GuyCarpenter

THROUGH THE LOOKING GLASS:

Interrogating the key numbers behind today’s cyber market

A business of Marsh McLennan

REPORT HIGHLIGHTS

The study brings greater clarity to the size and aggregation potential of the cyber insurance industry to benefit (re)insurers and other sources of current and future capacity.

- The cyber industry is now global in scope, with USD estimated 14 billion in premium (split between USD 9 billion for the US and USD 5 billion for non-US) and has leaped ahead of other established speciality lines in critical mass.
- This relationship with other lines has evolved due to the phenomenal growth experienced as well as the future potential of the class.
- A global event loss at the 1:200-year level is modeled to be between USD 15.6 billion and USD 33.4 billion. While this is a wide range, the divergence is narrower than that seen during earlier versions of these models.
- Model variation is surprisingly greater at lower return periods. This likely points to a greater need to interrogate the takeaways from precedents and “counterfactuals”–to better drive consensus.
- In loss ratio terms, cyber models are now lower in the tail than they have ever been. This has been driven by rate/exposure dynamics and successive methodology updates from the models.

CONTENTS

EXECUTIVE SUMMARY

In this report, we contextualize and quantify the evolution of the cyber market as a core line of business. This involves comprehensively assessing the size and shape of the industry, as well as for the first time providing a multi-model vendor view of the potential scale of a global cyber industry loss. As the market marches on, studies like this provide a useful waypoint in the journey from a bolt-on cover to a mainstay of the insurance industry, and make a compelling argument for new reinsurance capacity providers to enter the profitable cyber market.

The footprint of the cyber market looks notably different than the last time we examined the potential impact of catastrophic events in our 2019 industry loss study, *Beyond the Clouds*.[1] Coverage has expanded, shifted, and been refined with an increasingly broad product selection available. This is reflected in the rapid globalization of the market today where our research suggests the 2022 US-domiciled market comprised USD 9 billion, with the non-US market further contributing USD 5 billion. For reference, the US-only industry premium that we examined in our 2019 report *Beyond the Clouds* was approximately USD 2.6 billion. This points to rapid growth, however capacity constraints and the lack of penetration of certain markets signal that it is the tip of the iceberg.

Against the backdrop of a changed market, we look to a widened panel of catastrophe models to provide insights and opinions on the potential impact of a systemic event. Here we have examined the quantum of a possible global loss across the prominent cyber platforms today. What we see is a wide range of results for a 50-year event with a 5-fold difference from the smallest result at USD 5 billion to the largest at USD 25 billion. As the horizon broadens to more extreme events, views still differ significantly but the order of relative difference is reduced, with the average 200-year return period event loss at USD 25 billion.

Modeling divides opinion and requires robust scrutiny, a careful contemplation of context and strong feedback loops from the market. We always advocate for a nuanced and proportionate interaction with analytics platforms, collaborating to continually improve the interaction with data and modeling. When we compare these models to their natural catastrophe counterparts, especially for perils that are also infrequent and volatile in nature, there is a similar divergence of model consensus. The insurance industry has proven to be an adept and responsible vehicle for bringing risk and capital together. This precedent provides encouragement that we can navigate these challenges together and attract significant fresh capital to this growing space.

WE ALWAYS ADVOCATE FOR A NUANCED AND PROPORTIONATE INTERACTION WITH ANALYTICS PLATFORMS, COLLABORATING TO CONTINUALLY IMPROVE THE INTERACTION WITH DATA AND MODELING.

[1] Guy Carpenter, CyberCube: A US Cyber Industry Catastrophe Loss Study, 2019: Looking Beyond the Clouds. Beyond-the-Clouds.pdf (marshmclennan.com)

THE DYNAMICS THAT DEFINE THE MARKET TODAY

In the intervening years since Guy Carpenter's 2019 industry loss study, *Beyond the Clouds*, the relatively young cyber insurance market experienced exponential growth, weathered a significant test in fending off the significant increase in ransomware attacks, and transformed after experiencing a rapid and extreme hard market cycle. The hard market fundamentally changed the class of business, and resulted in the heightened collection and leverage of data to improve underwriting and claims response.

