howden

CYBER INSURANCE:
A HARD RESET

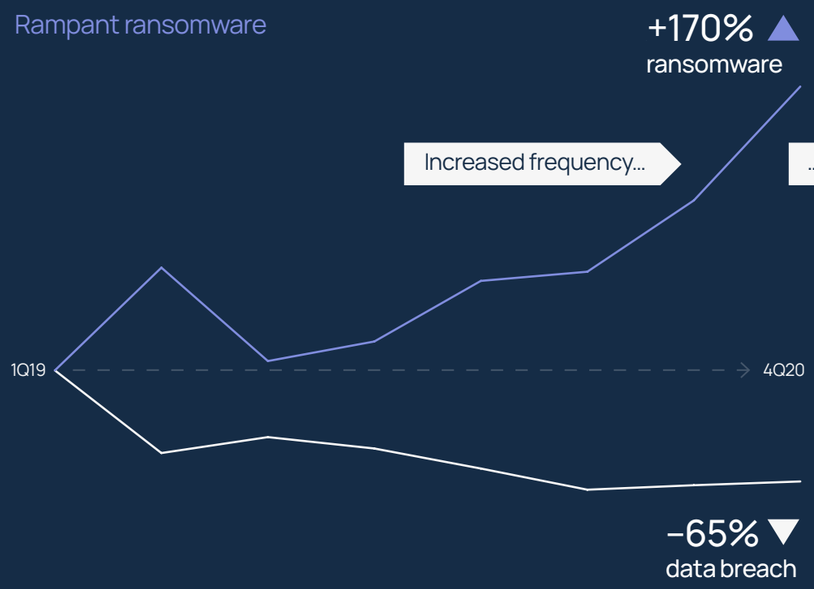
Key takeaways

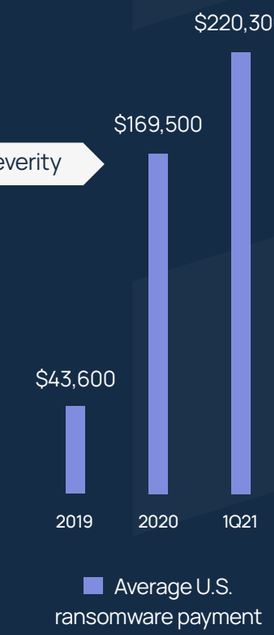
Ransomware and warning shots about risk aggregation have added a big dose of complexity into an already complicated cyber risk landscape.

Insurers are weighing the delicate balance of growth vs discipline in the face of surging claims and deteriorating profitability.

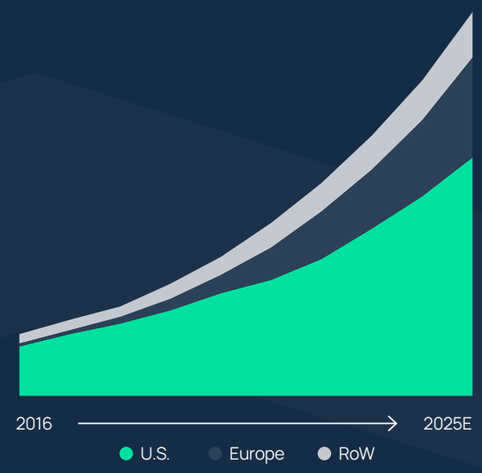
The three 'R's driving the market

Rampant ransomware

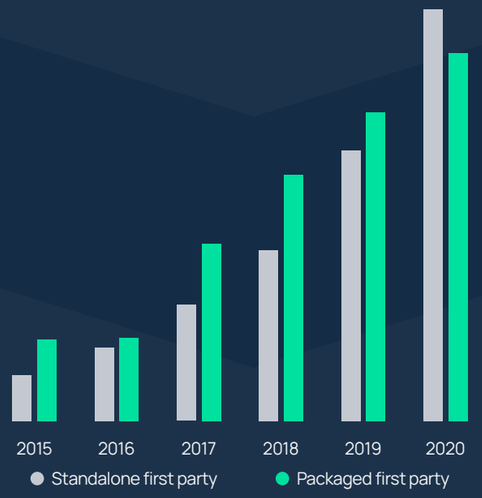




Gross written premium projections



U.S. cyber claims



Number of ransomware attacks worldwide up

170%

at 4Q20 compared to 1Q19

Source: SonicWall

Average ransomware costs worldwide up

145%

in 2021 compared to 2020

Source: Sophos

Average ransomware payment in the U.S. up

405%

at 1Q21 compared to FY 2019

Source: Coveware

30%+

insurance rate increases in 2021

Source: HX Nova Portal

70%

of brokers reporting capacity reductions

Source: Council of Insurance Agents & Brokers

Differentiated risk transfer advice can still unlock access to capacity. **Today's marketplace demands the very best of intermediary expertise and leadership** to help businesses secure the coverage they need.

Executive summary

2020/21 will forever be synonymous with COVID-19. But it will also be remembered for another (digital) pandemic that has transformed the cyber threat landscape: ransomware. The frequency and severity of ransomware incidents have grown considerably over the last year, with cyber criminals deploying new tactics and techniques to achieve one simple goal: to make money.

All the content provided in the pages ahead leads to one conclusion: ransomware is now the predominant cyber threat confronting businesses. With the prospect of risk aggregation and systemic events ever present – and reinforced in recent months by attacks on nation states that have targeted critical infrastructures and system providers – the insurance market is retrenching.

THE IMPORTANCE OF BEING PREPARED FOR A CYBER ATTACK CANNOT BE OVERSTATED

Risk appetite and perceived price adequacy for cyber exposures have been reset, with carriers reacting swiftly to get ahead of spiralling loss costs. The impacts for insurance buyers have been stark: supply is at a premium and rate rises for cyber insurance are amongst the highest across the entire market. Insurers are also demanding more from businesses' cyber resilience, and are only willing to deploy capacity if they are satisfied by the strength of companies' risk management frameworks. Or to put it differently, insurers are essentially cherry picking accounts based on companies' level of cyber security hygiene.

The importance of being prepared for a cyber attack cannot be overstated. The proprietary case studies within this report show how superior mitigation and response measures can support shareholder value and minimise reputational risks in the event of an attack. Unprepared companies, on the other hand, typically suffer disproportionate impacts that can lead to regulatory activity or litigation, and are now encountering more penal terms from insurers.

Preparedness is a key component of companies' cyber resilience. It involves building and testing a robust framework for the eventuality of an attack. For the benefit of our clients, we have invited some of our strategic partners, including KELA, Kovrr and WireX Systems, to contribute to this report and offer their insights into what companies need to do to achieve this. Despite the difficult market conditions, differentiated risk management and risk transfer advice can still unlock access to insurance capacity.

Today's marketplace demands the very best intermediary expertise and leadership to help businesses secure the coverage that meets their needs. It requires onboarding services, strong partnerships with third party experts, unrivalled relationships with insurers and, in the event of a cyber incident, the best minds in the business to help guide firms through to a quick and full recovery. Howden's exceptional cyber team provides all this and more. Come and talk to us.

01

A moment of reckoning

Cyber risk has undergone multiple episodes of change and development in its relatively short history, but nothing quite so impactful and fundamental as events over the last year.

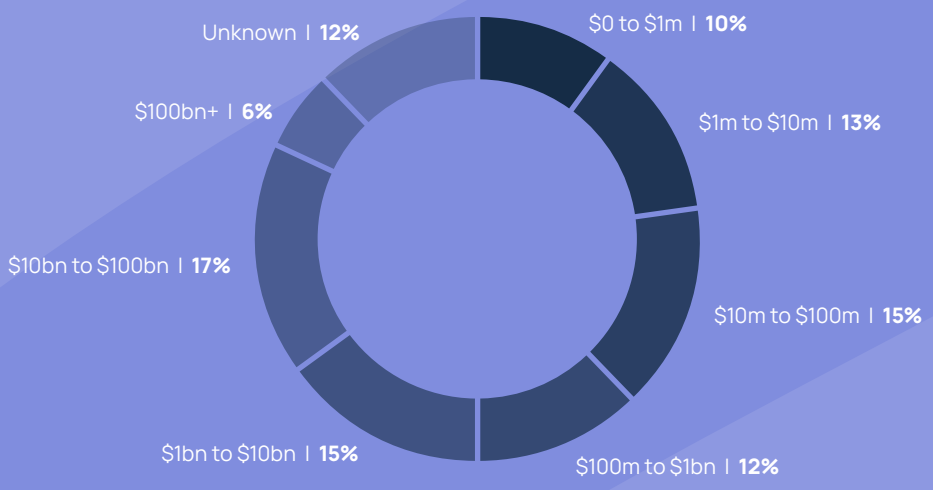
COVID-19 – and all of its attendant effects on technology adoption and cyber security – combined with independent or connected changes to the loss environment – including rampant ransomware incidents, the emergence of new attack vectors and rogue actors and more warnings shots about risk accumulations – have added a big dose of complexity into an already complicated risk landscape.

Cyber is unique in that the victims of wrongdoings are often viewed unfavourably by customers and regulators, and even penalised financially. This is a harsh reality, given it is next to impossible to prevent cyber attacks (although mitigating measures can, of course, minimise the fallout) and the risk landscape is complex, dynamic and indiscriminate.

CYBER IS UNIQUE IN THAT THE VICTIMS OF WRONGDOINGS ARE OFTEN VIEWED UNFAVOURABLY, AND EVEN PENALISED FINANCIALLY

Figure 1 shows that the growing number and sophistication of cyber attacks pose serious threats to all companies, irrespective of size.

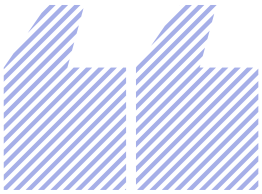
Figure 1: Proportion of cyber breaches by company size (revenue USD)
(Source: Advisen)



The damaging effects of cyber attacks are laid bare by the degree of disruption (network and supply chain impacts / failures), financial costs (remedial charges, business interruption, loss of income, share price movements) and occasional intangible impacts (reputational damage, loss of intellectual property) organisations are forced to navigate following a breach.

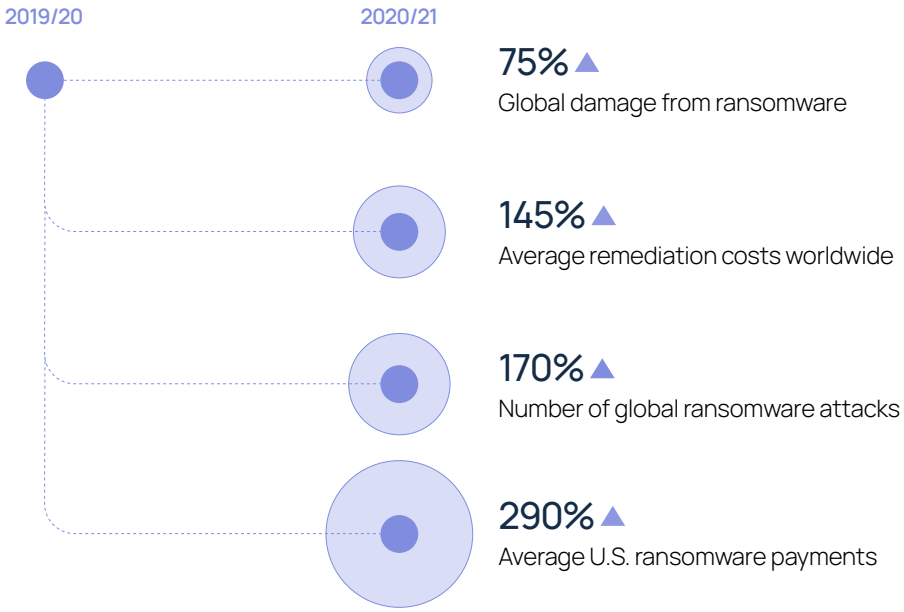
Dynamic loss profile

From a cyber perspective, only two types of companies exist: those that have been hacked and those that will be hacked. Exposures are growing rapidly and now cut across virtually every aspect of business. Whereas risks were concentrated initially around third party data protection and privacy liability, more recent incidents point to a shift towards first party extortion, business interruption, reputational harm and even physical damage. The surge in ransomware has been one of most consequential developments of the last 12 months, bringing about a sea change to the frequency and severity of attacks, and the cyber risk landscape more generally.



