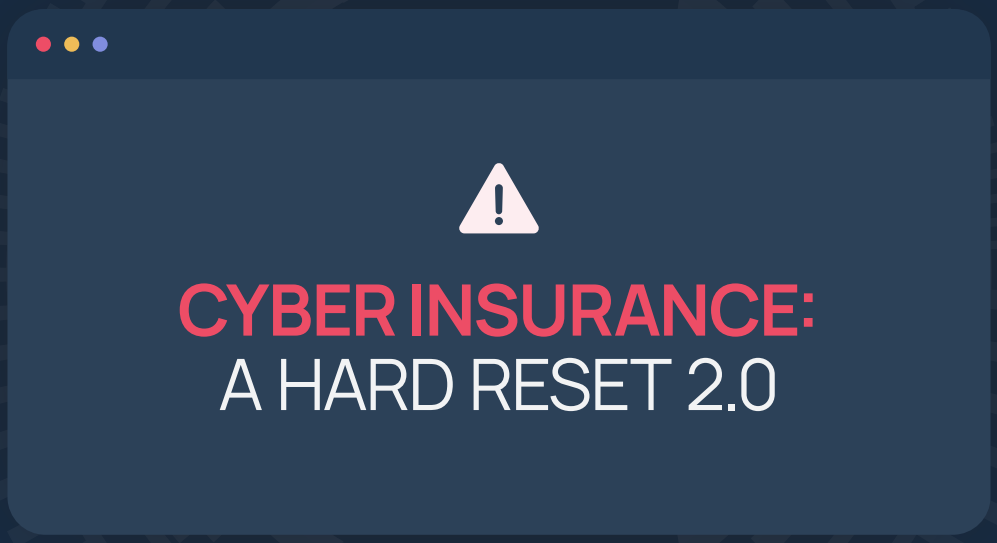
howden



CYBER INSURANCE:
A HARD RESET 2.0

Key takeaways

Ransomware, war in Ukraine and triple-digit rate increases encapsulate a period of colossal change for cyber insurance.

Market conditions remain difficult, but actions taken by companies and insurers to build resilience are starting to pay dividends.

Number of brokers reporting rising demand

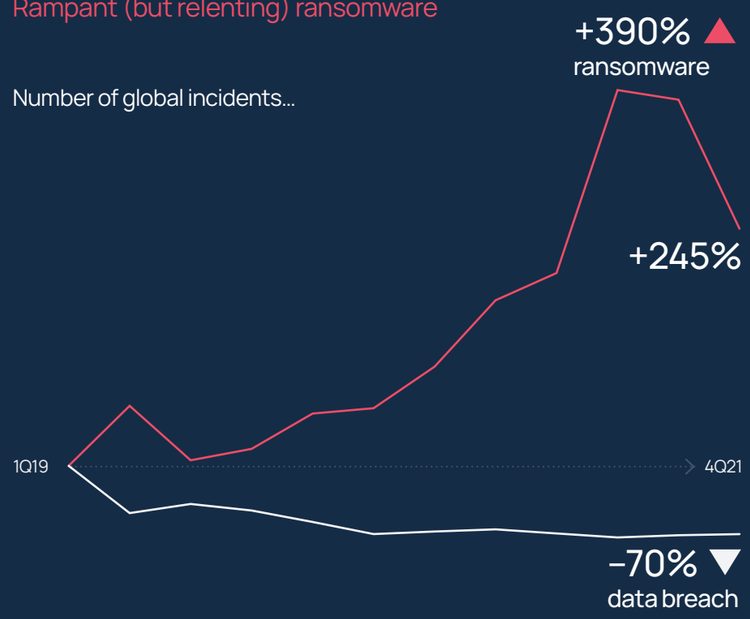
+89%

Number of brokers reporting an increase in claims

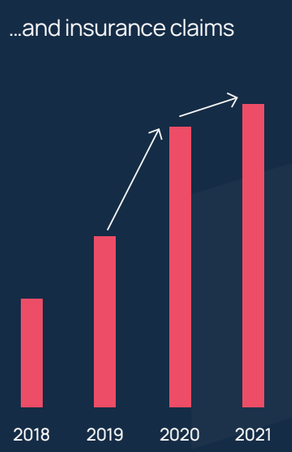
+72%

Source: CIAB

Rampant (but relenting) ransomware

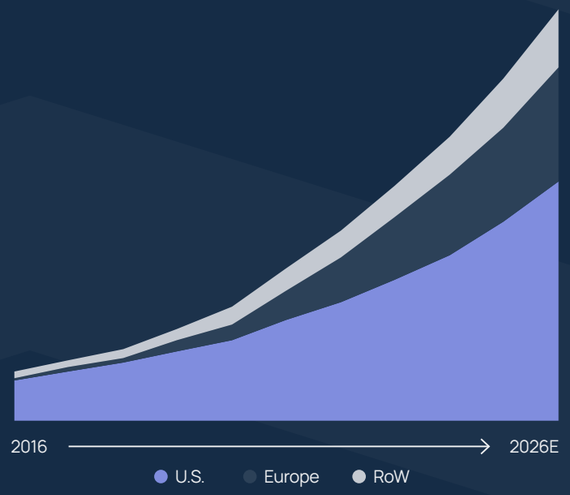


Source: Howden, SonicWall, Risk Based Security



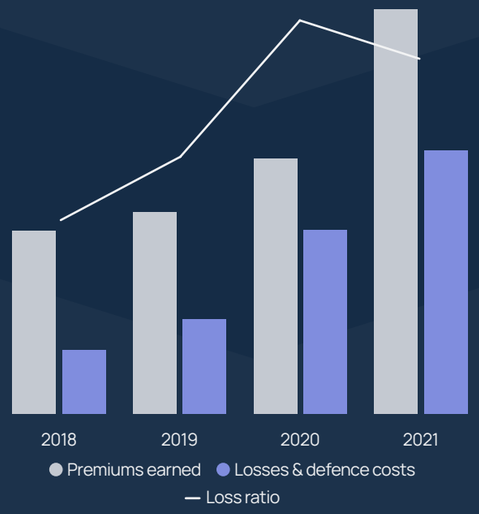
Source: NOVA, S&P

Gross written premium projections



Source: Howden, Munich Re, EIOPA

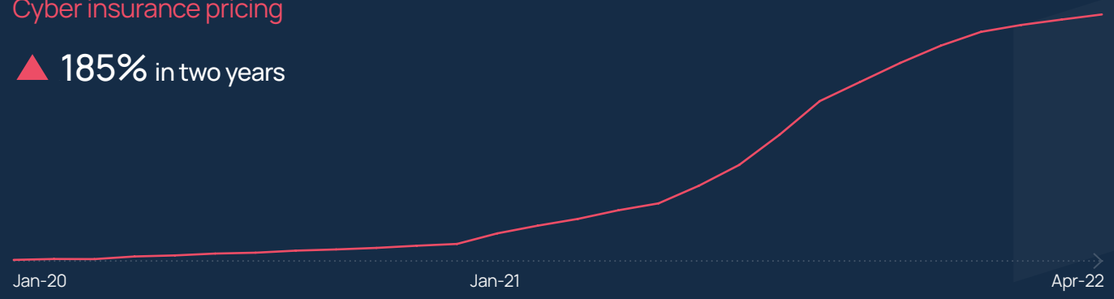
U.S. cyber market



Source: NOVA, S&P

Cyber insurance pricing

▲ 185% in two years



Source: NOVA

Insurers are only deploying capacity if they are satisfied by the strength of companies' cyber controls. Today's marketplace demands the very best of intermediary expertise to navigate a meticulous and prolonged placement process.

Executive summary

A year has passed since Howden released its last cyber report – *A Hard Reset (1.0)* – but twelve months is a long time in this market. Subsequent developments are testament to that, with ransomware, which has developed into a lucrative industry for cyber criminals, and the war in Ukraine demonstrating how different threat scenarios can transform the operating environment.

Ransomware incidents led to significantly higher loss frequency and severity in 2020/21. The accompanying retrenchment of insurance capacity, coupled with a wave of demand globally, has caused a supply and demand imbalance of such extremity that the average cost of cover today is more than double what it was last year. This has understandably caused consternation amongst buyers, who, despite paying these considerable rate hikes, are often left with less cyber protection post-renewal.

THE FOCUS ON RISK MANAGEMENT APPEARS TO BE PAYING OFF.

Such structural shifts to loss trends cannot be addressed by underwriting actions alone. They require fundamental changes to risk management frameworks, which is something the insurance market has accelerated significantly by requiring companies to have basic standards of cyber security in place in order to access capacity. Carriers' risk appetite is now correlated directly to the sophistication of businesses' risk controls, which is in effect incentivising better cyber resilience.

This focus on risk management appears to be paying off. Trends so far this year point to reduced ransomware frequency, although this should be caveated by pointing out that activity is coming off an extremely high base and the fallout from the war in Ukraine remains highly uncertain. Whilst the conflict appears to have reduced cyber frequency in the near-term as both warring sides (which host some of the worst offending ransomware gangs) focus their efforts on conventional warfare, the situation remains highly volatile and a lot can still change. The scope of cyber coverage and war exclusions have inevitably come under close scrutiny since the start of the conflict.

All of which reinforces the need for companies to have access to differentiated insights and advice. The pages ahead analyse the major cyber developments of the last 12 months – rampant (but potentially relenting) ransomware trends, risk aggregation, the Ukraine war, economic sanctions and the spectre of cyber warfare – and assess how the insurance market has performed through this period of flux. We have also invited some of our strategic partners – CrowdStrike, Guidewire, KYND and XCyber – to offer their expertise on matters such as risk management and cyber security during conventional warfare to help clients unpick the deep complexities that exist in what remains a highly unpredictable environment.

The uncertainty notwithstanding, there are signs that conditions in the cyber insurance market could start to moderate or even stabilise from here. The ingredients for a more mature marketplace are now in place: hardened cyber defences have left companies less vulnerable to prolonged disruption in the event of an attack or breach, and the cost of cover is now more commensurate with loss costs. Should trends around reduced cyber frequency post-Ukraine invasion persist, buyers can expect a more rational cyber market to emerge later this year, with better risk profiles improving underwriting performance and attracting much needed new capacity into the market.

