

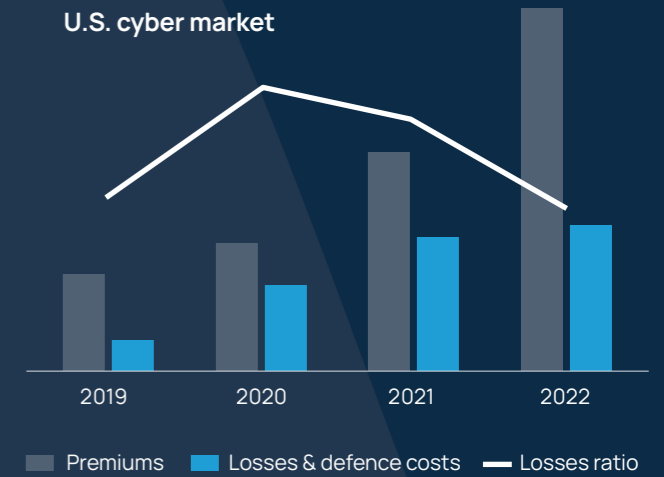


CYBER INSURANCE
COMING OF AGE

Key takeaways

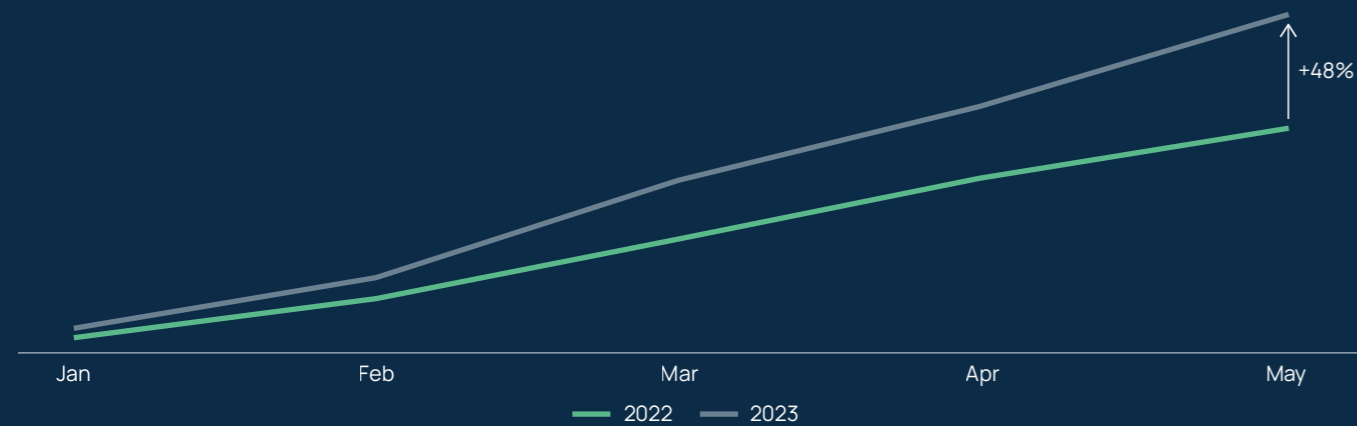
Cyber insurance is at a decisive moment in its growth journey. Conditions are stabilising and by tackling key challenges around distribution, tail-risk and capital the market is on the cusp of transformational growth.

Strengthened cyber resilience is paying dividends, as improved underwriting results yield positive outcomes for insurance buyers.

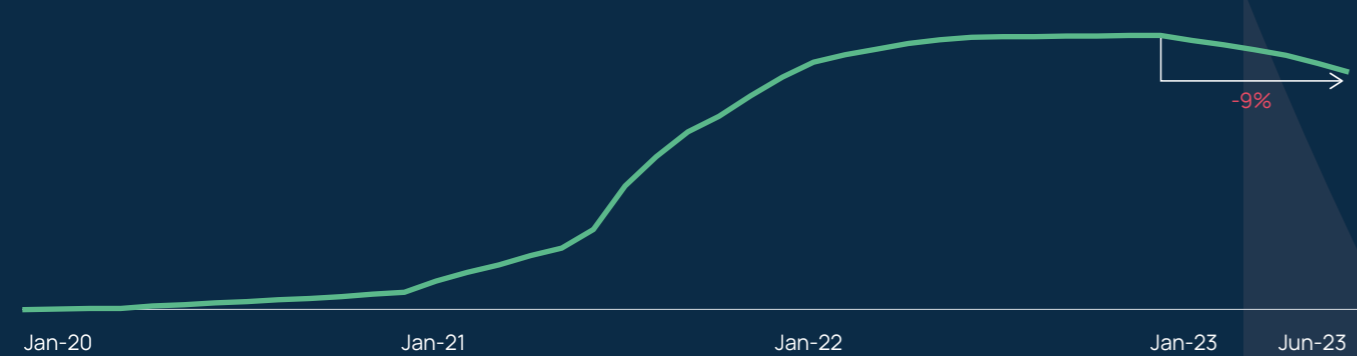


Ransomware incidents vs premium increases

Ransomware activity up nearly 50% so far in 2023 vs 2022...

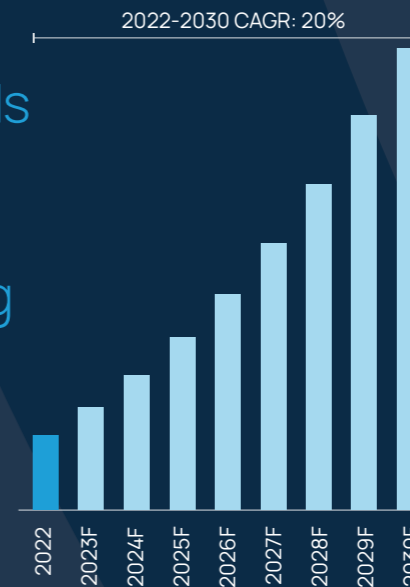


...cyber insurance pricing down overall in 2023

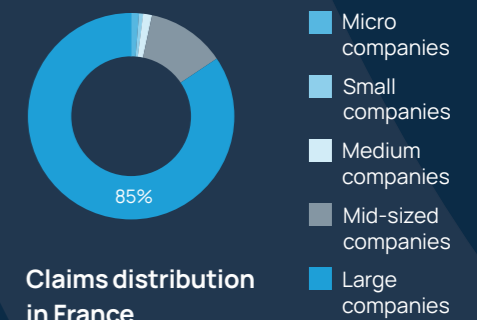


To fulfil its true potential, the cyber market needs to move beyond existing premium pools by increasing uptake in under-penetrated markets.

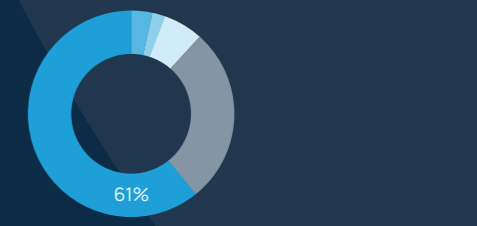
GWP projections



Premium distribution in France



Claims distribution in France



Capital is key to unlocking the full potential of the cyber market by facilitating product innovation tailored for new territories and an expanded client base, as well as building resilience against extreme tail risk events.

Executive summary

Few areas of (re)insurance get as much attention as cyber (this is Howden's third cyber report in as many years). There are several reasons for this – the pervasive threat environment, its interactions with technology and geopolitics, the inherent unpredictability, the exciting growth potential but, above all, its relevance to clients worldwide.

Businesses in all regions continue to rank cyber as one of their most pre-eminent risks, a seemingly well-founded view considering the myriad of shocks companies and insurers have faced in the last three years alone, from rapid digitalisation post-COVID (and the proliferation of attack surfaces) to rampant ransomware and the war in Ukraine.

No other line of business has such a dynamic risk landscape on the one hand, and such growth potential on the other. These dynamics continue to play out in the market. Following a major market correction off the back of surging ransomware claims in 2020 and 2021, which led to the cost of cyber cover more than doubling, conditions started to stabilise last year as activity relented and more robust risk controls deterred or mitigated attacks.

Strengthened cyber resilience has continued to pay dividends into 2023, as resurgent ransomware activity in the first half of the year has so far not been accompanied by a corresponding rise in losses or claims. Concomitant benefits to underwriting results are yielding positive outcomes for insurance buyers, with programmes renewing flat or even with decreases as pricing comes off recent historical highs.



THE CYBER INSURANCE MARKET IS AT A DECISIVE MOMENT IN ITS GROWTH JOURNEY.

Achieving relevance

With existing carriers looking to increase capacity deployments, boosted further by a number of new entrants, the foundations are in place for the cyber market to scale up to the size of other major P&C business lines. The realisation of this potential is tied in part to external factors such as geopolitics and macroeconomics, but by focusing on key issues within its control – including distribution, tail-risk management, attracting capital and talent – the market is on the cusp of potential transformational growth.

The war exclusions issue is centre stage currently, as the Ukraine war and rising geopolitical tensions elsewhere have prompted certain markets to look to clarify their positions around what is insurable. The introduction of new war language was always going to be contentious, but clients are increasingly recognising the importance of proactively scoping out the parameters of cover for cyber warfare, both for their own benefit (i.e. eliminating coverage ambiguity) and for providing underwriters and investors with the confidence needed to commit to the market.

Maintaining clients' confidence in the product during this process is pivotal to realising cyber's growth potential, as is the need to penetrate into new territories and company demographics. Achieving relevance requires insurers and brokers to find better ways to bring small and medium-sized enterprises (SMEs) into the cyber market. Attracting capital will be crucial to achieving all these goals, a task which should not be underestimated given the difficult macroeconomic backdrop and capital constraints in the reinsurance market currently. The direct market's use (or reliance) on reinsurance is the single biggest differentiator between cyber and any other class of business.

Bringing all this together, the cyber insurance market is at a decisive moment in its growth journey. Considerable progress has been made in a short space of time, but more work needs to be done to meet demand globally. Speed of innovation will be crucial to tapping into new pools of capital and providing solutions for unpenetrated (and less cyber-sophisticated) markets.

Howden exists to do just that. We look forward to supporting clients (new and old) through this period of transition and working on their behalf to create a sustainable and relevant market designed for today's and tomorrow's fast-moving cyber threat landscape.

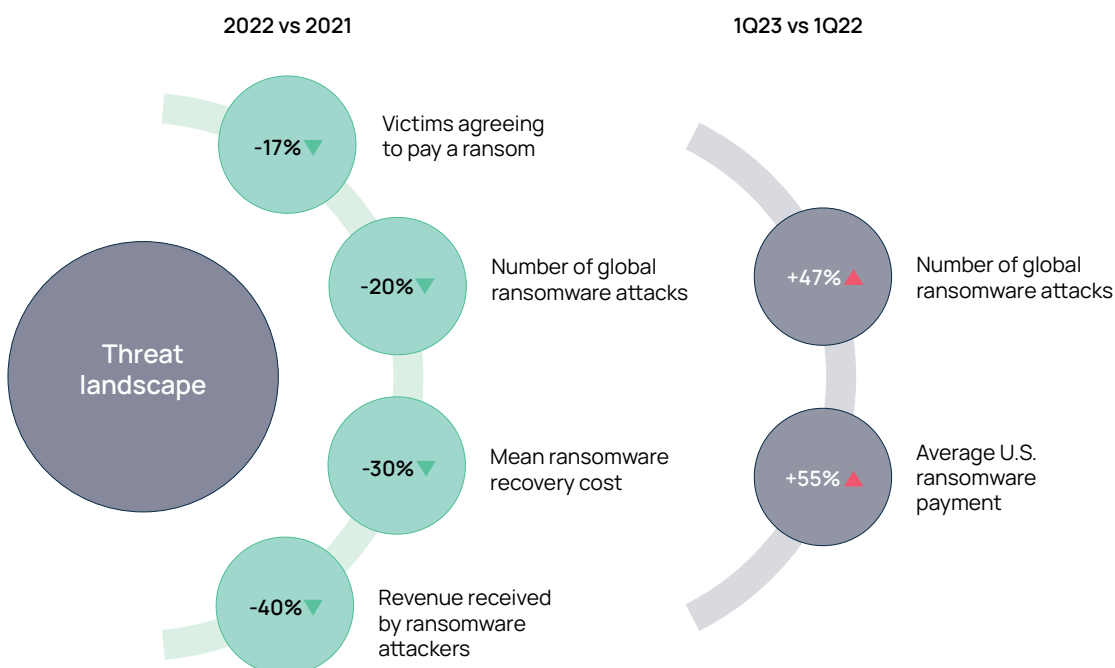
Rampant ransomware

Following major upheaval in 2020 and 2021 caused by COVID-19 and the proliferation of ransomware, the last 18 months have represented a period of relative calm for the cyber insurance market as claims have subsided and competition has returned.

But cyber rarely stands still and developments in the first half of 2023 point to a nuanced marketplace, with optimism around more favourable supply dynamics for buyers (off the back of improved underwriting performance for insurers) tempered by signs of resurgent ransomware activity and ongoing concerns around how the market should manage potential systemic losses. Conditions in the reinsurance market also remain challenging.

