by forcing companies to pay to maintain the confidentiality of exfiltrated data.

## Highly capable state actors

The most sophisticated hackers are backed by nation states and they remain closely focused on conflict and geopolitical goals rather than making money. Gen AI could nevertheless be used by these actors to enhance malware capabilities should priorities shift, which would in turn present increased risk of spillover and loss aggregation.

---

<sup>5</sup> Department for Science, *Innovation and Technology, Cyber security breaches survey, 2024*

## Defensive capabilities

The net impact of AI on cyber attacks, and resulting insurance losses, will inevitably depend on how defenders respond. On this front, companies have grounds for optimism. Most importantly, current defences should be strong enough to withstand the uptick in the frequency of relatively straightforward and predictable attacks.

Looking ahead, cyber security experts are positive on AI's ability to reinforce defences. Several use cases already stand out as both powerful and readily achievable.

---

### Pre-release software scanning

Software developers can use AI to scan code for errors and vulnerabilities prior to release. This would mean that they would no longer need to scramble to address vulnerabilities once published, a critical lag that hackers exploit.

---

### Maintaining open-source software

LLMs can be used to update open-source software by, for example, translating obsolete code into a more secure language. This is important because open-source software is an underappreciated backdoor to many networks (see S-RM's contribution on 'digital cornerstones' on page 25), as it can be both widely used and relatively insecure due to its maintenance by the crowd rather than vendors.

---

### Data classification

AI can be used to automate the process of data classification according to its sensitivity. This is an important use case because current data classification approaches often rely on employees, who are error prone, to do it manually. In addition, this would help to defend against the emerging threat of hackers using LLMs to spot high-value data at pace.

---

### Threat hunting

Analysts can use AI to assist with scouring the network faster and more accurately for threat actors who have slipped in under the radar. For example, an LLM could be trained to spot suspicious activity such as spikes in network traffic volumes. Over a fifth (22%) of CISOs have reportedly begun to do this.<sup>6</sup>

---

<sup>6</sup> Splunk, *The CISO report*, October 2023.

# Gen AI's impact on the cyber threat landscape

---

**Matt Hull**

Director Global Threat Intelligence  
at NCC Group

---

**Jon Renshaw**

Deputy Director of Commercial  
Research at NCC Group

Gen AI brings opportunities for both cyber attackers and defenders and looks set to significantly impact the threat landscape by enabling more advanced attacks from sophisticated actors and lowering barriers to entry for novice hackers. The good news is that new AI-driven defences are developing at pace and effective use of more traditional risk controls can shore up resilience.

## Enabling cybercriminals

The threat from AI systems remains relatively unknown. Amidst considerable speculation and even sensationalism around how Gen AI will impact the cyber risk landscape, it is important to understand the true threat. At this relatively early stage of the development cycle, we see three primary use cases that businesses need to prepare for:

- 1. Enabling social engineering**  
LLMs are already enabling criminals to create plausible content quickly and easily. This is being used for simple, yet important tasks like correcting the language, tone, spelling and grammar of phishing emails, which means they are more targeted and credible.
- 2. Deep fakes and voice cloning**  
Criminals and hacktivist groups are already cloning a genuine person's voice and images for online fraud, social engineering and, in some more recent cases, to spread disinformation across social media. High-profile cases where deep fake videos have been deployed to deceive targets and extract large payments reveal a step change in sophistication for capable threat actors.
- 3. AI as an enabler**  
Entry-level cybercriminals are using services like OpenAI to (rapidly) expedite the learning curve in executing attacks whilst more experienced individuals focus on maximising efficiency. Examples include debugging code, translating documents, generating scripts, retrieving and collating publicly available information about targets and researching possible ways to compromise systems.

## Heightened threat at both ends of sophistication spectrum

As alluded to above, we are already seeing the sophisticated use of audio and video deepfakes in highly targeted authorised push payment fraud. These are currently low likelihood, high impact attacks. As capabilities continue to increase, we expect the barriers to entry for this type of sophisticated and targeted fraud to be lowered.

They will nevertheless still require a degree of sophistication (and effort) that should prevent their deployment on a mass scale, but it is important for businesses to understand that the realism of fakes is ever increasing, as is the likelihood of successful attacks.

At the other end of the sophistication scale, cybercriminals are using LLMs to improve the quality of written communications in phishing attacks and other financially motivated scams. This is likely to increase the chances of success of high volume (rather than targeted) attacks.

AI also lowers the barriers to cyber criminality, hacking-for hire and hacktivism. This easier access will likely result in an increased volume of financially motivated cyber activity such as ransomware, and broader and more impactful hacktivist activity.

From what has been recorded so far, we expect to see an increased impact and volume of attacks, mostly because of an uplift in capability across research, reconnaissance and social engineering.

## Attacking AI

NCC Group research<sup>7</sup> has previously highlighted the potential of threat actors attacking AI systems to deny service or incur heavy costs for victims. These sorts of attacks are unlikely to be motivated by financial gain for the attacker, but instead to gain notoriety or for ideological motivations.

Additionally, trained models represent a significant investment in intellectual property (IP) by AI developers. Unscrupulous groups could launch attacks to extract training data and model weights, thereby securing access to IP to gain a competitive advantage. NCC Group recently published an advisory for a Domain Name System rebinding vulnerability in the Ollama LLM framework, showing that traditional application security is still just as relevant, even when that application is AI.

## AI defences developing at pace

Machine learning models have been built into cyber defence tools for many years now, providing automation capabilities that allow organisations to amplify their cyber defence efforts. Natural language interfaces have also been added for search, and now the availability of LLMs means that tool developers are able to integrate conversational interfaces providing access to data and functionality.

Using AI to detect and defend against AI attacks is relatively nascent, but it is certainly an area that is developing at pace. For example, the UK Home Office Accelerated Capability Environment recently launched a deepfake detection competition.<sup>8</sup> Large technology organisations and AI developers are also exploring watermarking<sup>9</sup> and provenance<sup>10</sup> techniques to detect when media has been generated by AI or to prove that it has not.

Whilst the pace of change can seem overwhelming, the advice to companies remains focused on employee awareness and practical tips such as avoiding acting under pressure, being wary of scenarios that seem too good to be true, checking with an independent colleague or via another medium and even asking potential scammers to prove their authenticity by, for example, putting on sunglasses or a hat.

## Prepare now

There is mounting evidence to suggest that AI will act as an attack accelerator over the next one-to-three-year horizon and that companies should be prepared for both an increase in novel / sophisticated scams and more attacks on established vectors.

The good news is that there are proven and effective mitigation factors: education and awareness amongst staff, good cyber hygiene including patch management, vulnerability scanning and penetration testing and incident response planning and testing. Each are vital to organisations' cyber resilience and are needed now more than ever.

“

**Companies should be prepared for both an increase in sophisticated scams and more attacks on established vectors.**

---

<sup>7</sup> [research.nccgroup.com/2022/07/06/whitepaper-practical-attacks-on-machine-learning-systems](https://research.nccgroup.com/2022/07/06/whitepaper-practical-attacks-on-machine-learning-systems)

<sup>8</sup> [ace.blog.gov.uk/2024/04/16/unmasking-deception-join-the-deepfake-detection-challenge](https://ace.blog.gov.uk/2024/04/16/unmasking-deception-join-the-deepfake-detection-challenge)

<sup>9</sup> [deepmind.google/technologies/synthid](https://deepmind.google/technologies/synthid)

<sup>10</sup> [c2pa.org](https://c2pa.org)

# The path to maturity

Despite the highly fluid threat environment, the foundations for a mature cyber (re)insurance market are now in place with the prospect of steady exposure-led growth, ongoing profitability and innovation.

Competition is returning to the market as improved cyber hygiene has mitigated losses and delivered strong underwriting performance.



“

Opportunities  
in international  
geographies and  
the SME space  
are poised to  
drive growth.