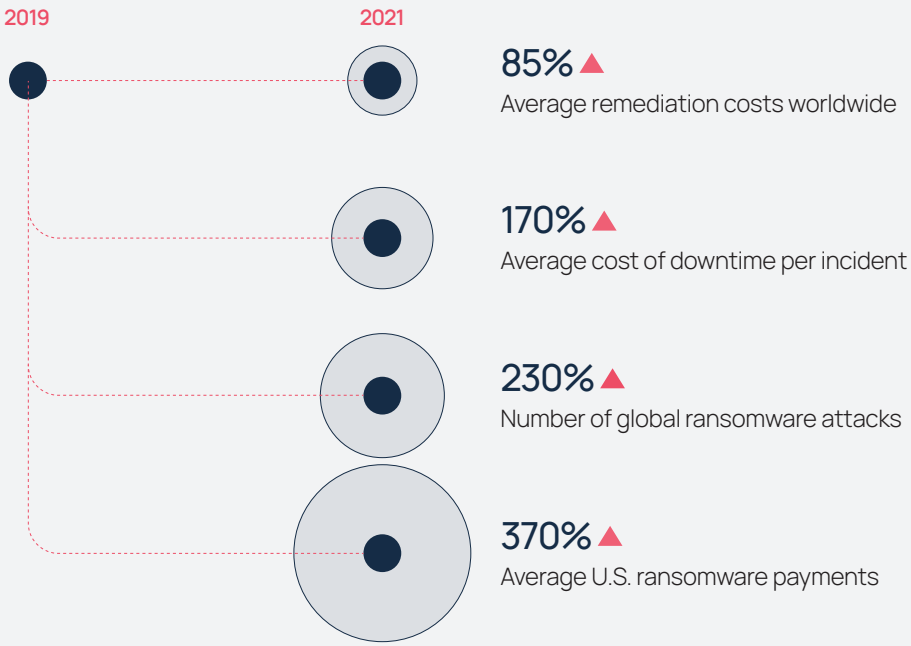
Now more than ever, risk management and risk transfer advice can make a crucial difference to renewal outcomes. With little prospect of a let up in the demands insurers are making around cyber security, market expertise and leadership are needed to help businesses secure cyber protection at the best terms possible. Howden exists to provide just that. We look forward to supporting clients through this period of transition and working on their behalf to forge a path towards a more sustainable market designed to navigate today's fast-moving threat environment.

01

Rampant (but relenting) ransomware

Cyber risk has undergone several episodes of change in its relatively short history, reflecting its highly fluid disposition. Escalating frequency and severity in 2020 and 2021 was nevertheless unlike anything experienced previously, with the proliferation of ransomware, in addition to a series of large-scale, single point of failure attacks, resetting the risk landscape.

Figure 1: Increased frequency and severity of ransomware incidents – 2019 vs 2021
(Source Howden, Coveware, Safety Detectives, SonicWall, Sophos)



BUSINESSES AND (RE)INSURERS ARE ADAPTING IN THE FACE OF ADVERSITY.

The first few months of 2022 have brought more change. Just as companies and (re)insurers have been adjusting to this new ransomware reality, Russia's invasion of Ukraine has added a big dose of complexity into an already complicated operating environment.

The situation in Ukraine remains highly volatile – cyber security implications are linked closely to the war's nature, reach and duration – and the spectre of war-related cyber activity has lead Western intelligence agencies to urge commercial organisations and state entities to prepare for and mitigate against cyber incidents, both within and beyond the conflict region. The immediate effect of the conflict, however, appears to be a dampening ransomware frequency, as both warring sides refocus their efforts and resources.

The spillover potential from the crisis is nevertheless real, as demonstrated by NotPetya in 2017, in which an alleged Russian attack infected software used widely by Ukrainian organisations and spread to tens of thousands of companies worldwide. More recent attacks on system providers and critical infrastructure – including the SolarWinds software breach in 2020 and last year's ransomware incidents targeting Colonial Pipeline and Kaseya, each of which have been attributed to Russian-affiliated groups – are additional reminders, if any were needed, of the threat posed by potential systemic events.

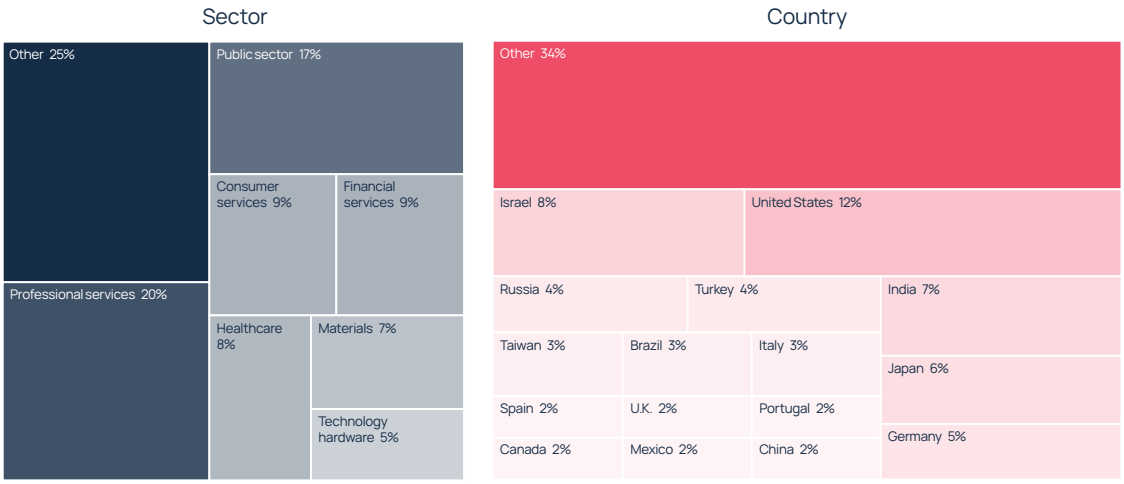
All this, along with COVID-19's ongoing effects on working practices, technology adoption and cyber security, encapsulates a period of colossal change. But even as cyber lives up to its dynamic reputation, businesses and (re)insurers are adapting in the face of adversity and are now better prepared to deal with the fallout. Insurance has proved to be critical to this fightback by indemnifying losses, incentivising better cyber hygiene and strengthening resilience.

> INSURANCE IS NOT ONLY INDEMNIFYING LOSSES BUT ALSO INCENTIVISING BETTER CYBER HYGIENE AND STRENGTHENING RESILIENCE.

A pervasive risk

The rise of ransomware has been the most important cyber development of the last two years, bringing about a sea change to the frequency and severity of attacks, and the threat landscape more generally. Virtually every business is now at risk, irrespective of size, sector or geography. Only two types of companies exist: those that have been targeted and those that will be.

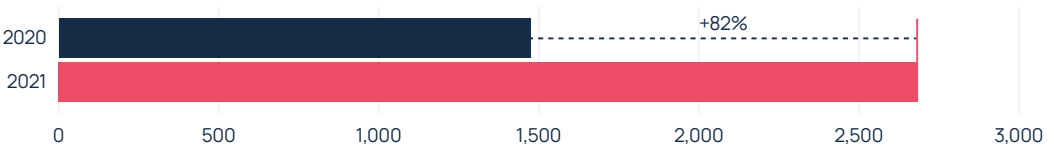
Figure 2: Ransomware attacks by sector and country
(Source: Coveware, Check Point Research)



This escalation is attributable primarily to cyber criminals deploying new tactics to exploit weaknesses and achieve one simple goal: maximise financial gain. Ransomware has developed into a lucrative industry in its own right. The availability of turnkey (and low cost) ransomware kits – otherwise known as ransomware-as-a-service (RaaS) – on the dark web has fuelled the proliferation of incidents. Lower barriers to entry typically bring a flood of new market entrants, and ransomware has been no exception. The number of attacked companies has spiked, as a result.

Severity, meanwhile, has been fuelled by double or triple extortion, which not only involves data exfiltration but is also accompanied by additional threats or actions that can include publishing stolen data or even launching distributed denial-of-service (DDoS) attacks in the event of no negotiation or no payment. Figure 3 shows that CrowdStrike recorded an 82% increase in ransomware-related data leaks in 2021 compared to 2020.

Figure 3: Increase in ransomware-related data leaks – 2021 vs 2020
(Source: CrowdStrike)



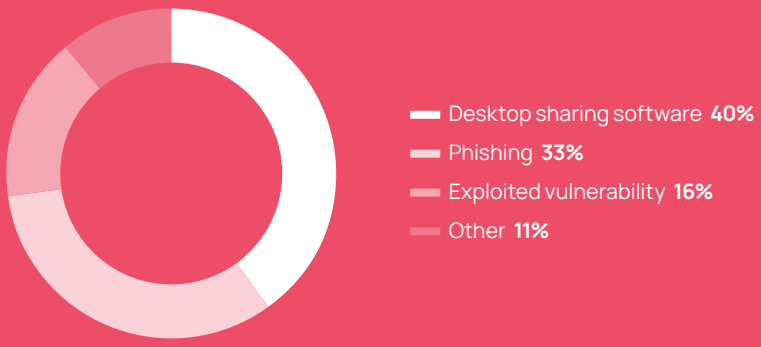
Basic mitigation actions (e.g. data backups alone) are no longer a sufficient defence against threat actors intent on stealing sensitive data or initiating separate attacks. Not only does this give attackers additional leverage in demanding ransom payments, but it also provides breached companies extra incentive to pay the ransom. This has led to more incidents, longer downtimes and higher losses.

Ransomware vulnerabilities

Guidewire provides the following insights using a combination of event level ransomware incident data from Coveware (which is representative of mid-cap businesses) and their own proprietary scanning infrastructure.

Understanding how ransomware gangs gain access to networks is key to reducing the risk of a successful breach. There are a number of vectors that threat actors can exploit to achieve this. Figure 4 shows that nearly nine out of ten successful attacks occur via three vectors: desktop sharing software, phishing and exploited vulnerability.

Figure 4: The way in – ransomware attack vectors (Source: Guidewire)



Desktop sharing software is still the most common attack vector, accounting for 40% of all successful ransomware breaches. It has nevertheless fallen from a previous high in 2020, as companies have reduced the number of internet-accessible instances.

Phishing – essentially tricking victims to open attachments or links that contain malicious files – is a more successful tactic when targeting larger companies. Whilst this may seem surprising on the surface – larger companies are after all supposed to have dedicated security personnel and programmes – the risk of a successful breach rises with the number of employees. Thousands of employees means more potential targets, and attackers require just one success. Phishing therefore continues to be an effective initial-entry attack vector for companies of a certain size. There are nevertheless signs of progress: successful phishing campaigns now show a downward trend when the largest of corporations are targeted, likely due to the increased effectiveness of security awareness and user education programmes.

There are important lessons for companies in these trends and data. For all the warnings and concern over the increased use of zero-day attacks – and there was a significant uptick in 2021 – 'mistakes' are still the preferred initial-entry access point for ransomware. Whilst mistakes may not be deliberate – e.g. users trusting a malicious email – or conform to best practice – e.g. exposing remote desktop ports directly to the internet – they are the most readily addressed.

These are the areas where companies should focus their attention. It is important to remember that the vast majority of successful attacks occur in systems where patches have not yet been applied whereas no patches exist for zero-day attacks, even if the window of opportunity (i.e. the time between the discovery of a vulnerability and attacker exploitation) continues to decrease.

Frequency and severity

Frequency and severity trends are shown in Figures 5 and 6. Figure 5 charts the number of global ransomware incidents by quarter since 2019, and for context, how they compare to data breach incidents. The surge in ransomware attacks in 2020 and the first half of 2021 particularly was striking, as incidents accelerated at an unprecedented rate whereas the number of data breaches remained largely stable. The latter part of 2021 nevertheless brought early signs of moderation for ransomware incidents (due in part to more stringent law enforcement globally and stronger risk controls locally), and the market will be watching closely to see if this trajectory is sustained in 2022. Early signs on this front are positive, even as the Ukraine conflict continues (more on this later).