Loss activity, rate reset and coverage realignment

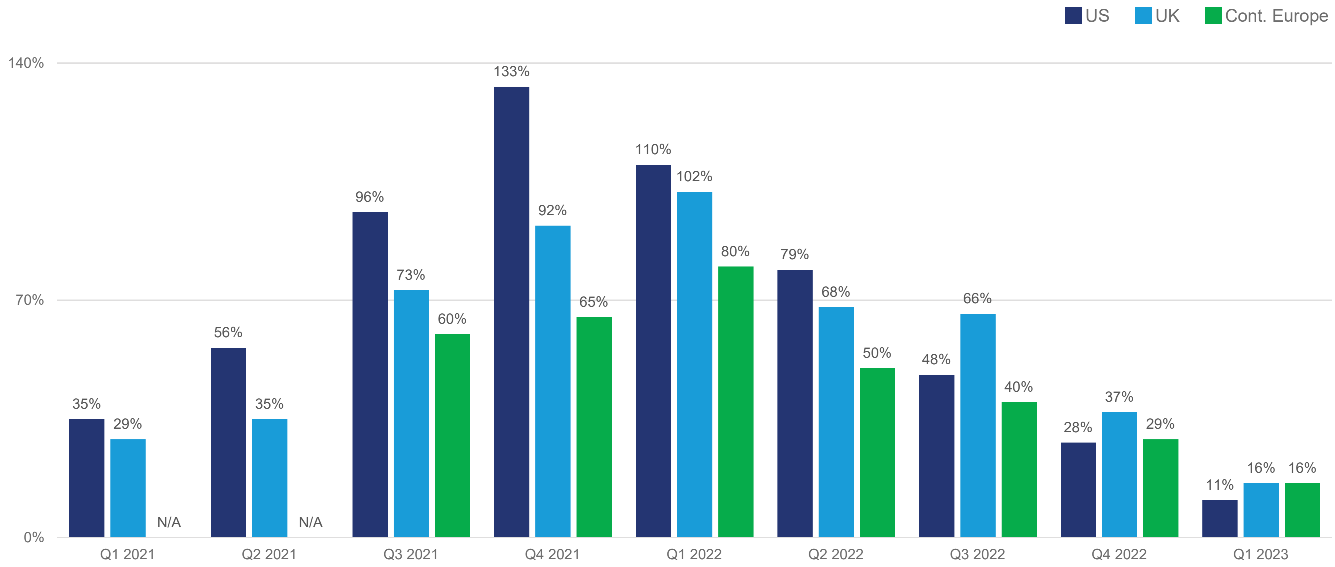
In 2019, an uptick in claims activity driven by ransomware began pushing the market toward unprofitability for the first time, and brought about cyber's first hard market cycle as it became a sizable standalone market. Initial rate increases coupled with limited reinsurance capacity supercharged rate rises, with many insureds experiencing nearly 200% cumulative rate increases since the first quarter of 2021.

Beyond the hardening of rates, the cyber market also saw a tightening in coverage. Policy forms looked explicitly at business interruption and contingent business interruption as key coverages impacted by subpar security hygiene and exercised additional scrutiny to deploy full limits. The most significant change to cyber coverages came from exclusionary language, particularly around Critical Infrastructure and War. Beginning in 2021 the Lloyd's Market Association (LMA) sought to guide the evolution in war exclusionary language culminating in mandate Y5381, which came into effect in April 2023.

Technology and data science have become a key part of developing cyber strategies as carriers look to collect and harness data to improve bottom-line returns. Scanning technology and suites of cyber security and breach response tools have become integral for insurers to better underwrite cyber risk and to improve their own view of aggregation. A comprehensive study by Marsh McLennan compared cybersecurity controls to claims activity to identify the effectiveness of various controls on loss frequency.[2] Figure 2 shows the 12 key security controls to reduce losses.

Insurtechs have been instrumental in embedding technology in underwriting with proprietary suites of software capturing extensive policy level data, identifying emerging trends by evaluating market wide claims information, and offering direct customer engagement to better inform and educate policyholders. The breadth of information captured by internal and external venders offers a granular look at portfolio aggregation and provides detailed estimates of event exposure, which is attracting meaningful support from traditional (re)insurers.

Figure 1: Quarterly Rate Change by Territory



Source: Marsh McLennan Cyber Analytics Center

[2] Marsh McLennan: Using Data to Prioritize Cyber Security Investments https://www.guycarp.com/content/dam/guycarp-rebrand/pdf/Insights/2023/Using_data_to_prioritize_cybersecurity_investments_report.pdf

Figure 2: 12 Key Cybersecurity Controls Identified by Marsh McLennan as Having a Large Impact on the Frequency of a Successful Cyber Event.

- **Multifactor authentication (MFA)**
- **Endpoint detection and response (EDR)**
- **Secured, encrypted, and tested backups**
- **Privileged access management (PAM)**
- **Hardening techniques, including remote desktop protocol (RDP) mitigation**
- **Logging and monitoring/network protections**
- **Email filtering and web security**
- **Patch management and vulnerability management**
- **Cyber incident response planning and testing**
- **Cybersecurity awareness training and phishing testing**
- **End-of-life systems replaced or protected**
- **Vendor/digital supply chain risk management**

Source: Marsh McLennan Cyber Analytics Center

Unlocking reinsurance capacity to fuel growth

Improvements in risk quality, a diversifying portfolio base, and a growing data set with which to feed catastrophe models are instrumental to attracting capital to the cyber market. The recent market cycle has expanded the range of reinsurance structures beyond quota shares and aggregate stop losses to better align risk appetite with reinsurance needs and has laid the framework for a true bifurcation of catastrophe risk from attritional loss. Event covers and nascent insurance-linked securities (ILS) structures have encouraged alternative capital to begin supporting cyber risk, which is expected to provide much-needed additional capital to support the ongoing market expansion.