Figure 1: Frequency and severity of ransomware incidents

(Source: Howden analysis using data from Coveware, SonicWall, NCC Group, Chainalysis, Sophos)





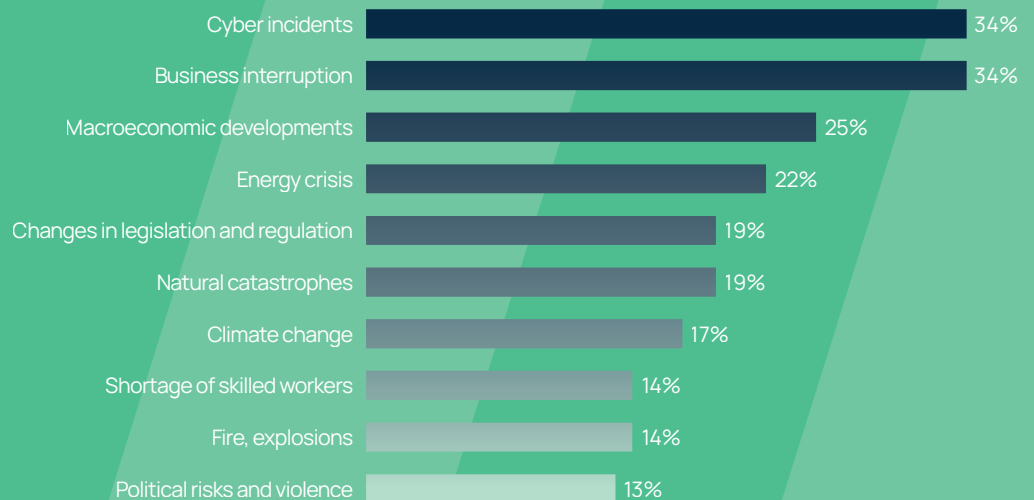
OPTIMISM ABOUT MORE FAVOURABLE SUPPLY DYNAMICS IS BEING TEMPERED BY INCREASED RANSOMWARE ACTIVITY.

The war in Ukraine has highlighted the unpredictability of the cyber threat landscape, with reduced claims activity in 2022 refuting expectations that the conflict would trigger more frequent and severe attacks. The situation nevertheless remains volatile, with the war's reach and duration profoundly affecting global cyber security. Geopolitical risks have increased elsewhere too, with tensions mounting between China and the United States as well as within the Middle East.

Concern and scrutiny around state-sponsored activity has moved certain markets to update war exclusions and clarify their applicability to highly destructive but remote cyber scenarios, including Lloyd's insurers. Little surprise then that executives continue to rank cyber and business interruption as two of the most significant risks facing corporations today (see Figure 2 for results from the 2023 Allianz Risk Barometer).¹

Even as cyber lives up to its dynamic reputation, businesses are now better prepared to deal with the fallout. Insurance is proving to be critical to this fightback by indemnifying losses, incentivising better cyber hygiene and strengthening resilience.

Figure 2: Allianz Risk Barometer 2023¹ (Source: Allianz Global Corporate & Specialty)



¹ Figures represent how often a risk was selected as a percentage of all survey responses from 2,712 respondents. Figures do not add up to 100%, as all respondents were able to select up to three risks per industry.

Responding to ransomware

Cyber risk has undergone several episodes of change in its relatively short history, but escalating ransomware frequency and severity in 2020 and 2021 was unlike anything experienced previously.

The availability of turnkey (and low cost) ransomware kits – otherwise known as ransomware-as-a-service – drove the proliferation of incidents during this period whilst tactics such as double or triple extortion – where gangs threatened to publish stolen data or even launch distributed denial-of-service (DDoS) attacks in the event of non-payment – saw costs spiral (see Figures 3 and 4).

Figure 3: Frequency index for ransomware vs data breach incidents – 1Q19 to 4Q22

(Source: Howden analysis based on data from SonicWall, Risk Based Security and Flashpoint)

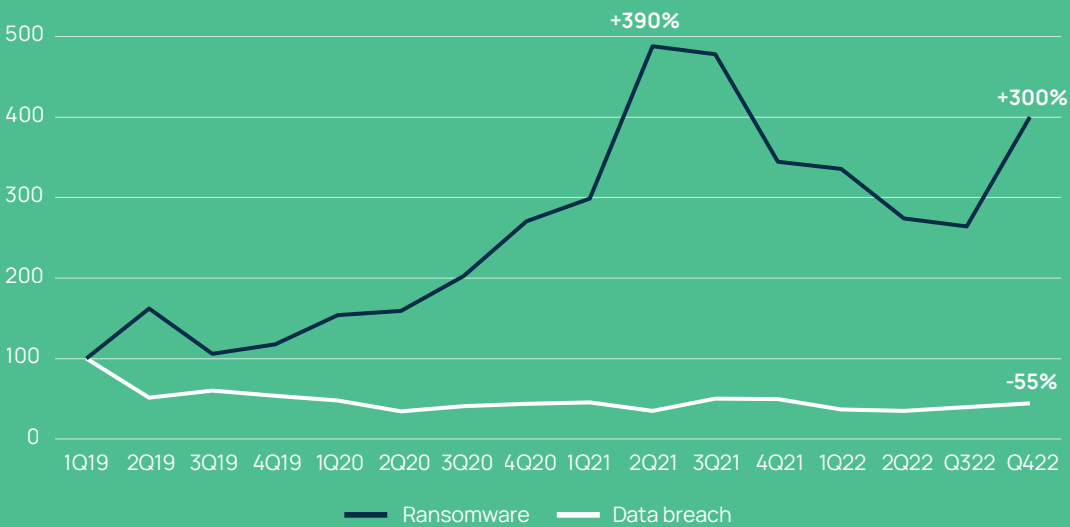
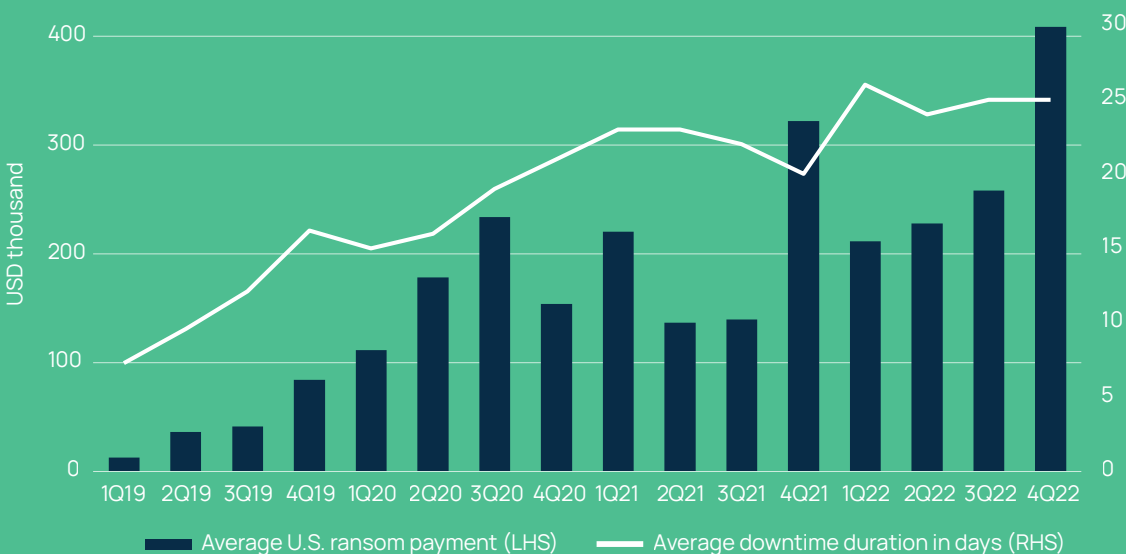


Figure 4: U.S. ransom payments and average downtime duration – 1Q19 to 4Q22

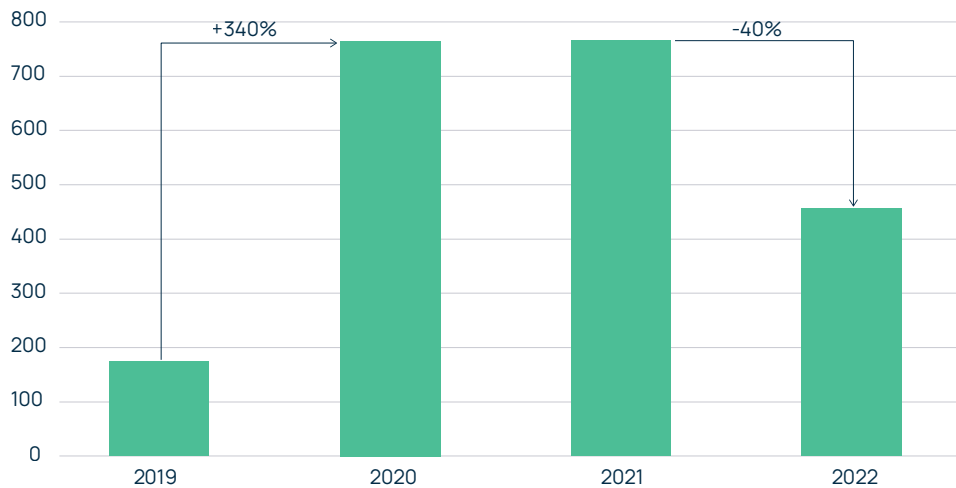
(Source: Howden analysis based on Coveware data)



Fears that Russia's invasion of Ukraine in early 2022 would fuel already elevated ransomware activity proved to be unfounded (initially at least), as both warring sides, host to some of the worst offending ransomware gangs, refocused their efforts and resources on conventional warfare. Data from Chainalysis in Figure 5 shows that revenue generated by threat actors from ransomware fell significantly in 2022 compared to the elevated levels of the preceding two years.

Economic sanctions, increased pressure on gangs from Western law enforcement and attendant disruption to the franchise model led to less successful extortion campaigns last year, even if frequency and severity remained elevated relative to 2019 levels.

Figure 5: Revenue received by ransomware attacks – 2019 to 2022 (Source: Chainalysis)

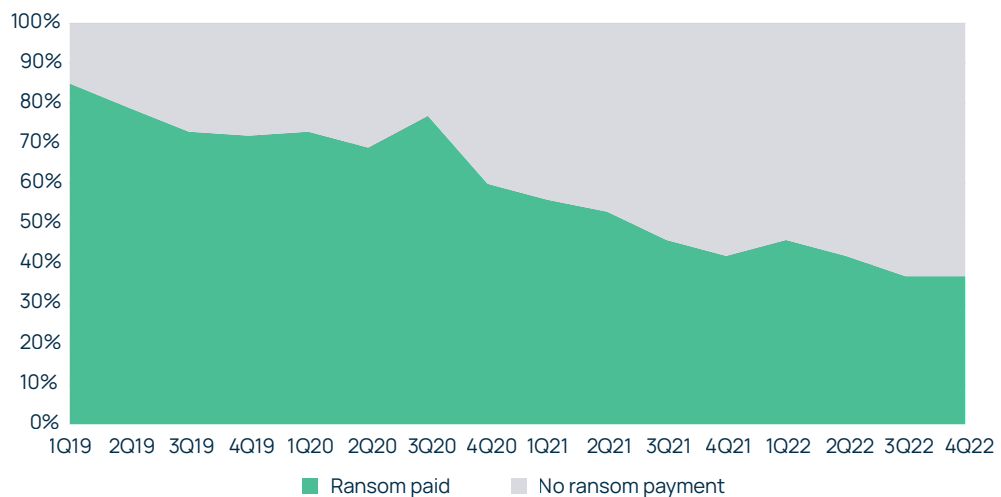


Improved cyber hygiene has also made companies less susceptible to material impacts, rebalancing cost-benefit considerations for some over whether to pay ransoms. Data from Coveware in Figure 6 shows a decreasing trend in paid ransoms between 2019 and 2022 (averaging close to 40% last year compared to 70% in 2020).

Organisations with cyber insurance remain more likely to pay ransoms than those without cover, with separate data from Sophos showing 58% of companies with standalone cover paying ransoms versus just 15% with no cyber insurance at all.²

Figure 6: Proportion of ransomware victims paying a ransom – 1Q19 to 1Q23

(Source: Howden analysis based on Coveware data)



² Sophos, *The State of Ransomware 2023*, May 2023.

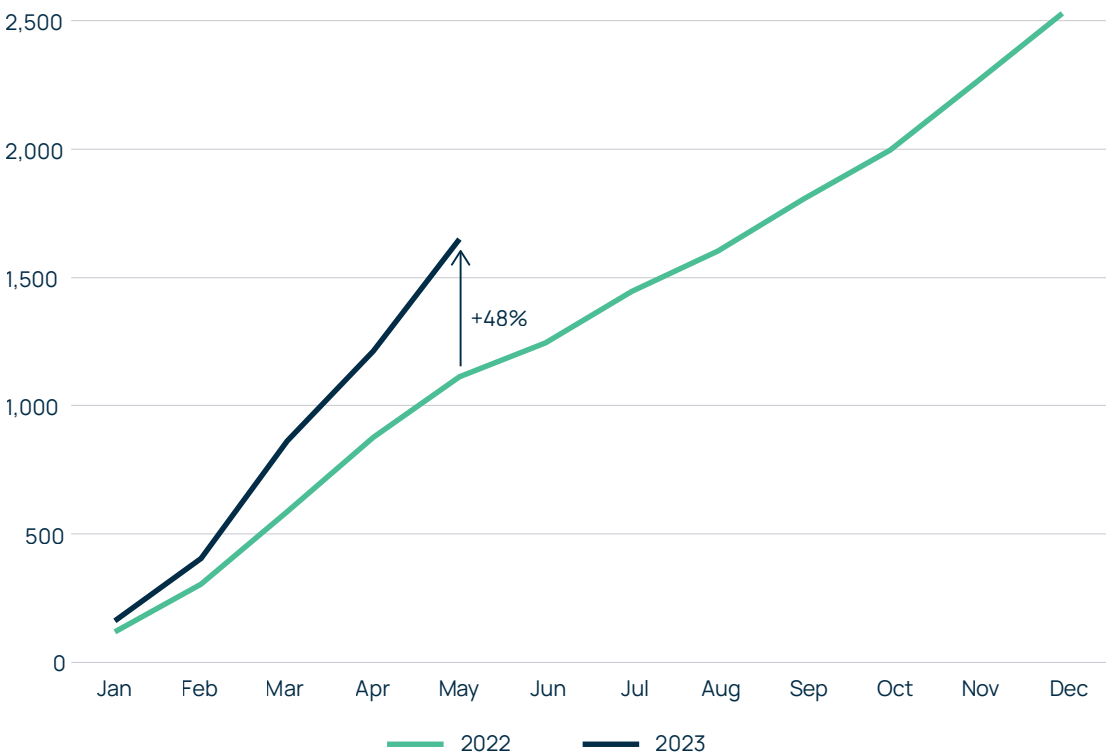
Resurgent ransomware

Ransomware is likely to continue to dominate the cyber loss landscape in 2023 and there are already signs that the relative stagnation of activity may be unravelling. Following early signs in 4Q22 that ransomware frequency was rebounding, the first five months of 2023 have seen a significant increase in attacks.