Figure 5: Frequency index for ransomware vs data breach incidents – 1Q19 to 4Q21
(Source: Howden analysis based on data from SonicWall and Risk Based Security)

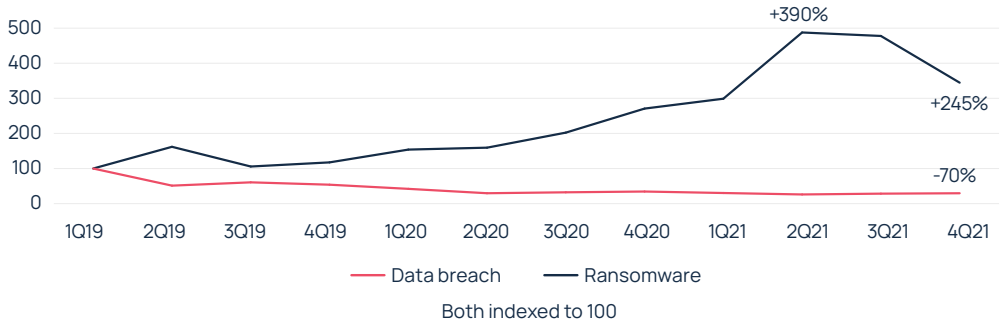
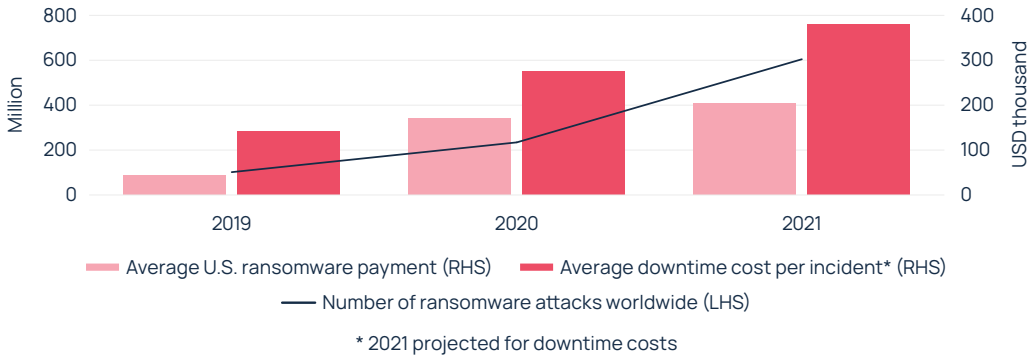


Figure 6 incorporates some financial metrics to show how increased ransomware frequency has been accompanied by rising losses. The monetary impact is equally stark, with average ransomware payments currently unrecognisable to those recorded only three years ago. The bulk of this spike occurred in 2020: for U.S. companies that opted to pay a ransom that year, the average payment increased by nearly 300% compared to 2019. Average payments continued to rise significantly in 2021, albeit at a more moderate pace in the mid-cap space specifically, and early indications are that payment costs stabilised in 1Q22.

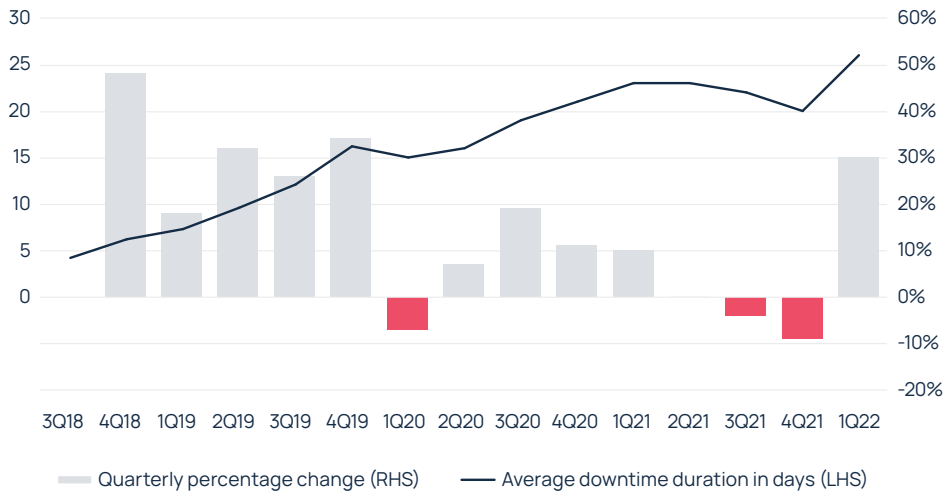
Ransomware-induced downtime costs have also jumped since 2019, with 2021 levels estimated to be 170% higher than those recorded two years prior and 40% up on 2020. And these figures exclude some of the (adverse) intangible impacts on items such as client relationships, brand and reputation that can follow periods of downtime and hurt long-term performance.

Figure 6: Global ransomware incidents vs U.S. ransom payments and downtime – 2019 to 2021
(Source: Howden analysis based on data from SonicWall, Coveware and Safety Detectives)



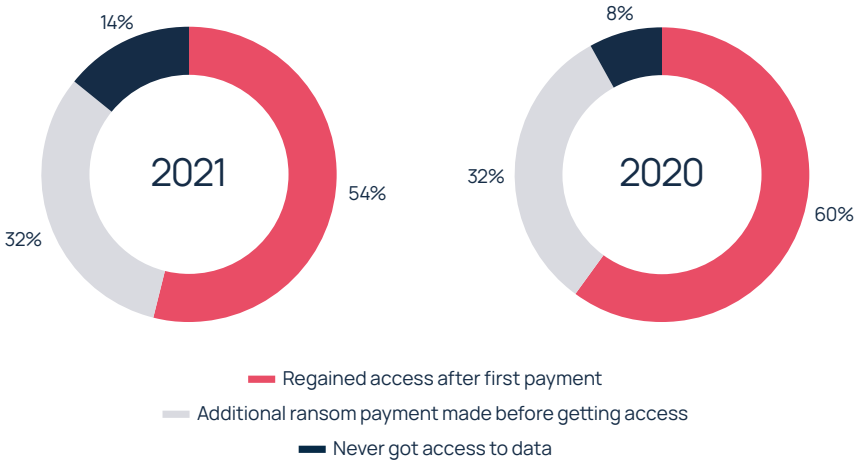
Rising lost production costs are in line with data in Figure 7, which shows that the average (annualised) downtime duration in 2021 was 22 days, compared to 18 days in 2020. Analysis of the most recent, quarterly data available paints a mixed picture, with the number of downtime days showing a gradual decline in the second half of 2021 before hitting a new high of 26 days in 1Q22.

Figure 7: Average ransomware-induced downtime duration in United States – 3Q18 to 1Q22 (Source: Howden analysis based on data from Coveware)



This is important, as business interruption is one of the most serious ransomware-related costs to organisations, even when accounting for additional payments or problems restoring access to data that a significant number of companies encounter after pursuing the ransom payment route. The proportion of companies that failed to achieve data restoration despite meeting the initial ransom demand increased to 46% in 2021 from 40% in 2020 (see Figure 8).

Figure 8: Outcomes following ransom payments – 2021 vs 2020 (Source: Howden analysis based on data from Proofpoint)



Remediating ransomware

As long as ransomware remains a viable option for financially-motivated threat actors, vulnerable businesses are at risk of potentially existential losses. Whilst it is impossible to eradicate the threat entirely, an overarching cyber risk management strategy is critical to risk mitigation.

Not only does this mean practicing good IT hygiene, it also requires training and educating employees, engaging with third parties, conducting table top (or war gaming) exercises, creating (and testing) business continuity and disaster recovery plans, having experts at the ready and knowing who to call should the worst happen. Put simply, companies must be prepared for ransomware and other destructive attacks if they are to avoid debilitating losses.

Insurance has been an important enabler in this regard by requiring companies to adopt a better risk posture in order to access capacity. At a minimum, this involves endpoint detection and response (EDR), next generation anti-virus deployment, multifactor authentication (MFA) for remote network access, data encryption and protection, regular backups, patching of critical systems / software and internal cyber awareness training. Risk transfer offers more than just indemnification and is in effect incentivising better cyber resilience, a positive (and much needed) development given the current environment.

COMPANIES MUST BE PREPARED FOR RANSOMWARE AND OTHER DESTRUCTIVE ATTACKS IF THEY ARE TO AVOID DEBILITATING LOSSES.

Q&A with CrowdStrike

Marko Polunic, EMEA Director of Business Development - Insurance & Legal Services, CrowdStrike

Q. What can companies do to prevent a ransomware attack?

A. A significant number of today's ransomware attacks begin with the misuse of valid user credentials, often obtained through a phishing attack or purchased on the dark web. The most effective way to prevent a breach is through the early detection of behaviours or tactics used by threat actors on companies' end user login credentials and endpoint systems. Solutions such as EDR and identity protection can help detect malicious actions (which typically include suspicious logins, privilege escalation, lateral movement, data exfiltration, malicious process execution and infected files) and enable early intervention to stop the breach before threat actors have the opportunity to execute their payload and encrypt systems.

Q. What happens in the event of a successful breach?

A. Once threat actors have obtained valid credentials and gained access to networks, they typically escalate their privileges so they can begin to move laterally across systems, looking for valuable data to either exfiltrate and / or encrypt in order to hold that data to ransom. Recovery at this point becomes extremely difficult and time consuming, especially in a widespread attack across a highly distributed environment. In this case, recovery time can take weeks, causing significant business disruption and downtime costs.

Q. How can companies minimise the fallout?

A. Time is of the essence. The traditional approach to recovery – reimaging systems from backup and rebuilding servers – is time consuming and disruptive. A more rapid (and effective) response can be achieved by engaging with specialist cyber incident response firms able to deploy technology that delivers immediate threat visibility, active threat containment, accelerated forensic investigation and a real time response. Such an intelligence-led approach can surgically undo malicious actions and restore systems remotely within 48 to 72 hours, with minimal disruption to end users. This is crucial to minimising any business disruption costs. In more severe cases where threat actors succeed in exfiltrating data and encrypting systems, full enterprise remediation will be required to restore and rebuild systems.

02

Systemic risks

Companies that have strong cyber hygiene are not only reducing the risk of being targeted by cyber criminals, they are also getting prioritised access to insurance capacity at a time of serious supply constraints. This makes them more resilient to conventional, financially motivated cyber attacks, but it also means that they are better prepared to navigate a highly volatile geopolitical climate that brings considerable cyber risks and the potential for large-scale events.

SYSTEMIC CYBER EXPOSURES PRESENT CHALLENGES FOR AN INSURANCE INDUSTRY BUILT ON **UNDERWRITING MOSTLY GEOGRAPHICALLY CONTAINED AND UNCORRELATED (PHYSICAL) RISKS.**

SENSITIVITY TOWARDS RISK ACCUMULATION HAS RISEN SINCE THE UKRAINE CONFLICT STARTED.