As a maturing market, cyber sees a comparatively high cession to reinsurers versus other classes of business, with a median cession rate across Guy Carpenter's client base of 50%. High cession rates and a limited range of non-proportional structures are proving insufficient to support the rapid growth of the cyber market and fail to provide the flexibility an emerging market needs to adequately cover changing exposure bases. The surge in underlying rates and the increase in claims activity pushed reinsurers to limit their exposure by pushing loss ratio caps down on proportional treaties and reducing the risk of triggering cover by moving attachment points up on aggregate stop loss programs. Combined with the decrease in exposure, the resulting structures were less efficient than in previous years and consequently cedents began to explore alternative structure options, opening the door for new capital to enter the space.

Historically, in cyber, event covers have been a challenge due to the ambiguity in event definitions and the lack of confidence in modeled results, but a variety of wordings have emerged, allowing cedents to design a bespoke product that addresses key concerns grounded in modeled output. Event covers have created an opportunity to attract catastrophe-specialist alternative capital to the space as a first foray into the cyber market. Despite the rapid evolution of cyber insurance, insurance-linked securities (ILS) funds have been slow to enter the space. ILS funds rely on modeled output in conjunction with an understanding of the underlying risk to provide their investors with the level of comfort required to deploy capacity. Improvements in data quality coupled with poor performance from other catastrophe exposed lines has helped position cyber as a more attractive investment for alternative capital funds. Some progress was seen in 2022, with several transactions providing a stepping stone for ILS funds to bring new capacity to the market.

The changing reinsurance landscape and the beginning of a cyber ILS market is due, in part, to the increasing maturity of commercial cyber models. As the underlying data quality improves and the modeling continues to evolve, so will the ability of the cyber market to create a true view of an industry loss and ultimately draw new capacity into the space.

THE SIZE AND SHAPE OF THE INDUSTRY

Estimating a global 2022 written premium

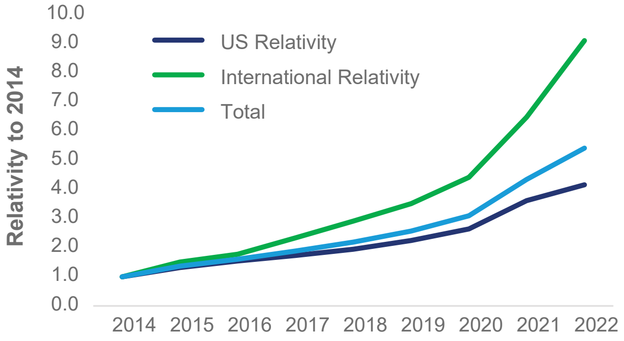
The cyber market has been growing consistently over 2 decades. However, there have been various challenges in attempts at robustly quantifying the size of the industry to date. This stems from the varying territories and distribution networks for the product, the transient nature of the growing exposure, as well as the nature of blended policy exposure by comparison to standalone. Guy Carpenter's Cyber Data Lake, which we will describe in more detail later, gives unique insights into the breadth and depth of the cyber insurance industry today. For the first time, we use it to infer the potential size of the global cyber insurance industry.

Guy Carpenter estimates the global 2022 cyber industry premium at USD 14 billion. This reckoning comprises standalone cyber policies as well as packaged/endorsement policies, from across the world. The methodology used has been compared against a variety of sources that have released global or partial estimates, and the access to Marsh McLennan proprietary information allows a deeper validation than other sources have available.

Cyber as a global product line

As global premiums grow, the footprint of where premium originates has also seen a change. While the majority of global premium is still generated by US-focused carriers, the UK and European markets have seen accelerated growth. Many of the large US cyber insurtechs are now focusing their expansion planning on the UK and European markets in order to capitalize on this rapid increase in growth.

Figure 3: The growth of international and US written premiums by year, based on Guy Carpenter client reported incomes since 2014.



Source: Guy Carpenter

Utilizing the extensive information that is available in Guy Carpenter's proprietary Cyber Data Lake, we can observe the historical premium growth trajectory and ascertain a real-time snapshot of the global cyber product line. Officially launched in 2022, the Guy Carpenter Cyber Data Lake is built upon the largest available dataset of actual policies, claims, portfolio experience and vendor model outputs. It demonstrates the full breadth and depth of Guy Carpenter's big data analytics as compared with other synthetic "Industry Exposure Databases" in the market. Breaking down the exposure base by premium, an inference to the global level of allocation can be shown that has certain central hallmarks while exhibiting some regional nuances.