A pause in global premium growth last year due to the transitioning market cycle notwithstanding, opportunities in international geographies and other un(der)penetrated areas (SMEs in particular, alongside rapid technological advancements) are poised to drive rapid growth for the remainder of the decade. The evolving threat landscape, heightened risk awareness and more stringent regulations will also support demand.

With existing carriers looking to increase deployments, boosted further by a number of new entrants (including InsurTechs focused on the SME market), market conditions offer an attractive proposition for both buyers and carriers.

## Cyber recycled

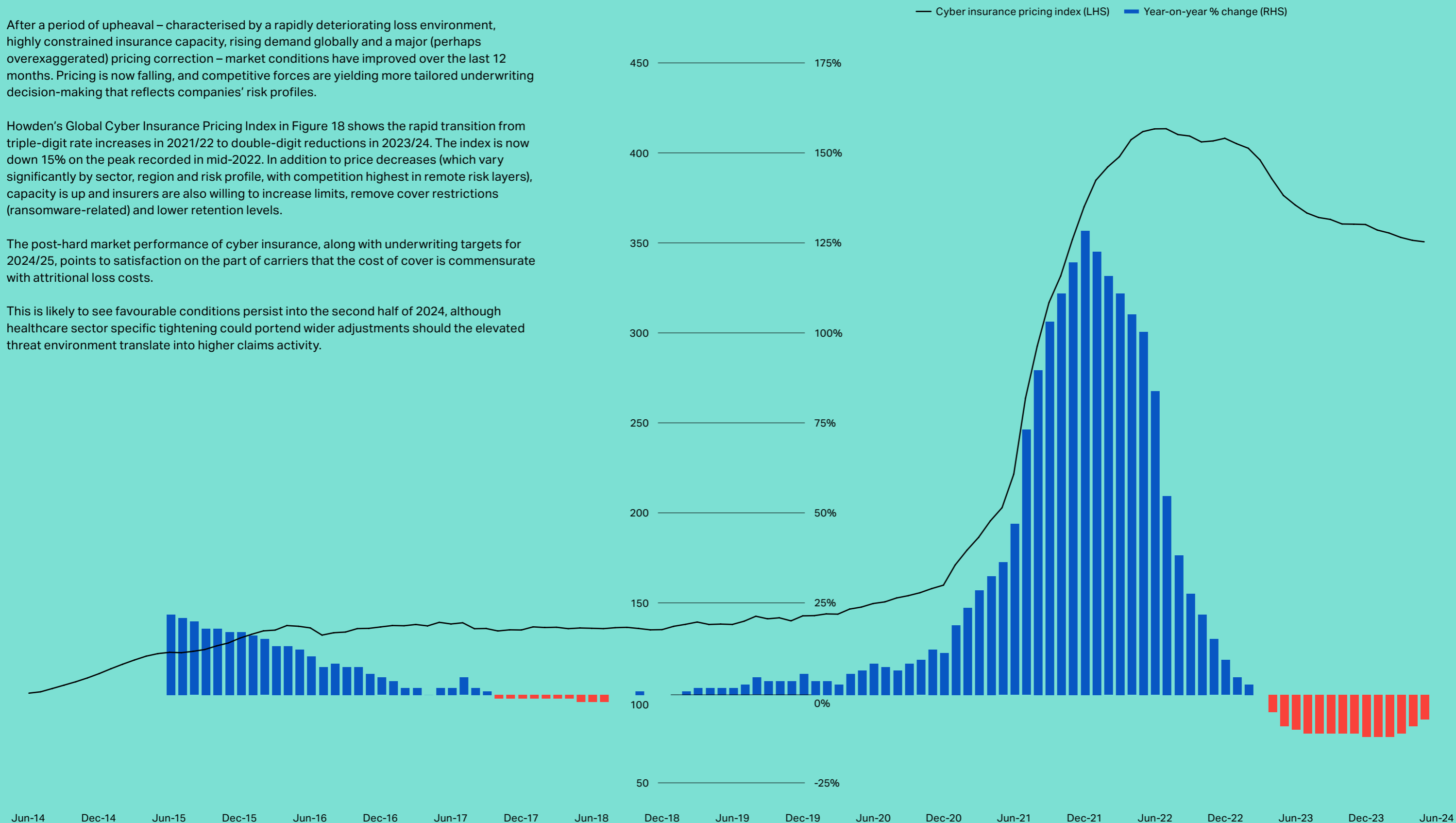
After a period of upheaval – characterised by a rapidly deteriorating loss environment, highly constrained insurance capacity, rising demand globally and a major (perhaps overexaggerated) pricing correction – market conditions have improved over the last 12 months. Pricing is now falling, and competitive forces are yielding more tailored underwriting decision-making that reflects companies' risk profiles.

Howden's Global Cyber Insurance Pricing Index in Figure 18 shows the rapid transition from triple-digit rate increases in 2021/22 to double-digit reductions in 2023/24. The index is now down 15% on the peak recorded in mid-2022. In addition to price decreases (which vary significantly by sector, region and risk profile, with competition highest in remote risk layers), capacity is up and insurers are also willing to increase limits, remove cover restrictions (ransomware-related) and lower retention levels.

The post-hard market performance of cyber insurance, along with underwriting targets for 2024/25, points to satisfaction on the part of carriers that the cost of cover is commensurate with attritional loss costs.

This is likely to see favourable conditions persist into the second half of 2024, although healthcare sector specific tightening could portend wider adjustments should the elevated threat environment translate into higher claims activity.

Figure 18: Howden's Global Cyber Insurance Pricing Index – 2014 to 2Q24 (Source: Howden)