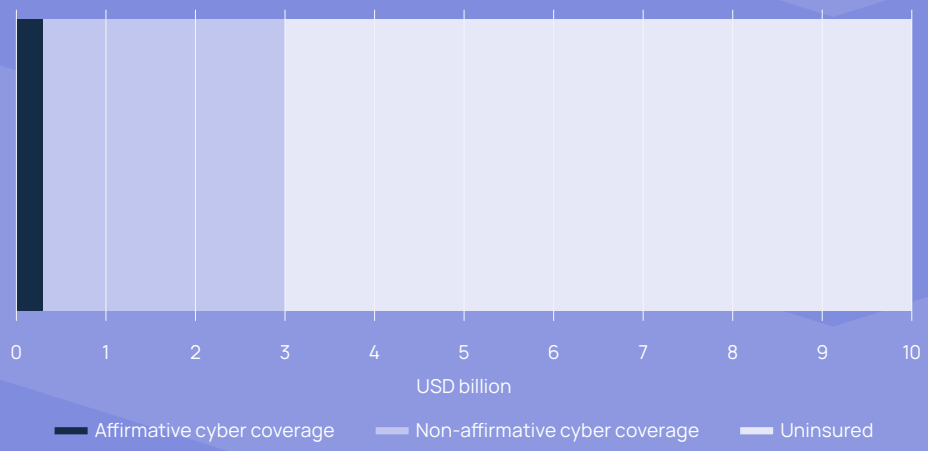
Aggregated warning shots

Even before the outbreak of war in Ukraine, insurers' cyber risk appetite was being held back by concerns around systemic losses. Sensitivity towards risk accumulation has inevitably risen since the conflict started, as carriers adjust to the situation and consider the tail potential of the crisis.

Systemic cyber exposures present challenges for an insurance industry 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 provided a painful illustration of how borderless and non-physical threats have the potential to see losses spiral quickly.

This threat is not new to the cyber market. The WannaCry and NotPetya attacks in 2017 highlighted the potential for claims to be brought simultaneously, as thousands of companies across geographies and sectors sustained damages from the same incident. NotPetya also revealed non-affirmative (or silent) cyber exposures (see Figure 9 for the breakdown of losses), a threat that has reduced in recent years but is still thought to be prevalent.

Figure 9: Breakdown of economic and insured losses for NotPetya
(Source: Howden, PCS)



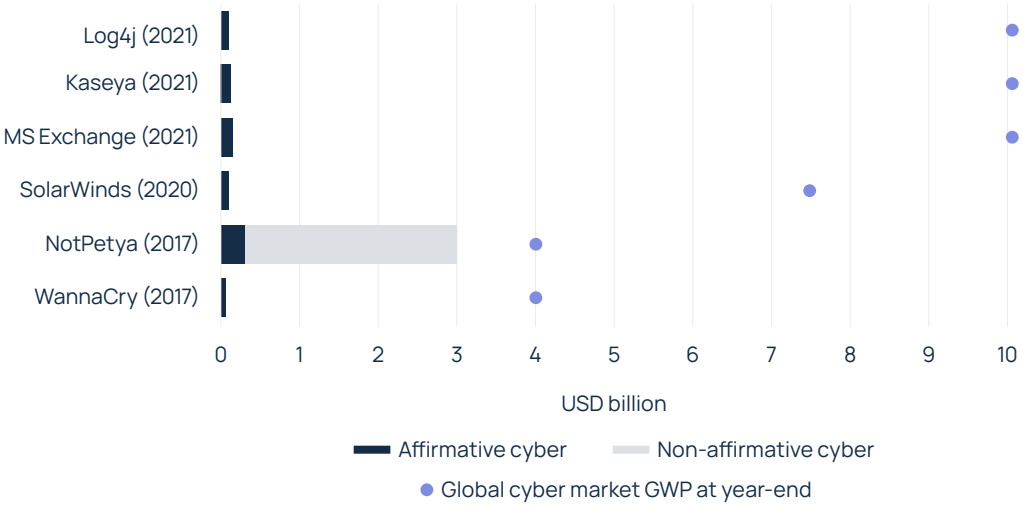
Perception vs reality

A series of more recent attacks on system providers and critical infrastructure – including SolarWinds, Microsoft Exchange, Colonial Pipeline, Kaseya and Log4j – were additional reminders of the ongoing risk. Speculation about the potential for wide-scale losses followed each of these incidents, with some commentators questioning the insurability of events that target service providers or single point of failure technologies. A few, isolated carriers have even looked to add exclusionary language around 'systemic risks' in policies.

And yet, market losses from these specific attacks have been limited. Figure 10 shows that NotPetya remains the biggest individual cyber loss so far – only 10% of which was absorbed by dedicated cyber policies – with all subsequent major events causing manageable (or even negligible) losses.

Improved cyber security is likely to have played an important part in mitigating the financial impact of recent attacks. Additionally, the ability of the cyber market to absorb economic losses of the quantum often associated with systemic events will grow over time as it approaches the scale of other major P&C lines of business, and pricing reaches levels commensurate with risks. Gross written premium (GWP) has more than doubled in the five years since NotPetya and is expected to exceed USD 25 billion by the end of 2026.

Figure 10: Insured loss estimates for high profile 'systemic' cyber events vs GWP for global cyber market (Source: Howden, PCS)

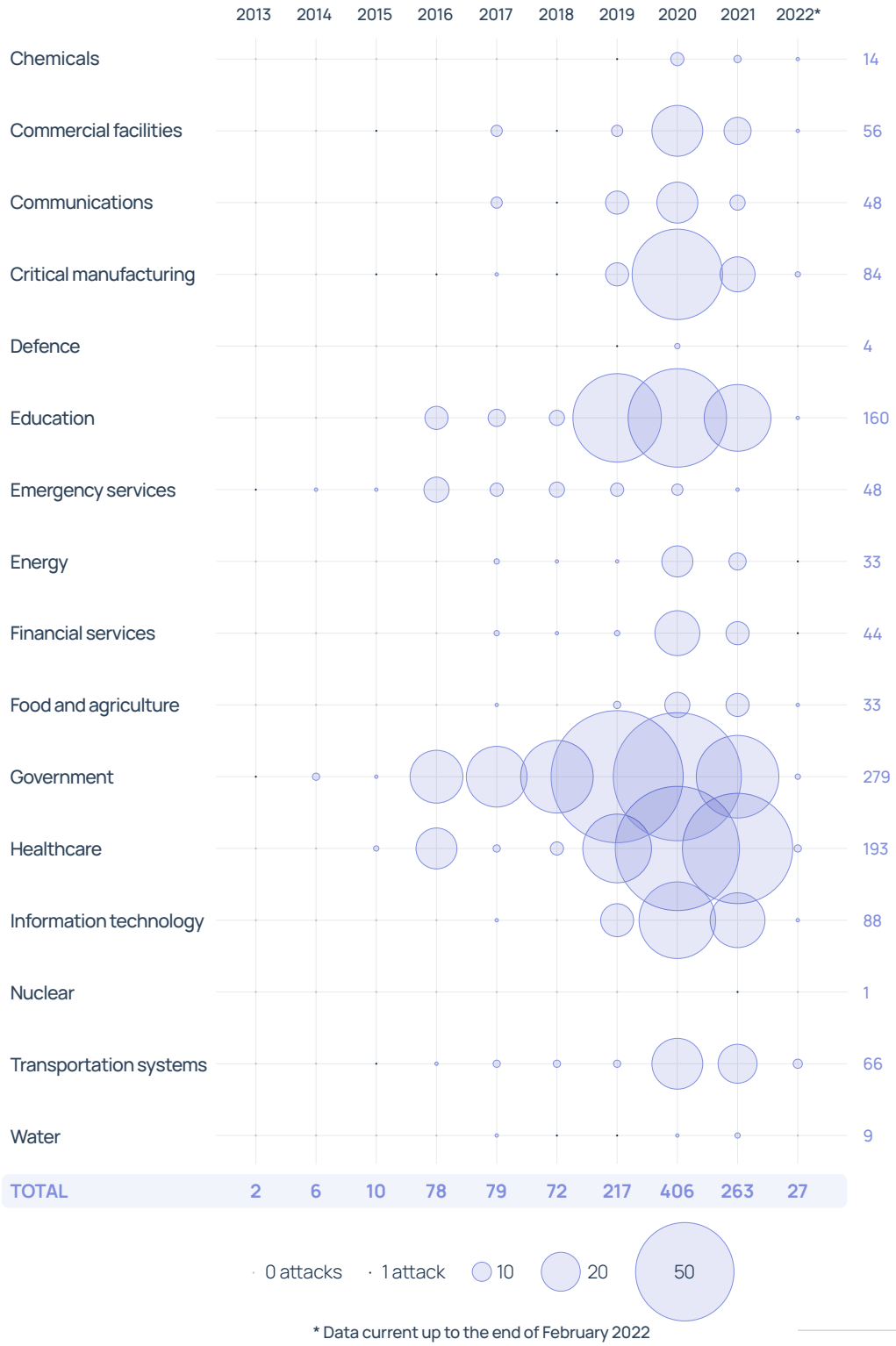


This is of course not to say that the threat of systemic losses is exaggerated, nor that the situation will not escalate from here. A large-scale event that resulted in a widespread cloud outage, for example, would clearly stress the market, although this is true of any tail event in other lines of business.

And hopes that (Russian) state-affiliated groups may have overreached even their hosts' tolerances last year after stirring a strong U.S. response to the Colonial Pipeline attack[1] have now all but evaporated with the outbreak of war in Ukraine. The recent reappearance of the 'DarkSide' ransomware gang (suspected of launching the Colonial Pipeline attack) is symptomatic of this.

More rigorous law enforcement is likely to have contributed to a marked fall in the number of ransomware attacks that targeted critical infrastructure last year, even if levels remained comparatively high (see Figure 11). Escalating tensions around the war in Ukraine have prompted warnings from governments that providers of critical infrastructure are likely to be targeted by state-affiliated threat actors who have already shown the intent and capacity to launch attacks in more tranquil geopolitical times.

Figure 11: Number of ransomware attacks on critical infrastructure worldwide – 2013 to 2022 YTD (Source: Howden analysis based on data from Temple University)[2]



* Data current up to the end of February 2022

[1] Government action in the U.S. and internationally followed the Colonial Pipeline attack, bringing a more coordinated and systematic response to counter attacks. The FBI also helped recover over half of the cryptocurrency ransom paid by Colonial Pipeline.

[2] 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.

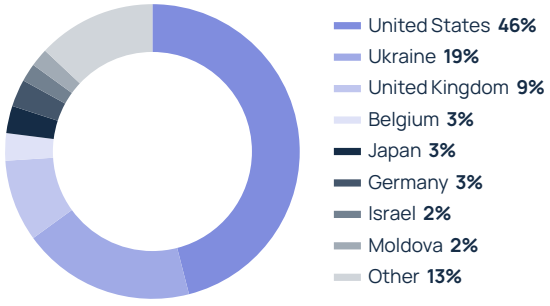
A new security landscape

The cyber risk landscape is shifting once again, with uncertain implications for cyber security, both within (and beyond) the Ukraine conflict zone. Insights provided by XCyber overleaf provide intelligence-led expertise into what can be expected in relation to the fallout from the war.

The array of groups operating in the cyber battlefield complicates distinctions between state-orchestrated attacks and those carried out by affiliate groups. Given the protagonists in this conflict, the prospect of cyber warfare and spillover to other states is real. Most cyber activity linked to the war so far has nevertheless been relatively low-level and the large-scale attacks widely predicted in the run up to invasion have not (yet) occurred.

The insurance market will be watching closely to assess whether this is a temporary lull or whether the priorities of conventional warfare reduce the focus on and efficacy of cyber operations. Whilst delineations between warfare and state affiliated activity can be made at this stage of the conflict, future developments may still test war exclusions.

Figure 12: Countries targeted by suspected state-sponsored attacks – July 2020 to June 2021 (Source: Microsoft)



THE EARLY EFFECT OF THE UKRAINE WAR APPEARS TO BE REDUCED CYBER FREQUENCY WORLDWIDE, **AS BOTH SIDES PRIORITISE CONVENTIONAL WARFARE.**

Cyber exclusions

Inconsistent terms and language across most 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 now taken on more weight post-crisis.