Table 1: Exposure Breakdown by Country

Country	Proportion of global premium income
US	62.5%
UK	9.3%
Canada	6.4%
Germany	6.1%
France	2.1%

Source: Guy Carpenter

Table 2: Exposure Breakdown by Industry

Industry Sector Standard Industrial Classification (SIC)	Proportion of global premium income
Services	42.6%
Finance, Insurance and Real Estate	14.6%
Manufacturing	14.4%
Retail Trade	9.9%
Non-classifiable	8.0%

Source: Guy Carpenter

Table 3: Exposure Breakdown by Revenue Band

Organization Size	Proportion of global premium income	Revenue Band
Large	41.7%	USD 1 billion-plus
Medium	19.8%	USD 250 million to 1 billion
Small	26.8%	USD 10 million to 250 million
Micro	11.6%	0 to USD 10 million

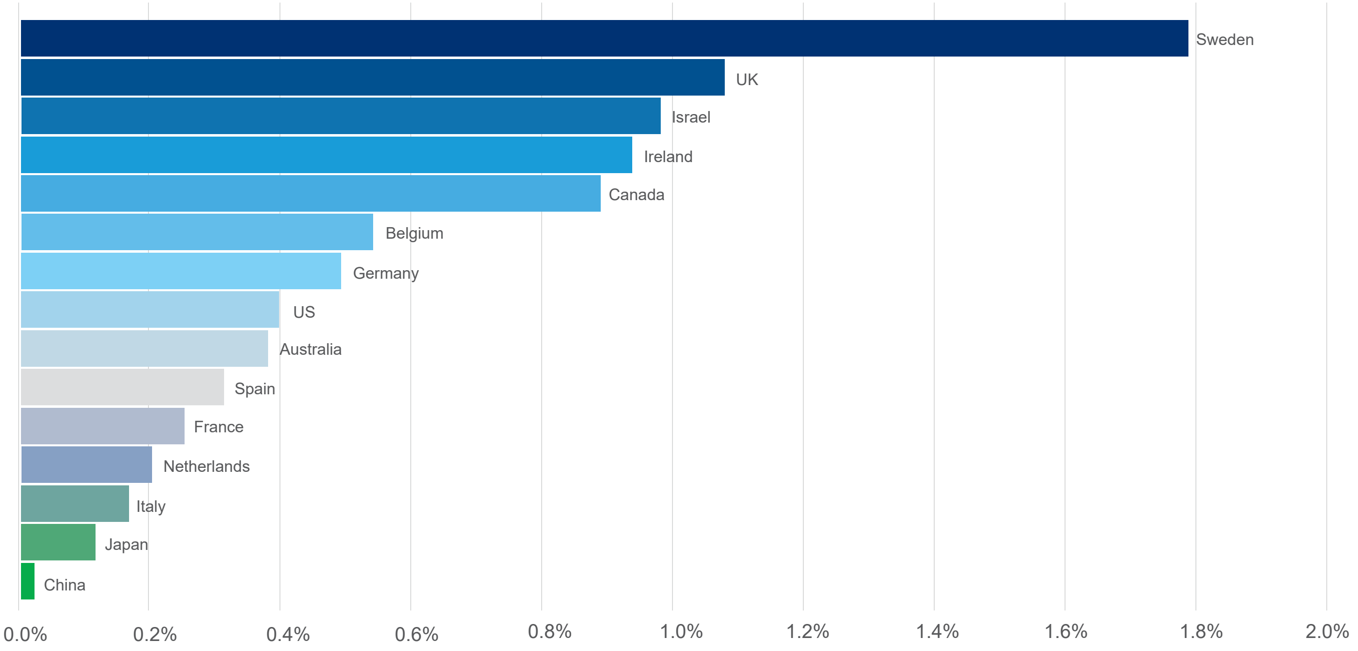
Source: Guy Carpenter

The geographic breakdowns above confirm that the US continues to be the largest market by some distance, with international growth accelerating. When we review country splits set against total non-life premiums estimated by country, we see the relative representation of cyber varies considerably. This helps identify those territories where the cyber product has found its market most successfully among insurance buyers.

In Figure 4 below, we examine the largest 15 country contributors to our cyber premium breakdown. There are some relative surprises here, such as Sweden, which is leading the way with a projected cyber penetration share somewhat in excess of the UK, which is in second place. Despite the dominance of the US cyber market, the balance of the much larger non-life penetration in the market means cyber is 0.4% of the total. This follows from the fact that the US market accounts for approximately 50% of non-life premiums globally. These assessments give us valuable context for cyber in each national market.