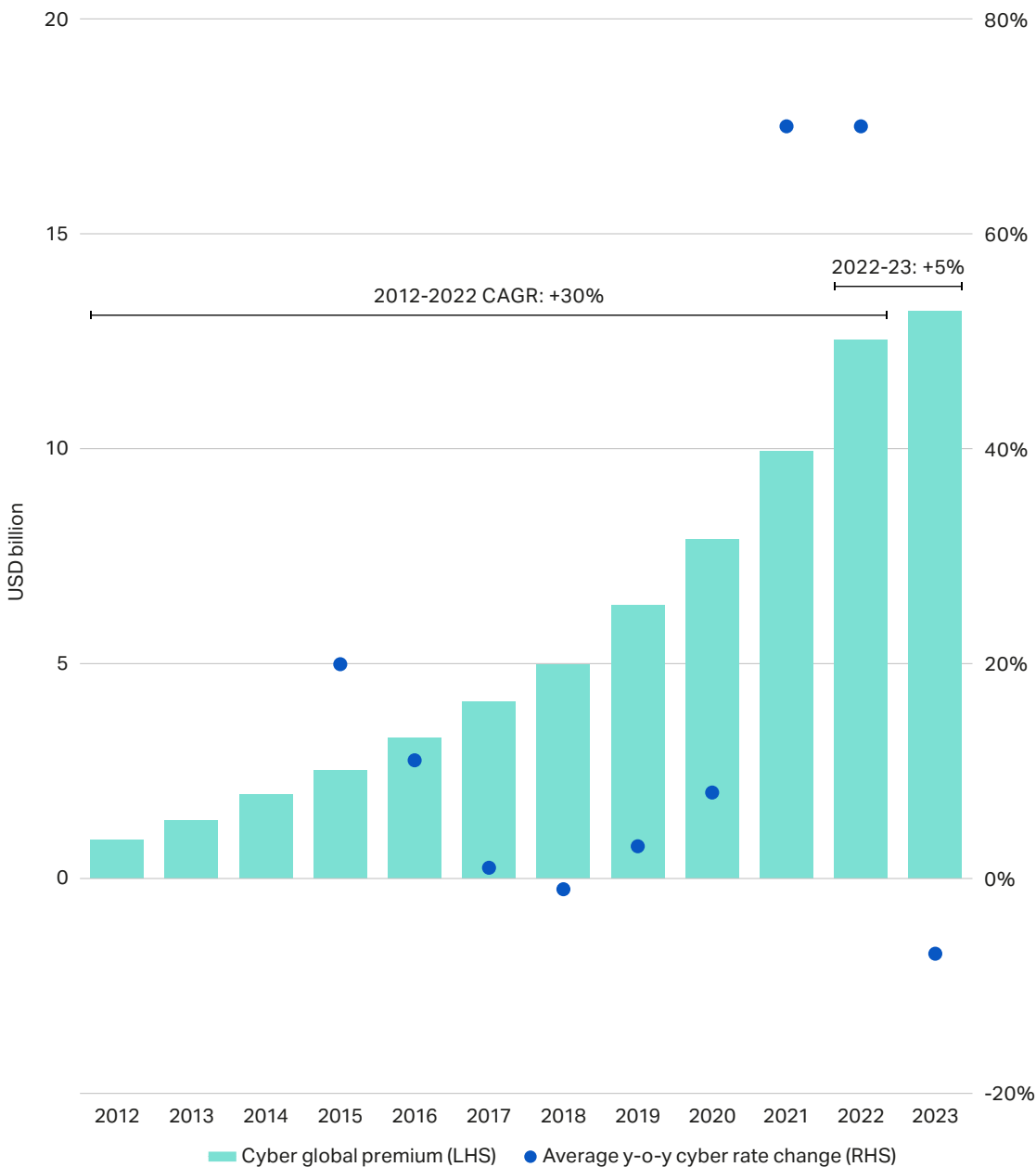


## Growth profile

Cyber insurance has been one of (if not) the fastest growing areas of insurance for the best part of a decade. Annualised growth of 30% during this time (as shown by Figure 19) compares to the single-digit percentage range of the broader P&C commercial sector.

Premium volumes are driven by a blend of exposure and pricing, and whilst both helped to drive growth up to 2020 (albeit skewed far more to the former), the pricing environment precipitated a notable shift in 2021/22, when high double-digit annualised price increases more than offset underwriting actions and the ensuing reduction in overall exposures.

Figure 19: Cyber global gross written premium – 2012 to 2023 (Source: Howden)



“

Pricing from here is unlikely to drive market expansion to the extent it did during the 2020-2022 correction.

2023 marked the slowest rate of growth since the market's inception (up 5%). Underwriting targets were not met last year, with several major players missing income goals. Absent any shocks, pricing from here is unlikely to drive market expansion to the extent it did during the 2020-2022 correction, requiring ambitious plans for exposure growth.

### Easing pressures

Improved market conditions reflect underwriting actions taken by carriers during the hard market, alongside ongoing investments made by businesses in strengthening their risk postures and claims management practices.

Analysis provided by S-RM overleaf explains how a combination of actions across multiple fronts have mitigated the cost of claims and ultimately facilitated a positive turnaround in market conditions.

## S-RM on relenting cyber claims

At a time of complex and rapid changes to the cyber claims environment, data continues to be challenging to aggregate and leverage across market participants. Whilst we may not have seen the absolute number of claims fall over the past two years, the average cost of claims has clearly reduced.

Several factors are driving this trend.

**Improvements in underwriting practices.** Insurers have significantly improved underwriting practices by investing in training programmes to upskill underwriting teams. The corollary has been a more developed understanding of risk management practices, the adoption of risk quantification tools and the refinement of risk modelling to suit businesses' risk profiles.

**Claims management practices:** Businesses are placing more trust in the utilisation of panel vendors, resulting in greater control of claims costs and best practices for containment and risk management. This is being driven by improved awareness of the value of experienced panel vendors and increased investment from carriers to maintain high-quality expertise on panels.

**Access to technical expertise.** Claims handling models are prioritising access to technical expertise for first-party loss events that require immediate technical support. First notification of loss is increasingly routed to either in house or third-party technical experts equipped to provide immediate advice to limit the spread and impact of a security event, thereby improving control of costs.

**Focus on response and recovery readiness.** Organisations have invested proactively in prevention, detection and response controls for several years now, meaning potentially significant events are being intercepted early in the attack chain, limiting business impact. Most organisations are now shifting focus from investment in prevention to operational resilience in order to improve their ability to recover quickly, minimise downtime and avoid business interruption losses.

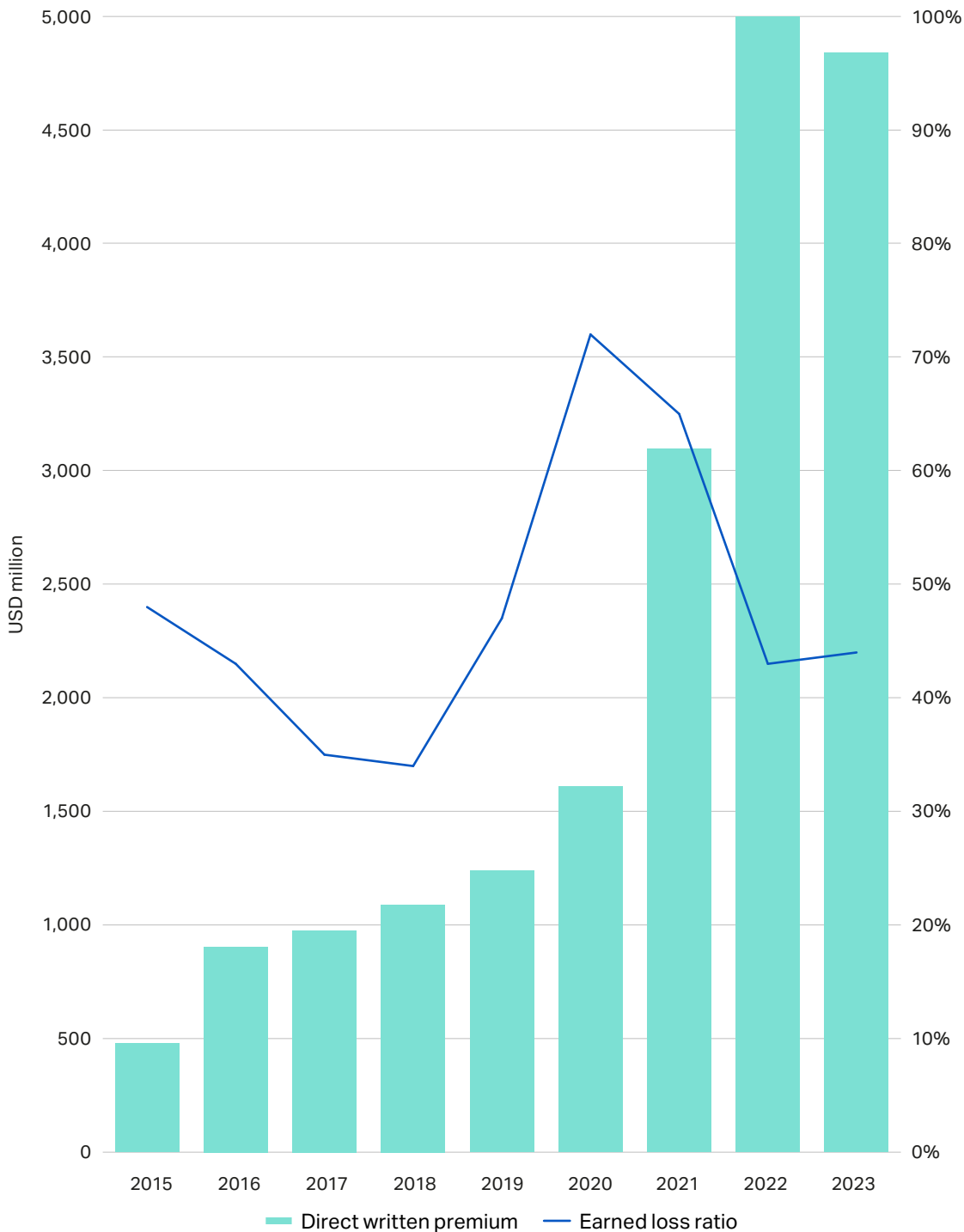
**Law enforcement.** Law enforcement is becoming more effective at disrupting some of the more active ransomware groups. By the end of 2023, two groups – LockBit and BlackCat – were responsible for a third of all known ransomware attacks. Targeted law enforcement action in early 2024 disrupted both groups, which contributed to LockBit falling out of the top three most prolific groups. BlackCat reportedly shut down its servers after its successful hack on Change Healthcare.