Figure 7 compares cumulative ransomware activity in 2022 and 2023, with the latest data from NCC Group in May showing frequency up 48% compared to the corresponding period last year. Disclosures from a number of insurance carriers in 1Q23 suggest this has not (yet, at least) been accompanied by a corresponding rise in claims, pointing to the success of risk controls in making companies more resilient and supporting more stable insurance market conditions this year despite higher ransomware activity.

Figure 7: Cumulative global ransomware activity by month – 2023 vs 2022³

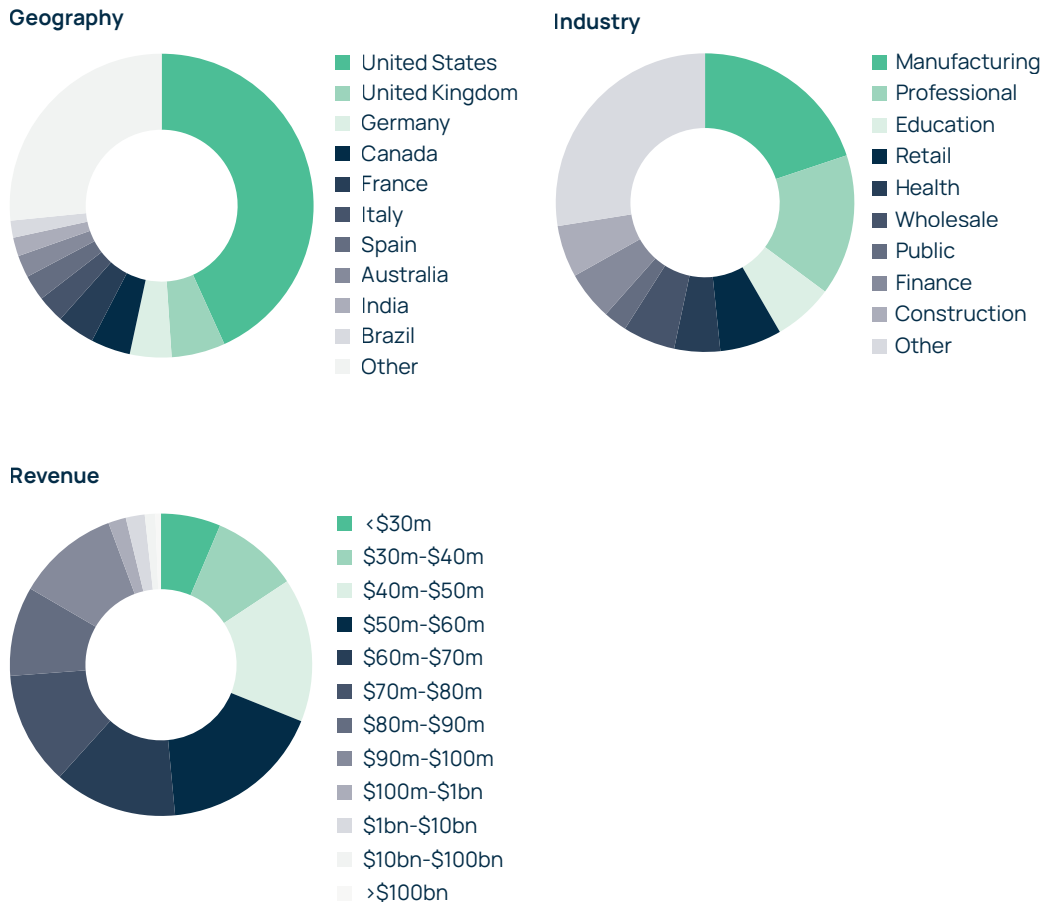
(Source: Howden analysis based on data from NCC Group)



³ 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.

Established gangs (starved of funds following the drop in revenues last year), along with the emergence of new groups, are driving the acceleration in frequency. Companies across a wide spectrum of sectors and geographies (albeit U.S. predominantly) are being targeted, with mid-sized organisations in particular experiencing a high number of attacks as gangs weigh up ability to pay against security measures in place (see Figure 8).

Figure 8: Ransomware victims by geography, sector and revenue – 2Q22 to 1Q23
 (Source: Howden analysis based on data from Black Kite)



**RANSOMWARE FREQUENCY
 IN 2023 IS UP NEARLY
 50% COMPARED TO THE
 CORRESPONDING PERIOD
 LAST YEAR.**



AVERAGE RANSOM PAYMENTS IN EARLY 2023 WERE CLOSE TO DOUBLE THOSE PAID IN 2022.

Threat actors' tactics are also shifting. In addition to double or triple extortion, certain groups are now accessing networks to change or even destroy data and then demanding ransoms to disclose what has been targeted. There have also been growing instances of physical threats made to company executives and their families or broader contacts to force victims into negotiations.

All of which is indicative of resurgent ransomware severity following last year's lull. According to Sophos, average ransom payments in early 2023 were close to double those paid in 2022, with 40% of companies surveyed reporting payments of USD 1 million plus compared to just 11% last year (see Figure 9).⁴ Some extreme ransom demands this year have exceeded the USD 100 million mark.

Figure 9: Distribution of ransom payment amounts - 2023 vs 2022 (Source: Sophos)



⁴ Sophos, *The State of Ransomware 2023*, May 2023.

Identifying vulnerable companies

Ransomware is back and businesses are at renewed risk of being targeted and suffering major disruption. **Alex Tenenbaum**, Director of Services at cyber analytics firm CyberCube, says it is essential in this environment that companies have robust processes in place to identify and remediate vulnerabilities that pose the greatest potential for exploitation by threat actors.

Despite an ever-changing and complex threat landscape, a select few threat actors remain responsible for a disproportionate number of breaches and losses. According to Abnormal Security, the five most active ransomware groups were responsible for more than half of all related attacks from mid-2020 to mid-2022.

Using forensic analyses of past attacks, as well as intelligence from the broader cyber threat research community, it is possible to apply a framework to identify vulnerable companies. First, organisations using technologies known to be targeted and exploited by top ransomware groups are inherently at higher risk, as exploiting digital supply chains is a route for breaching a company. Threat actors are also likely to have identified weakness(es) in technologies that they target repeatedly. For example, Windows Operating Systems 8.1 and earlier are no longer supported, and nor are Windows Server 2008 and earlier.

Secondly, companies that have security signals or security control deficiencies commonly exploited as part of threat actors' playbooks are at heightened risk. If companies have multiple security lapses, they are at greater risk given the higher likelihood of hackers successfully progressing along each killchain step to achieve their objectives.

Combining these two concepts can help identify companies most at risk from predominant threat types (including ransomware), as well as the groups behind the majority of attacks. Carriers are increasingly utilising these types of insights for underwriting decision-making and it is critical that companies work with their intermediaries to address any relevant red flags before they engage with their insurance partners.



**COMPANIES MUST HAVE
ROBUST PROCESSES IN PLACE
TO IDENTIFY AND REMEDIATE
VULNERABILITIES.**

The geopolitical effect

Companies that have strong cyber security hygiene are reducing the risk of being targeted by cybercriminals. Low barriers to entry afforded by the 'as-a-service' model have been a key facilitator of ransomware and malware activity in recent years, and a recently discovered 'phishing-as-a-service' programme, where victims are directed to authentic-looking decoy login webpages, is indicative of a constantly changing threat landscape.

Investment in cyber security is crucial in this environment. 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 a highly volatile geopolitical climate that carries considerable cyber risks and the potential for large-scale events.



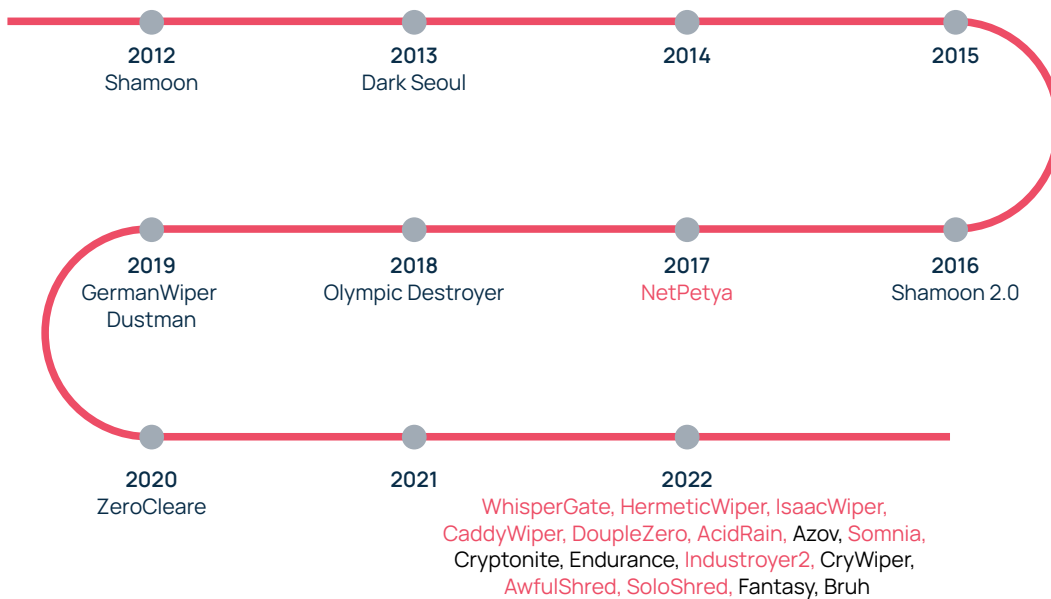
STAYING ONE
STEP AHEAD
OF ATTACKERS
MEANS THAT
COMPANIES ARE
**BETTER PREPARED
TO NAVIGATE A
HIGHLY VOLATILE
GEOPOLITICAL
CLIMATE THAT
CARRIES
CONSIDERABLE
CYBER RISKS.**

Rise of malware

Whilst the high-impact cyber attacks widely predicted in the lead up to the war in Ukraine have not (yet) occurred, the last 18 months have stood out for the marked increase in wiper malware attacks. 2022 saw the number of new wiper variants (designed to permanently erase files and immobilise computer systems) surge to unprecedented levels as Russia moved away from sophisticated operations designed to avoid detection, and towards quick and disruptive malware on specific strategic targets.

Figure 10 puts the rise of wipers into context by showing that new variants detected last year exceeded the combined number recorded throughout the previous 10 years. 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 precedence in certain phases and bring a sudden and profound change to the threat landscape. The realities of kinetic warfare go some way to explaining the diverging trajectory of malware and ransomware activity last year.

Figure 10: Recent history of notable wiper malware (Source: Fortinet, IBM)



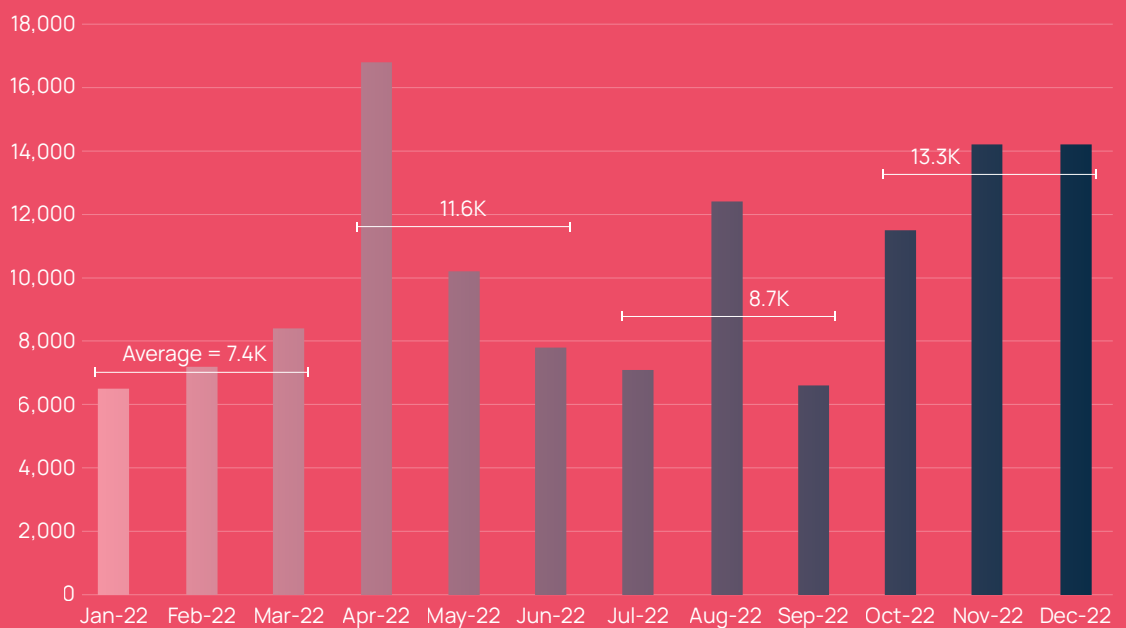
Red font denotes variants used to target Ukrainian government, military and commercial assets (initially at least)

Wiper attacks, already at a high base in 1Q22 in the lead up to and following Russia's invasion of Ukraine, accelerated through much of last year (frequency in 4Q22 was up 53% vs 3Q22 – see Figure 11). Some variants first identified in Ukraine are now being used by commercial hackers for malicious operations on targets worldwide, although perceived difficulties in extracting financial gain from wipers are likely to see cybercriminals continue to pursue more lucrative methods of attacks (such as ransomware).



NEW WIPER MALWARE VARIANTS DETECTED IN 2022 EXCEEDED THE COMBINED NUMBER RECORDED THROUGHOUT THE PREVIOUS 10 YEARS.