FROM A CYBER PERSPECTIVE, ONLY TWO TYPES OF COMPANIES EXIST: **THOSE THAT HAVE BEEN HACKED AND THOSE THAT WILL BE HACKED**

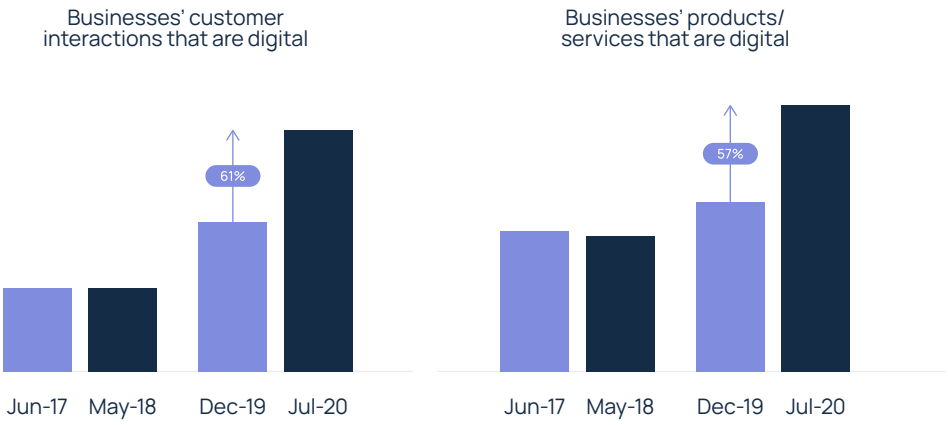
Figure 2: Increased frequency and severity of ransomware incidents
(Source: HX Analytics, Sophos, SonicWall, Coveware, Purplesec)



The COVID impact

COVID-19 has amplified risks further. With virtually no preparation, companies have been forced to rethink tried and tested ways of conducting business, and are now having to accommodate some of the permanent changes that lockdown has brought, such as remote working, accelerated digitalisation and increased reliance on third party technology and applications.

Figure 3: Impact of COVID-19 on digital adoption
(Source: HX Analytics, McKinsey)



Proportion of executives that expect changes to stick...

Increase in remote working / collaboration

54%

Increase in cloud migration

54%

Increase in data security spending

53%

Whilst homeworking and accelerated cloud migration have helped businesses trade through the last 15 months, they have also introduced more attack surfaces. Data shows how bad actors have exploited interest / concern around COVID-19 and other topical current affairs issues to entice users to click on malicious links or attachments. Delays in breach discovery and response due to fewer on-premises employees have exacerbated the situation.

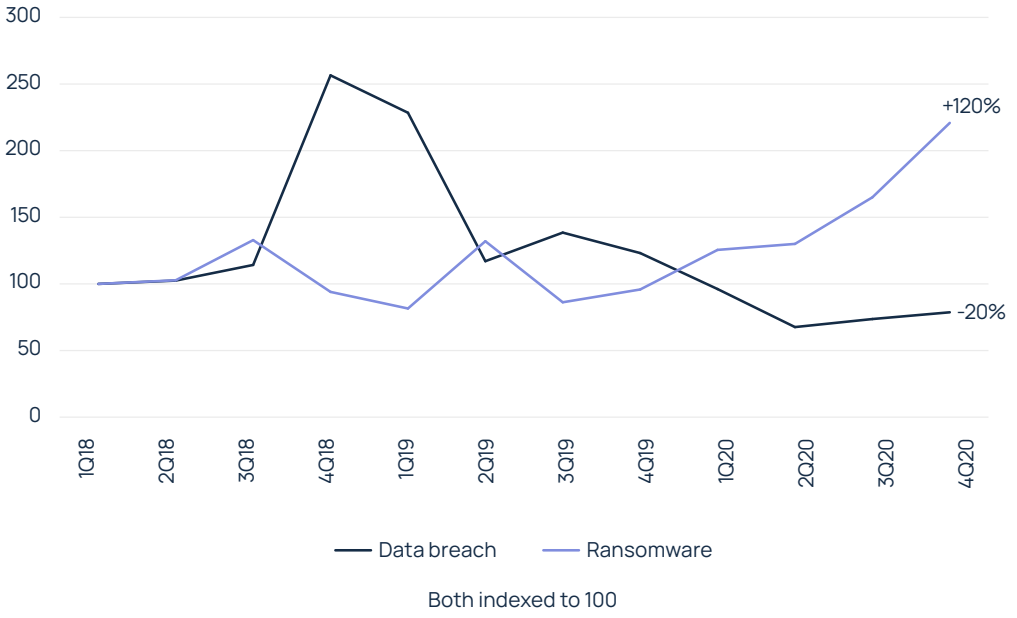
The pandemic has also revealed pre-existing vulnerabilities to an interdependent and interconnected world on the one hand but a greater reliance on digital technologies on the other. Whilst companies are investing heavily in areas like data and cloud security, bad actors are often one step ahead and will continue to target weaknesses in order to cause disruption, steal data and make money.

Rampant ransomware

Ransomware has become the weapon of choice to do this, and is now the most prominent cyber threat for businesses. The availability of turnkey (and relatively low cost) ransomware kits – otherwise known as ransomware-as-a-service (RaaS) – on the 'Dark Web' has fuelled the proliferation of incidents.

Figure 4 compares the number of ransomware and data breach incidents over the last two years, and the marked shift towards ransomware in early 2020 that became more pronounced as the year progressed. Costs for data breaches (at an average of close to USD 4 million) remain at elevated levels, however, even if the frequency has moderated.

Figure 4: Frequency index for ransomware vs data breach incidents – 1Q18 to 4Q20
(Source: HX Analytics, SonicWall, Risk Based Security)



Ransomware attacks are also becoming more sophisticated, with criminals infiltrating more deeply into networks prior to deploying their attacks. In a practice known as 'double extortion', tactics have shifted from data encryption alone to threats to release exfiltrated data into the public domain. This has led to more targeted attacks (larger firms with sensitive data are increasingly being pursued), longer downtimes, higher business interruption costs and increased litigation and regulatory activity.

KOVRR's take

The surge in ransomware attacks over the last 12 months has been led primarily by two developments: double extortion and RaaS.

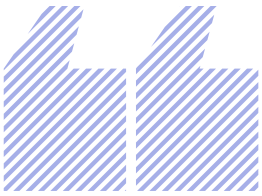
⟶ Double extortion: the adoption in the latter half of 2020 of a new attack method which not only involves data encryption but is also accompanied by threats from the same malicious actor(s) to publish the stolen data. The result = increased loss severity.

⟶ Ransomware-as-a-service: a model that enables potential attackers to purchase and deploy existing ransomware kits. Lower barriers to entry typically bring a flood of new market entrants, and ransomware has been no different. The number of attacked companies has swelled. The result = a higher probability of loss.

Kovrr has researched 16 active double extortion ransomware campaigns in the last year. Of these, 75% use social engineering (phishing emails) to propagate an attack, whilst the remaining 25% exploit vulnerabilities in remote access software.

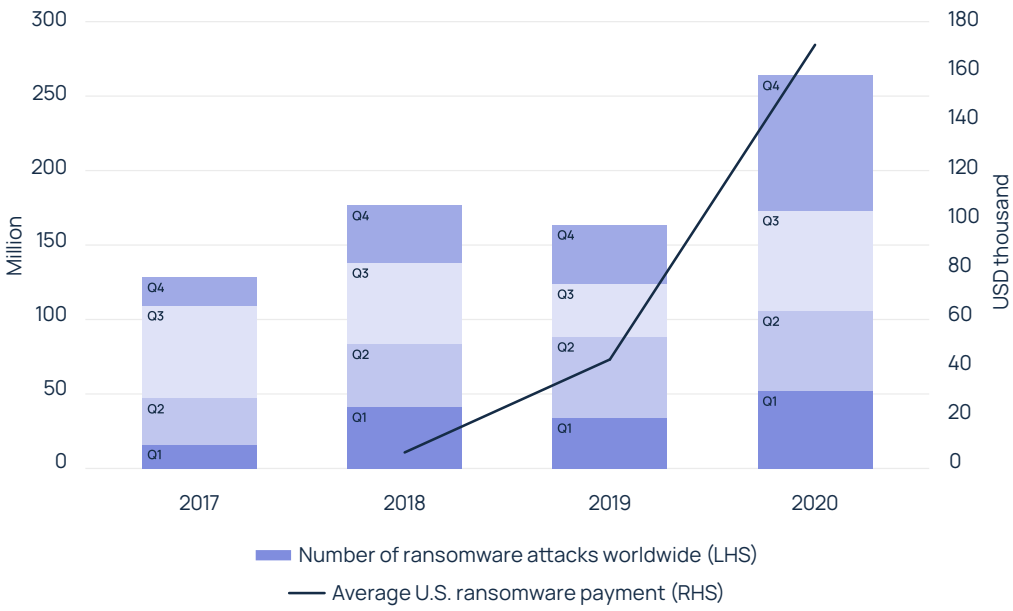
Two recent campaigns – Avaddon and Nefilim – stand out for their use of the double extortion method, with the option to purchase RaaS. Whereas Avaddon typically targets small to medium-sized businesses (SMBs) located in the United States and is propagated through social engineering, Nefilim ransomware is distributed through remote desktop protocol and has a more diverse target market, albeit with concentrations in the manufacturing sector. Both campaigns have resulted in proprietary data leakage, and are fuelling the increased frequency and severity of attacks that have characterised the last 12 months.

Figure 5 provides more granularity around ransomware trends to help contextualise the degree of change experienced last year. The number of incidents rose significantly, up 50% compared to the previous record (2018). But it is the severity and financial impact of incidents that are really starting to tell: for U.S. companies that decided to pay a ransom in 2020, the average payment increased by nearly 300%. Additionally, the Ransomware Task Force estimates that victims of attacks in the U.S. paid a total of USD 350 million in ransom last year, a 311% increase over 2019.