“

Organisations have invested proactively in prevention, detection and response controls for several years, meaning potentially significant events are being intercepted early.

All these mitigating factors are reflected by U.S. supplemental filings data, which provide a snapshot of claims trends and underwriting performance. Figure 20 shows that profitability remained strong in 2023 as the U.S. market recorded a loss ratio of 44%, in line with 2022 and significantly better than 2021 (65%) and 2020 (72%).

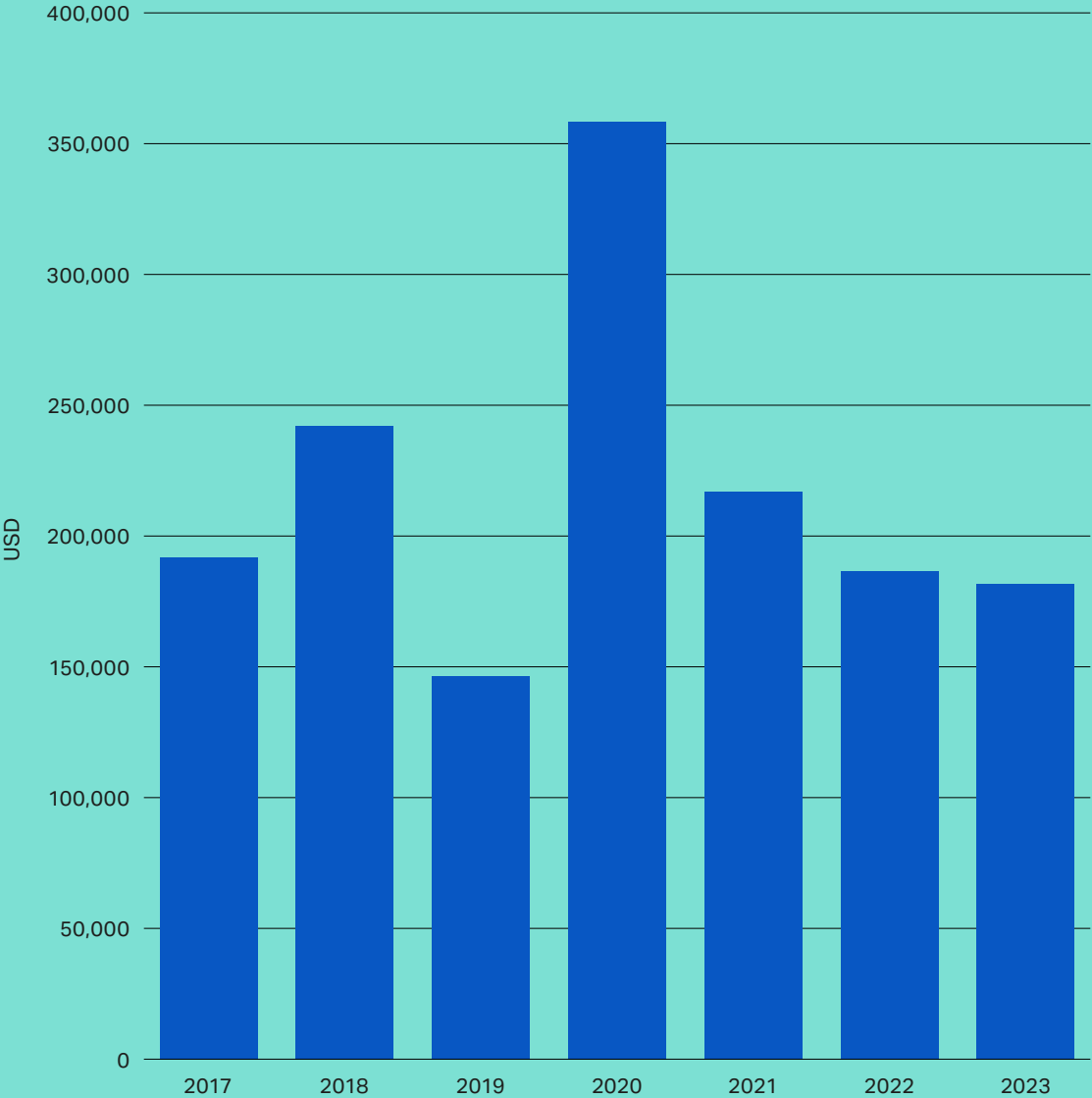
**Figure 20: Loss ratio and direct written premium for U.S. standalone cyber policies – 2015 to 2023** (Source: Howden, NOVA, NAIC)



Marginally reduced premium flow into U.S. domestic admitted and surplus lines last year (down 3% year-on-year, the first decline on record) had a limited bearing on results, as the quantum of losses and defence costs remained relatively stable.

Figure 21 shows the severity of claims recorded by the U.S. market since 2017, with the notable decrease in recent years coinciding with improved risk postures that have ultimately helped to contain costs. These underlying trends are being replicated in most other major cyber markets.

**Figure 21: Mean claims for U.S. standalone market – 2017 to 2023<sup>11</sup>**  
(Source: Howden, NOVA, NAIC)



<sup>11</sup> Direct losses and defence costs divided by the number of paid claims.



# S-RM on containing costs

---

**Roddy Priestley**

Director, Cyber Security at S-RM

---

**Martijn Hoogesteger**

Head of Cyber Security, Benelux  
at S-RM

Effectively mandating the implementation of controls such as multifactor authentication (MFA) and backups has had a huge impact in improving the underlying risk of cyber insurance portfolios. The absence or misconfiguration of these controls has been one of the primary factors leading to significant losses.

Even in the event of these controls being circumvented, incidents can be prevented and costs contained by properly managing controls across three key phases of the attack lifecycle.

## P1

### 'Entry' phase

In 2023, the most common method of entry in our ransomware response cases was via external remote services. Six of the 10 largest cases S-RM responded to resulted from direct network access via VPNs unprotected by MFA.

MFA should be used not just to protect the network perimeter, but also to prevent threat actors from accessing privileged accounts needed to complete key steps in the attack chain such as deleting backups and removing antivirus.

## P2

### Through phase

Well managed identity and access management (IAM), network segmentation and monitoring are critical to detecting and containing intrusions. Once an actor is inside a network, the most valuable control to prevent escalation is managed detection and response (MDR). A good MDR service monitors activity across firewalls, endpoints, cloud services, email and other key systems.

A core component of an effective MDR service is the endpoint detection and response (EDR) software. In more than two-thirds of S-RM's cases between 2022 and 2023, EDR tooling was absent. EDR software, augmented with additional logging from other security tooling and monitored by an expert third party provider, is the most effective way of identifying malicious activity and containing it before it becomes a claim.

## P3

### Out phase

Although business interruption is typically the largest cost in an incident, losses can be mitigated by proper backups that are immutable and regularly tested. Threat actors rarely manage to access cloud-hosted backups, and even when they do so, immutability in cloud providers like Azure and AWS means they cannot irreversibly delete the backups.