Figure 11: Frequency of global wiper malware attacks (Source: FortiGuard)



With nation states increasingly bolstering their cyber capabilities to seek political, economic and military advantage, and distinctions between state-orchestrated attacks and those carried out by affiliate groups becoming increasingly blurred, a big dose of complexity has been introduced into an already complicated cyber risk environment. Insights provided by XCyber overleaf provide intelligence-led expertise into what can be expected in relation to the fallout from the Ukraine war.

New age of warfare: Ukraine 12 months on

Milo Wilson, Lead Intelligence Analyst, XCyber

The war in Ukraine, a clash of titans in terms of cyber security, has considerable implications for the cyber threat landscape. For the purposes of this piece, we have broken down our analysis into three key sections: 1) a review of Ukraine war-linked cyber activity to date, 2) read-across implications for future conflicts and 3) the threat posed by other hostile countries.

1. Cyber activity in the conflict zone

Russian cyber activity aimed at the West has seen no discernible increase, with the exception of countries in close vicinity to the conflict zone, most notably Poland. Concern that untargeted cyber attacks could spread out of the conflict zone, or even trigger a NATO response if deemed an act of war, has contained Russia's cyber ambitions so far.

For all the focus on state-sponsored attacks in the current geopolitical climate, lower level activity carried out by criminal gangs still poses the biggest threat to Western businesses. Of the USD 10 billion cyber-related losses reported by the FBI in the U.S. last year, the majority were carried out by criminal groups, not state-sponsored actors.

With Russian actors less able to shield behind a veneer of plausible deniability, the response threshold appears to be lower.

For example, the wiper malware discovered in Ukraine over the last 18 months has had its ability to self-replicate set very low when compared to the Russian-linked NotPetya ransomware in 2017, which started in Ukraine and then wreaked havoc when it spread across the globe. It is also possible that Russia is focussing its outward cyber efforts on espionage, both to prepare for future attacks and gather intelligence on other countries' responses to the war.

Pro-Ukraine cyber activity has mostly focused on the release of confidential information and other sensitive material, although hackers based in other former Soviet territories have recently lifted an informal embargo on attacking Russian-speaking companies in protest against Russian aggression.



RUSSIAN CYBER ACTIVITY AIMED AT THE WEST HAS SEEN NO DISCERNIBLE INCREASE, APART FROM COUNTRIES CLOSE TO THE CONFLICT ZONE.

2. Read-across implications for future conflicts

How cyber is deployed in any war depends heavily on the warring factions involved but developments in Ukraine may offer some insights for future conflicts where at least one of the state actors has advanced cyber capabilities, such as China, Israel or the U.S.

The blending of military and cyber goals is one such area. By focussing some of its conventional warfare efforts into capturing physical cyber infrastructure, such as network cables and data centres, Russia has set the dominance of Ukrainian cyberspace as a clear military goal, something confirmed by the recent Vulkan leaks (the unauthorised disclosure of documents relating to Russian IT contractor NTC Vulkan). There is also precedent for governments experiencing stringent economic sanctions to shield criminal actors and encourage cybercrime to boost their own economies.

Other disclosures from the Vulkan leaks have revealed the (long suspected) role private Russian companies play in causing cyber disruption or carrying out digital espionage at the behest of the state. Russian cyber activity has undoubtedly been consolidated further during the war, raising the potential for the state to carry out strategic attacks on Western targets, disguised behind the actions of criminal gangs (further complicating the attribution issue).

Indeed, Western organisations that have offered support to Kyiv appear to have been targeted specifically, with U.S. officials claiming the intent of the attacks was to disrupt supply chains and logistics important to Ukraine.

Such strategies may offer a glimpse into how a conflict between China and Taiwan could progress, with China looking to replicate some of Russia's cyber efforts were a conflict to occur. The West is looking to strengthen existing partnerships in response to the threat. As an example, U.S. Congress has proposed new bipartisan legislation under the Taiwan Cybersecurity Resiliency Act to bolster cyber security and collaboration.

How cyber is deployed in other conflict zones will differ depending on the circumstances. Despite Russian involvement in several conflicts in Africa in the form of Wagner group mercenaries, limited cyber attacks have been recorded here.

Russia's co-ordinated disinformation campaigns may nevertheless be paying dividends: a recent European Union report drew a link between Russia's information operations in the global south (i.e. Africa, Latin America and Southeast Asia) and the limited number of countries in the region that have joined the sanctions regime imposed by the West.

3. Threats from other hostile nations

Geopolitics and cyber security are inextricably linked, and whilst attention is focused on Ukraine, it is important to remember that Russia is not the West's only cyber adversary. China, Iran, North Korea and Venezuela are also hostile to Western interests and are actively seeking to disrupt, exploit and influence to further their goals.

China generally focuses its cyber activity on espionage, both for strategic geopolitical gains and the theft of intellectual property to boost its domestic industries. In 2021, the Chinese government passed a law that made the reporting of 'zero-day' vulnerabilities to authorities before public release compulsory, which appears to have significantly boosted China's offensive cyber capabilities. Iran has pursued a more aggressive cyber policy since President Ibrahim Raisi assumed power, as demonstrated by the hacking of the Albanian government in 2022 (which led Albania to consider invoking NATO's Article 5 collective defence clause).

The war in Ukraine has created a complex web of risks and geopolitical alliances, with national strategic interests being temporarily put aside to shape direction at the transnational level. The best demonstration of this is China playing both the West and Russia, according to its best outcome. The blocs being formed in the physical world are being replicated in the cyber world. Iran is supplying Russia with drones to use in Ukraine in exchange for cyber surveillance technology.

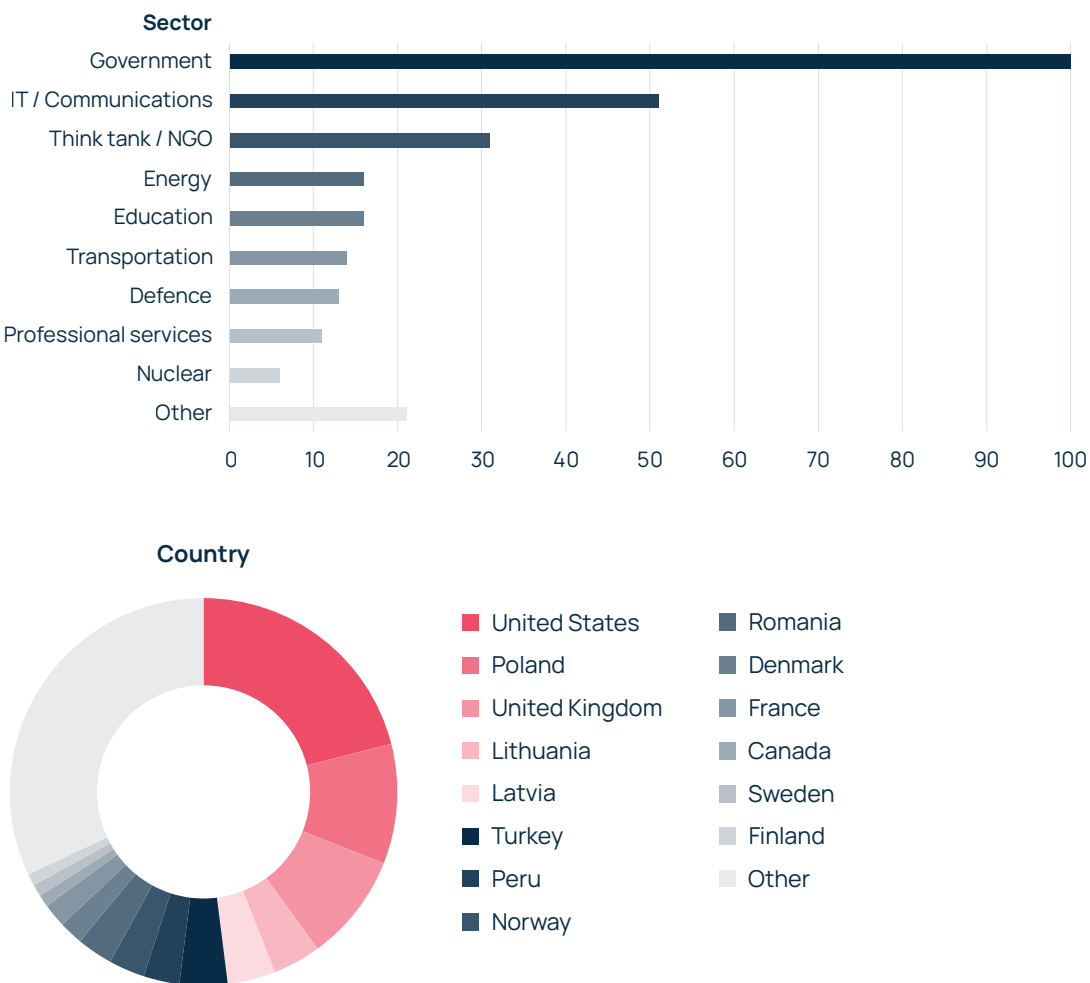
Russia, China and Iran all have offensive cyber capabilities and each has signed co-operative agreements around cyber security. Any attempt to collaborate further and form a tripartite group would likely trigger a response from the West, where friendly countries do often co-ordinate in cyberspace. There is also the danger of false flag attribution, particularly where cybercriminal groups engage in activity that has an impact on defence companies, national utilities or infrastructure. These could be classed as an act of war and escalate responses accordingly.

Spectre of systemic risk

Cyber warfare and the attendant risk of systemic losses have long cast a shadow over the cyber (re)insurance market. The issue has become even more pressing since war broke out in Ukraine. Using data from Microsoft, Figure 12 provides a snapshot of sectors and geographies (outside of Ukraine) targeted by Russian threat actors in the 12 months since the invasion.

Recorded activity against government and IT entities was higher than all other sectors combined during this timeframe, and a number of countries close to Russia's border, the eastern flank of NATO especially, were targeted heavily.

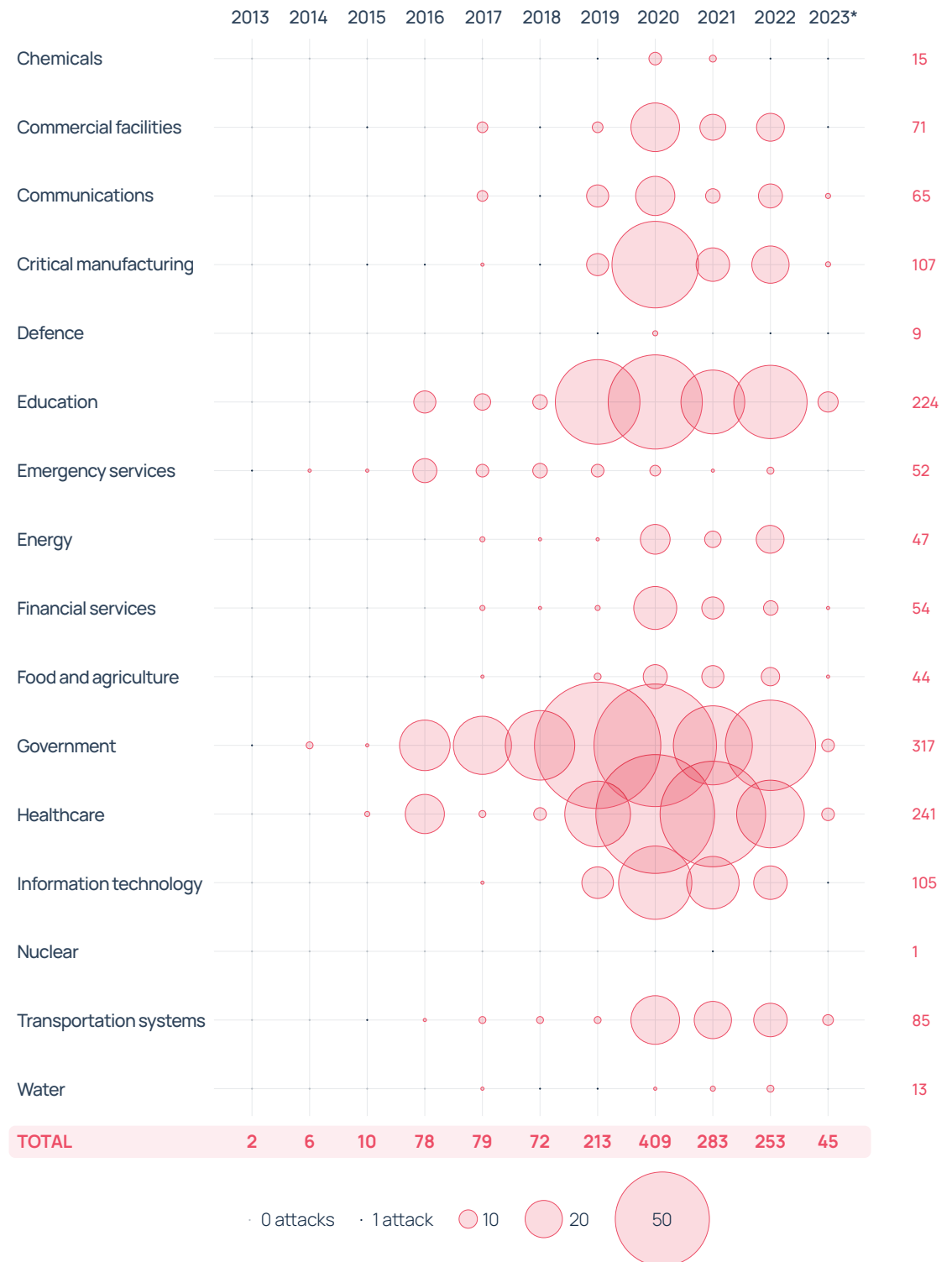
Figure 12: Sectors and countries outside of Ukraine targeted by Russian threat actors since invasion (Source: Microsoft)



Much of this activity has been relatively low-level, ranging from reconnaissance to data exfiltration. The risk of contagion is likely to have contributed to the reduction in the number of ransomware attacks that targeted critical infrastructure last year compared to 2020 and 2021, even if levels remained comparatively high (see Figure 13).