AVERAGE RANSOMWARE PAYMENTS IN THE U.S. **ROSE BY NEARLY 300% IN 2020**

Figure 5: Global ransomware incidents and U.S. ransom payments – 2017 to 2020
(Source: HX Analytics, SonicWall, Coveware)

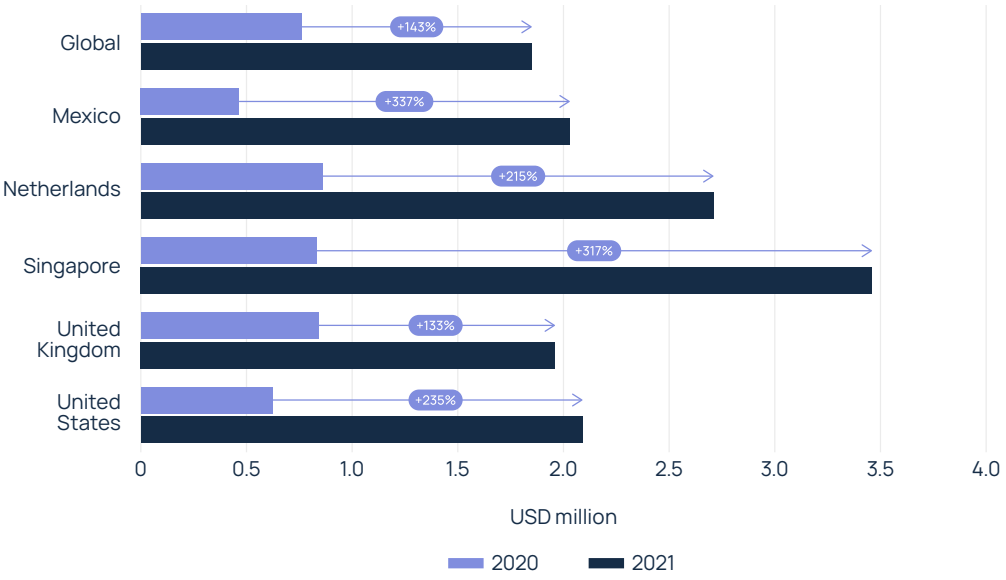


And as shown by Figure 6, the average cost of ransomware remediation[1] globally has more than doubled over the last 12 months. The variances displayed by country reflect a number of factors, including higher costs in advanced economies and the time required to remediate an attack, as well as preparedness / defences. Targets of frequent cyber attacks in general have higher levels of defences, which can help mitigate the financial impacts.[2]

[1] Remediation costs encapsulate several factors, including people time, downtime, business interruption, network cost, lost opportunities and ransom paid, where applicable. Whilst data on the frequency and severity of cyber incidents is notoriously difficult to access given the sensitivities involved, the surge on both fronts in recent years is undeniable. Data quality is something that needs to be improved as the cyber insurance market matures.

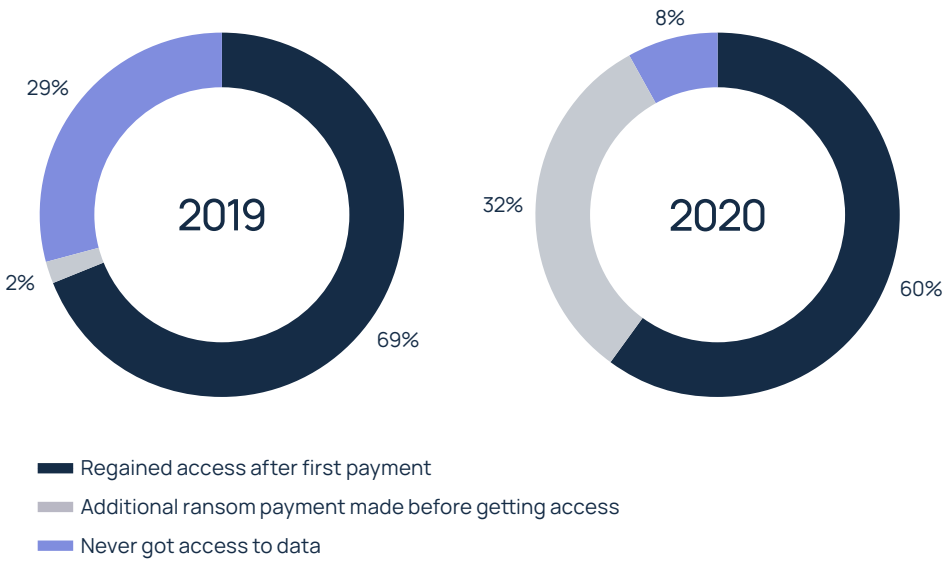
[2] Sophos, *The state of ransomware 2021.*

Figure 6: Average ransomware remediation costs for selected countries – 2021 vs 2020 (Source: HX Analytics, Sophos)



Whilst the differential between remediation costs and ransom payments appears on the surface to be significant, additional costs that typically accompany or follow ransom payments can narrow or even reverse the position. Downtime / business interruption costs can be as high, or surpass ransom payments. Average days of downtime rose from 15 at 1Q20 to 23 at 1Q21 – a rise of more than 50% in just 12 months, according to Coveware. It should also be noted that a minority of companies that choose the ransom payment route end up being forced to make additional payments or never getting access to their data (see Figure 7).

Figure 7: Outcomes following ransom payments – 2019 vs 2020 (Source: HX Analytics, Proofpoint)



The value of preparedness

The best solution for any cyber incident is preparation, both from an IT and risk transfer perspective. As stated earlier, cyber attacks cannot be prevented but businesses can put robust measures in place to mitigate impacts – more to come on this in the pages ahead.

To illustrate the point, HX Analytics has conducted a study into a number of high profile cyber incidents by grading the response actions of each impacted company[3], and measuring any individual share price deviations relative to local equity markets in the lead-up to and following each breach.

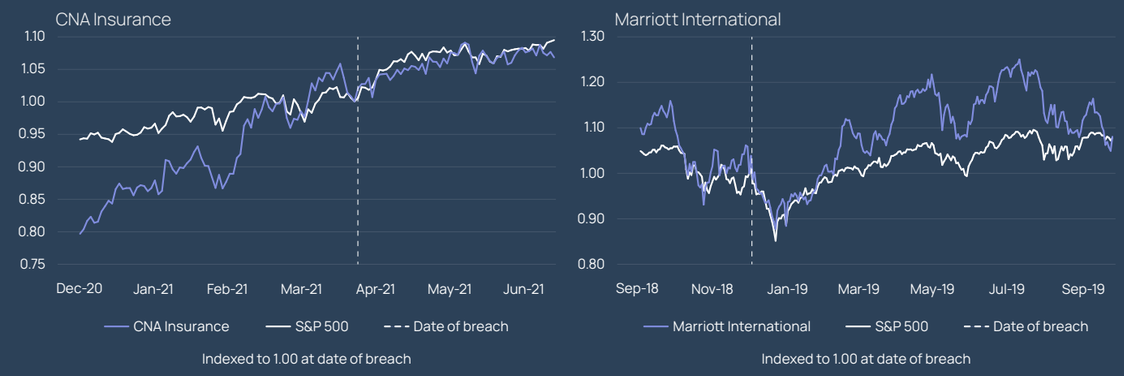
Whilst stock price impacts are of course shaped by a myriad of factors, as well as the specific dimensions of each cyber incident (including the size of the breach, the sector involved, the sensitivity of data exposed and any subsequent regulatory activity or litigation), a clear pattern emerges from our exercise that points to more limited stock price impacts for companies that are well prepared for cyber breaches.

The two top performers in our database – CNA Insurance (hit by a ransomware attack in March 2021) and Marriott International (data breach in November 2018) – scored highly in the mitigation, communication and risk transfer categories. This was instrumental in limiting the damage caused by their respective breaches, and any share price impacts (see Figure 8).

Despite Marriott's fine of GBP 18 million under GDPR legislation, its insurance policy covered nearly all of its total losses, meaning the company incurred negligible costs of its own. This is reflected by Marriott's share price movements over a 12-month period, which saw close alignment with the S&P 500 for the first few months post-breach and then outperformance for much of the remaining timeline. CNA's stock price has (so far) tracked the S&P 500 closely, after the company moved quickly to contain the impact of the ransomware attack.

[3] HX Analytics' index grades companies' responses to cyber incidents by assessing four different criteria: preparedness, mitigation, communication and risk transfer. Stock price impacts are measured retrospectively and prospectively from the date of the breach.

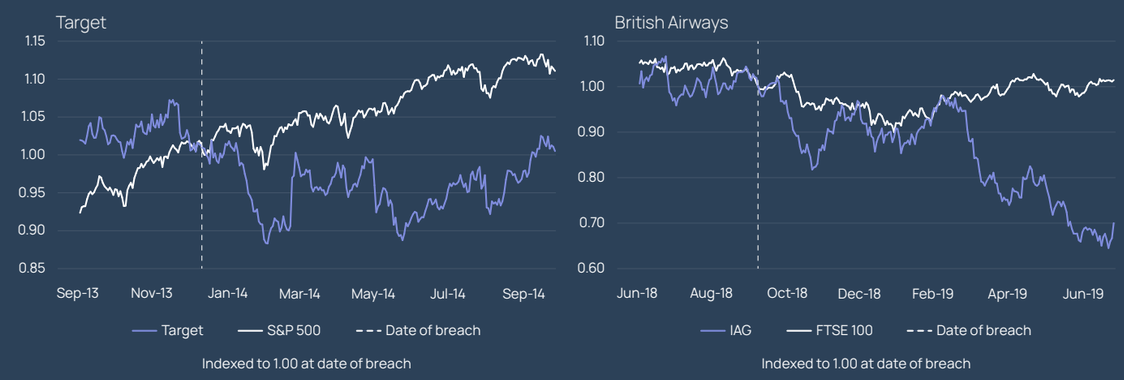
Figure 8: Strong performance post-cyber breach (Source: HX Analytics, Bloomberg)



Companies that are ill prepared for cyber attacks do not fare so well. Both Target (data breach in December 2013) and British Airways (data breach in September 2018) fall towards the bottom of our index, with low scores for preparedness, mitigation and risk transfer. Data for 40 million credit and debit cards were lost in the Target breach, along with personal information of an additional 70 million customers. More than 400,000 customers' personal details were compromised in the British Airways attack. This drew regulatory action and litigation against both companies, which ultimately told on their stock prices, as the losses were mostly retained.

Unlike the examples cited earlier, there was a significant post-breach fall to both Target's and British Airways' stock price after a month or so had passed and once the implications (including lack of preparedness and poorly handled responses) of the breaches became apparent (see Figure 9). Target underperformed the broader market for much of the remaining timeline, whilst British Airways' price deteriorated further as speculation grew about the size of its GDPR fine. After a charge of GBP 183 million was initial set, it ultimately settled at GBP 20 million in late 2020 after investigators took into account the airline's financial plight post-COVID.

Figure 9: Substandard performance post-cyber breach (Source: HX Analytics, Bloomberg)



The results of the exercise underline how unprepared companies can see events spiral out of control, which, in turn, often leads to regulatory action and / or litigation and more long-term impacts, such as sustained stock price falls and reputational harm. The clear takeaways to emerge from the study are simple: planning is crucial and investment in cyber security and incident response is money well spent. Developing a tested, comprehensive response plan and having a robust cyber insurance programme in place can help contain the impact and control external risks around customer and shareholder perceptions, even in this highly dynamic loss environment.