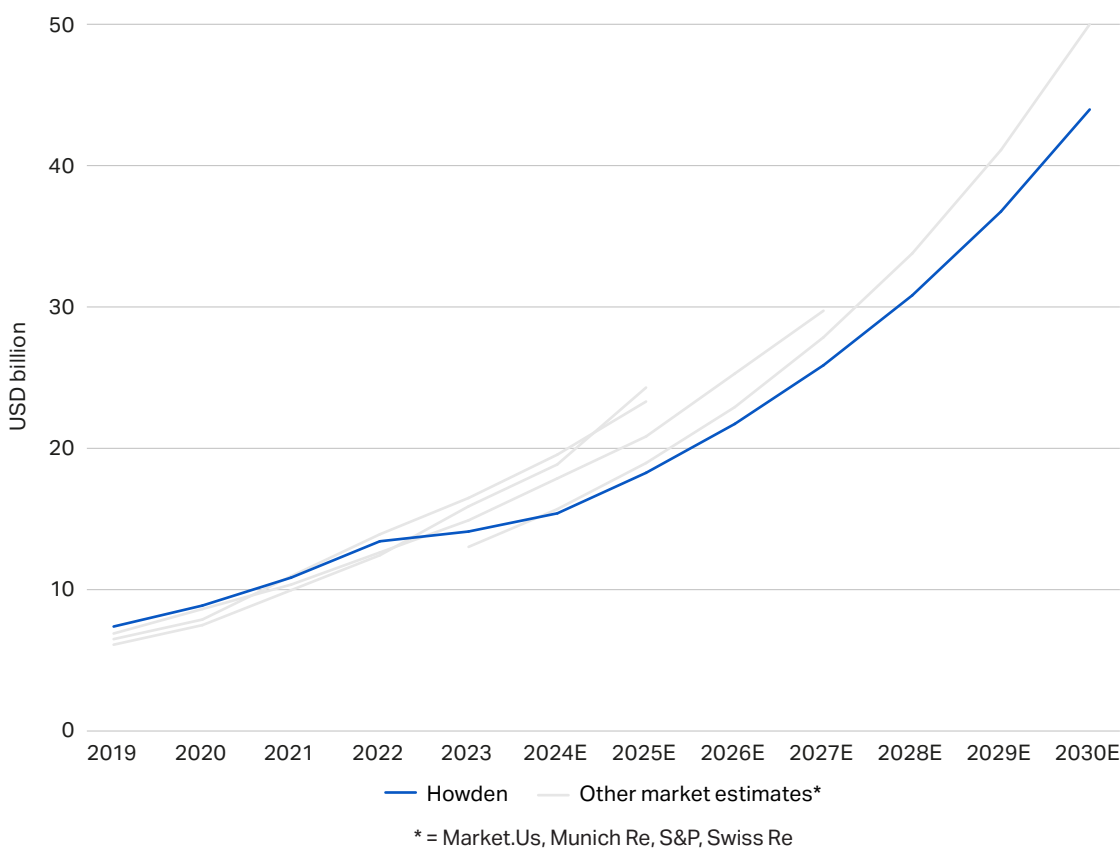
This provides responders with the option of recovering networks without needing to pay a ransom, which lowers the costs of the response and, in the long term, reduces the number of payments being made to ransomware groups.

## Shifting growth dynamics

Improved cyber hygiene and a more stable underwriting environment puts the cyber market in a strong position to restore the trajectory of growth after the premium base stabilised in 2023. Now that pricing tailwinds are reversing, the market needs to refocus on innovation to grow its exposure base and achieve the growth trajectories outlined by Howden and other companies in Figure 22. This projection is down on our USD 50 billion estimate made last year due in large part to flat growth in the United States.

**Figure 22: Global cyber gross written premium projections up to 2030**

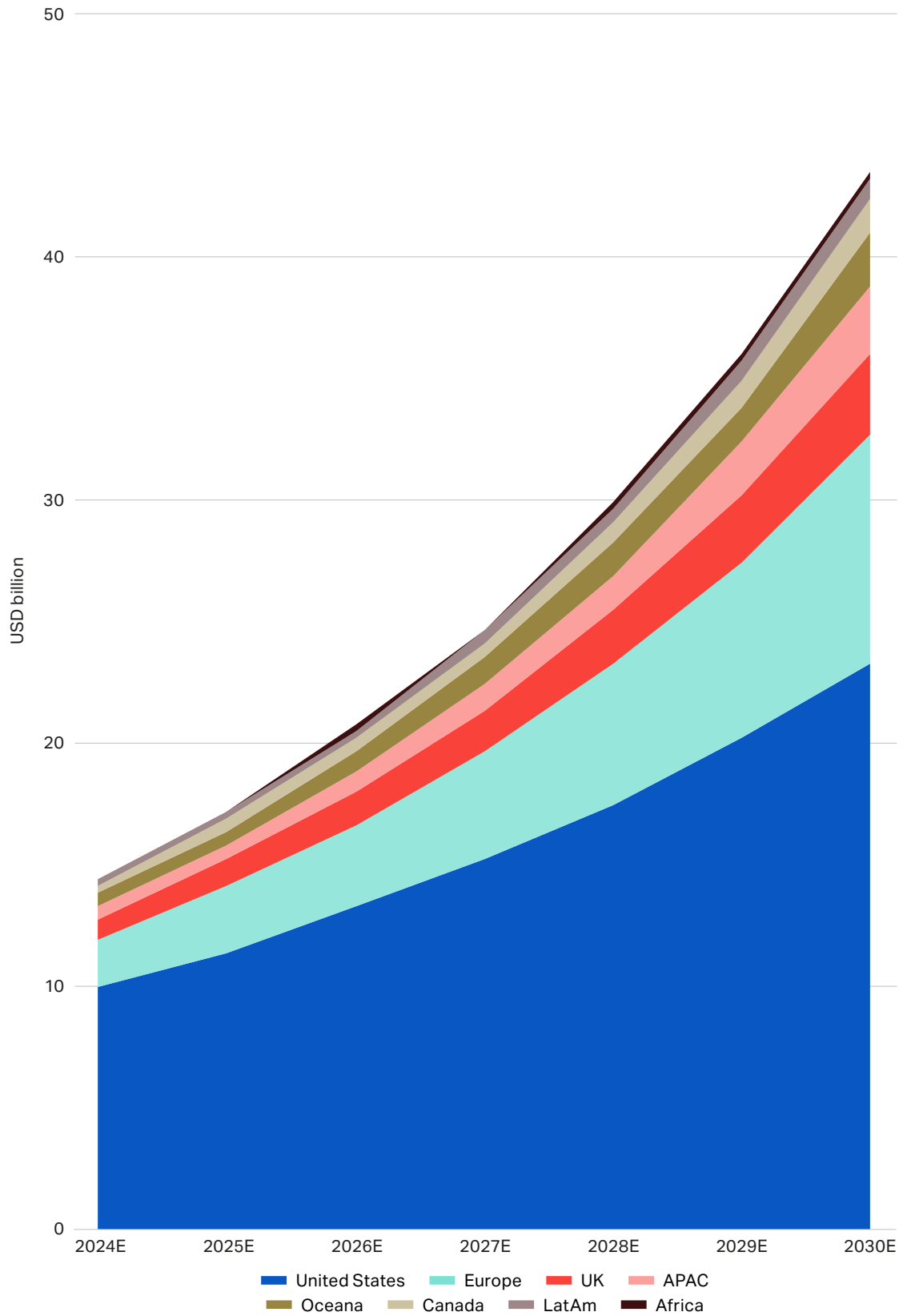
(Source: Howden, Market.U.s, Munich Re, S&P, Swiss Re)



Even accounting for the slowdown in 2023, the market could still be on course to achieve a premium base of close to USD 40 billion by the end of the decade. The realisation of this potential will inevitably be tied to external factors such as macroeconomics and geopolitics, but by focusing on key issues within its control – including SME penetration (e.g. easing the buying process), geographic expansion and continued model development – the market can secure long-term relevance.

Howden stands at the forefront of these efforts. By working with insurers to deliver pioneering solutions that help break into company segments and geographies currently underserved by the market, we see these projections as eminently achievable (necessary in fact) in order to meet the demands of clients worldwide.