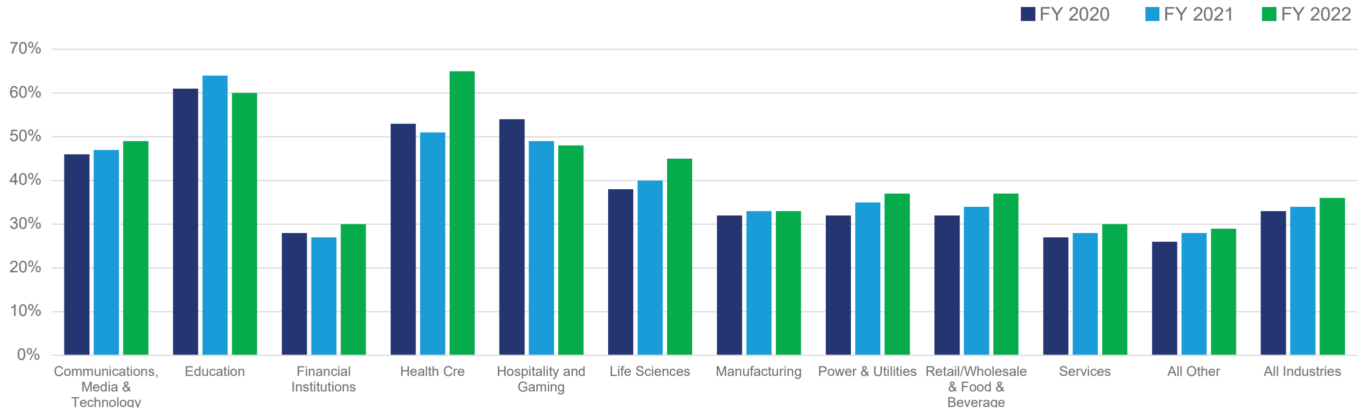
We should note that our assessment suggests global cyber product penetration is still some way below other classes, albeit with significant variation by territory and industry. While distribution and product awareness are growing among small and medium-size enterprises (SMEs), penetration rates show that actual purchasing lags far behind other classes. Coverage variation further exacerbates the insurance coverage gap.

Figure 4: Cyber as Proportion of Total Non-Life Premium



Source: Guy Carpenter

Figure 5: Cyber Insurance Take Up Rates by Industry



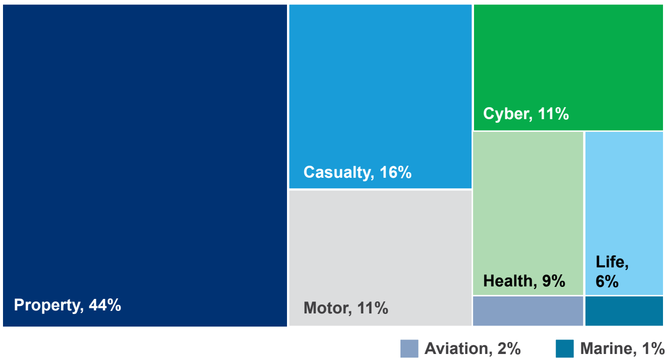
Source: Marsh Specialty and Global Placement (All US Marsh Clients)

Our research indicates cyber insurance penetration averages at 36% for Marsh's US client base. In the UK, penetration rates are at 38% average across Marsh's UK Risk Management clients, but for technology, media and financial institutions this penetration increases to closer to 60%. Industries like manufacturing, heavy industry and utilities are lower at around 20%. But penetration rates fall further in the mid-market and corporate sectors to approximately 26% and just over 10% respectively.

Cyber as an increasingly heavyweight class of business

It is evident that cyber has achieved the critical mass reflective of a core insurance product line. The below infographic sets out the relative "mentions" of different classes of business on earnings calls among a cross-section of the insurance industry. These calls cover a range of themes of relevance, but they can act as a useful barometer for the attention of company executives.

Figure 6: Total hits by topic (2022 distribution)

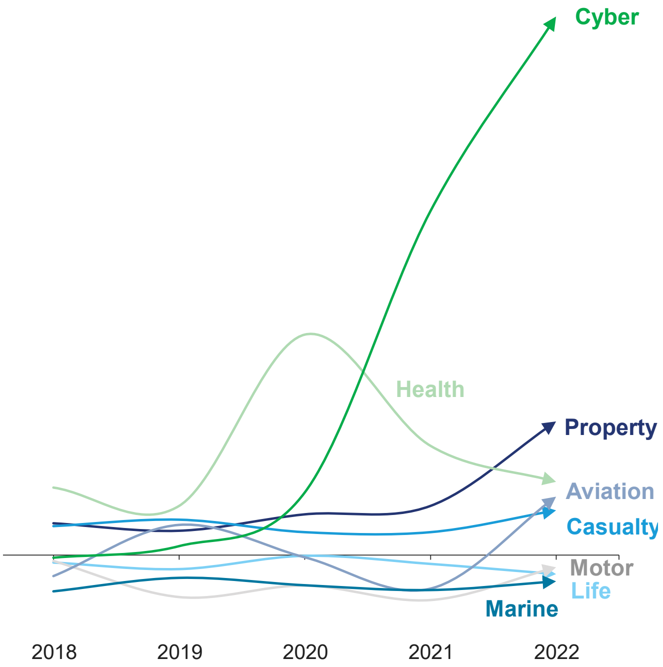


Source: Alpha Sense—Earnings conference call transcripts

Cyber commentary now occupies a growing share of the dialogue that industry leaders have with their shareholders. This weighting is notable in that it is larger than the current market size of the cyber product compared with other classes, which helps signpost the growth trajectory.