Aggregating warning shots

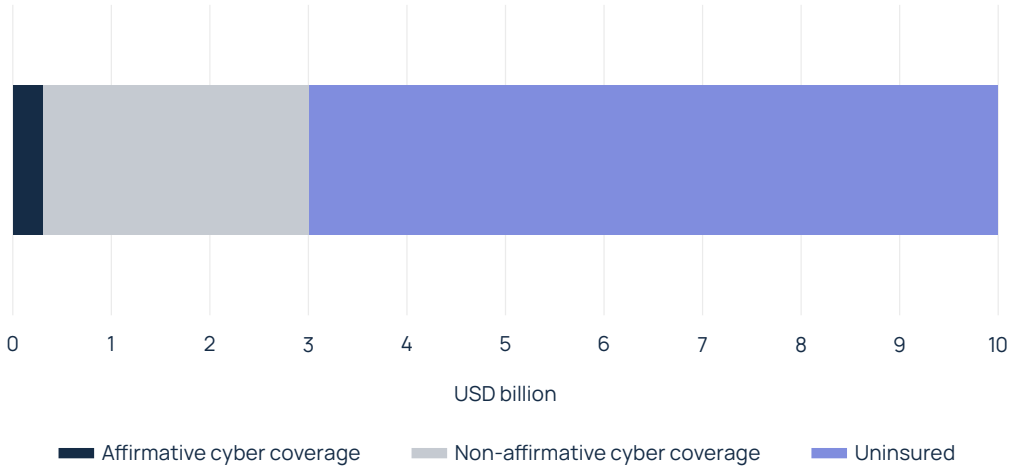
Companies that today have inadequate cyber security hygiene are not only exposing themselves to disproportionate impacts to cyber attacks but also more penal terms from insurers, who are now prioritising (in relation to price, terms and capacity deployment) companies able to demonstrate robust and tested security measures.

Risk appetite is also being impacted by the increased frequency of events that pose potential aggregated or systemic losses. The WannaCry and NotPetya attacks in 2017 revealed 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 10), an issue that is still likely to be prevalent today, even with the multitude of ongoing market and regulatory initiatives to address the matter.

UNPREPARED COMPANIES ARE NOT ONLY EXPOSING THEMSELVES TO **DISPROPORTIONATE IMPACTS TO CYBER ATTACKS BUT ALSO MORE PENAL TERMS** FROM INSURERS

Figure 10: Breakdown of economic and insured losses for NotPetya
(Source: HX Analytics, PCS)

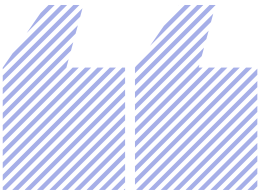


Catastrophic cyber presents challenges for an insurance industry built on underwriting mostly geographically contained and uncorrelated (physical) risks, and being guided in the process by historical loss data to help manage aggregations, estimate potential losses and price policies. Business interruption is one of the more dominant exposures associated with catastrophic cyber, and COVID-19 has provided a painful illustration of how non-affirmative coverages can surprise and spiral for global, systemic events.

Targeted (and increasingly frequent) cyber attacks on system providers and critical infrastructures in recent months – such as the SolarWinds' Orion software breach late last year, the Microsoft Exchange incident in January, the attempted hack at a water treatment facility in Florida in February and the ransomware attack on Colonial Pipeline in May (where no multifactor authentication was in place) – are stark reminders, if they were needed, of the critical threat posed by such events.

The sophistication of some of these attacks points to unattributable but probable state acts, which, in turn, challenges the utility of defined perils and war exclusions. This is an ongoing concern: a high proportion of cyber exposures are still embedded within traditional coverages, and events are now showing signs of spreading along supply chains and transcending entire sectors and regions.

The cyber insurance market is undergoing one of its most transformative changes since the first cyber policy was underwritten some 20 years ago. Carriers are responding to the rapidly changing risk landscape by deploying capacity more cautiously and raising prices. With no end in sight for adverse loss trends, (re)insurers must help businesses build resilience and continue to push the boundaries in providing comprehensive protection whilst weighing the delicate balance of leveraging what is undoubtedly one of their main growth sources and safeguarding solvency.



THE CYBER INSURANCE MARKET **IS UNDERGOING ONE OF ITS MOST TRANSFORMATIVE CHANGES** SINCE THE FIRST POLICY WAS UNDERWRITTEN SOME 20 YEARS AGO

KOVRR's take

Cyber catastrophes are different to natural catastrophes in that they do not respect the boundaries of geography or time, which creates real challenges when attempting to assess and model accumulated risk. Following extensive analysis of historical cyber events, which revealed risk concentrations around third party service providers and technologies relative to companies' locations, industries and size, Kovrr has developed CRA-Zones to help (re)insurers monitor catastrophic cyber exposures.

As more information becomes available on the recent SolarWinds and Microsoft Exchange incidents, analysis around 'target victims' highlights some interesting trends.

⟶ 1. Figure 11 shows that more than three-quarters of companies impacted by SolarWinds reside in just 23 CRA-Zones out of a total of 81 identified zones. This points to a clear accumulation of companies within a relatively narrow range of CRA-Zones, including small U.S. entities operating in the transportation & communication and educational services industries. The distribution also shows that the United States is the leading country for SolarWinds usage. Businesses with these types of characteristics were therefore more likely to be affected by the SolarWinds breach.

⟶ 2. For companies identified by Kovrr as being exposed to the ProxyLogon vulnerability in the Microsoft Exchange breach, 20% of businesses are concentrated in just 3% of the 4,176 CRA-Zones. The results also show concentrations by geography and industry: 60% of vulnerable companies are located in five countries – United States, United Kingdom, Canada, Germany and Italy – and an accumulation of companies operate in four sectors – business services, government, telecommunications and education (see Figure 12).

⟶ 3. Results from these two case studies contain some important information for (re)insurance carriers. Put simply, risk diversification is key. Careful consideration around portfolio composition based on the three minimal elements identified here (i.e. company location, industry and size) will help reduce the likelihood of loss aggregation.

⟶ 4. This is a relatively new area of research but by sharing insights like these, Kovrr hopes to support risk carriers in taking on more cyber risk and facilitating more efficient risk transfer.

Figure 11: Distribution of vulnerable companies to SolarWinds (Source: Kovrr)

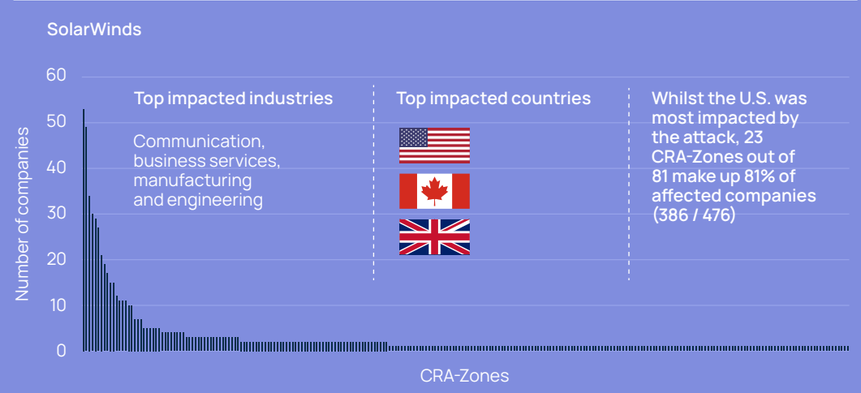
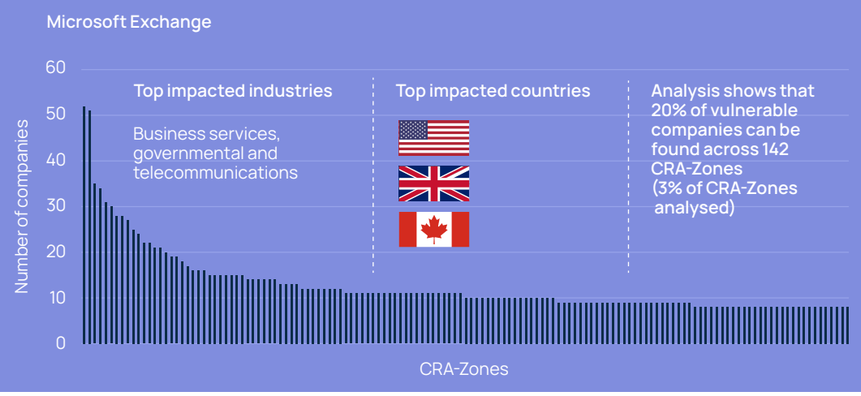


Figure 12: Distribution of vulnerable companies to Microsoft Exchange (Source: Kovrr)



02

Growing pains

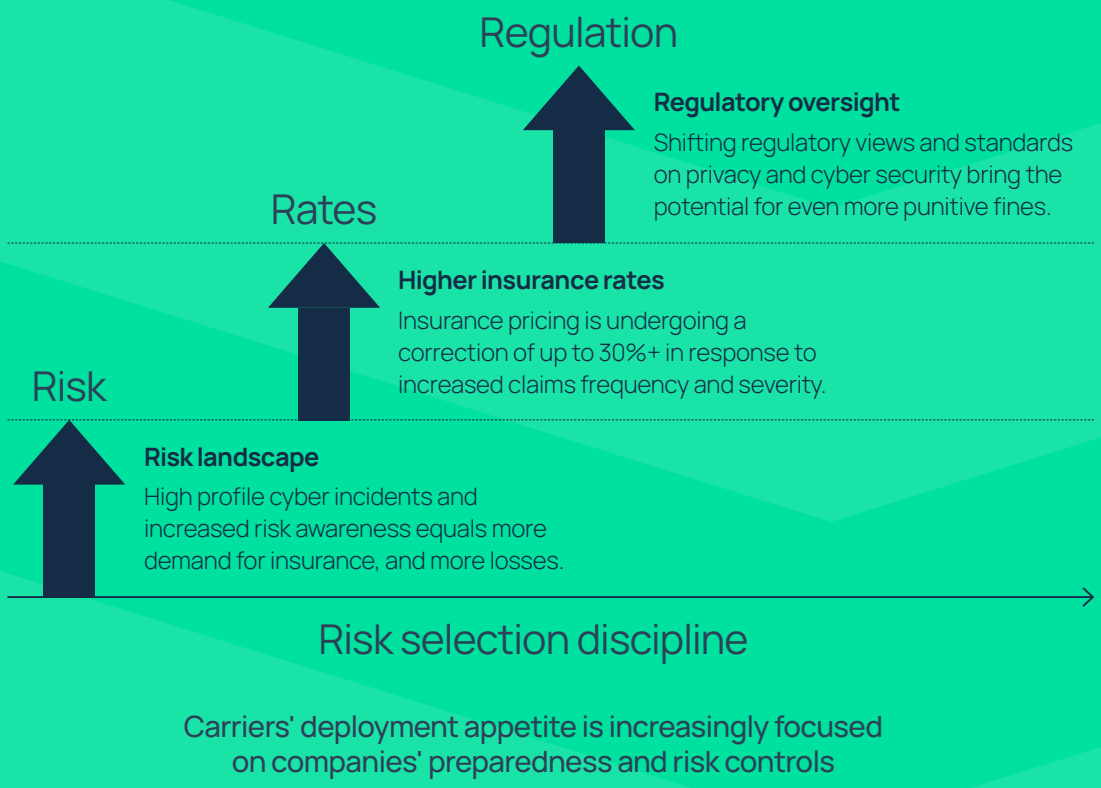
With cyber risk growing in perception and reality, strong momentum is building across the cyber insurance market. No other business line has such a fluid risk landscape, on the one hand, but such growth potential, on the other.