Although spillover concerns appear to have contained Russian ambitions up to this point, the risk of more destructive attacks remains elevated in such a volatile geopolitical environment. Western governments continue to warn of the threat to critical infrastructure from state-affiliated threat actors who have already shown the intent and capacity to launch attacks in more tranquil times.

Figure 13: Number of ransomware attacks on critical infrastructure worldwide – 2013 to 2023
 (Source: Howden analysis based on data from Temple University)⁵



* Data current up to 31 March 2023

⁵ Rege, A. (2022). "Critical Infrastructure Ransomware Attacks (CIRA) Dataset". Version 11.9. Temple University. Online at <https://sites.temple.edu/care/ci-rw-attacks/>. Funded by National Science Foundation CAREER Award #1453040. ORCID: 0000-0002-6396-1066.

Warning shots

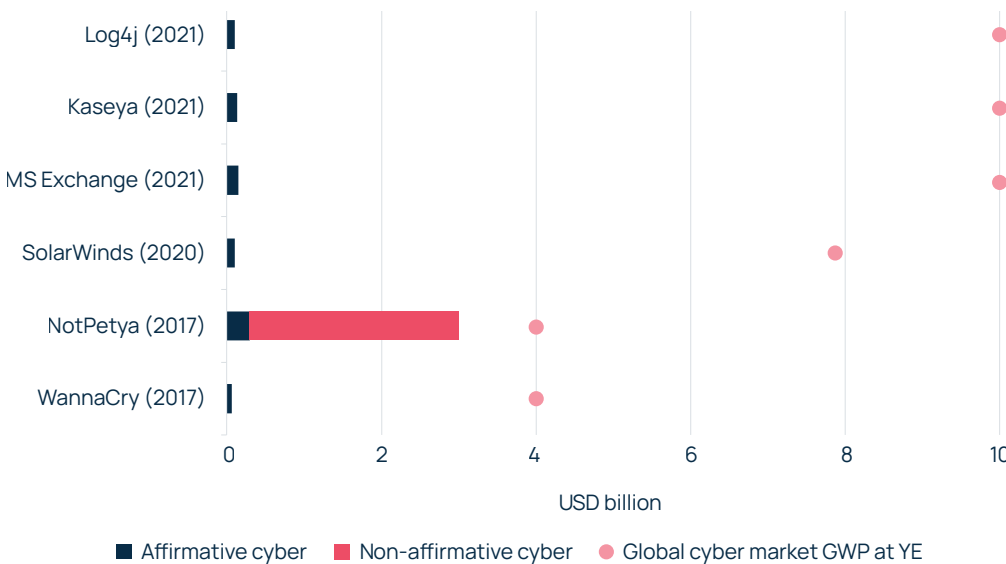
Systemic cyber exposures present challenges for an insurance market built on underwriting mostly geographically contained and uncorrelated (physical) risks, and being guided in the process by historical data to help manage aggregations, estimate potential losses and price policies. Business interruption is one of the more dominant exposures associated with large-scale cyber attacks, and COVID-19 offered a glimpse into how borderless and non-physical threats have the potential to see losses spiral quickly.

Cyber incidents, including WannaCry, NotPetya, SolarWinds, Microsoft Exchange, Colonial Pipeline, Kaseya and Log4j, highlighted the potential for systemic losses, even if the quantum ultimately ended up being manageable for the insurance market. The recent MOVEit hack is another reminder of how companies need to manage supply chain risk, even if losses from this particular incident are unknown at this stage.

Figure 14 shows that NotPetya remains the biggest individual cyber insured loss so far. It is important to point out here that approximately 10% (or USD 300 million) of the NotPetya loss was absorbed by dedicated cyber policies, with a near 100% payment record. Recent, high profile claims litigation around NotPetya has been centred on all-risk property policies, and not standalone cyber.

The ability of the cyber market to absorb economic 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. Buyers will also benefit from further innovation, increased competition and higher limits (or increased risk appetite) as the market scales up. The growth potential is huge: gross written premium (GWP) has more than doubled in the five years since NotPetya and could reach USD 50 billion by 2030.

Figure 14: Insured loss estimates for high profile cyber events vs GWP for global cyber market (Source: Howden, PCS)



This is of course not to say that the threat of aggregated losses is exaggerated. A large-scale event that resulted in a widespread cloud outage, for example, clearly poses a serious risk to the market (as the Q&A overleaf with cloud downtime insurer Parametrix indicates), although this is true of any tail event in other lines of business.



BUSINESS
INTERRUPTION
IS ONE OF THE
MORE DOMINANT
EXPOSURES
ASSOCIATED WITH
SYSTEMIC CYBER
ATTACKS, AND
**COVID-19 OFFERED A
GLIMPSE INTO HOW
BORDERLESS AND
NON-PHYSICAL RISKS
HAVE THE POTENTIAL
TO SEE LOSSES
SPIRAL QUICKLY.**

Q&A: Cyber supply chain risk

Jonathan Hatzor, CEO, Parametrix Insurance

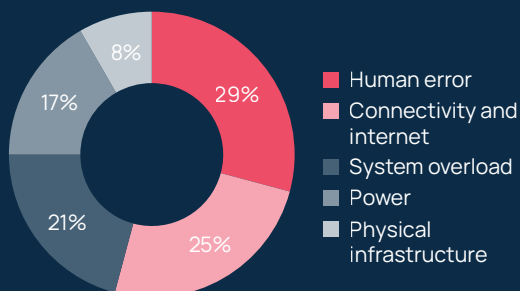
The digital supply chain is invisible. It operates in the background but is essential to the day-to-day functioning of most businesses. As data is increasingly transferred through extended global supply chains, and threat actors look to exploit vulnerabilities through single entry points (as demonstrated by the recent MOVEit hack), organisations need to manage and mitigate exposures in a fast moving risk landscape.

Q. Which vendors and events pose the biggest single point of failure risk?

A. The cloud services market is highly concentrated, with about two-thirds of global supply provided by three companies: Amazon Web Services, Microsoft Azure and Google Cloud Platform. These companies tend to report only major disruptions to their services, yet hundreds of performance interruptions occurred in 2021 and 2022 at a monthly average of 25. In other words, the cloud goes down almost every day.

The drive for innovation in the hosting sector comes with trade-offs: it is difficult to maintain uninterrupted service when new technology is constantly being rolled out. Despite cloud providers' investment in data centre resilience, downtime can occur due to an array or blend of issues around software, hardware and infrastructure. The most common reported cause of outages last year was human error, including misconfiguration and faulty maintenance activity (see Figure 15). This really matters as downtime can cause considerable financial and reputational damage to companies.

Figure 15: Causes of critical cloud outage events in 2022 (Source: Parametrix)



Q. What are the main exposures for companies in the event of a major outage?

A. Companies should consider five main risks arising from a major outage. The two most obvious are financial and reputational risks. An outage can shut down critical sales channels at any time, preventing customers from initiating a purchase. Some may come back to the affected brand, but others will seek an alternative and never try again, leading to current and future financial loss. Brand is at the centre of the reputational risk. Social media is fertile ground for sharing negative sentiment, and drives customers to look elsewhere for available services. Nearly 40% of small businesses have reported that they lost customers due to downtime.

Then there are legal, operational and fulfilment risks to consider. Legal risks can arise when contractual obligations are missed or when shareholders or regulators pursue action due to underperformance or lacklustre customer service. Operational risks include lost productivity. Most companies rely on the cloud for file use and management, communications, development and other key operational functions, meaning the internal costs from downtime, an idle workforce in particular, are considerable.

Finally, missed service level agreement thresholds present fulfilment risks. Many businesses are contractually obliged to provide certain services within a specific period, but may find fulfilment impossible in the event of an outage.

In combination, the risk in some circumstances can be large to catastrophic. We estimate that an outage on the U.S. east coast which lasted 24 hours could cause an insured loss of USD 10 billion.

Q. Are certain sectors and geographies more exposed to outage risk?

A. Leading companies have begun to map and understand the potential effects of cloud outages on their businesses. Impacts vary dramatically depending on their profile. Technology companies that supply software, platforms or infrastructure as a service are particularly vulnerable because their core activities cease when cloud services are down. Slightly less immediate, but no less severe, would be the outcome of a six-hour plus outage to a major airline, where the interruption to various systems that facilitate flight would cause cancellations and severe delays, and could take more than a day to recover.

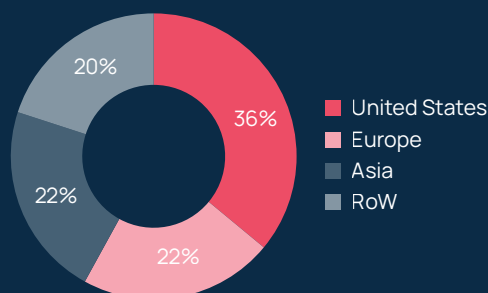
At the other end of the spectrum, companies that require less sophisticated technology to operate, such as manufacturers and traditional retailers, are unlikely to be as badly affected. Exceptionally extended outages may nevertheless have an impact on inventory management, which could lead to severe loss of revenue.

In terms of geographical impact and timing, Figure 16 shows that about a third of events impacted the U.S. last year. The remainder of critical events were split evenly between Europe, Asia and the rest of the world. Put simply, cyber supply chain risk is something that companies operating in all sectors and geographies need to measure, manage and mitigate.



CYBER SUPPLY CHAIN RISK IS SOMETHING THAT COMPANIES OPERATING IN ALL SECTORS AND GEOGRAPHIES NEED TO MEASURE, MANAGE AND MITIGATE.

Figure 16: Geographical split of critical cloud outage events in 2022 (Source: Parametrix)



Cyber warfare

Whilst there have been no cyber attacks of comparable scale since the invasion of Ukraine (with perhaps the exception of the MOVEit attack), the scope of cyber insurance, and the war exclusions issue specifically, has taken centre stage as carriers look to clarify their positions on cyber warfare and buyers seek reassurance that existing levels of protection will be maintained.

Inconsistent terms and language across cyber (re)insurance policies – and their enforceability in relation to attribution especially but also the circumstances and context of each attack – were concerns that pre-dated the war in Ukraine, and have taken on more weight as the conflict continues and geopolitical tensions escalate elsewhere.

Much has happened on this front over the last 12 months, with a lot of noise around Lloyd's of London war exclusions that came into effect at the end of 1Q23. The Q&A overleaf with Howden experts breaks down the key points and what it means for buyers and markets.



**WAR EXCLUSIONS ARE
CENTRE STAGE AS CARRIERS
LOOK TO CLARIFY THEIR
POSITIONS.**



CONCERNS ABOUT
INCONSISTENT
LANGUAGE AND
TERMS ACROSS
CYBER POLICIES
PRE-DATED THE
WAR IN UKRAINE,
**AND HAVE TAKEN
ON MORE WEIGHT
AS THE CONFLICT
CONTINUES AND
GEOPOLITICAL
TENSIONS ESCALATE
ELSEWHERE.**

Q&A on war exclusions

The introduction of new war exclusions by Lloyd's has been the source of considerable discussion and concern. Howden's **Sarah Neild** (Head of Cyber Retail) and **Dan Leahy** (Associate Director) suggest that the new wordings bring much needed clarity for clients.

Q. Why have new cyber war exclusions been introduced by Lloyd's?

A. There have been long-held concerns across the insurance market about the applicability of traditional war exclusions to large-scale cyber incidents, particularly state-sponsored attacks. Traditional exclusions are designed for property-related policies, where cause (physical war) and attribution (state(s) or group(s) involved) can be more easily established than is the case for cyber.

The scope of traditional exclusions is also broad, covering risks such as 'insurrection, hostilities and acts of foreign enemies', typically with no requirement for war to be declared. Equally important for cyber, most do not specify that excluded acts must be 'physical' and the potential for cross-border consequences (a real risk associated with cyber warfare) is not addressed. Whilst a carveback for 'cyber terrorism' worked its way into many traditional war exclusions, the language is often broader than its originally intended scope, leaving another area for dispute on untested language.

In these discussions, it is important to remember that there are war exclusions in all cyber policies (like most lines of insurance) that are untested and were not originally drafted with cyber risks in mind. The desire to develop new language therefore stems from the need for something more suitable, with defined parameters and thresholds more appropriate for cyber. Getting this right is crucial to the relevance and sustainability of the market.

Q. Can you briefly explain what the new exclusions do (and do not) cover?

A. Following teething problems early in the process (with multiple new clauses in circulation offering varying degrees of complexity and a lack of uniformity around their application), Lloyd's and

the broking community have landed on something more workable (in the form of LMA5567A/B). Despite some reporting to the contrary, these exclusions do not exclude all state attacks. Coverage will remain for all but the most catastrophic of events, even if undertaken or supported by state actors.

Under the standard wording, losses will not be covered if they: 1) arise directly or indirectly from a physical war, and / or 2) arise from a cyber attack that is carried out as part of a physical war, and / or 3) arise from a state-sponsored cyber attack that causes a major detrimental impact to the essential services required for the functioning of a sovereign state.

Q. How do they compare to traditional war exclusions?

A. What the exclusions seek to do is provide a framework designed for cyber's unique risk profile and offer clients more certainty around the parameters of cover (in other words, what is insurable and what exceeds the threshold of insurability).

One key addition to the new war exclusion is a carveback for point #3, that reinstates cover should any collateral damage occur to assets in countries that have not been targeted directly. So if an incident spreads outside of the target country, within a global network, only losses arising from the local outage would be excluded, not the broader cross-border losses. This level of clarity and scope of cover does not exist in traditional war exclusions.

Detail around definitions adds to the differentiation from traditional exclusions. War is clarified as being 'armed conflict involving physical force' whilst the (albeit unquantified) 'major detrimental impact' clause introduces an impact threshold that means the exclusion should only come into force when a country's ability to function is jeopardised.

Essential services, including financial institutions and associated financial market infrastructure, health services or utility services, would need to be significantly impacted for this to happen. The threshold has an intentionally high bar: an attack on a number of banks, energy suppliers or similar would not trigger the exclusion unless it is of such scale that it disrupts the availability or delivery of services to the country as a whole. Cyber insurers have confirmed that they do not consider any attack to date (including NotPetya) would be of sufficient scale to trigger the exclusion.