Figure 13: Summary of four London Market Association exclusions released in December 2021 (Source: Howden, LMA)

		Clause 1 (LMA 5564)	Clause 2 (LMA 5565)	Clause 3 (LMA 5566)	Clause 4 (LMA 5567)
1	Excludes any cyber operation (whether or not in the course of war?)	YES	NO	NO	NO
2	Excludes retaliatory cyber operations between specified states (China, France, Germany, Japan, Russia, U.K., U.S.)?	N/A	YES	YES	YES
3	Excludes cyber operations that have a major detrimental impact on functioning of a sovereign state?	N/A	YES	YES	YES
4	Provides full limit cover for cyber operations other than (2) and (3) above?	N/A	NO	YES	YES
5	Disapplies (3) above for direct or indirect effect on a bystanding cyber asset?	N/A	NO	NO	YES

* Note that green indicates that the particular clause takes the most policyholder-friendly option (between the four clauses) on a particular point, not that Howden approves of the clause on a self-standing basis.

Despite recent efforts by the insurance market to address these issues and make exclusions more watertight – for example, the Lloyd's Market Association (LMA) released four new exclusions late last year (see Figure 13) – consensus remains elusive. More work needs to be done in finding a balance between buyers' demands for coverage certainty on the one hand and assuaging (re)insurers' systemic concerns on the other.

Ensuring businesses achieve consistency and clarity of cover is just one area where differentiated intermediary expertise and advice can help businesses succeed in getting the level of protection they desire.

(Hybrid) war in Ukraine

Cyber analysis by Matthew Lane, CEO and co-founder of XCyber

The war in Ukraine is a highly complex situation that brings considerable implications to cyber security worldwide. For the purposes of this piece, we have broken down our analysis into three key sections: 1) activity in Russia and Ukraine, 2) developments beyond the conflict zone and 3) what we expect to happen over the medium-term.

1. Cyber activity in the conflict zone

Russia's military operations in Ukraine have been supported by a number of disruptive cyber attacks. Targets have included satellite communications and a variety of assets deemed important to Ukraine's military effort, with instances of wiper malware deployment. Other (softer) Russian cyber operations have included social media disinformation campaigns, although these have been relatively limited and often targeted at non-combat populations thought to be persuadable to Russia's intentions in the war.

Pro-Ukraine activity has largely emanated from state-backed hackers and various politically motivated groups such as Anonymous, which are likely to include individuals from NATO countries as members. Most of these attacks have been relatively low-level and focused on the release of confidential information and other sensitive material. The hacking of Russia-based ransomware gang 'Conti', and the leaking of its tools and tactics, also appears to have led to a small activity uptick from certain ransomware groups.

Overall, analysts have commented on the relatively low severity of attacks in the conflict region to date. General expectations pre-war were that a full invasion of Ukraine would be accompanied by extensive cyber operations. This has not happened for two key reasons. First, Ukraine has successfully built up its cyber defences in recent years after Russia had used it as a testing base for some of its more ambitious cyber attacks. (For example, Ukrainian authorities invested heavily in cyber security after Russian-linked hackers brought down parts of Kyiv's energy grid in 2015).

And second, cyber operations are less useful and effective during conventional warfare. Russia has often used cyber as a tool to sow confusion and allow itself a veneer of deniability, which is no longer necessary. Intelligence also suggests that Russia has been reluctant to target Ukrainian critical infrastructure, given the reliance of its troops on the internet and phone masts to communicate.

2. Cyber activity beyond the conflict zone

There is limited evidence to suggest that the war has led to a discernible change in the global cyber threat landscape. The bulk of activity associated with the war so far (in terms of attack frequency and most active groups) has occurred in Russia and Ukraine.

But this does not mean that attacks outside the conflict zone have not occurred or been attempted. Various entities in NATO countries – including those that run critical infrastructure – have reportedly been targeted but not breached. It is highly likely that any major attack launched since the start of the war was either kept secret or not reported.

Groups linked with all three of Russia's intelligence services – the FSB (Federal Security Service), SVR (Foreign Intelligence Service) and GRU (Military Intelligence) – have reportedly attempted attacks in recent months. One group with suspected links to the GRU (often known as 'Sandworm') is understood to be preparing to target critical infrastructure, although no attacks have been publicised yet.

The threat of more large-scale attacks has emerged elsewhere too. U.S. authorities recently discovered a highly sophisticated toolkit designed to hack into industrial control systems (ICS) and damage pieces of critical infrastructure. Malware designed specifically to target ICS is extremely rare, and its sophistication points to both the intent and capabilities of threat actors.

Although it was not assessed to have been used, the malware was aimed at targeting safety systems and appears to have been highly customisable, allowing attacks on a variety of targets. Due to the way parts of it were configured, there has been some speculation that the toolkit was designed to target liquid natural gas suppliers, which would align with Russian strategic goals around energy supply. Whilst the U.S. did not attribute the incident to Russia directly, it said the level of sophistication pointed to origination from a state-sponsored group. The deployment of such capabilities would of course need to be weighed against retaliatory responses.

These types of incidents are nevertheless relatively isolated currently, and there does not yet appear to be a significant escalation of attacks or dedicated campaigns outside of Russia or Ukraine.

3. Future expectations

Given the complexity and fluidity of the crisis, ascertaining the full picture of the threat landscape is extremely difficult. But three months into the conflict, intelligence-led analysis offers some insights into what we can expect in the near- to-medium-term.

A protracted conflict, along with tough economic sanctions, is expected to see Russia become increasingly isolated. This could result in increasingly hostile cyber activity from the country. As sanctions start to bite, Russian groups, which include some of the worst offending ransomware gangs in the world, may become increasingly brazen in their hacking attempts. It is also possible that the Russian government will look to monetise these (and other sympathetic) groups, further increasing their willingness to commit offensive cyber operations with impunity. This could lead to an increased volume of low-level, but disruptive, attacks across the world.

The targeting of critical infrastructure will also remain a threat. In April, the Five Eyes intelligence alliance warned that the Russian government is exploring options for potential cyber attacks against critical national infrastructure in the West.

Although it appears unlikely that a new type of cyber attack or threat will emerge in the near- to medium-term, and we are more likely to see increased volume of current attack tactics, Russia may look to become more organised in the cyber space. Whilst Russia has a reputation as being one of the most aggressive cyber actors in the world, some of its efforts are notably less formalised than in other hostile countries, including China and North Korea.

Should Russia look to emulate these better organised territories, and facilitate closer coordination with affiliates or even form alliances with them, it would ingrain further 'state-sponsored' criminal groups as 'instruments of the state', emboldening and supporting their activities beyond the current status quo of passive permissibility.

Companies need to do what is necessary to protect themselves in this highly uncertain environment: update software, secure and monitor technical infrastructure, provide end-user training and have well-rehearsed incident response plans in place.

03

In the line of fire

The spectre of warfare comes at a time of stress in the cyber insurance market. The last 24 months have been characterised by higher pricing, contracting capacity and restrictive terms, including reduced limits, higher retentions and coinsurance for ransomware.

Recognising the structural shift in loss trends, insurers have employed controls that mandate minimum hygiene levels for policyholders in order to access capacity. The (immediate) investment burden on companies notwithstanding, it has helped to instil much needed resilience to rapidly moving threats, including potential claims arising from the war in Ukraine.

> IMPROVED RISK CONTROLS HAVE HELPED INSTIL MUCH NEEDED RESILIENCE TO **RAPIDLY MOVING THREATS, INCLUDING RANSOMWARE AND THE WAR IN UKRAINE.**

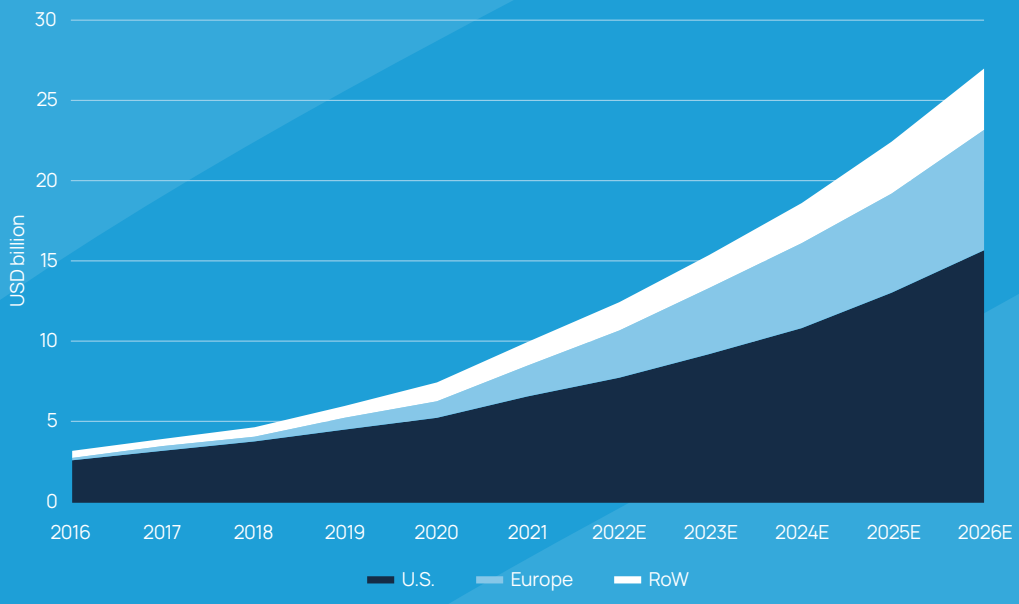
Fastest growing market

Capacity reductions have not held back market growth. In fact, the cyber market remains the fastest growing area of insurance by some distance: annualised growth of 20% plus in recent years compares to the low-to-mid single digit percentage range of the broader P&C commercial sector. No other line of business has such growth potential, on the one hand, but such a fluid risk landscape, on the other.

These conflicting dynamics continue to play out in the market. As cyber insurance has become a must-have for businesses, elevated claims have tempered insurers' underwriting appetites. Market growth is a product of exposures and pricing, and whilst both combined in unison to deliver strong growth through 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 14 shows that higher than expected rate changes last year propelled the size of the market at year-end 2021 to approximately USD 10 billion. This exceeded estimates made before the price spikes of 2021. Even higher rates of growth were only prevented by carriers abiding by pre-agreed premium budgets.