When we interrogate this in greater depth, we have seen a rapid growth over the last few years in this focus. The figure below sets out the relative movement in earnings call commentary of cyber set against other established classes of business.

Figure 7: Total hits by topic, rebased to 2015 (2018-2022)



Source: Alpha Sense—Earnings conference call transcripts

When examining this data set, we see that the relative growth in focus on cyber commentary even outstrips that of health commentary during the COVID-19 pandemic. It is apparent from this information that cyber is now increasingly an overarching strategic theme for the industry. While dialogue of earnings calls is not necessarily a proxy for the size of the market presently, it is likely to be predictive of the future as cyber outgrows many traditional product lines. This has made the focus on the potential downside risk to the industry all the more important. In support of this, it is noteworthy that the cyber market has passed the global aviation market in premium size and is likely to pass the marine market in the next few years.

Product needs by territory and the backdrop of regulation

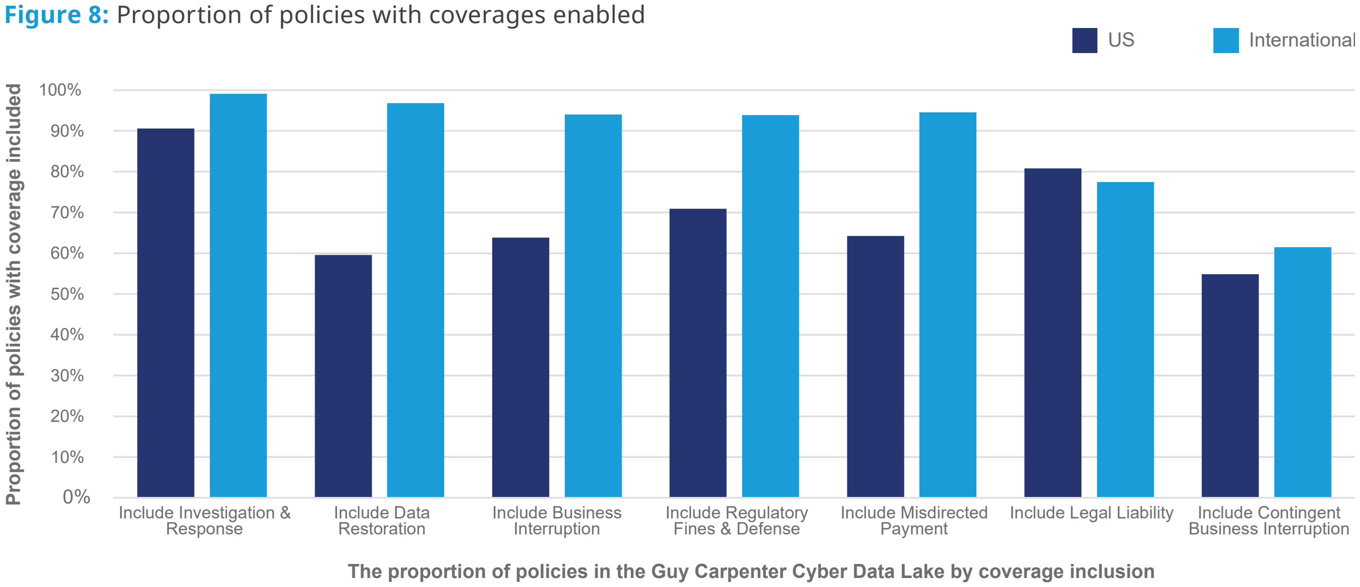
Historically, the drivers for cyber purchasing have been data privacy legislation, most notably in the US, and more recently, the General Data Protection Regulation (GDPR) in Europe and Critical Infrastructure Regulation in Australia. The prolific increase in ransomware attacks—and subsequent business interruption losses—saw the demand for cyber insurance increasing for heavy industry, manufacturing, energy, logistics and other areas, for companies across the Americas, Europe and Australia.

Globally, while we have seen the introduction of data protection laws in many more territories, we have not always seen a corresponding increase in cyber purchasing. We note heavy regulation in territories such as the US, Europe and Australia, where there is greater uptake in cyber insurance, but the awareness of cyber risk is higher in these countries. However, Asia, Latin America, the Middle East and North Africa, where cyber regulation is increasing, are recently experiencing growth in cyber offerings but take-up rate of cyber insurance remains relatively low.