Q. Do the exclusions deal with the attribution issue?

A. Proving attribution in cyber attacks remains a controversial topic and much of clients' concerns from the outset have centred on this issue. Some progress has been made, however. Original language that allowed insurers to rely on certain governmental statements and other sources attributing responsibility has been watered down or removed entirely.

LMA5567A reiterates that the burden of proof is on insurers, and allows both parties to 'consider' (not rely on, or be bound by) objectively reasonable evidence. This goes no further than is already the case in any dispute resolution mechanism. LMA5567B, meanwhile, removes attribution language entirely, although insurers require Lloyd's agreement to use this, with evidence of a satisfactory dispute resolution process that contemplates the application or misapplication of war exclusions. This is our preferred option of the LMA issued model clauses.

Q. To sum up, would you say that the new exclusions are a positive or negative development?

A. It has been a long road getting to this point, during which time we have fought hard against some of the more restrictive language in earlier clauses.

The rollout process has been difficult and has not shown the cyber insurance market in the best light. More positively, the clauses are now designed explicitly for cyber risks, providing increased clarity in a number of areas. This was a discussion that needed to take place, and whilst we expect developments to continue, it is a useful starting point.

Participants have also taken a crucial step in delivering a sustainable market. War exclusions are standard in nearly all other insurance products and the insurance market simply does not have the capital base for the potential aggregations associated with cyber warfare. The process of defining the limits of cover specific to cyber acts of war, whilst ensuring that they remain limited in remit and scope, is therefore needed to fulfil the full potential of the market and, more broadly, to secure the relevance of insurance for the long term.

This is not to say further refinements cannot be made, particularly around clearly defined impact thresholds. We expect increased uniformity as the year progresses, as large reinsurers impose similar exclusions at remaining renewals this year and from 1 January 2024, which will help the divergence of language issue for larger insurance programmes, with multiple participating insurers. We remain committed to advocating for clients as the market adapts to what is a fluid and highly charged threat environment.



**CYBER WAR EXCLUSIONS
OFFER CLIENTS MORE
CERTAINTY BY PROVIDING
A FRAMEWORK DESIGNED
FOR CYBER'S UNIQUE RISK
PROFILE.**

Primed for growth

Cyber insurance dynamics have shifted significantly over the last 12 months. After a period of upheaval – characterised by a rapidly deteriorating loss environment, highly constrained insurance capacity, rising demand globally and a major pricing correction – market conditions are stabilising off the back of much improved underwriting results. Pricing has plateaued, or fallen in some territories (albeit from elevated levels), limits are increasing and competitive forces are yielding more tailored underwriting decision-making that reflects companies' risk profiles.

The turnaround correlates directly to better cyber security as well as to the initial fallout from the Ukraine conflict and the attendant drop-off in ransomware activity, although, as shown earlier, this is now reversing. Risk transfer has proved to be an important enabler to the first point, with insurers' capacity deployment strategies incentivising more robust risk controls.

Strengthened cyber resilience is paying dividends for policyholders now that the threat environment is ramping up. Despite the marked increase in ransomware activity so far in 2023, underwriting performance appears to be holding up relatively well. With existing carriers looking to increase capacity deployments, boosted further by a number of new entrants, the foundations for a more mature cyber market are now in place.



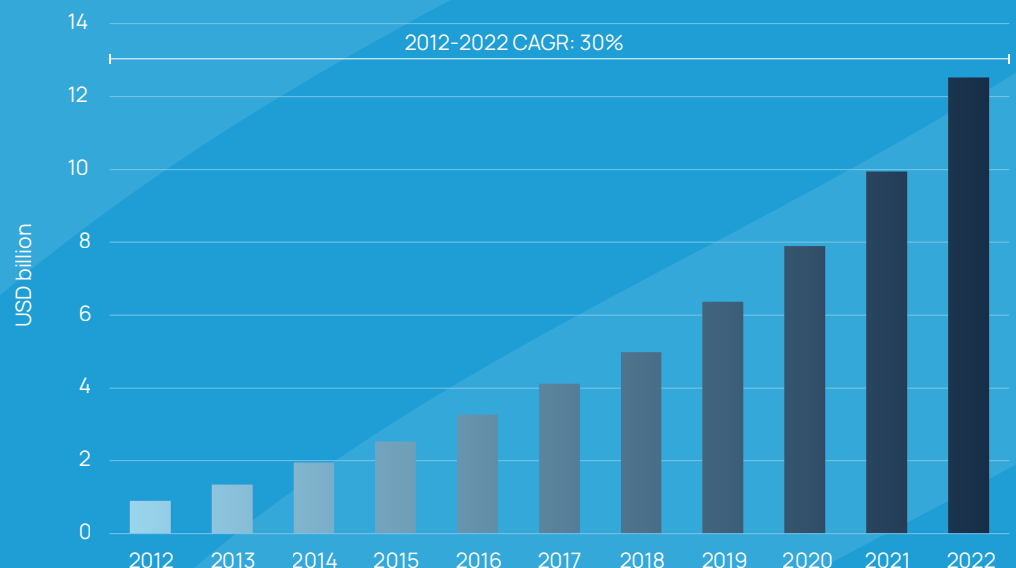
AFTER A PERIOD OF UPHEAVAL, MARKET CONDITIONS ARE STABILISING DUE TO MUCH IMPROVED UNDERWRITING RESULTS.

Growth profile

The cyber market remains the fastest growing area of insurance by some distance. Annualised growth of 30% over the last decade (as shown by Figure 17) compares to the single-digit percentage range of the broader P&C commercial sector.

Premiums are a product of exposures and pricing, and whilst both combined in unison to drive growth up to 2020 (albeit weighted more to the former), the pricing environment precipitated a notable shift in 2021, when high double- or even triple-digit price increases more than offset underwriting actions and the ensuing reduction in overall exposures.

Figure 17: Cyber global gross written premium – 2012 to 2022 (Source: Howden)



Sustaining this level of expansion will require close collaboration across the market in confronting issues like systemic risk, capital inflows and global uptake (more on these shortly). The pedigree is strong given how far the market has come in such a short space of time.

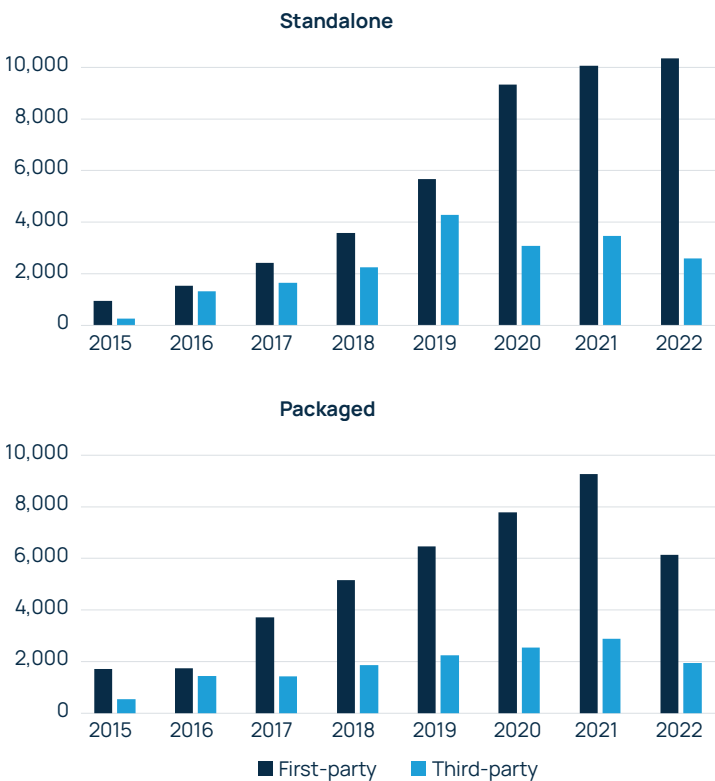
A hard reset

The cyber market is the latest example of what the insurance sector has done so well many times over: innovating and developing solutions for the changing needs of clients. Wide-ranging cyber coverages have been developed in relatively short order and the market has maintained a strong claims payment record despite the highly dynamic threat landscape.

The correction that started in 2020 nevertheless represented a watershed moment for cyber insurance. Prior to this point, a relatively benign loss environment had fed abundant capacity, expanding coverage terms and favourable pricing (perhaps to detrimental levels for both). What followed led to the highest annual rate increases across the entire insurance market. Risk appetite and perceived price adequacy for cyber exposures were reset, with carriers reacting swiftly to get ahead of spiralling loss costs.

Using U.S. supplemental filings data, Figure 18 shows how claims have trended in the U.S. market since 2015, with both standalone and packaged policies seeing a surge in the number of first-party claims from 2019/20, due almost exclusively to escalating ransomware attacks. The frequency of first-party claims nevertheless levelled off in 2021 and 2022 whilst the quantum of third-party claims remains modest in comparison, although this could of course change.

Figure 18: Reported first-party and third-party cyber claims for U.S. standalone and packaged policies – 2015 to 2022 (Source: NOVA, S&P Global Market Intelligence)



DATA PRIVACY RISKS MERIT CLOSE ATTENTION AFTER ADVERSE RULINGS IN CERTAIN U.S. STATES.

Return of data privacy

For all the well-founded focus on first-party (ransomware) claims in recent years, as well as the cyber aggregation issue, an older risk (data privacy) merits close attention following recent rulings in certain U.S. states around the Biometric Privacy Data Act (BIPA) that have revealed huge potential exposures. (Pixel litigation in the U.S. is another emerging trend to watch).

Companies that collect and retain biometric data such as fingerprints and face scans without obtaining proper consent face the risk of significant penalties given damages accrue per scan and can date back as far as five years. With BIPA carrying a penalty of up to USD 1,000 for each negligent violation and USD 5,000 for each reckless or intentional violation (plus fees and costs), the dollars at stake in terms of damages are potentially substantial.

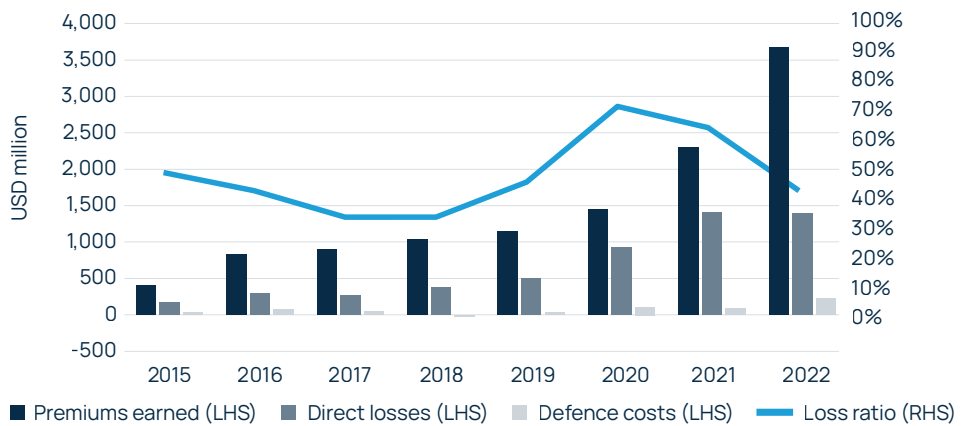
A number of judgements have already decided in favour of plaintiffs – one high profile (jury-led) settlement landed at over USD 200 million – and with little visibility around how many U.S. companies are potentially exposed to BIPA (biometric data is often collected by third-party vendors), not to mention the relatively long tail associated with such claims, the issue represents one of the more impactful known unknowns confronting the cyber insurance market.

Easing pressures

Bringing considerably higher premiums into the equation, underwriting results were much improved for U.S. cyber insurers last year, with most carriers comfortably back into profitable territory. When looking at data in aggregate for standalone cyber policies specifically, the sector's performance was strong in 2022, with the loss ratio falling to 44% from 65% in 2021 (see Figure 19). Significantly increased premium flow into the U.S. market last year (up 60% year-on-year) had a strong bearing on results, as losses and defence costs remained relatively stable.

Figure 19: Loss ratio for U.S. standalone cyber policies – 2015 to 2022

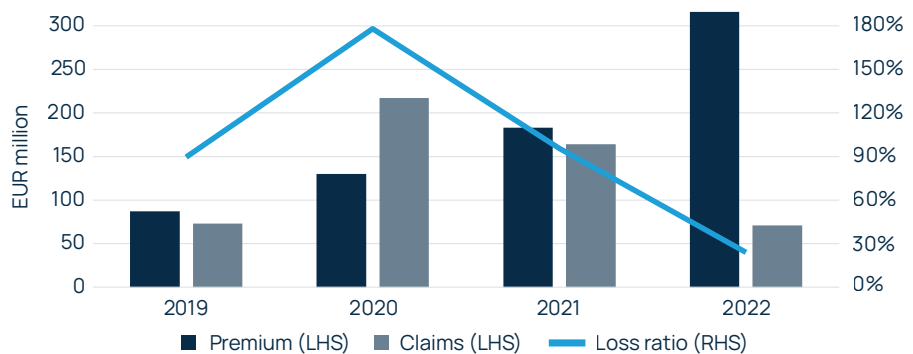
(Source: NOVA, S&P Global Market Intelligence)



These underlying trends are being replicated (and amplified) outside of the U.S., including France, where the loss ratio fell to an even more favourable 22% last year (see Figure 20). There was considerable variability within this overall figure, however, with the loss ratio for large companies (with >EUR 1.5 billion turnover) sitting at 16% compared to 100% for medium-sized companies with turnover of between EUR 10 million and EUR 50 million.

Figure 20: Performance of France cyber insurance market – 2019 to 2022

(Source: AMRAE)



Improved cyber hygiene has been a decisive factor in delivering improved underwriting performance post-2020. The investments companies have made in getting to this point have been considerable, but hardened cyber defences have left companies less vulnerable to prolonged disruption or outsized losses in the event of a breach.