**Figure 23: Estimated cyber gross written premiums by region – 2024 to 2030**  
 (Source: Howden)

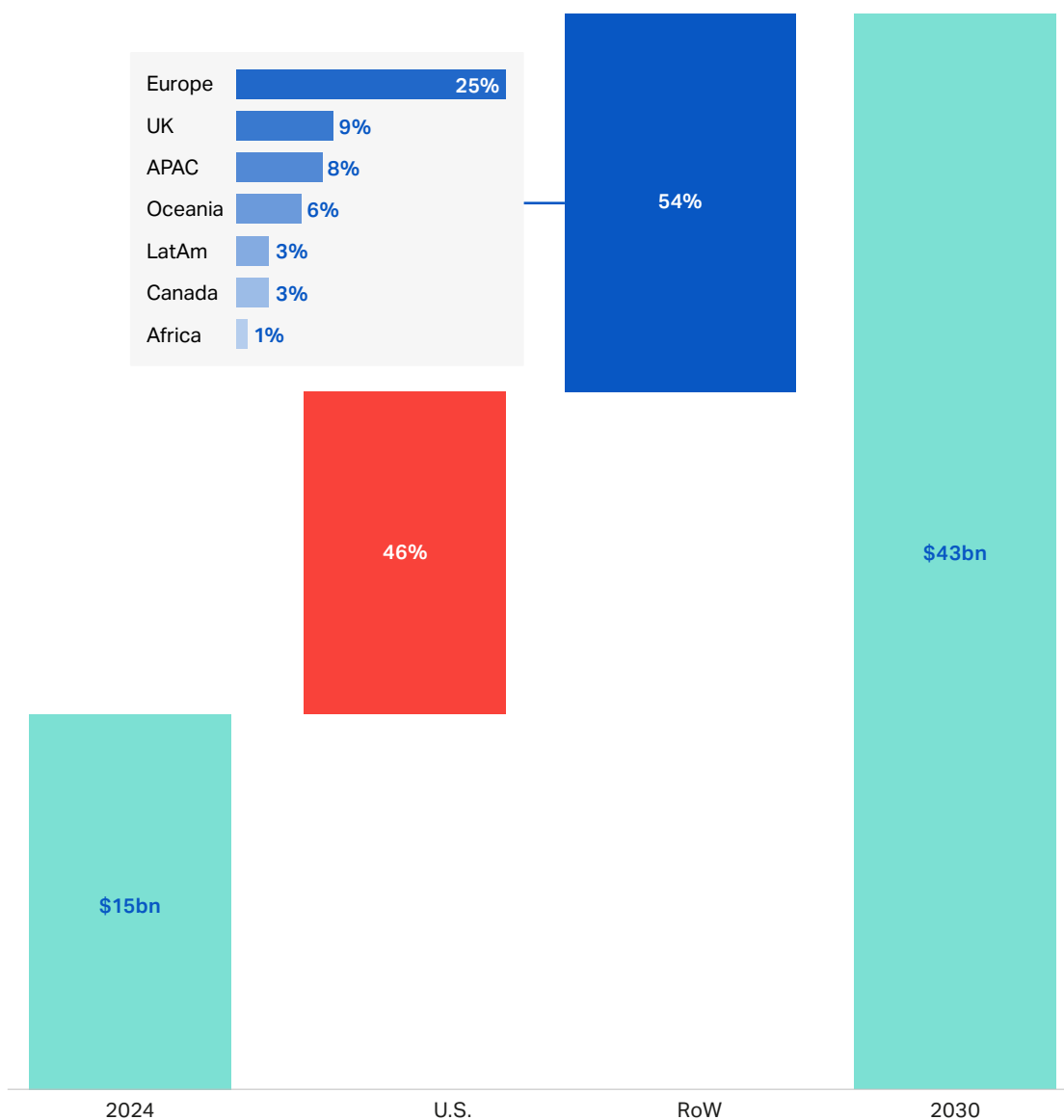


## Geographic expansion

Cyber insurance has up until recently been dominated by the U.S., representing approximately two-thirds of the global market. As this segment has become increasingly penetrated, the impetus for growth is shifting to other territories to satisfy pent up corporate demand amidst heightened threats, rising risk awareness and regulatory changes. Figure 24 shows that international business is set to make up the majority of growth up to 2030, with Europe, along with the UK, Asia Pacific, Oceania and Latin America, standing out as the pre-eminent high-growth international regions.

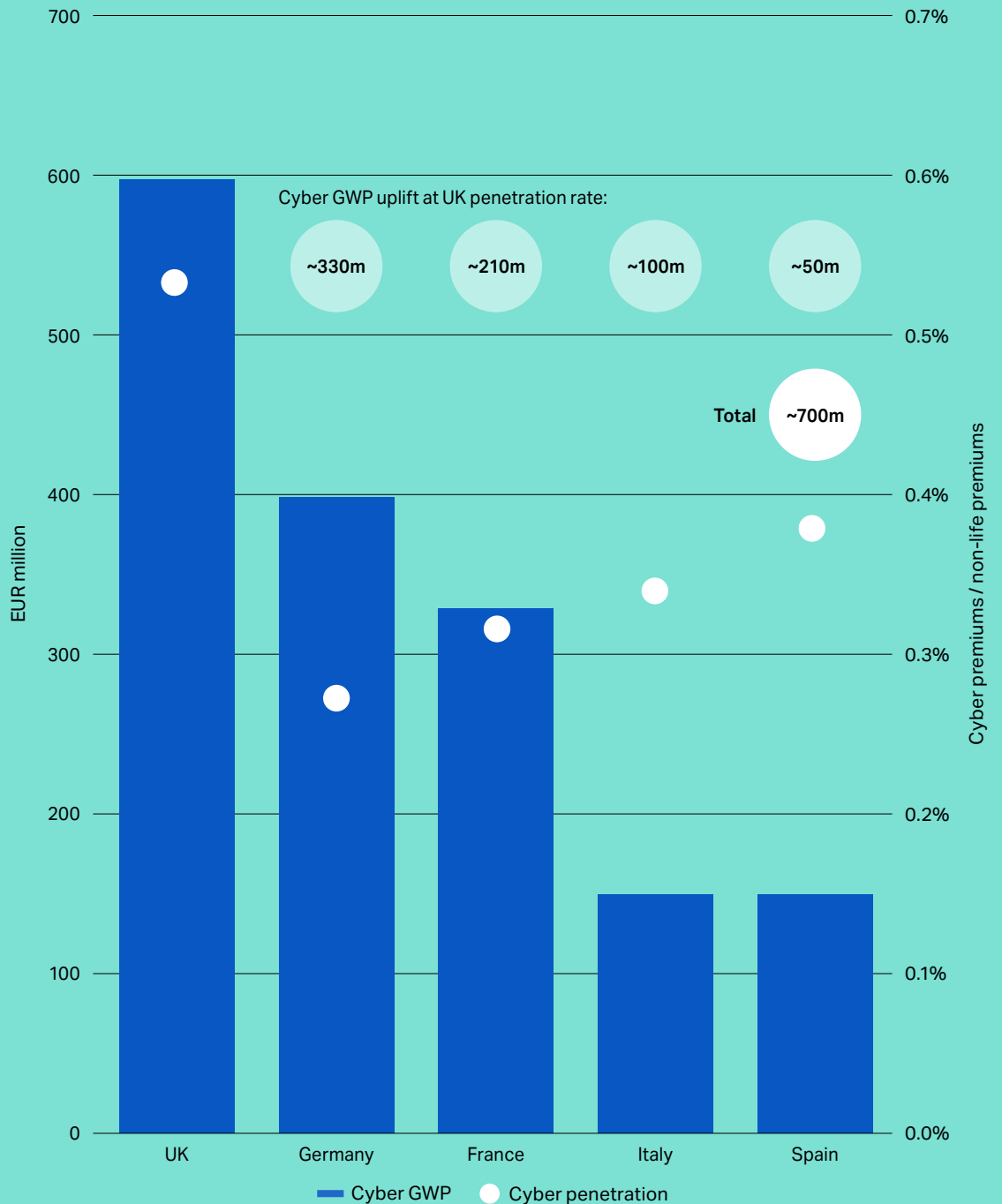
**Figure 24: Share of global cyber premiums growth by region – 2024 to 2030**

(Source: Howden)



Major economies in Europe especially have considerable growth potential given current penetration levels. Figure 25 shows how cyber premium and penetration rates in Germany, France, Italy and Spain compare to the United Kingdom, one of the more mature cyber markets.