Figure 14: Gross written premium for global cyber insurance market – 2016 to 2026
(Source: Howden, Munich Re, EIOPA)



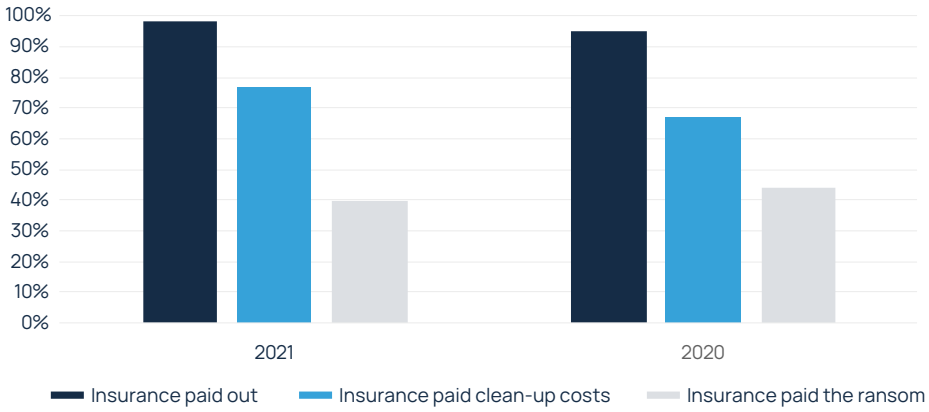
Given the pricing environment, rising demand and the prospect of more capacity post-remediation, a similar, but faster, rate of expansion is predicted for the global cyber market over the next few years (at a CAGR of 25%), which would see GWP exceed USD 25 billion by 2026. Whilst the U.S. will remain the biggest market by some distance, Europe, starting from a much lower base, is expected to close the gap somewhat and experience significant growth over the next few years.

Strong payout record

Rapid growth and the proliferation of ransomware notwithstanding, cyber insurance has continued to uphold its strong reputation for rapid claims payments.[3] Data collected by Sophos shows that cyber insurance paid out for 98% of companies hit by ransomware in 2021 (see Figure 15). 77% of respondents reported that clean-up costs were covered by insurance (up from 67% in 2020). There was nevertheless a slight decline in insurance payouts for ransom payments, likely reflecting decisions by a small number of insurers to stop reimbursing payments.

This downward trend for ransom payments is likely to be sustained this year, given the imposition of sanctions on Russia following its invasion of Ukraine.

Figure 15: Cyber insurance claims payment record for ransomware incidents – 2021 vs 2020 (Source: Sophos)



Sanctioning ransom payments

The ability of companies to pay ransoms and receive insurance recoveries has been an area of considerable scrutiny over the last 18 months. Even in calmer geopolitical times, the U.S. Treasury's Office of Foreign Assets Control (OFAC) was examining sanctions risks associated with ransomware payments. An advisory circulated in October 2020 reminded victims that making or facilitating such payments could violate OFAC regulations, and that they should involve the FBI and OFAC in the event of an attack. It highlighted specifically that OFAC would consider the timeliness of reporting and cooperation in the event of sanctions-related enforcement action.

Whilst the advisory did not change the U.S. government's pre-existing position, its issuance and focus reinforced the importance of businesses using reputable intermediaries and authorised third party payment mechanisms to arrange and make payments. This applies equally to businesses that proceed independently of insurance (e.g. companies with large retentions).

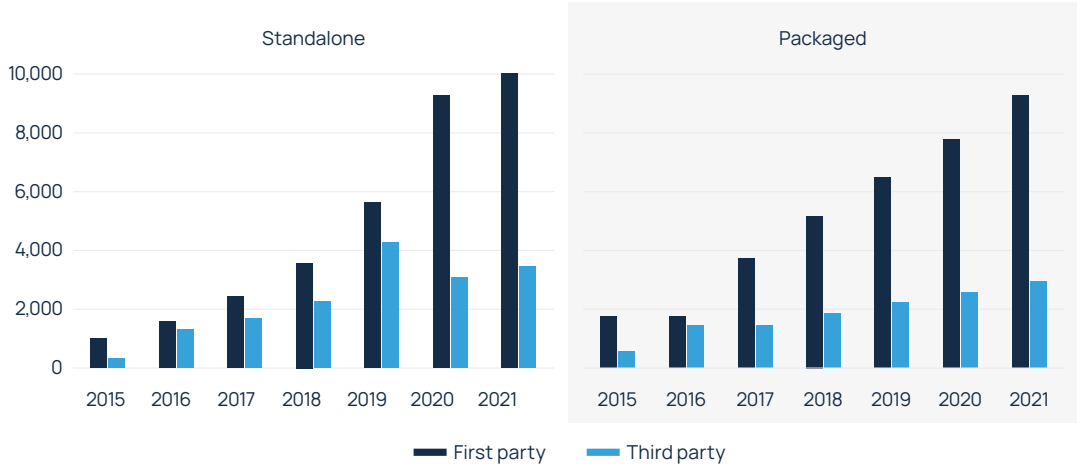
The war in Ukraine raises the stakes from an insurance perspective. Most cyber policies include clauses that disavow liability for any payment that places them in breach of U.S., U.K. or European sanctions. Whilst specific ransomware gangs have been subject to sanctions for some time, the highly fluid landscape since Russia's invasion has complicated the position further. Given the sensitivity of the situation, insurers will need to be made comfortable that indemnification will not benefit a sanctioned entity or individual. Whilst this due diligence is now a prerequisite to making all ransom payments, it is not acting as a barrier to payment and resolution in most cases.

Growing pains

Market conditions remain challenging for buyers. Whilst acknowledging some limitations to the supplemental filings data provided in Figures 16, 17 and 18 in depicting the full performance of the U.S. market[4], they do paint a picture of deterioration overall, albeit with some signs of improvement in 2021.

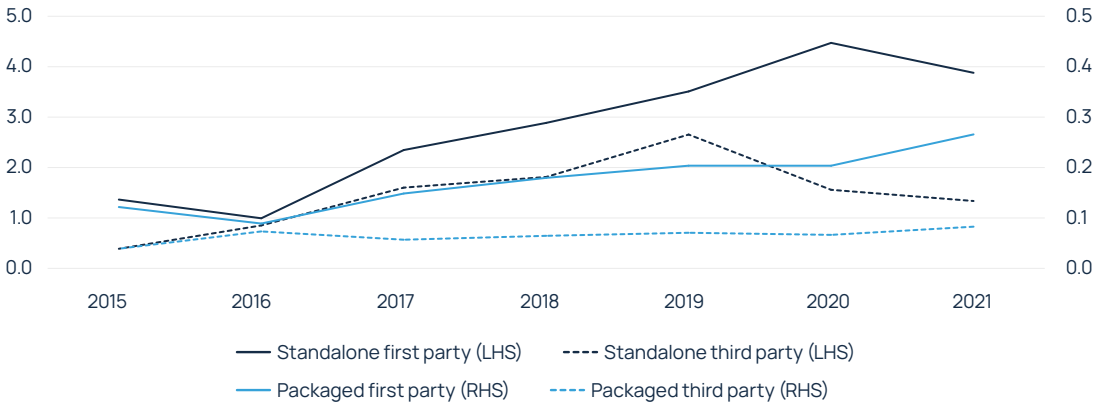
Figure 16 shows how the loss environment has trended since 2015, with both standalone and packaged policies in the United States recording a surge in the number of claims. After a notable spike in first party standalone claims in 2020, due almost exclusively to escalating ransomware attacks, the rate of growth moderated last year.

Figure 16: Reported first party and third party cyber claims for U.S. standalone and packaged policies (Source: NOVA, S&P Global Market Intelligence)



This is supported by Figure 17, which breaks data down to the frequency of reported claims per 100 policies, and shows a moderating trend for first party claims in standalone policies, down to 3.9 from 4.5 per 100 policies. More favourable frequency was nevertheless offset in part by severity, as the overall average claim size increased to over USD 100,000 from USD 75,000 in 2020.

Figure 17: Reported first party and third party cyber claims per 100 policies in force for U.S. standalone and packaged policies (Source: NOVA , S&P Global Market Intelligence)

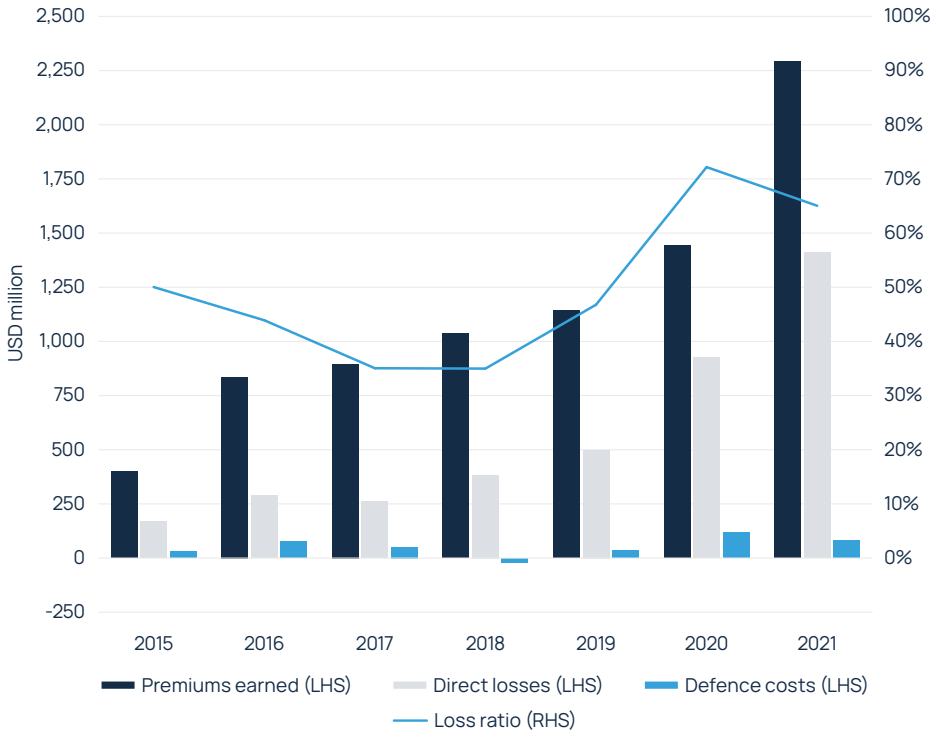


[3] Recent, high profile claims settlement litigation from the NotPetya attack was centred on all-risk property policies, and not standalone cyber.

[4] Cyber supplemental filings, for example, are often dated and may not include all claims costs or the effects of reinsurance on results.

Taking all this together, and bringing (higher) premiums into the equation, results were mixed for U.S. cyber carriers last year, with several still in loss making territory. But when looking at data in aggregate for standalone cyber policies specifically, the sector's performance improved in 2021, with the loss ratio falling to 65% from 72% in 2020 (see Figure 18). Increased premium flow into the U.S. market last year (up 60%) was sufficient to offset another big rise in incurred direct losses and defence costs, whose combined total increased nearly 45% over the course of the year.

Figure 18: Loss ratio for U.S. standalone cyber policies – 2015 to 2021 (Source: NOVA, S&P Global Market Intelligence)



Improved risk posture

These results suggest that actions taken by companies and (re)insurers, the focus on cyber hygiene in particular, are starting to pay dividends. With capacity deployment appetite now correlated directly to the sophistication of security controls, companies have invested heavily to improve their risk posture. Those unable or unwilling to make these changes have struggled to secure any coverage at all.

Carriers are still able to cherry pick clients at this stage of the market cycle: focusing on a smaller (lower risk) pool of clients to fill largely stagnant capacity targets aligns with current risk appetites. Some of the basic controls needed to 'qualify' for cyber insurance, which have come to be regarded as cyber equivalents to pre-emptive alarms and sprinkler installations, are highlighted opposite.