The cost of insurance cover is also more commensurate with attritional loss costs. Having sustained one of the most painful market corrections in recent times, conditions are now relenting and buyers that have the necessary risk controls in place are being rewarded with more favourable pricing and terms.

Fulfilling the potential

This puts the market on a sound footing for profitable growth. Should current growth trends be maintained for the remainder of this decade, an ambitious but feasible scenario given the high level of demand globally and the amount of capacity returning to the market, GWP could exceed USD 50 billion by 2030, rivalling the scale of other major P&C lines of business such as D&O (see Figure 21 and 22).

Whilst the U.S. will remain the biggest cyber market by some distance, Europe, starting from a much lower base, is expected to close the gap somewhat during this time. Territories seeing particularly robust growth include France, Germany, Israel, Scandinavia and the United Kingdom.

The growth potential for cyber insurance is unparalleled. The realisation of this potential is tied in part to external factors such as geopolitics and macroeconomics, but by focusing on key issues within its domain – including penetration, tail-risk management and reinsurance capacity – the market can overcome potential growth limitations and secure long-term relevance.

Figure 21: Gross written premium projections for global cyber insurance market – 2022 to 2030 (Source: Howden)

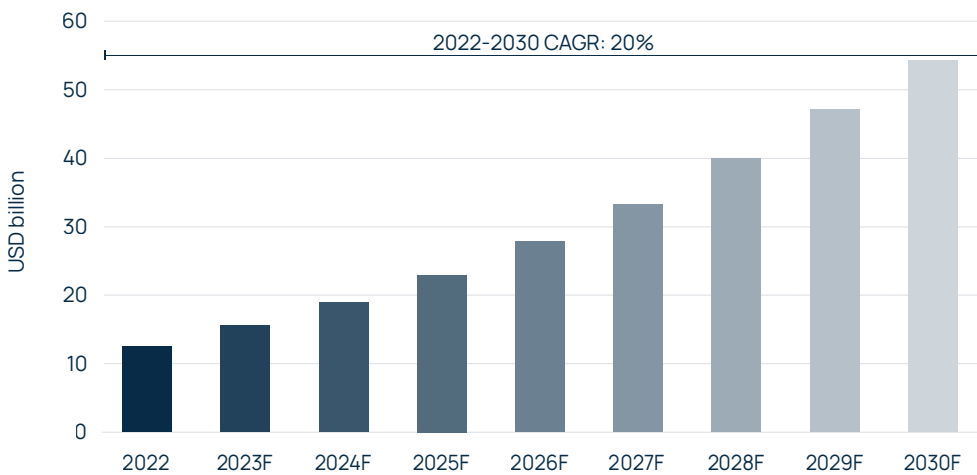
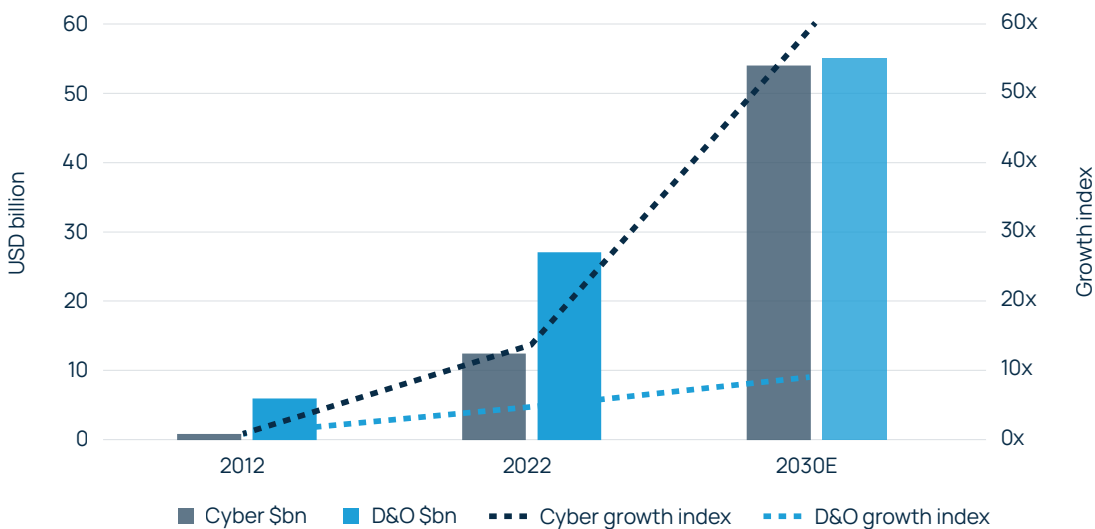


Figure 22: Market size projections by 2030 – cyber vs D&O (Source: Howden)





THE REALISATION
OF THE CYBER
MARKET'S GROWTH
POTENTIAL IS TIED TO
GEOPOLITICS AND
MACROECONOMICS,
BUT ALSO SME
PENETRATION,
TAIL-RISK
MANAGEMENT
AND ATTRACTING
CAPITAL AND
TALENT.

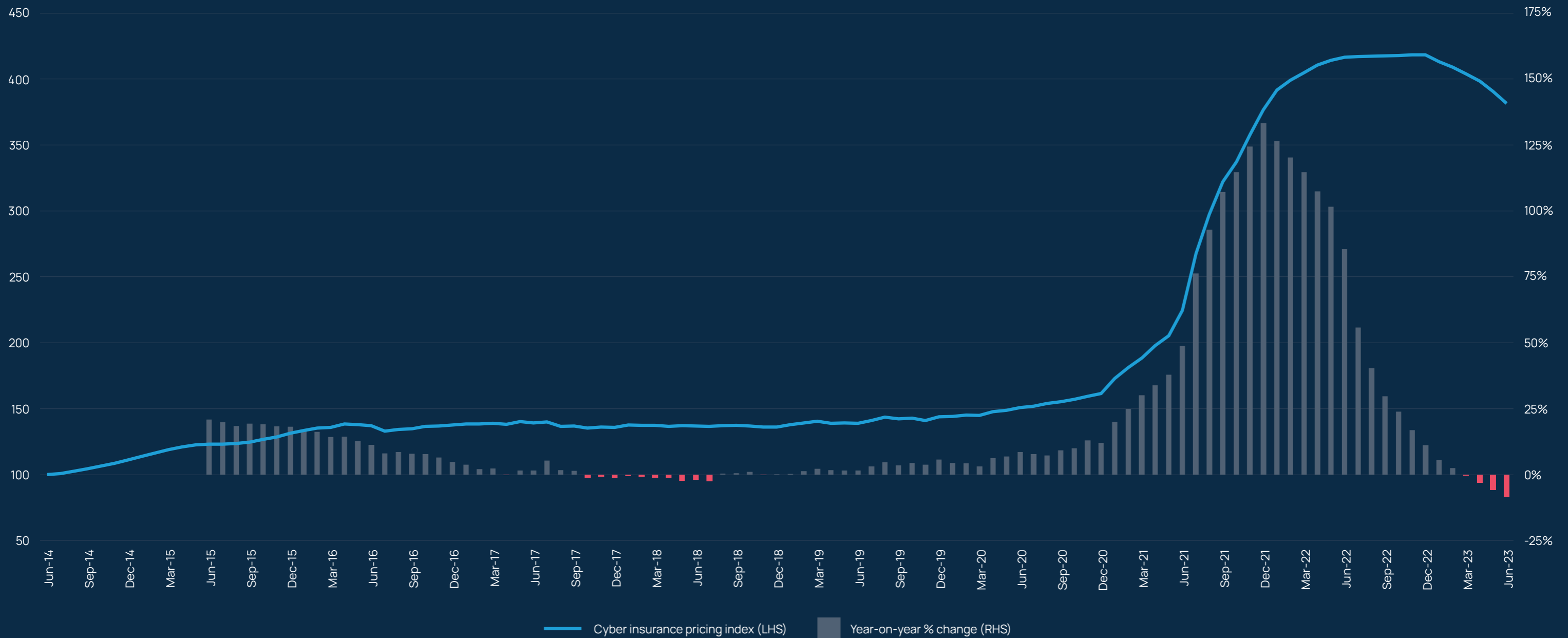
Challenge #1: Growing the pie

Pricing increases in recent years, from 2020 onwards especially, have driven the growth of the cyber market, but these tailwinds for insurers are now unwinding or even reversing in certain areas. Figure 23, which shows Howden's Global Cyber Insurance Pricing Index from 2014, along with year-on-year changes, attests to this. Whereas annual rate increases of more than 100% were recorded during the first half of last year, the corresponding period in 2023 has seen flat renewals or even decreases of up to 10% in recent months as pricing has come off recent historical highs.



PRICING TAILWINDS FOR INSURERS ARE NOW UNWINDING OR EVEN REVERSING IN CERTAIN AREAS.

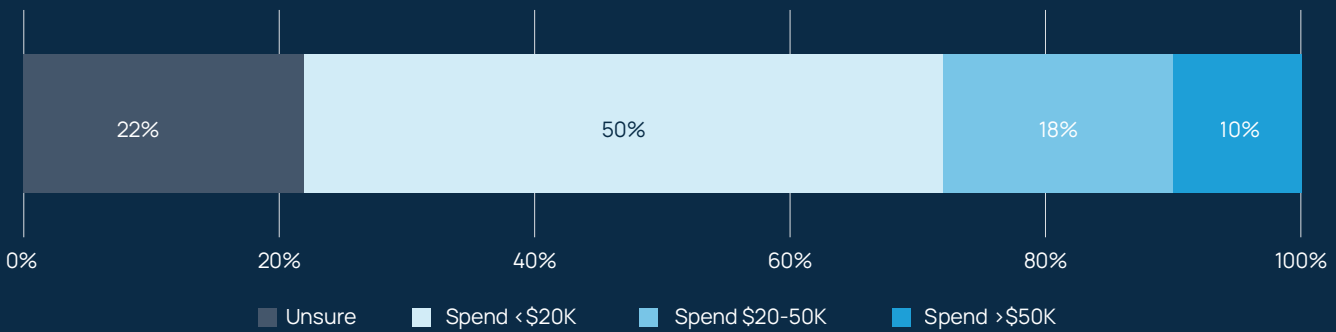
Figure 23: Howden's Global Cyber Insurance Pricing Index – 2014 to 2Q23 (Source: Howden)



Absent any further shocks, pricing is unlikely to drive market expansion to the extent it did during the 2020-2022 correction (when several carriers hit their underwriting targets early), requiring ambitious plans for exposure growth. To fulfil its true potential, the cyber market needs to move beyond existing premium pools by doing more to meet the demands of large buyers – reduced limits and (obligatory) higher retentions have forced some large buyers in Europe to look at captive solutions – and, equally important, increasing uptake in under-penetrated territories and demographics.

Penetration rates vary significantly by geography and company size. Although cyber risk awareness is growing across the board, and uptake amongst mid-sized companies is improving, cyber insurance essentially remains a large corporate market. More work needs to be done in engaging with smaller companies especially. Figure 24 shows the relatively lower spend on cyber security for SMEs in Australia, the United Kingdom and the United States.

Figure 24: SMEs budget spend on cyber security⁶ (Source: OpenText Security Solutions)



CYBER INSURANCE ESSENTIALLY REMAINS A LARGE CORPORATE MARKET.

⁶ OpenText Security Solutions polled 1,332 security and IT professionals from SMEs (i.e. companies with up to 1,000 employees) in Australia, the U.K. and the U.S from 24 September to 10 October 2022.

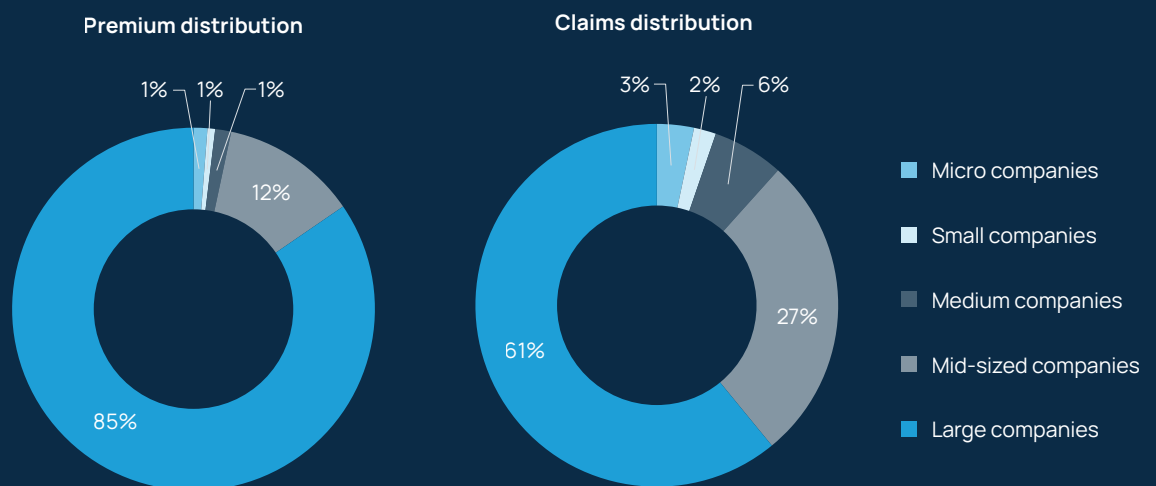


BROKERS AND INSURERS NEED TO FIND BETTER WAYS TO BRING SMEs INTO THE CYBER MARKET.

The direct relationship between risk controls and access to insurance coverage underscores the amount of work that still needs to be done within the SME space, especially outside the United States where data consistently shows low cyber insurance uptake overall.

In France, for example, of the premiums paid for cyber insurance in 2022, 85% came from large companies (with revenues >EUR 1.5 billion). Mid-sized companies (revenues of EUR 50 million to EUR 1.5 billion) and SMEs (revenues <EUR 50 million) accounted for the remaining 15% but were responsible for a disproportionate share of reported claims (see Figure 25).⁷

Figure 25: Cyber premiums and claims distribution in France in 2022
(Source: AMRAE)



⁷ AMRAE, *LUMière sur la CYberassurance*, 2023.