**Figure 25: 2023 cyber premiums and penetration rates in UK vs major European economies**  
 (Source: Howden, AMRAE, BaFin, Swiss Re)



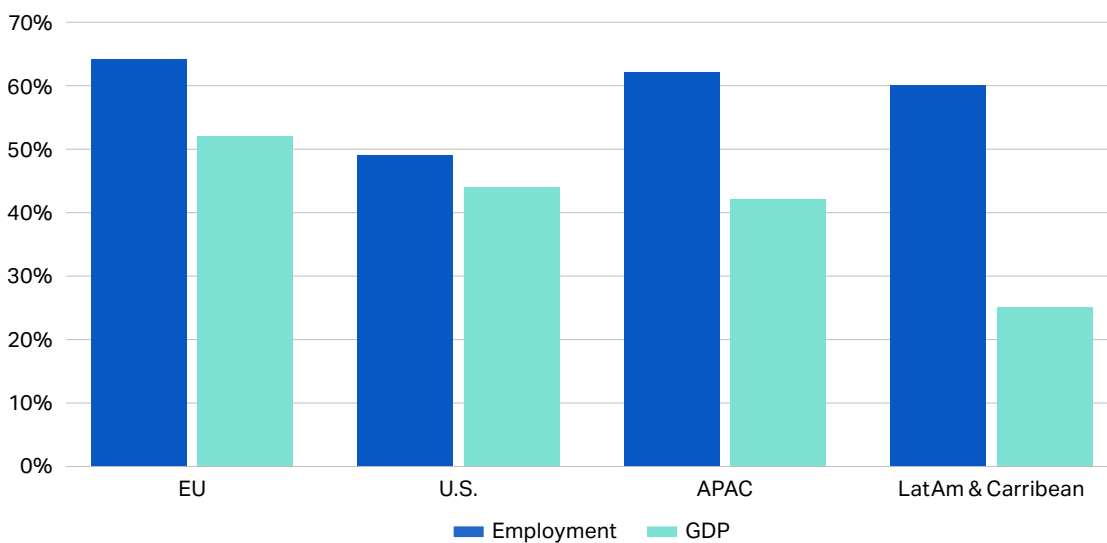
Whereas cyber GWP in the UK is currently close to EUR 600 million, other comparable economies in Europe lag significantly. The gap widens further when accounting for the relative size of the non-life market in each country, Germany being the biggest. All told, these territories could see a combined premium uplift of approximately EUR 700 million in just replicating current UK penetration levels.

## SME penetration

More work also needs to be done in engaging with SMEs, a segment that remains largely untapped for the cyber market. SMEs are the backbone of economic activity in advanced economies (see Figure 26) and are increasingly reliant on technology for their operations. Despite being the incubator of innovation with high growth potential, SMEs have historically been underserved by the cyber insurance market.

**Figure 26: SME share of economy by region**

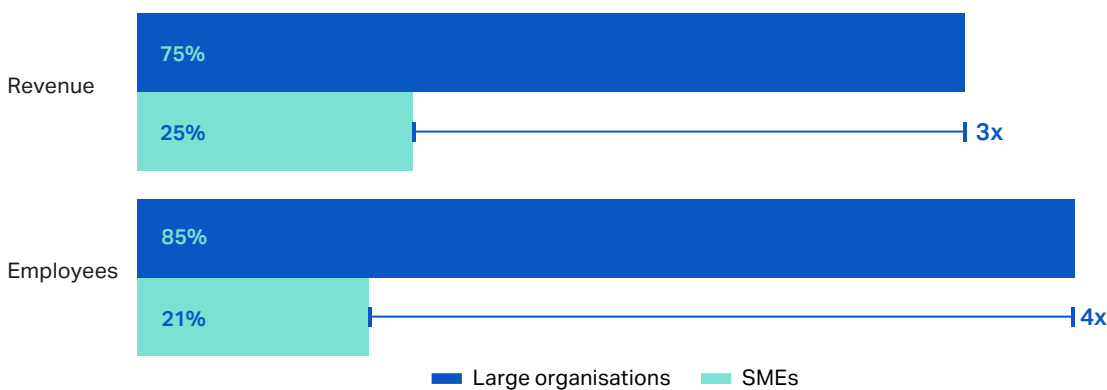
(Source: European Commission, U.S. Chamber of Commerce, Asian Development Bank, Asia-Pacific Economic Cooperation, OECD, Development Bank of Latin America & The Caribbean)



Research from the World Economic Forum lays bare the opportunity in this space; with only one in four SMEs currently protected by cyber insurance (see Figure 27). To compound matters, many lack the resources and knowhow to recover from a cyber attack.

**Figure 27: Share of organisations with cyber insurance globally in 2023**

(Source: World Economic Forum)

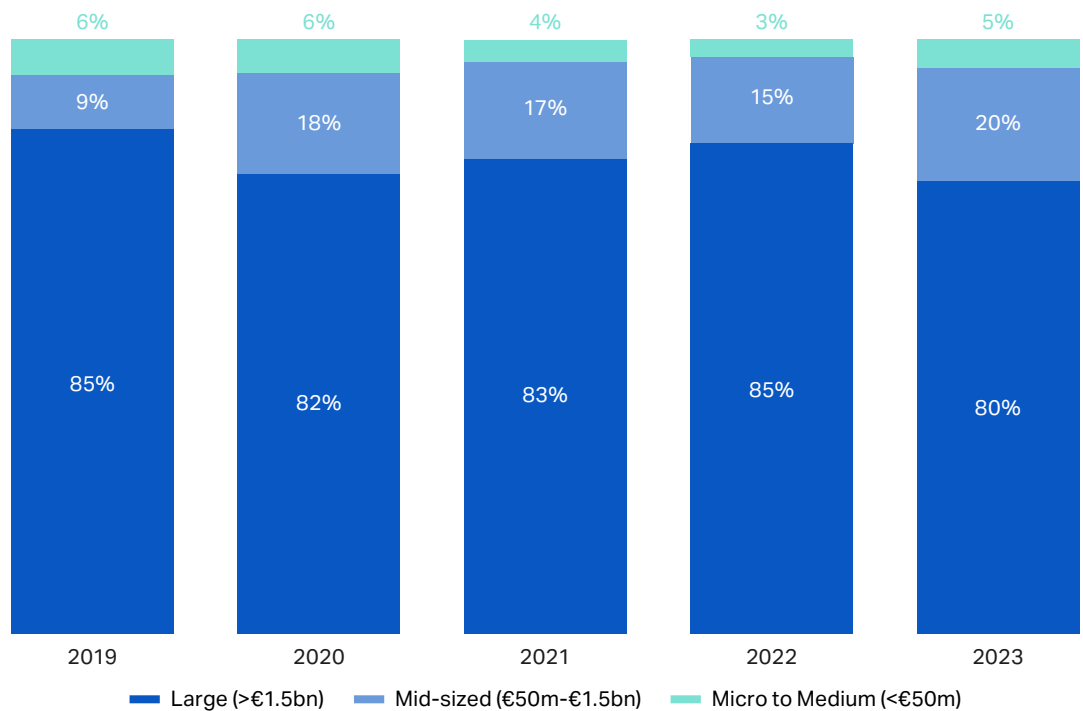


Note: SMEs defined as business with <250 employees or <\$250m in revenue, Large organisations defined as business with >100,000 employees or >\$5.5bn in revenue

Progress is already being made in certain markets, with data specific to France showing that companies categorised from micro to mid-sized have increased their share of the cyber insurance premium pool from 15% in 2019 to 25% in 2023 (see Figure 28).