Basic risk controls mandated by insurers

- Good cyber and information security governance
- Comprehensive anti-virus & anti-malware software
- Email security (i.e. screening, filtering, quarantine services)
- Employee cyber awareness & phishing training
- MFA for all remote access to networks and critical applications
- Established backup procedures (ideally immutable backups)
- Privileged access management (PAM) tool(s)
- Endpoint detection and response (EDR) tools
- Robust patching policy
- Business continuity plans and disaster recovery plans
- Protection and encryption of sensitive data
- Ransomware preparedness, with a table top or playbook established
- Managing end-of-life applications
- Vulnerability scanning
- Utilisation of a 24/7/365 SOC and SIEM tools
- Network segmentation

Increased scrutiny around these controls – EDR, MFA and backups especially – are taking place alongside structural changes to programmes. Even companies able to demonstrate best practice in these areas have been hostage to market conditions, with many raising retentions and / or cutting limits due to the lack of capacity offered by the market. Tighter coverage terms, including sublimits, coinsurance for ransomware losses and exclusions, have also become more prevalent.

Companies therefore continue to face difficulties in finding the right cover at the right price. Frustration is now setting in for buyers often subjected to triple-digit price rises for less protection, especially those who have done everything asked of them from a risk posture perspective. Indeed, some businesses are now questioning whether they are best suited to managing risks internally and refocusing their spend on cyber security and tail risk mitigation.

The value of cyber insurance nevertheless continues to prevail for most. Buyers are looking to maintain existing levels of coverage overall, but this is inevitably causing strain in an environment of constrained capacity and rapid rate increases. Whilst this adjustment has been painful, the cost of cover is now more commensurate with attritional loss costs, and improved cyber hygiene means companies are less vulnerable to prolonged disruption and outsized losses.

These dynamics seemingly played out in 1Q22, with tangible signs of improved underwriting performance for certain carriers. This should encourage the market to loosen capacity restraints and look to attract much needed capital into the market.

A time for perspective

Clients with access to the best broking advice are using the placement process as an opportunity to reassess coverage prioritisation and explore whether any changes to terms can help unlock additional capacity.

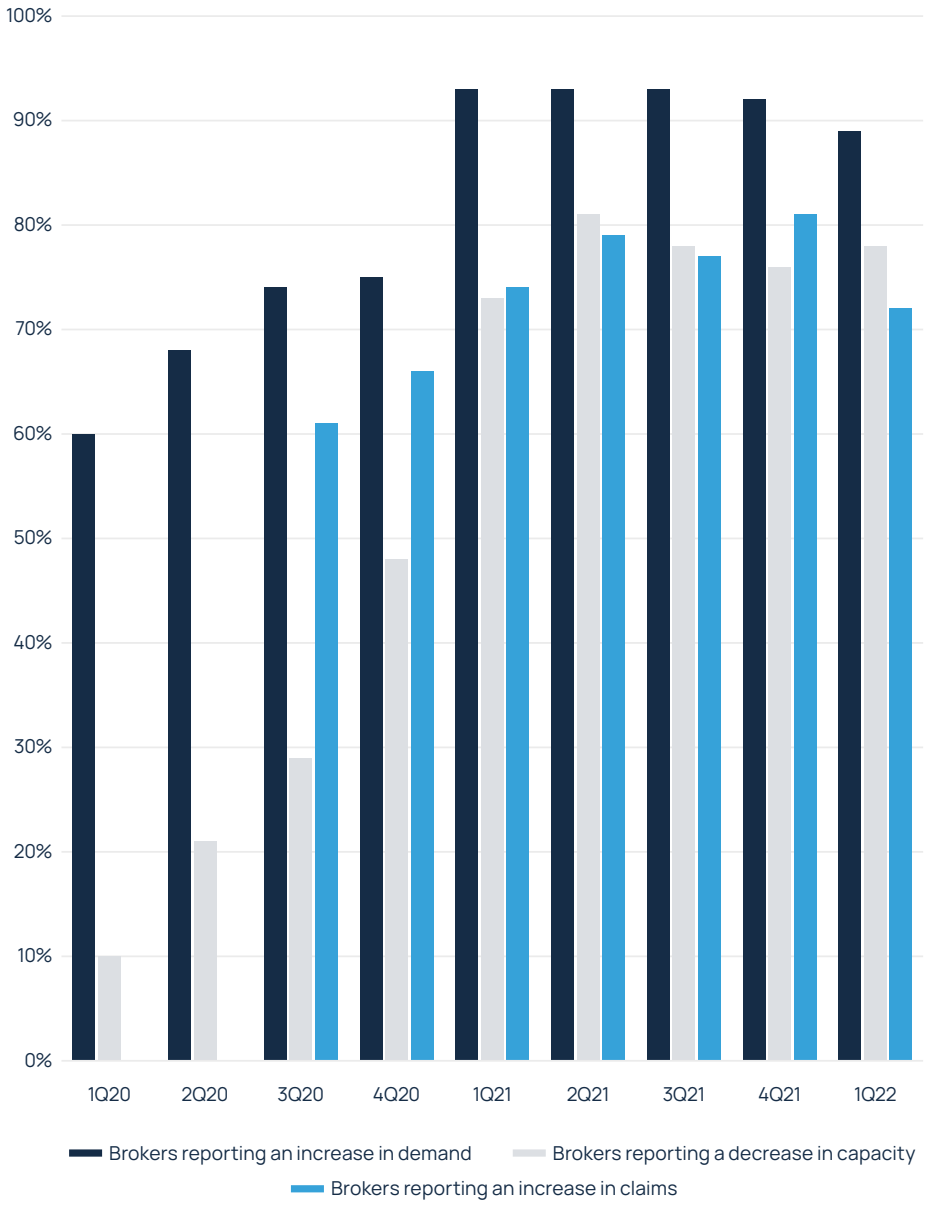
In partnership with third parties, brokers can arm clients with actionable insights around scenario-based modelling (across multiple return periods) and the losses expected to unfold under these scenarios to inform the viability of structural changes (e.g. limit / retention adjustments, sublimiting less pertinent coverage) without impairing the scope of coverage required.

This process ensures programmes are optimised fully to current market conditions, and eliminate redundancies and legacies from distant soft market dynamics.

A turning point?

Data published by the Council of Insurance Agents & Brokers (CIAB) underlines the task confronting the market in meeting surging demand. Figure 19 shows that the number of U.S. intermediaries reporting tightening cyber capacity was above 75% at 1Q22, a reduction from the high watermark of 81% in 2Q21 but still at an elevated level. And there is little sign of let up in demand: U.S. intermediaries reporting increased demand for cyber cover has hovered around 90% for five consecutive quarters now. Importantly, the number of respondents reporting rising claims fell to 72% in 1Q22 from a high of 81% the previous quarter.

Figure 19: Capacity, claims and demand trends in U.S. cyber market – 1Q20 to 1Q22
(Source: Howden analysis based on data from CIAB)



How these dynamics play out for the rest of the year will be instrumental in shaping the pricing environment. For the best part of a year, cyber has experienced the most extreme rate increases across the entire insurance market. The degree of repricing is visualised by Figure 20, which shows Howden's real-time, global cyber insurance pricing index, along with average year-on-year rate movements, dating back to 2014.

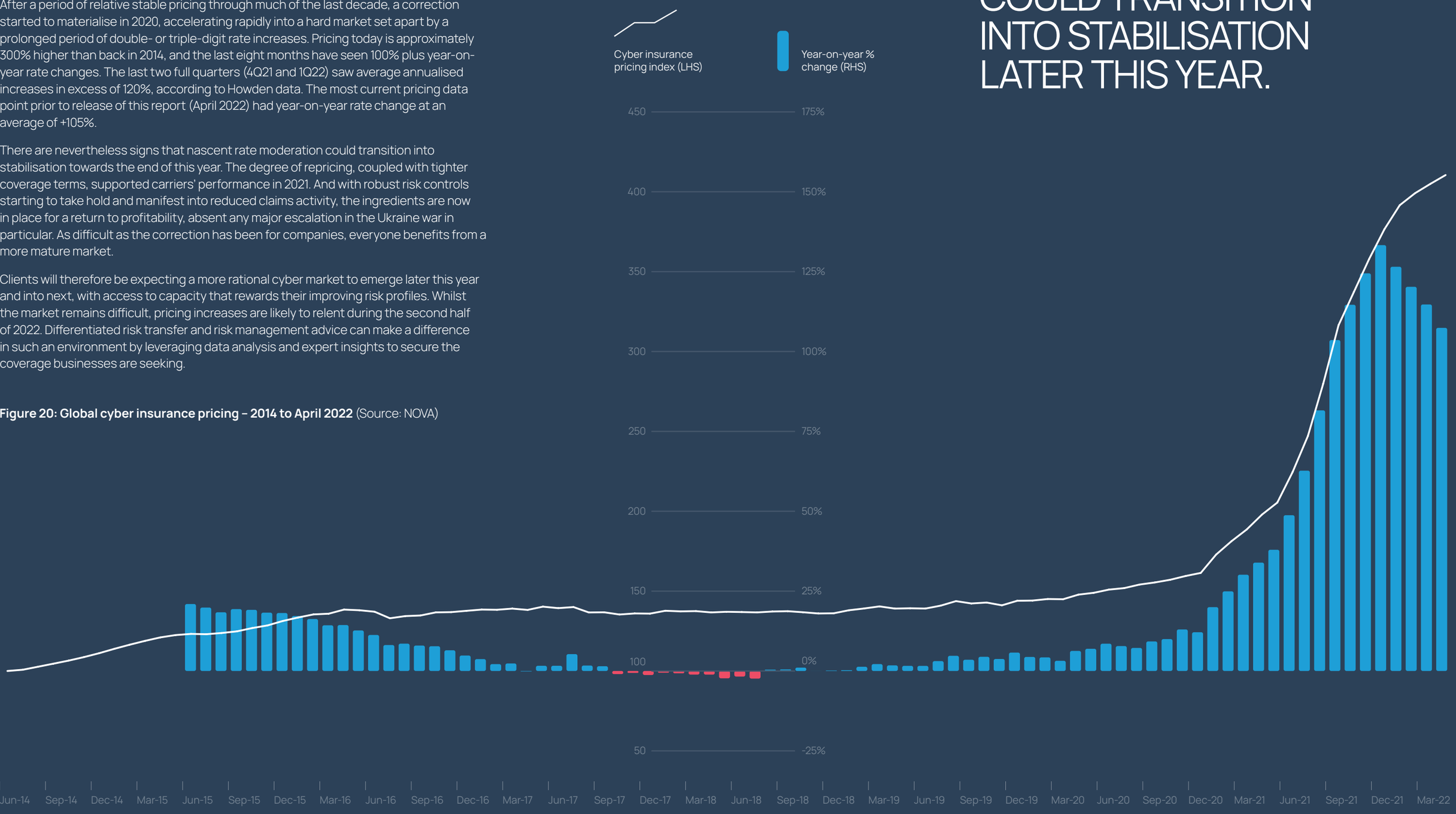
After a period of relative stable pricing through much of the last decade, a correction started to materialise in 2020, accelerating rapidly into a hard market set apart by a prolonged period of double- or triple-digit rate increases. Pricing today is approximately 300% higher than back in 2014, and the last eight months have seen 100% plus year-on-year rate changes. The last two full quarters (4Q21 and 1Q22) saw average annualised increases in excess of 120%, according to Howden data. The most current pricing data point prior to release of this report (April 2022) had year-on-year rate change at an average of +105%.