The global cyber product increasingly taps into a diverse array of insurance buyers, and coverages have evolved to meet that demand. Figure 8 below sets out the increasing breadth of coverages found within the product and their respective levels of take-up across the market. The figure provides a flavor of the level of product coverage, as well as data capture across US and international territories.

> **"THE INDUSTRY C-SUITE RECOGNIZES THE ROLE OF ROBUST ANALYTICS IN ATTRACTING CAPACITY AND GROWING THE CYBER MARKET. MOODY'S RMS HAS A LONG HISTORY OF DEVELOPING SPECIALTY CLASSES THROUGH TECHNICAL EXPERTISE, INVESTMENT AND INDUSTRY COLLABORATION. OUR COMMITMENT TO CYBER IS SIGNIFICANT, AND WE WILL CONTINUE TO HELP THE MARKET BUILD RESILIENCE AND DEVELOP NEW OPPORTUNITIES,"**
>
> **Diya Sawhny, Head of Strategy, Moody's RMS**

Figure 8: Proportion of policies with coverages enabled



Source: Guy Carpenter

THE GLOBAL CYBER ACCUMULATION POTENTIAL

Introduction

A healthy cyber market needs to be built on the foundation of a strong modeling framework. The expertise, tools and technology have advanced significantly since the inception of the first cyber vendor models approximately 8 years ago. As exposure data has improved, the potential exists to explore the size of an industry loss. Guy Carpenter first considered the potential for US industry loss in our 2019 report *Beyond the Clouds*.

The emergence of new capital to serve the market necessitates a growing collective understanding of cyber quantification. This does not mean narrow views that are not sufficiently dynamic or suffering from anchor bias. Unlike individual modeling tools, aggregation models are more concentrated, with 3 primary platforms with a significant and longstanding investment in this space.

In this section, we provide an assessment of the implied market losses across the 3 vendors with the longest pedigree in this class, CyberCube, Guidewire Cyence and Moody's RMS, each with several versions and a continually evolving view of the risk. The evaluation of a global cyber accumulation has been performed using only the aggregation components of the vendor models, with all of them providing an additional attritional model, which was deemed out of scope for inferring cyber catastrophe losses. This methodology allows this study to have a stronger foundation for effective comparisons.

The results make clear that there are still varied views to the potential quantum of the extreme tail. This variation is lower than it has been at any point in the past, but still reflects some of the challenges of assessing extreme downside scenarios. Guy Carpenter always recommends focusing as much on the "why" as the "how much" of model divergence.

Evaluating the vendor platforms

Over the years, cyber catastrophe models have gone through many iterations, updates and scrutiny. As part of our risk management services, Guy Carpenter deploys a number of cyber models to provide our clients with a range of cyber risk analysis tools.

Each model vendor is unique in its offering and novel in its approach to accumulation modeling. This may stem from the scenario framework or the data used to parameterize these models. While this is a strength, it makes a direct comparison between them a particular challenge. However, Guy Carpenter developed an approach to bring a consistent view across the 3 key vendors by categorizing scenarios into common themes of event type. In this endeavor, we can create event distributions for the most material of cyber events and add another layer of understanding on vendor interpretation.

When evaluating the usage of the different catastrophe models, Guy Carpenter has considered the following factors:

- **Scope of coverage:** Different models may cover different categorizations of risks for individual threat types, industry verticals or geographic areas. It is important to assess which models align with the specific risks and exposures of portfolios.
- **Data sources:** Catastrophe models rely on comprehensive granular data to develop risk scenarios and assess potential losses. Key considerations include the quality and accuracy of data captured, its predictive power, and its sensitivity from a modeling perspective.
- **Methodology:** Each catastrophe model uses its own framework to assess risk, and these methodologies can vary widely. Guy Carpenter evaluates the strengths and limitations of each methodology and its suitability and fitness for risk management strategies.
- **Transparency and validation:** It is important to evaluate the transparency of the model and the extent to which the model has been validated against historical events, which can help ensure the accuracy and reliability of risk assessments.
- **User experience:** Finally, the usability of each model and the ease with which clients can access and interpret the model's results heavily influence its success. This can help ensure that clients are able to use the model effectively to manage their risks.

Overall, by carefully evaluating the differences between catastrophe models, Guy Carpenter can help our clients make informed decisions about their risk management strategies and ensure that they are effectively managing their exposures.