Challenge #2: Systemic risk and cyber warfare

Systemic risk has already been addressed in detail in this report. The issue continues to be (re)insurers' primary concern – cyber's inherent aggregation risk brings a higher cost of capital – hence the introduction of new policy language to better manage exposures specific to cyber acts of war. There is much at stake as constituents across the insurance value chain work to find solutions that are palatable to both clients and markets.

Avoiding a messy fallout from any future systemic or war-related cyber loss (and the inevitable litigation that would follow) is crucial to the prospect of the cyber insurance market achieving the growth trajectory set out in Figure 21, as well as maintaining clients' confidence in the product.


COVID-19 demonstrated how coverage ambiguity for extreme, non-physical loss scenarios benefits no one. Policyholders, believing that their business interruption losses would be indemnified, felt aggrieved by the wave of claims denials. Carriers, on the other hand, were left confronting unanticipated (and unpriced) losses initially, and damaged reputations latterly.

It is important that insurance carriers and buyers learn the lessons from the pandemic. This is why Howden supports efforts to get ahead of the cyber warfare issue and attempt to determine proactively the scope of cover should any major loss materialise, especially in such uncertain geopolitical times.

Clarity and communication are key: the latter will be crucial to allaying lingering concerns amongst clients around the applicability of cyber exclusions (and stressing that policies will continue to cover all but the remotest of nation state attacks) whilst the former will provide underwriters and investors with the confidence needed to commit to the market.



**CLARITY AROUND CYBER
WARFARE WILL PROVIDE
UNDERWRITERS AND INVESTORS
WITH THE CONFIDENCE NEEDED
TO COMMIT TO THE MARKET.**



AVOIDING A MESSY
FALLOUT FROM
ANY FUTURE
SYSTEMIC OR WAR-
RELATED CYBER
LOSS IS **CRUCIAL**
TO FULFILLING
THE CYBER
MARKET'S GROWTH
POTENTIAL, AS WELL
AS MAINTAINING
CLIENTS'
CONFIDENCE IN
THE PRODUCT.

Challenge #3: Reinsurance capital

Reinsurance capital is vital for the cyber market to achieve its growth ambitions and is perhaps the single biggest challenge to overcome. With approximately 45% of cyber premiums ceded to reinsurers currently (typically via quota share arrangements), which is far higher than for most other lines of business, broad capacity constraints and price corrections in the reinsurance market present potential limitations.

Figures 26 and 27 talk to the supply and pricing pressures across the global reinsurance market currently. Significant capital erosion, combined with elevated catastrophe losses and a series of macroeconomic and geopolitical shocks, have converged to create the most challenged conditions in recent memory.

Figure 26: Dedicated reinsurance capital – 2012 to 1H23 (Source: NOVA)

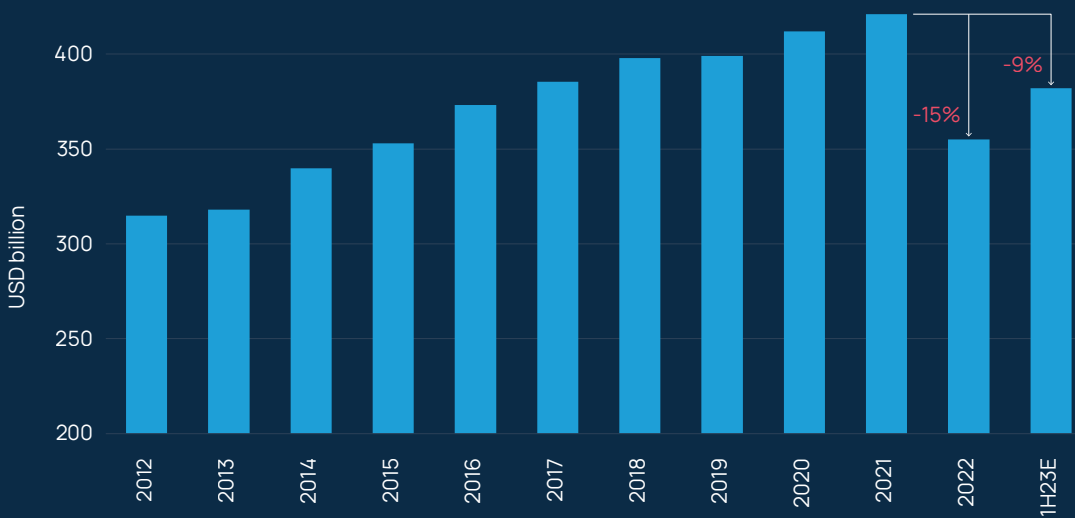
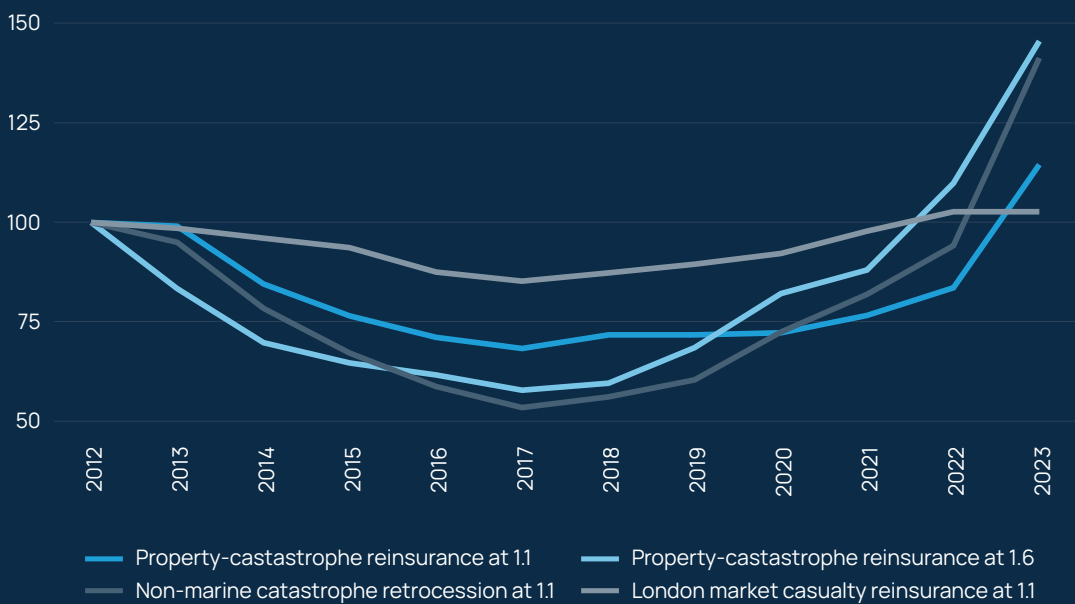


Figure 27: Howden pricing indices for property reinsurance and retrocession markets

(Source: NOVA)

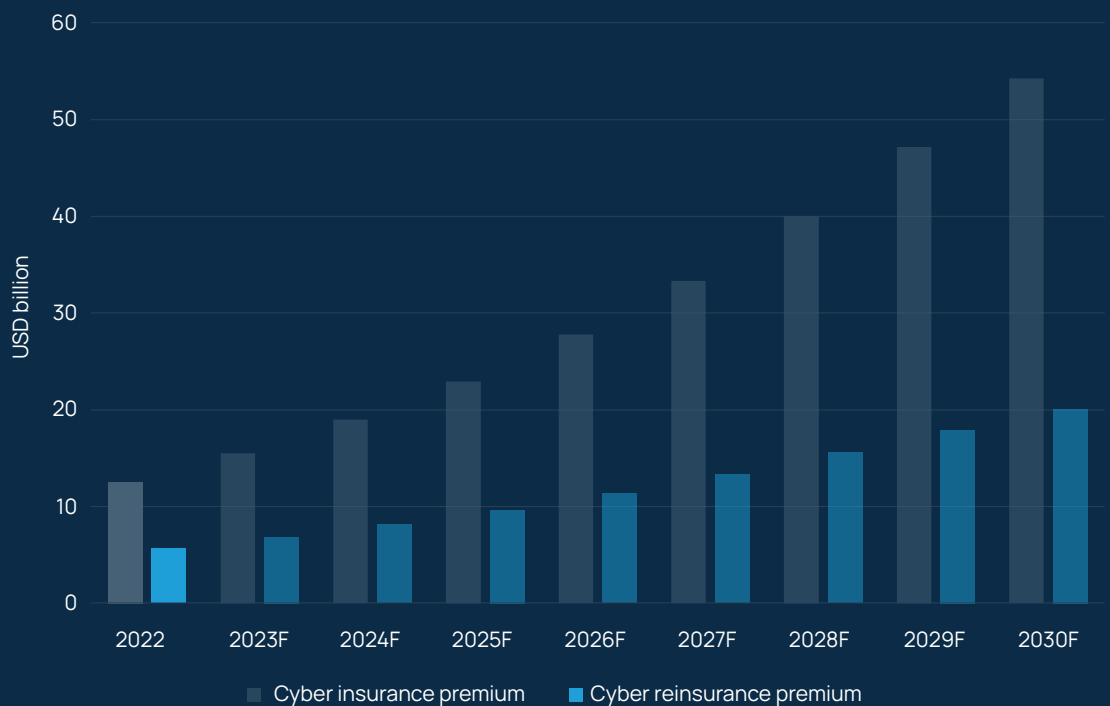


Conditions in the cyber reinsurance market specifically have relented this year, with pricing stabilising after a period of significant hardening. Although reinsurers are benefitting from improvements in underlying portfolios following recent pricing corrections, cyber reinsurance supply will need to increase significantly if it is to meet demand between now and 2030.

This backdrop presents a potential impediment to cyber insurance's growth projections. Whilst cyber reinsurance premiums are currently in the range of USD 6 billion, they would need to increase more than three times over in order to fulfil growth expectations by the end of the decade (even when assuming slightly tapered cession rates – see Figure 28). Such high levels of growth would be ambitious during favourable market conditions, let alone when supply is as constrained as it is currently in the reinsurance market.

This underscores the need for the cyber reinsurance market to develop more products that enable insurers to retain more risk, especially now that cedents are more comfortable managing attritional losses. Large insurers are already moving away from quota share to more efficient capital structures (such as excess-of-loss and tail-risk occurrence covers), a development that will facilitate a wider availability of reinsurance capital to support future growth.

Figure 28: Cyber insurance and reinsurance premium projections up to 2030
(Source: Howden)



Further innovative thinking around matching risk to capital is needed to realise the full potential of cyber (re)insurance from here. Continued investments into modelling solutions to help carriers manage and price (systemic) exposures, and, in turn, better articulate results to alternative capital providers, is a key requirement to unlocking more capacity. Another related point is increased engagement with capital markets. Growing consensus on risk definitions, alongside product innovation around systemic exposures in particular, are already attracting third-party investors. Maintaining focus and momentum in this area will be crucial to seeing alternative capacity becoming an integral part of the cyber market's capital structure.

Expert advice in extraordinary times

After three years of hardening, conditions in the cyber insurance market are now stabilising. This reflects the considerable investments made by businesses in improving their risk postures, alongside unwavering underwriting actions taken by carriers in increasing the cost of cover to be more commensurate with loss costs. This has led to improved supply dynamics in 2023.



THE CORE INGREDIENTS
FOR A **SUSTAINABLE
CYBER INSURANCE
MARKET ARE NOW IN
PLACE.**



CAPITAL IS KEY TO UNLOCKING THE FULL POTENTIAL OF THE CYBER (RE)INSURANCE MARKET.

The core ingredients for a sustainable cyber insurance market are now in place. Having navigated the early phases of development that often come with new, fast growing lines of business – cautious approaches initially, growing confidence (or complacency) off the back strong profitability, market changing losses and capacity withdrawals – competition is now returning as carriers not only look to renew existing programmes but also write new business.

Capacity constraints are relenting, but, as shown in this report, the cyber market needs to confront further challenges if it is to sustain its recent growth trajectory and meet the growing demands of clients worldwide. The future growth (and relevance) of cyber insurance centres around three key themes: penetrating new premium pools (with SMEs at the forefront), addressing the systemic risk issue and (key to both) the expansion of available capital.

Capital is key to unlocking the full potential of the cyber (re)insurance market by facilitating product innovation tailored for new territories and an expanded client base, as well as building resilience against extreme tail risk events. Intermediaries have a crucial role to play here, especially those with the (genuine) local knowledge and capital markets capabilities needed to penetrate into new geographies and attract capital at scale.

Today's marketplace demands the very best intermediary expertise and leadership that goes beyond transactional services. It requires sector experience, advice in building a better risk profile for submission, strong partnerships with third-party experts and unrivalled access to capital providers. This is what Howden brings to the table and more. Come and talk to us.

Contacts

Howden broking

Julian Alovisi

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

Sarah Neild

Head of Cyber Retail
+44 (0)7355 091 291
sarah.neild@howdengroup.com

Kristoffer Haleen

Deputy CEO
Stockholm
kristoffer.haleen@howden.se

Matthew Webb

Executive Director
+44 (0)20 3836 7668
matt.webb@howdentiger.com

Shay Simkin

Global Head of Cyber
+972 52 465 6090
shay@howden.co.il

Daniel Leahy

Associate Director
+44 (0)7923 246517
daniel.leahy@howdengroup.com

Ben Geffen

Associate Director
+44 (0)7355 090 687
ben.geffen@howdengroup.com

Expert contributors

CyberCube

Alex Tenenbaum

Director of Services

alexten@cybcube.com

Parametrix Insurance

Jonathan Hatzor

CEO

jonathan@parametrixinsurance.com

XCyber

Milo Wilson

Lead Intelligence Analyst

milo.w@xcybergroup.com

Howden

One Creechurch Place,
London, EC3A 5AF

T +44 (0)20 7623 3806

F +44 (0)20 7623 3807

E info@howdengroup.com

www.howdengroup.co.uk