A more transformational approach is nevertheless needed to accelerate penetration and cement relevance amongst SMEs. Important opportunities include increasing risk awareness, linking rates more closely to hygiene levels and simplifying the buying process.

**Figure 28: French cyber insurance premium distribution by company revenue band - 2019 to 2023** (Source: AMRAE)



## Howden's SME Cyber Platform

In May 2024, Howden launched a platform to enable SMEs with revenue of less than USD 250 million to buy up to USD 6 million of cyber cover in four simple steps. Crucially, this solution only requires name, industry, revenue and website to produce a quote for businesses. Supplementary data is gathered via open APIs, meaning that underwriting standards are upheld during the much-simplified purchase process.

Our platform has the potential to revolutionise the buying process for SMEs, which typically lack the resources to navigate existing submission demands. It combines differentiated cyber broking and carrier expertise with cutting edge technology and is the latest example of Howden pushing the boundaries to penetrate into this vital but currently underserved segment of the economy.



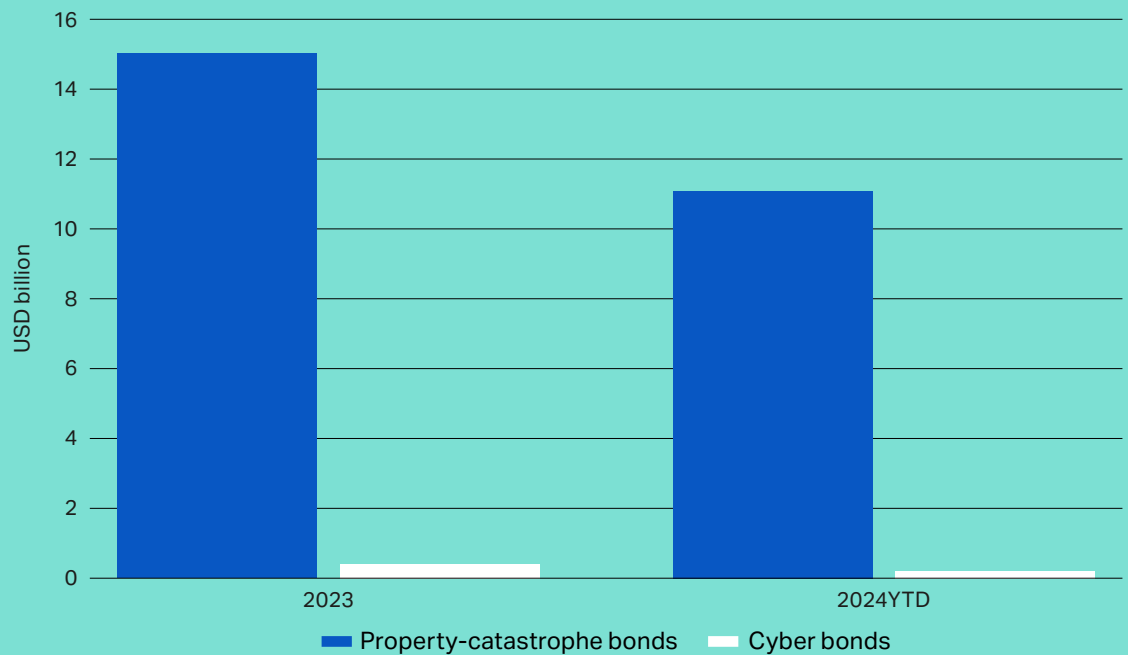
# 05 Matching risk to capital

Prospects for cyber insurance are strong, supported by a growing and increasingly diverse capital base.

This will be crucial as the market moves beyond existing premium pools to meet the demands of businesses worldwide.

There have been a number of positive developments on the capital front over the last 12 months. Beyond plentiful supply on the direct side, conditions in the cyber reinsurance market have also improved, with pricing softening and capacity more than sufficient to meet demand.

**Figure 29: Property-catastrophe vs cyber 144A catastrophe bond issuance – 2023/24**  
(Howden, Artemis)



Importantly, quota share cessions are now falling as insurers become more comfortable with attritional and large loss ratios, a trend which is likely to continue as cedents explore more efficient capital structures such as event-based excess-of-loss products.

Growing interest in this area has facilitated a series of landmark cyber catastrophe bond issuances since 4Q23. In addition to nearly doubling the size of the event-based excess-of-loss market, these transactions also point to a level of investor appetite that will drive additional activity from here. Room for growth is considerable; catastrophe bond issuance for property-catastrophe risk, a market that has existed for nearly 30 years, was around USD 15 billion in 2023 versus just USD 0.4 billion for cyber. Additional cyber deals have been closed in 2024.

Continued investments into modelling solutions to manage and price systemic exposures have been (and will continue to be) crucial to unlocking more capacity from capital markets (see Howden Re's *Re-framing cyber risk* report for the different approaches that carriers can adopt). Work in this area will need to be sustained in order to accelerate inflows (at the right price). Innovation, and not cover restrictions, is the route to long-term relevance, and new possibilities.

Intermediaries have a crucial role to play in realising the cyber market's growth potential, especially those with the (genuine) local expertise and capabilities needed to penetrate into new geographies and attract capital at scale. Today's marketplace demands a new approach to broking that is cycle-savvy, innovative, aggressively entrepreneurial and home to the sector's strongest talent. This is what Howden brings to the table and more. Come and talk to us.

# Meet the experts



**Julian Alovisi**  
Head of Research

+44 (0)7593 576 024  
julian.alovisi@howdengroup.com



**Peter Evans**  
Research Director

+44 (0)7443 377 340  
peter.evans@howdengroup.com



**Shay Simkin**  
Global Head of Cyber

shay@howden.co.il



**Jean Bayon de La Tour**  
Head of Cyber, International

jean.bayon@howdengroup.com



**David Rees**  
Head of Cyber, UK

david.rees@howdengroup.com



**Sarah Neild**  
Head of Cyber Retail, UK

sarah.neild@howdengroup.com

# Expert contributors

## S-RM

**Roddy Priestley**

Director, Cyber Security

[r.priestley@s-rminform.com](mailto:r.priestley@s-rminform.com)

**Martijn Hoogesteger**

Head of Cyber Security, Benelux

[m.hoogesteger@s-rminform.com](mailto:m.hoogesteger@s-rminform.com)

## XCyber

**Milo Wilson**

Lead Intelligence Analyst

[milo.w@xcybergroup.com](mailto:milo.w@xcybergroup.com)

**Bill Jarvis**

Head of Intelligence

[bill.j@xcybergroup.com](mailto:bill.j@xcybergroup.com)

## NCC Group

**Matt Hull**

Director Global Threat Intelligence

[matthew.hull@nccgroup.com](mailto:matthew.hull@nccgroup.com)

**Jon Renshaw**

Deputy Director of Commercial Research

[jon.renshaw@nccgroup.com](mailto:jon.renshaw@nccgroup.com)



Contact us at [info@howdenbroking.com](mailto:info@howdenbroking.com)  
or call us on 020 7623 3806.

One Creechurch Place, London, EC3A 5AF

T +44 (0)20 7623 3806  
F +44 (0)20 7623 3807  
E [info@howdenbroking.com](mailto:info@howdenbroking.com)

[howdenbroking.com](http://howdenbroking.com)

Howden Group Holdings Limited is registered in England and Wales under company registration number 2937398. Registered office:  
One Creechurch Place, London, EC3A 5AF. Calls may be monitored and recorded for quality assurance purposes. 06/24 Ref: 11050 V0.5