These tensions are currently playing out in the market, with demand for dedicated cyber cover increasing at a time of surging claims and deteriorating profitability. As a result, carriers are re-evaluating capacity deployments and increasing pricing rapidly, with rate rises amongst the highest across the entire market.

Figure 13 visualises the three key factors that are driving the cyber insurance market today: namely, a highly dynamic risk landscape, higher rates and shifting regulation – the three Rs.

NO OTHER BUSINESS LINE HAS SUCH A FLUID RISK LANDSCAPE, ON THE ONE HAND, BUT SUCH GROWTH POTENTIAL, ON THE OTHER

Figure 13: The three Rs driving the cyber insurance market



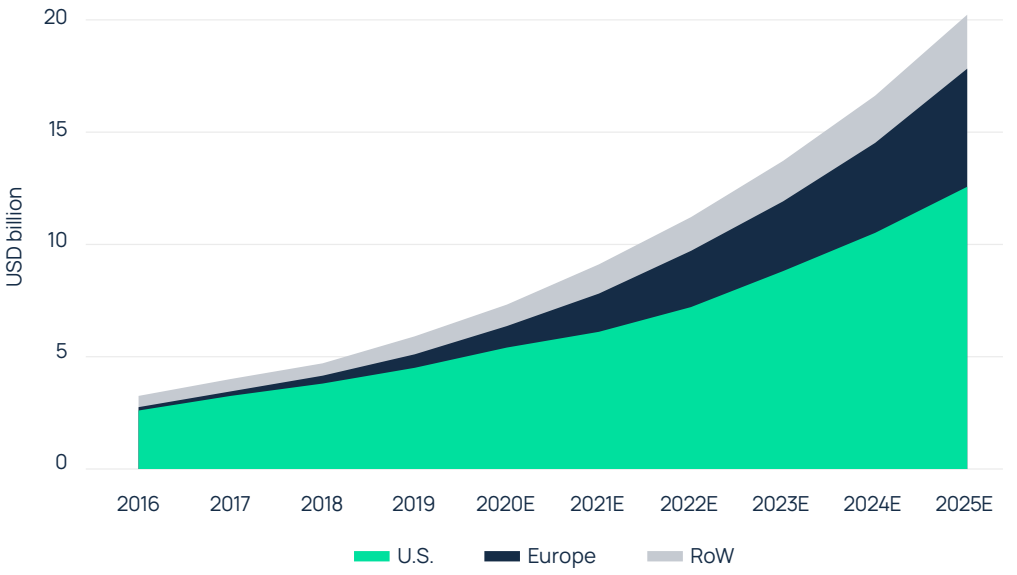
A story of growth…

Cyber has until recently been a lucrative business for (re)insurers, and the market has grown substantially in the last five years (see Figure 14). Gross written premium (GWP) has more than doubled since 2016 (growing at a CAGR of 22%), significantly outpacing the broader P&C commercial sector, which grew in the low-to-mid single digit CAGR range over the same period.

A similar rate of expansion is predicted for the global cyber market over the next few years (at a CAGR of 23%), which would see GWP approach USD 20 billion by 2025. 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.

The territories that are experiencing the highest growth rates include Australia, Germany, the Nordic countries, Israel, Italy, Spain, the United Kingdom and the United States. Despite being one of the most targeted regions globally, uptake in Asia remains low. Likewise with Latin America.

Figure 14: Gross written premium for global cyber insurance market – 2016 to 2025
(Source: HX Analytics, Munich Re, EIOPA)



…SMB penetration

Growth in the next few years is likely to see greater penetration into the SMB market. Whilst this is already happening in some territories, more work needs to be done in others. In France, for example, where cyber uptake continues to lag some of the aforementioned countries, only 8% of mid-sized companies are thought to have purchased cyber insurance, compared to 87% of large companies.[4] The underlying trend is more promising, however, as the number of French mid-sized companies to take out cyber insurance last year jumped by nearly 45%.

[4] L'Association pour le Management des Risques et des Assurances de l'Entreprise (AMRAE), *Lumière sur la Cybersecurity*, 2021.

87% OF LARGE COMPANIES AND 8% OF MID-SIZED COMPANIES HAVE TAKEN OUT CYBER INSURANCE IN FRANCE

Perceptions that cyber risks are skewed towards big corporations are now giving way to the realisation that SMBs suffer disproportionately from cyber attacks, and that cyber insurance extends beyond risk transfer and can supplement internal cyber security and risk controls. Indeed, insurance products are being created to help SMBs specifically prepare for and manage cyber incidents by identifying (and correcting) any security vulnerabilities. This bodes well for the future: a bigger pool of business and data will assist carriers in building greater cyber resilience and, over time, help deliver a sustainable, less volatile market.

...and innovation

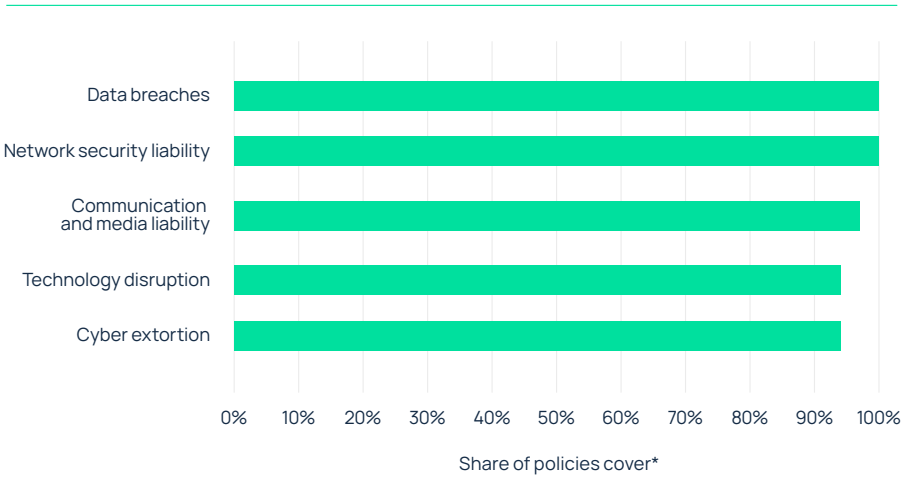
The degree of progression to date points to a cyber market that is adapting and responding to mega-trends that are bringing technology and digitalisation to the fore. Indeed, growing demand, coupled with the degree of rate increases in recent quarters, indicates that the GWP estimates in Figure 14 could prove to be conservative.

The cyber market is a fine example of the insurance sector doing what it has done so well many times over: innovating and developing solutions for the changing needs of clients whilst paying claims quickly and consistently in the event of a loss – 95% of all cyber claims have been paid to date for affirmative policies. Cyber coverages have come to market in relatively short order, and protection gaps are being filled as new threats emerge.

95% OF ALL CYBER CLAIMS HAVE BEEN PAID TO DATE FOR AFFIRMATIVE POLICIES

Figure 15 shows a selection of incidents covered by affirmative cyber insurance policies, protecting against a myriad of associated risks, including loss of data, data recovery, restoration costs, breach notifications, incident management, ransom payments, legal and defence costs, fines or other financial penalties, business interruption, reputational harm and professional liability.

Figure 15: Types of cyber incidents covered by affirmative cyber insurance policies (Source: OECD[5])



* Results capture cyber insurance policies in Australia, Canada, Japan, Netherlands, United Kingdom, United States or offered on a regional (Europe) or global basis.

The scope and comparative coverage clarity offered by affirmative cyber policies have been an important part of the growth story in recent years, providing businesses with a sustainable home for cyber exposures at a time when underwriters are coming under increased market and regulatory pressure to find solutions for non-affirmative cyber risks[6] in traditional lines of business such property and liability (i.e. either by affirming or excluding cyber from contracts).

Despite important progress on this front, more remains to be done: a high proportion of cyber exposures are still likely to be embedded within traditional P&C policies, and risk appetite today within the cyber insurance market is such that most underwriters are pulling back from any concept of risk aggregation. The prevailing mood is one of caution, and a number of businesses are finding themselves in a 'catch 22' situation where cyber exclusions or sublimits are being imposed in their property or liability policies and they are encountering supply issues in the dedicated cyber market.

[5] OECD (2020), *Encouraging Clarity in Cyber Insurance Coverage: The Role of Public Policy and Regulation*, https://www.oecd.org/pensions/insurance/Encouraging-Clarity-in-Cyber-Insurance-Coverage.pdf

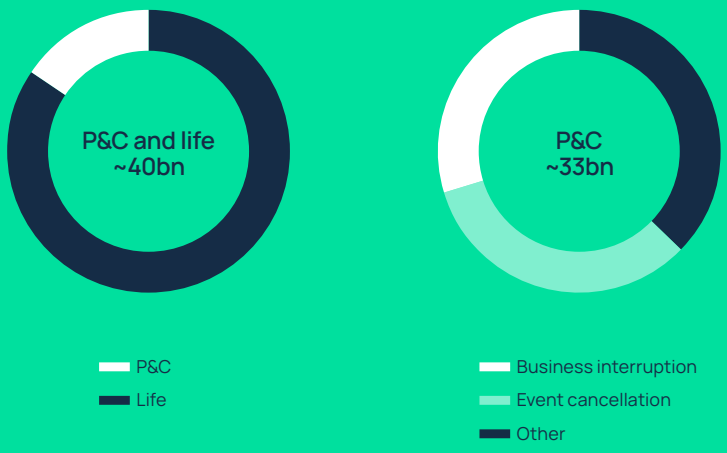
[6] Non-affirmative (or silent) cyber is a term used to describe cyber risks that are neither explicitly covered nor excluded in insurance policies.

[7] Average line of business breakdown across global, well diversified (re)insurers, where disclosed. Splits vary significantly by carrier depending on individual books of business.

A virus strain: non-affirmative risk

The COVID controversy around the applicability of business interruption cover has highlighted the limitations of standard P&C coverage for extreme, loss scenarios that cause huge loss accumulations. Policyholders, believing that their business interruption losses would be indemnified during the pandemic, felt aggrieved by the wave of claims denials. Carriers, on the other hand, were left confronting unpriced losses initially, and damaged reputations latterly.

Figure 16: Business interruption biggest insured loss component from COVID [7]
(Source: HX Analytics, HSBC, company reports)



COVID is a stark reminder that certain events are capable of causing losses at a global scale without any obvious physical consequences. Digital scenarios that result in cyber-triggered lockdowns or transnational business interruption claims are perfectly conceivable, and it is important from a solvency and reputational perspective that the insurance market learns the lessons from COVID and anticipates any potential digital equivalent by identifying and managing non-affirmative cyber exposures. The progress made so far in affirming or excluding silent cyber in traditional policies will go a long way to giving policyholders what they want – coverage clarity – and reducing the risk of unintended losses for insurance carriers.

There are also important differences between coronaviruses and computer viruses. Cyber attacks carried out to date by non-state actors have been mostly motivated by financial gain, rather than economic disruption. And whereas it took pharmaceuticals and governments the best part of a year to create a viable vaccine for COVID-19, the timeframe to patch systems in the event of any (conceivable) catastrophic cyber attack should be a lot shorter.

State-sponsored acts are potentially a different proposition, with different motivations and sophistications, and difficult questions remain about the attribution and certification of such attacks. But even here, cyber insurance policies have responded in the past and paid out when corporations have been targeted by suspected nation-state actors.