There are nevertheless signs that nascent rate moderation could transition into stabilisation towards the end of this year. The degree of repricing, coupled with tighter coverage terms, supported carriers' performance in 2021. And with robust risk controls starting to take hold and manifest into reduced claims activity, the ingredients are now in place for a return to profitability, absent any major escalation in the Ukraine war in particular. As difficult as the correction has been for companies, everyone benefits from a more mature market.

Clients will therefore be expecting a more rational cyber market to emerge later this year and into next, with access to capacity that rewards their improving risk profiles. Whilst the market remains difficult, pricing increases are likely to relent during the second half of 2022. Differentiated risk transfer and risk management advice can make a difference in such an environment by leveraging data analysis and expert insights to secure the coverage businesses are seeking.

Figure 20: Global cyber insurance pricing – 2014 to April 2022 (Source: NOVA)

NASCENT SIGNS OF RATE MODERATION COULD TRANSITION INTO STABILISATION LATER THIS YEAR.



04

Securing cyber

(Re)insurers are reacting to fast moving risk developments, which in turn is driving a rigorous insurance placement process characterised by more demanding cyber hygiene investigations. There is unlikely to be any let up in the scrutiny insurers are applying around cyber security, process improvements, data compliance and supply chains any time soon. Preparation and timing are paramount in this market, and companies need to anticipate a prolonged and meticulous placement process.

THERE IS UNLIKELY TO BE ANY LET UP IN **THE SCRUTINY INSURERS ARE APPLYING AROUND CYBER SECURITY.**

PREPARATION AND TIMING ARE **PARAMOUNT IN THIS MARKET.**

All of which elevates the importance of differentiated risk management and risk transfer advice. The following Q&A sections focus on these two specific areas and provide insights around what companies need to think about in terms of their risk posture and renewals strategy in order to achieve the best possible results.

Today's marketplace demands the very best intermediary expertise and leadership that goes beyond transactional services. It requires sector expertise, advice in building a better risk profile for submission, strong partnerships with third party experts and unrivalled relationships with insurers. Howden's cyber team provides all this and more. Come and talk to us.

Q&A: Cyber risk management

Melanie Hayes, Co-founder and CMO, KYND

In a constantly changing threat landscape, all constituents of the insurance value chain – businesses, brokers and underwriters – need to monitor cyber risks and exposures. Innovations in the risk management space have expedited and simplified this process and are helping companies build resilience by managing their exposures and facilitating risk transfer.

Q. What should companies do to build cyber resilience? Any advice in terms of where to focus spend?

A. Technology is the obvious answer, but companies need to take a more holistic approach to cyber hygiene that embraces process improvement too. Communication and training are crucial to creating what we call a 'human firewall' to prevent attacks. Employees need to know what to do if they suspect a breach and how to escalate suspicious activity. Ultimately, companies' best line of defence against any cyber threat is reducing the likelihood of human error and turning the workforce into a blockade against malicious activity.

For all the excellent cyber security software available on the technology side, we always recommend companies first consider the tools they already have at their disposal. The right solution can sometimes be found hidden inside existing software licences: throwing money at the problem does not always render the best results.

Q. How can companies best deploy technology to understand and manage their cyber exposures and stay one step ahead of attackers?

A. There is often a direct link between risk exposures and likelihood of attack, which places huge importance on exposure management. Whether this involves a one-off deployment or continual exposure management, we see value in both approaches.

Deploying a one-off risk exposure report is an excellent way to get a snapshot of any gaps or weaknesses in companies' systems and where points of exposure exist, which in turn offers a good starting point for risk management. The fast-moving nature of cyber risk is nevertheless increasingly demanding more continual risk management in order to detect new vulnerabilities and get advice on what needs to be done to mitigate threats.

Alongside these scans and reports, software can be used to test companies against threats such as phishing and email spoofing. Good cyber risk management technology – which, by the way, does not have to be overly complicated, expensive or intrusive – now makes it possible for companies to stay one step ahead attackers.

Q. How can companies ensure they get maximum 'bang for their buck' in their cyber security spend?

A. Understanding risk exposures is the crucial first step, as it allows companies to identify exactly where to direct their funding. From that point on, prioritisation is the most effective way to optimise cyber security investment. This means prioritising the most real and urgent risks – finding the difference between clear and present dangers versus theoretical dangers – and deploying resource and budget accordingly. Extra measures can also be built-in, such as enforcing MFAs and encrypting key areas.

Protecting areas that are deemed 'business-critical' is also important. This is no small task and will vary by firm and sector – for example, retailers and ecommerce organisations are likely to prioritise billing engines over their internal chat networks. Likewise with attack vectors: analysing the most vulnerable points (like customer profiles and Mobile POS for retail) should take priority over less accessible vectors. Once this exercise is complete, we recommend applying the advice I gave earlier – assess the tools at your disposal before committing to any further cyber security.

Finally, every business should have a continuity plan in place that covers everything from incident response to disaster recovery and backup restoration. This will provide a roadmap to a (more rapid) recovery in the event of a successful breach

Q. Does the current geopolitical environment require additional measures to pre-empt any potential state-sponsored attacks?

A. The war in Ukraine has certainly changed the security landscape, but state-sponsored attacks will ultimately follow similar patterns to more conventional incidents. State-backed ventures are of course going to be better resourced, and motivations could be focused on causing disruption rather just strictly financial, but our advice to companies remains the same: focus on cyber health and continue to keep employees educated about cyber risk in all its forms.

Q. What risk management advice do you have for companies looking to access insurance capacity for the first time?

A. Market conditions remain challenging, so any first-time buyer is going to have to provide evidence of good cyber hygiene alongside a strong internal security system – not just at submission and renewal but throughout the entire cycle. Exactly what this will look like will differ depending on each organisation's business and system design. At a minimum though, companies must be prepared for common threats that include ransomware, phishing and data breaches.

Building towards this goal will often require partnership with third parties. KYND's solutions allow for quick and easy cyber risk management, from reporting on and understanding a risk profile to keeping up to date with the latest threats. All of which have been designed to offer a clear route to market.

My final point about open communication is not necessarily in the purview of risk management but is so important. Companies need to be transparent and disclose upfront any potential issues with their brokers. Demonstrating the evolution of the risk management process is evidence of good cyber hygiene and removes the potential stigma associated with any previous breach.

THERE IS OFTEN A DIRECT LINK BETWEEN **EXPOSURES AND LIKELIHOOD OF ATTACK.**

Q&A: Insurance renewals

Shay Simkin, Global Head of Cyber, Howden

Preparedness is a crucial component of companies' cyber resilience. This is true from a risk management perspective but it applies equally to insurance renewals. Risk control demands from insurers can be challenging, and it is vital that companies work closely with their broking partners well in advance of renewal. Intermediary advice remains an important differentiator in today's marketplace.

Q. What should businesses expect in the lead up to their cyber insurance renewals?

A. Early engagement with their broker is a must. We are working with clients up to six months in advance of renewals to give them the time necessary to prepare for what is still an intensive process. Insurers are adapting their requirements as they learn from the last 18 months and probe deeper into clients' cyber controls. Not only are mandates around risk controls changing, but the degree and focus of investigations are often inconsistent across carriers, which is causing some consternation for buyers.

Questionnaires are more detailed and demanding – the scope is far more technical in nature than last year and new questions (around new vectors of attack, for example) are appearing on a regular basis. Some demands force clients to find additional budget for the solutions required, which has to be built into the timeline. The result is meaningful client engagements across multiple disciplines – risk, IT, finance, c-suite – and this inevitably takes time. But it is what is required to build a detailed renewal roadmap and, ultimately, secure cyber protection at the best terms possible.

Q. What are insurers' prioritising in terms of risks controls?

A. We have looked at basic hygiene requirements at length in this report, and these are generally non-negotiable for most carriers. But as I mentioned in my previous answer, there can be a lack of consistency in application across the market. Insurers insist on using their own questionnaires and views of risk, which is understandable, but their variability and inflexibility can be a source of frustration.

Another increasingly prominent area of focus is on privileged accounts. Admin access is what allows attackers to move laterally across systems, establish persistence and access sensitive data. Such areas of vulnerability are increasingly being probed by insurers, although this again differs by carrier.

Q. Is there anything the market can do to help businesses navigate the renewal process?

A. I would repeat what I have said already about providing clients with more consistency around risk controls. Conditions are difficult – we understand that – but one way of creating a more sustainable market from a client perspective is to offer more clarity here. We would advocate strongly for agreeing minimum cyber security thresholds that are consistent across carriers and clients, and stand ready to support the market in this endeavour.

Whilst insurers should be commended for helping to build cyber resilience (which ultimately is the best line of defence against threat actors), and they continue to prioritise companies that set a high bar for risk control standards by offering larger line sizes, more can still be done. As market conditions improve, we hope to see more alignment between companies' cyber hygiene and the cost of cyber protection. There is little pricing differentiation for risk management currently, something that needs to change when the market moves beyond its current hard phase.

One final thought for the longer term is on continuous underwriting. The fluidity and complexity of cyber requires something more dynamic than annual renewals. This ties back to the point I've just made about price – a stronger linkage between risk management and premium – and clients will over time expect more real-time rate movements to reflect their security investments through a traditional policy lifecycle.

Q. How do you expect market conditions to develop for the rest of the year?

A. As we show in this report, market conditions remain difficult, but some tailwinds may support performance in 2022. The first is off the back of more favourable ransomware trends following the underwriting actions taken by insurers over the last two years. The second is a lot more unpredictable, but the war in Ukraine has so far dampened cyber frequency further as both warring sides focus their efforts on conventional warfare.

This could of course change in an instant – for example, a ceasefire, a large-scale cyber attack, pressure on Russia's government to find new revenue streams as sanctions bite – but for now insurance claims are down significantly compared to last year. Even if ransomware incidents return to their pre-war trend, there are then question marks over whether any potential Russian-linked ransom payment claim could be prohibited by economic sanctions. Non-payment will certainly be the case for known Russian-affiliated groups, but potentially new entities too, as they may lack the credibility to trigger payment.

All this uncertainty notwithstanding, performance is likely to improve should these trends persist. This should help attract new (insurance and reinsurance) capacity into the market and avoid any repeat of waning capacity availability towards the end of this year (as we saw in 2021 after carriers hit their deployment targets early). The prospects for 2023 are therefore looking up, but, as is always the case with cyber, much will depend on geopolitical developments.

THE WAR IN UKRAINE HAS SO FAR DAMPENED CYBER FREQUENCY BUT THIS COULD OF COURSE CHANGE IN AN INSTANT.

Contacts

Howden broking

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

David Rees
Executive Director
+44 (0)7535 782 203
david.rees@howdengroup.com

Michelle To
Head of Business Intelligence
+44 (0)7710 705 627
m.to@howdengroup.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

David Flandro
Head of Analytics
+44 (0)7719 928 552
d.flandro@howdengroup.com

Expert contributors

CrowdStrike
Marko Polunic
EMEA Director of Business Development
- Insurance & Legal Services
+49-1590-440-1631
marko.polunic@crowdstrike.com

Guidewire
Lewis Guignard
Director of Data Science Solutions
+1 510 560 3716
lguignard@guidewire.com

KYND
Melanie Hayes
Co-founder and CMO
+44 (0)7500 605 455
mhayes@kynd.io

XCyber
Matthew Lane
CEO and co-founder
matt.l@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