Whilst future global pandemics will once again require substantial state intervention, cyber is a different case: it has a flourishing standalone market, backed by sophisticated modelling tools, that already protects against a myriad of risks. Conditions are certainly challenging at present but market cycles come and go. A sustainable private market solution exists for cyber. Increased insurance penetration will, over time, facilitate a better understanding of the risks and aggregations involved, and incentivise risk mitigation. This, in turn, will result in innovative (re)insurance and insurance-linked securities structures that attract more capital and, ultimately, underwrite more risks.

A point of inflection

Market conditions have nevertheless become considerably more difficult for buyers in recent months. After years of abundant capacity, expanding coverage terms and relatively favourable pricing, 2019/20 was a watershed moment for the cyber market.

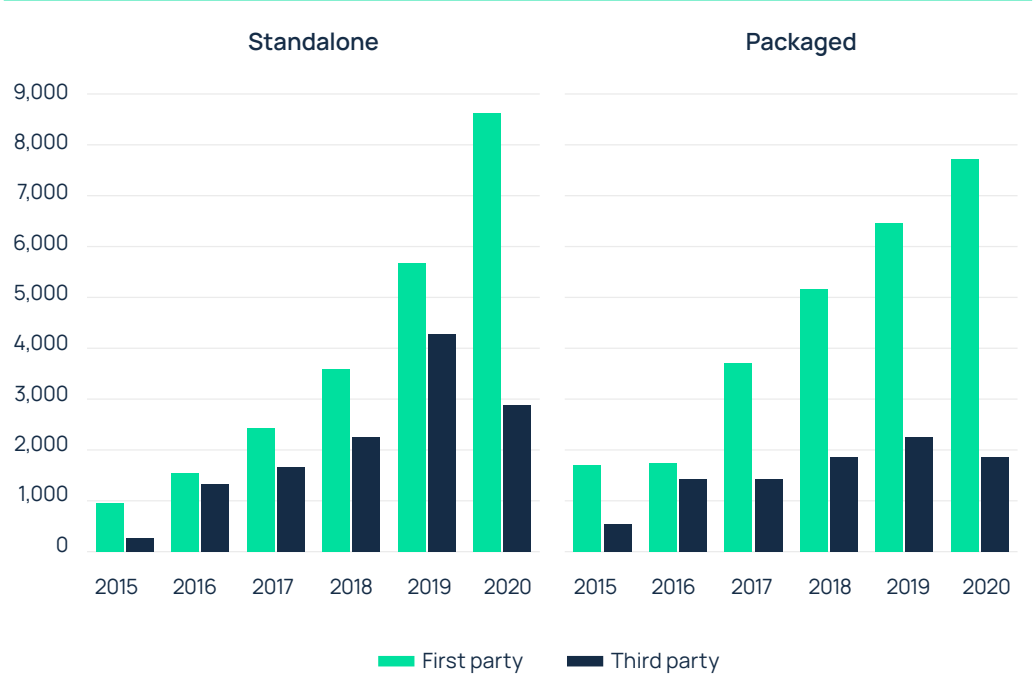
Prior to this point, the loss environment was relatively benign, restricted mostly to a manageable level of data breaches against individual companies. Complacency subsequently set in, with ill-disciplined underwriting that permitted loose risk selection criteria and little scrutiny around risk management. Put simply, cyber insurance was an under-priced product for part of the last decade.

Not if, but when

Lax underwriting standards have started to bite over the course of the last year or two, and the market has been turned on its head by proliferating ransomware attacks especially. There has been a remarkable shift in sentiment during this time from one of loss complacency to one of loss inevitability. Underwriters are now taking the view that losses are no longer a matter of if, but when, and, as a result, have high expectations around the sophistication of businesses' cyber security in order to 'qualify' for cyber insurance.

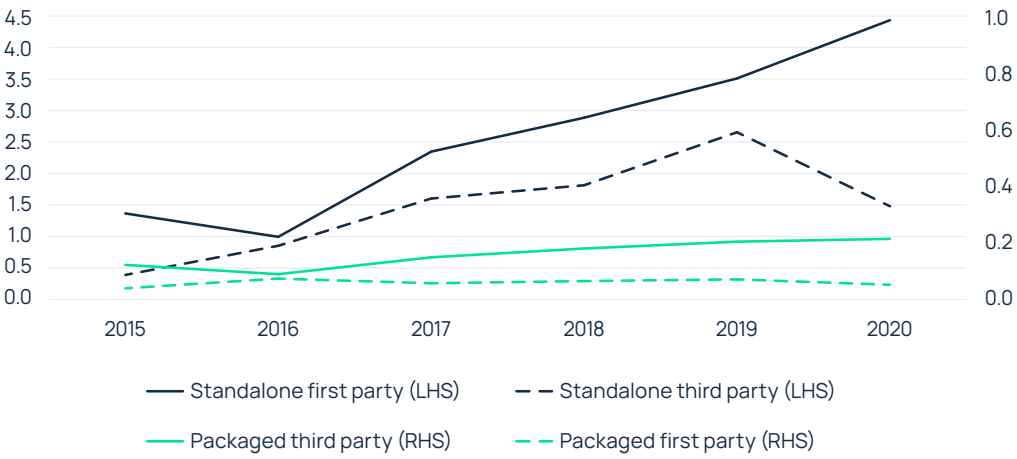
Figure 17 shows how the claims environment has deteriorated over the last five years, with both standalone and packaged policies in the United States recording a surge in the number of first party claims. The level of deterioration for standalone policies is especially eye-catching, with reported first party claims nearly nine times higher in 2020 compared to 2015, due primarily to proliferating ransomware attacks.

Figure 17: Reported first party and third party cyber claims for U.S. standalone and packaged policies (Source: S&P Global Market Intelligence, HX Analytics)



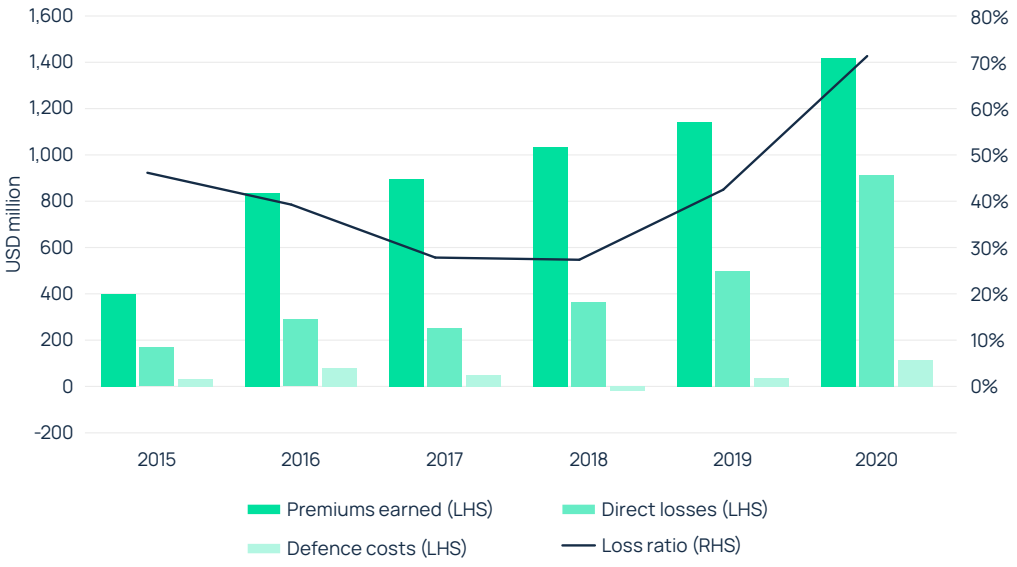
This is supported by Figure 18, which breaks data down to the frequency of reported claims per 100 policies in force, and also shows a steep upward trend for first party claims in standalone policies in particular.

Figure 18: Reported first party and third party cyber claims per 100 policies in force for U.S. standalone and packaged policies (Source: S&P Global Market Intelligence, HX Analytics)



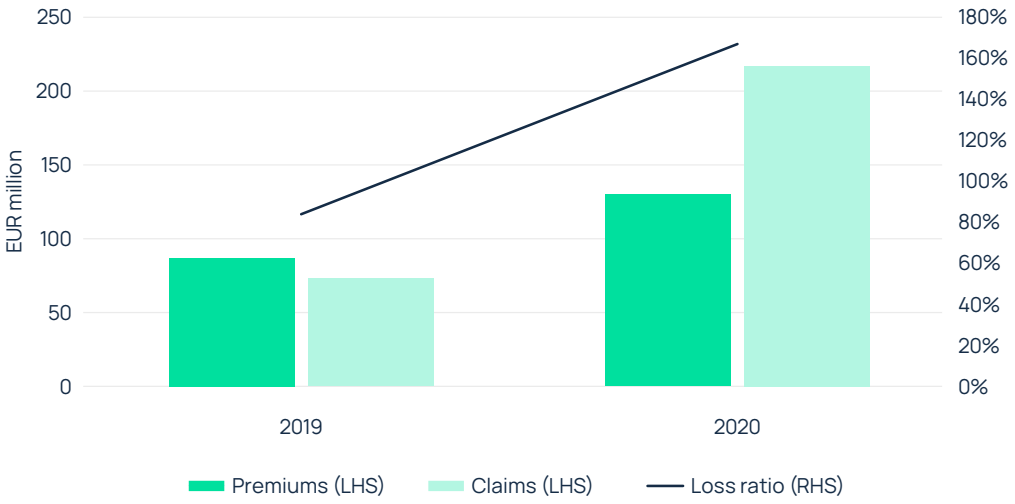
This has inevitably had an adverse impact on loss ratios , especially for U.S. standalone cyber policies, as the 70% threshold was breached for the first time last year, a big jump from 47% in 2019 (see Figure 19). Increased premium flow into the U.S. cyber market in 2020 was insufficient to offset the spike in direct losses and defence costs, whose combined total nearly doubled over the course of the year. This meant a number of cyber insurers fell into loss making territory, although performance varied widely by carrier.

Figure 19: Loss ratio for U.S. standalone cyber policies – 2015 to 2020
(Source: S&P Global Market Intelligence, HX Analytics)



These underlying trends are not unique to the U.S. and are being replicated across several other mature cyber markets, including France, where four large claims in 2020 were instrumental in pushing the loss ratio to a record high of 167% from an already elevated (and loss making) level in 2019 (see Figure 20). Without these four incidents, the loss ratio would have been broadly stable.

Figure 20: Loss ratio for French cyber market – 2020 vs 2019
(Source: AMRAE, HX Analytics)



Capacity crunch

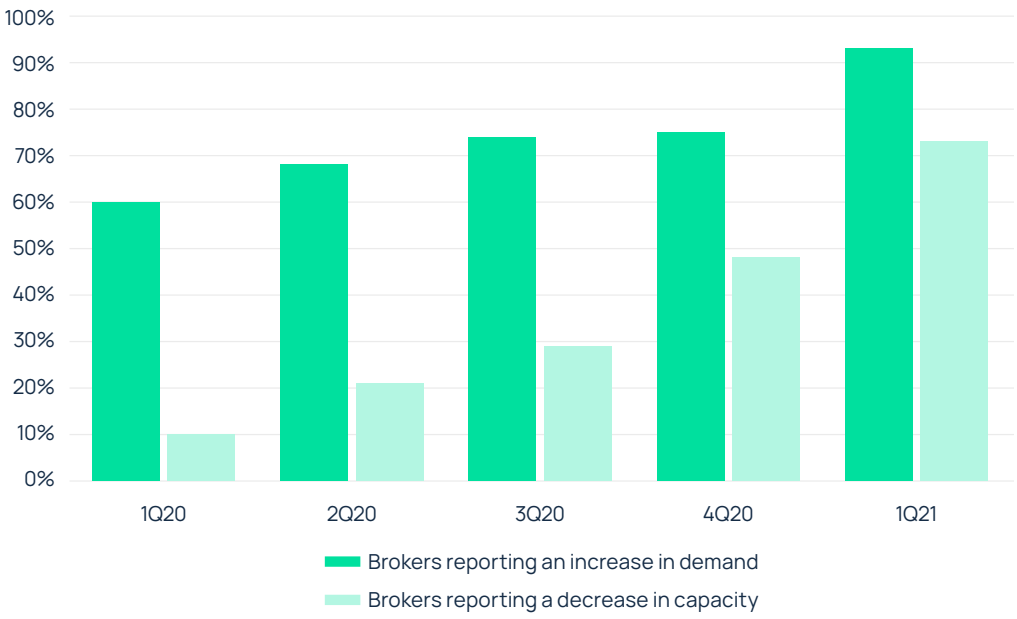
Insurance carriers have been quick to respond to the situation. Cyber is a short-tail class of business, and the confluence of factors identified in this report – increased frequency and severity of cyber incidents (ransomware especially), COVID-19 and greater regulatory oversight – has brought about a sea change to risk appetite and perceived price adequacy.

Put simply, the cyber market is currently being driven by a demand and supply imbalance (classic hard market territory), which shows no sign of relenting any time soon. This is corroborated by data published recently by the Council of Insurance Agents & Brokers (CIAB) in the United States.

Whereas only 10% of intermediaries in the U.S. reported declining capacity for cyber cover in 1Q20, the number jumped seven-fold in just 12 months (see Figure 21). Swelling interest in cyber insurance, fuelled by elevated loss activity and risk awareness, is accentuating competition over a shrinking pool of capacity. U.S. intermediaries reporting increased demand for cyber cover jumped from 60% to reach more than 90% during the same period. Or, to put it all differently, only 7% of brokers across the United States are not experiencing increased demand and only 27% are not encountering reduced supply.

THE CYBER MARKET IS CURRENTLY BEING **DRIVEN BY A DEMAND AND SUPPLY IMBALANCE**

Figure 21: Rising demand and falling supply in U.S. cyber market – 1Q20 to 1Q21
(Source: HX Analytics, CIAB)



The impact on underwriting strategies has been pronounced, with carriers now undergoing stringent portfolio remediation and essentially cherry picking accounts based on companies' risk management frameworks and cyber security hygiene. Only companies that are able to demonstrate best practice in these areas, especially around risk mitigation and incident response (e.g. by partnering with third party vendors and conducting table top exercises), are in a position to obtain the coverage that meets their needs.

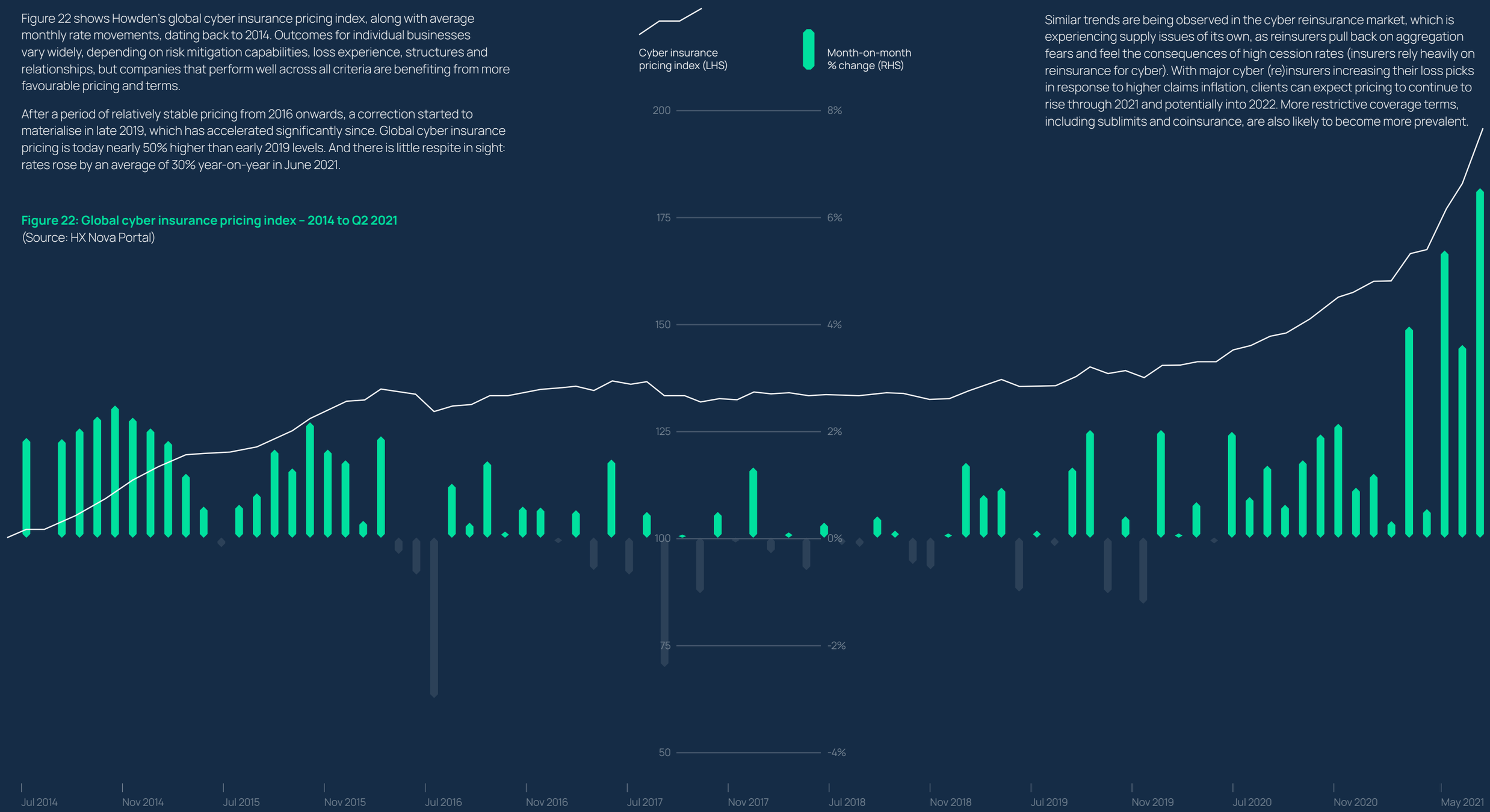
A hard reality

Risk management is also an important factor in determining price. Cyber continues to see one of the highest, if not the highest, rate increases across the entire insurance market, as carriers react swiftly to strive to reach price adequacy and get ahead of spiralling loss costs.

Figure 22 shows Howden's global cyber insurance pricing index, along with average monthly rate movements, dating back to 2014. Outcomes for individual businesses vary widely, depending on risk mitigation capabilities, loss experience, structures and relationships, but companies that perform well across all criteria are benefiting from more favourable pricing and terms.

After a period of relatively stable pricing from 2016 onwards, a correction started to materialise in late 2019, which has accelerated significantly since. Global cyber insurance pricing is today nearly 50% higher than early 2019 levels. And there is little respite in sight: rates rose by an average of 30% year-on-year in June 2021.

Figure 22: Global cyber insurance pricing index – 2014 to Q2 2021
(Source: HX Nova Portal)



The degree of repricing, coupled with tighter coverage terms, will likely support underwriting performance going forward, although questions remain whether it will compensate sufficiently should the recent uptick in losses be sustained. This is accentuating demand versus supply tensions, a situation exacerbated by carriers hitting their capacity deployment goals early due to higher than predicted rate increases and largely stable retention rates.

Similar trends are being observed in the cyber reinsurance market, which is experiencing supply issues of its own, as reinsurers pull back on aggregation fears and feel the consequences of high cession rates (insurers rely heavily on reinsurance for cyber). With major cyber (re)insurers increasing their loss picks in response to higher claims inflation, clients can expect pricing to continue to rise through 2021 and potentially into 2022. More restrictive coverage terms, including sublimits and coinsurance, are also likely to become more prevalent.

03

Securing cyber

Cyber has well and truly 'emerged' to become one of the pre-eminent risks facing businesses today. Barely a week goes by without another major cyber event hitting the headlines. But whilst the trajectory of incidents and insurance costs may at times seem uncontrollable, companies can still make a difference by strengthening their cyber security.

These measures must be sensitive to the fast changing risk environment. Until recently, companies that suffered ransomware attacks could minimise the damage and costs by simply backing-up data. But double extortion has changed the game, and companies must now prepare for the publication of stolen data, as well as encryption, during one incident.

KOVRR's take

Cost components from 'conventional' ransomware attacks, which result in data encryption only, typically include:

⟶ Extortion payment – depending on the jurisdiction, insurance carriers will reimburse the amount of money paid as a ransom.

⟶ Lost income – business interruption costs caused by the encryption process which cuts access to systems and data.

⟶ Recovery expenses – costs incurred by restoring data and systems following an attack.

⟶ Forensic costs – expenses incurred to identify the source of vulnerability in order to prevent future security breaches.

Double extortion has changed the rules, however. Data back-ups are no longer a sufficient defence against malicious actors increasingly intent on stealing sensitive data. Not only does this new tactic give attackers leverage in demanding ransom payments, but it also provides attacked companies extra incentive to pay the ransom. This has inevitably led to a higher number of successful attacks and insurance claims. Crucially, in cases where companies refuse to pay a ransom or the attacker publishes the data despite payment, the attack then becomes a de facto data breach event, which often brings additional cost components that can include:

⟶ Notification costs – expenses incurred when notifying customers, regulators and other required authorities of a data breach.

⟶ Monitoring – services in the event of identity theft or credit card fraud that have to be supplied to individuals whose data was stolen in a breach.

⟶ Regulatory fines and legal expenses – losses arising from third party claims whose private data was stolen in the incident.

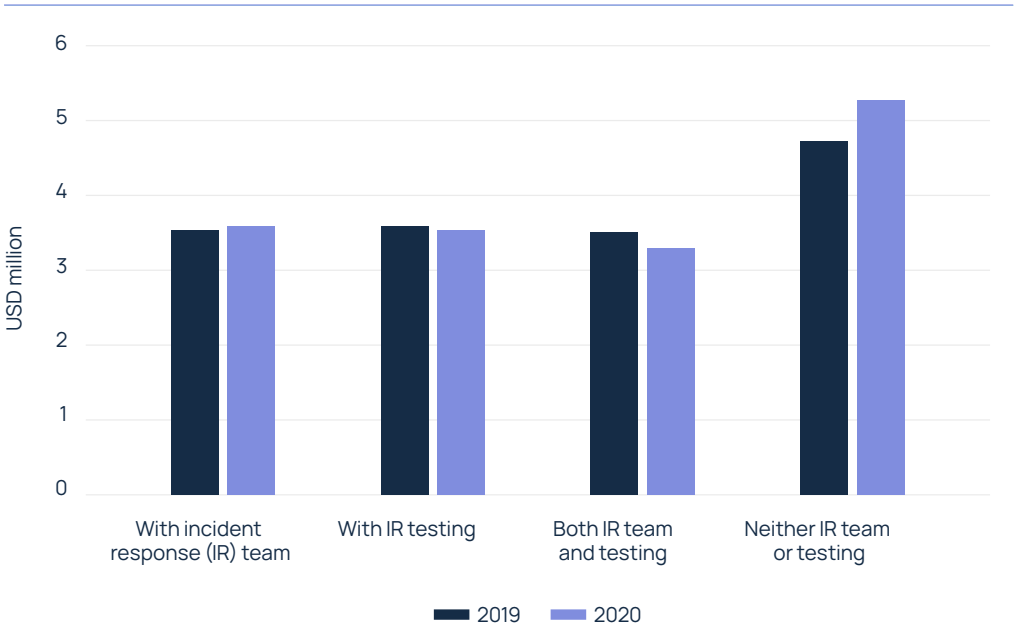
⟶ Public relations – expenses from PR, crisis management and/or legal advice incurred by companies seeking to prevent or limit adverse effects of any negative publicity.

Preparation is key

Preparedness is a crucial component of companies' cyber resilience. It involves building and testing a robust plan for the eventuality of an attack, requiring close collaboration across organisations, including board level stakeholders and key IT and security leaders. The plan needs to be meticulous, incorporating a series of steps that include training and educating employees, engaging with third parties, conducting table top (or war gaming) exercises, simulating how different events will transpire, knowing who to call should the worst happen and having experts at the ready. The very best insurance intermediary advice will provide oversight of this process as part of an onboarding service, which is unique to cyber.

Speed is of the essence following a cyber attack, and having these protocols in place will expedite companies' responses to any potential attack and help limit the damage and costs. Figure 23 shows the how incident response measures can reduce the cost of data breaches: companies with a tested incident response team paid almost 40% less on average in 2020 than those without.

Figure 23: Impact of mitigation on average cost of data breach
(Source: HX Analytics, IBM)

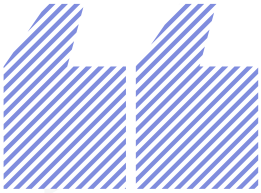


But even the best prepared companies cannot eliminate the risk of a successful attack entirely, and here specialist advice is available to help firms mitigate their risks and recover from any incident.

Differentiated broking

Businesses perceived to have weak cyber security hygiene are increasingly being offered less favourable insurance pricing and terms, or no cover at all. Market conditions are highly fluid, unsettled even, as carriers react to fast moving risk developments. Supply is now at such a premium that carriers are merely selling capacity (not price). This is likely to be the hardest cyber insurance market since its inception.

Despite all this, differentiated risk management and risk transfer advice can still unlock access to capacity. Today's marketplace demands the very best intermediary expertise and leadership that goes beyond plain vanilla placement services. It requires onboarding services, strong partnerships with third party experts, unrivalled relationships with insurers and, in the event of a cyber incident, the best minds in the business to help guide firms through to a quick and full recovery.



DESPITE DIFFICULT MARKET CONDITIONS, DIFFERENTIATED RISK MANAGEMENT AND RISK TRANSFER ADVICE **CAN STILL UNLOCK ACCESS TO INSURANCE CAPACITY**

Cyber threat intelligence

David Carmiel, CEO KELA

One of the most important things to remember when assessing the cyber risk landscape is that everyone is a target. Organisations must therefore be proactive in seeking to detect threats and defeat cyber criminals before they cause harm. Having access to cyber threat intelligence can help companies understand attackers' tactics and techniques, and even detect and disrupt incidents.

Q. What is driving the dramatic increase in cyber incidents?

A. The Dark Web represents a wide variety of goods, products and services offered by (and to) cyber criminals. Traditionally concentrated in forums, these services have sprawled into different mediums – instant messaging platforms, closed communities and automated shops, to name a few – and are now being used by bad actors to exchange access to monetisable cyber crime products, such as compromised networks, stolen credentials and leaked databases.

Q. So more of the same is to be expected for the foreseeable future?

A. Yes. The focus on automation and servitisation is aimed at aiding the cyber crime business to grow at scale, something we have seen with the recent spike in ransomware attacks. It is not all bad news though: defenders can exploit these ecosystems by gaining visibility into the inner workings of the underground ecosystem, allowing them to trace the same vulnerabilities, exposures and compromises that would be leveraged by bad actors and remediate them before they get exploited.

Q. What advice do you have for companies looking to mitigate their vulnerabilities?

A. There are several ways organisations can manage cyber threats, but let's break them down into two: human and digital. First and foremost, we recommend businesses train all employees on how to use their personal information and credentials online safely. This training should include advice on how to identify suspicious activities, such as possible scam emails, or unusual requests from unauthorised sources. The larger the organisation, the bigger the threat. The human factor plays a major role in cyber security, and education is one of the most effective (and cheapest) steps in strengthening cyber resilience.

Q. What about the digital dimension?

A. In three words, cyber security investment. Cyber criminals are continually searching for new opportunities to achieve one simple goal: monetise the data they obtain. They are active in the hardest-to-reach corners of the cyber crime underground, and the deployment of automated and scalable monitoring is highly effective in reducing attack surfaces and ultimately minimising the risk of a successful breach. Staying up-to-date on newly discovered vulnerabilities can also help firms prioritise patching by weighing up the relative severity levels of all the cyber threats that they face.

Q. Looking ahead, where do you see the main challenges for companies in managing their cyber risks?

A. Identifying where the threat actors are, understanding their language and communication and extracting relevant and critical intelligence from these sources are likely to remain areas of difficulty for businesses. Threat intelligence, especially Dark Web intelligence, is what arms organisations with the critical information that they need to make tactical, strategic and operational business decisions. Put simply, our goal is to help keep companies one step ahead of cyber criminals.

Forensic investigations

Tomer Saban, WireX Systems CEO and Andrea Bonime-Blanc, GEC Risk Advisory CEO

The recent, exponential rise in cyber attacks is creating serious difficulties for organisations and insurers looking to perform quick and successful forensic attack investigations in a way that is both cost efficient and reputationally sound. Cyber forensic teams are increasingly encountering problems around insufficient data and toolsets (to name a few) at impacted firms, which can prolong the investigation process and inflate recovery costs.

Q. In the event of a cyber incident, what would you say is the most important attribute in minimising the fallout?

A. Speed. The importance of a rapid response cannot be overstated. The time it takes for hackers to infiltrate a targeted network is getting shorter. State-sponsored hackers can infiltrate a system in as little as 19 minutes. Independent attackers average around 10 hours. The crux of the problem is the huge time disparity between attack infiltration and company response. Ideally a threat should be identified and isolated immediately. If it is not, hackers have time to target more hosts, take over systems or lie in wait silently whilst extracting data without detection.

Q. What are the main impediments to detection?

A. It varies by organisation but two common factors are imperfect data and bottlenecks. Many aspects of the security process are automated today. Prevention and detection tools flag potential threats and attempt to automatically stop them from executing. While the techniques used to identify threats and create alerts vary widely from identifying predefined and pre-programmed patterns to machine learning and artificial intelligence, the end result is the same – the threats join an ever-growing queue, contributing significantly to 'alert fatigue' syndrome.

Q. And this creates the bottlenecks?

A. Yes. It is next to impossible to triage and investigate all alerts. Security teams either do not have the required visibility into their own environments or they struggle to properly store needed forensic data to support a deeper investigation (or both). High level metadata logs provide at best limited insights into events. This means that the majority of the investigation process falls on already stretched security personnel, who have to dig manually for evidence to understand the cause of the breach, how it happened and what was accessed. Without forensics data, it will take weeks, if not months, to get the answers. All the while, businesses' financial and reputational costs mount.

Q. How can these challenges be overcome?

A. Security teams need to adopt a solution that takes the guesswork out of the process. Instead of investing time in trying to correlate high-level metadata, they need a solution that automatically visualises all relevant data, from the big picture (the forest) to the minute details (the trees, branches and leaves). Analysts need answers to a myriad of questions – how and which file servers were accessed, what was uploaded or downloaded, how many records were accessed, what transactions were executed? And they need them in minutes, not hours, days or weeks. Only then will companies' financial and reputational bottom lines be truly protected.

Risk transfer

Shay Simkin, Global Head of Cyber, Howden

Q. If you could pick out three key cyber insurance market trends, what would they be?

A. We have identified the three Rs in this report – risk, rates and regulation – as being instrumental in driving the market. Beyond that, carriers are becoming increasingly discriminatory when weighing up capacity deployment and are demanding extremely high cyber security standards. Impeccable cyber security hygiene is therefore crucial for companies looking to purchase cyber insurance cover. Not only does it open up capacity availability, it also helps provide more favourable pricing and terms.

Q. How do you expect rates and coverage terms to develop for the rest of the year?

A. More of the same. Pricing pressure shows no sign of abating and we are already seeing terms tighten significantly, particularly around coinsurance and business interruption cover. One important point to make, however, is the distinction between renewals and new business. For the former, insurers continue to place value on relationships (broker and client), which are making renewals easier to manage. Ultimately, there is still an alignment of interest across the value chain – insureds, brokers and insurers – and this is clear during live incidents where carriers are often highly responsive and decisive in bringing an event to a quick conclusion.

Q. Given difficult current market conditions, and with insurers' now incentivising cyber security, what steps would you encourage businesses to take to become 'better' risks?

A. Our partners contributing to this report – KELA, Kovrr and WireX – have articulated well how risk quantification, threat intelligence and forensics investigations are crucial to businesses' cyber security hygiene. I would just reiterate that preparedness is key. This is where we feel Howden's broking value proposition is highly differentiated: when we are the direct broker, we arrange client onboarding, assist with table top exercises and, should the worst happen, coordinate the event response. We are the first (or second – after the CEO) people to call in the event of a breach.

Q. Any advice for companies with renewals between now and the end of the year?

A. We are engaging with clients months before renewals. It goes back to the preparedness point, and assisting clients in building a better risk profile for submission. In anticipation of queries that will inevitably come from carriers, we can help identify any vulnerabilities in security defences and apply the required fixes, but this takes time.

One additional point worth making is around capacity availability towards the end of the year. Given the higher than expected rate increases so far in 2021, carriers are hitting their deployment targets early, which points to an acute capacity crunch later this year. Howden has workaround solutions for this but collaboration across the market is needed to ensure businesses are able to secure the coverage that they need as the year progresses.

Contacts

HX Analytics

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

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

Man Cheung
Head of Actuarial
+44 (0)7834 178 989
man.cheung@howdengroup.com

Iain Davie
Head of Catastrophe Modelling
+44 (0)7923 2103 45
iain.davie@howdengroup.com

Mark Shumway
Head of Advisory
+44 (0)7761 516 537
mark.shumway@howdengroup.com

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

Cyber broking

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

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

Chris Cotterell
Divisional Chair – Cyber
+44 (0)7566 794 516
chris.cotterell@howdengroup.com

Expert contributors

KELA
David Carmiel, CEO
jdavidic@ke-la.com

Kovrr
Yakir Golan, CEO & Co-founder
yakir@kovrr.com

WireX Systems
Tomer Saban, CEO
tomer@wirexsystems.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.com