Modeling a global industry loss

Headline views

To model a global industry event loss, Guy Carpenter leveraged the proprietary exposure database from

Table 4: Occurrence Exceedance Probability (USD)

Return Period	CyberCube V4	Cyence M5	Moody's RMS V6
Global			
50	24,373 million	9,964 million	5,530 million
200	33,370 million	25,768 million	15,631 million
US			
50	16,859 million	6,612 million	3,512 million
200	23,360 million	17,619 million	10,009 million
International			
50	8,271 million	3,511 million	2,384 million
200	10,694 million	9,493 million	6,053 million

Source: Guy Carpenter

the Guy Carpenter Cyber Data Lake. The Cyber Data Lake encompasses 1.8 million actual cyber policies with detailed terms and conditions in the latest calendar year alone, representing more than USD 6 billion of gross written premium. This robust exposure database, along with extensive claims listing, catastrophe model outputs and cyber reinsurance treaty metrics, provides a credible foundation for the global industry loss study and in-depth validation analyses.

Guy Carpenter then examined the market exclusions that currently exist across the client base and compared them to the scenario selection from the vendor models. To provide an accurate representation of how a global insured loss could manifest, the scenarios that Guy Carpenter determines as being excluded have been removed from the analysis.

Using the USD 14 billion industry premium estimate and policy details from the Guy Carpenter Cyber Data Lake, a set of portfolios was constructed to model geographical segments of the industry and extrapolate up to represent the global premium. This methodology allowed considerations for the geographical exposure mix, the rate environment in the prior years, and the portfolio record size to be taken into consideration. In the table above, we represent the results broken out by the combined global view, the US domiciled market and the international segments (non-US domiciled).

The table above highlights a large amount of variation for the models at a global scale, reducing towards the extreme tail. The international segment shows losses of around half the size of the US segment, or a third of the global loss.

Interestingly, we are seeing proportionately greater variation in lower return periods than higher. This is not necessarily intuitive given that lower return periods are likely to be more informed by experience and counter-factual analysis. This suggests that we as an industry need to focus carefully on a collective interpretation of what recent events and near-misses have taught us.

Regional differences

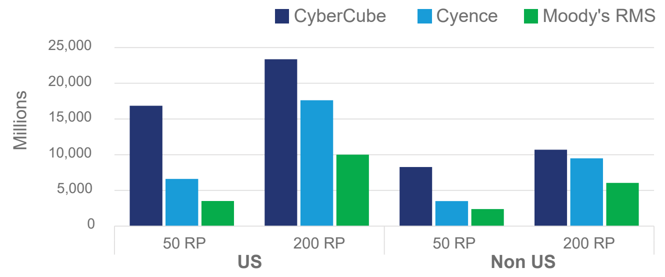
When comparing the impacts of a modeled cyber event across the world, the vendors have a different view of the relative impacts of a non-US event versus one that is localized to the US.

There are 2 aspects that need to be considered for the international market. Firstly, the firmographic and technographic composition of the region. This is driven by regional software vendors and infrastructure platforms, and the nuanced threat landscapes in which these entities operate. Secondly, the understanding of cyber resiliency across jurisdictions and how that aligns with regulatory and reporting requirements is needed. This can have a consequential effect in recovery efforts in the instance of a cyber event and the resulting financial loss.

We can see that the vendors have included considerations for how different regions outside of the US will react to cyber events by the change in observed relativities between the regions. However, there is further research and data required as the suitability of the scenarios and the accuracy of parameters linked to these jurisdictions will be more closely scrutinised as the international market develops.

This is reminiscent of the initial iterations of the vendor models, where parameterization of the US SME market was derived at a time when reference data was not readily available and visibility of the impact of events relied heavily on broader assumptions. The reliance on broader regional assumptions goes some way to describe the convergence that is observed for the 200 return period.

Figure 9: Geographical Breakout

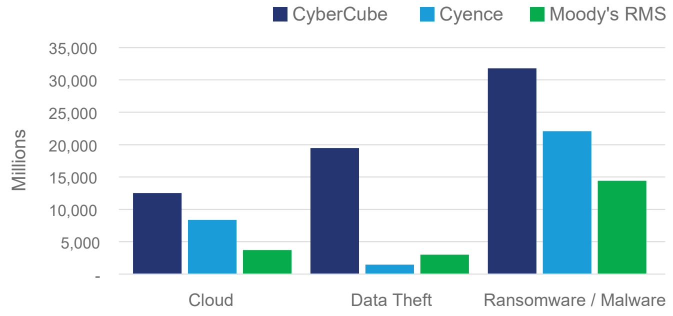


Source: Guy Carpenter

Event drivers

Using the Guy Carpenter method of categorizing scenarios, the comparisons for each of the methods become more succinct.

Figure 10: 1:200 Scenario OEP



Source: Guy Carpenter

Looking across the scenario set, the key scenarios that emerge are the cloud, data theft and ransomware/malware scenarios. When viewing these in terms of the quantum of loss generated, there is consensus among the vendor models that *ransomware/malware* events are the largest driver of losses in the 200-year return period. The results mirror the market consensus in that *ransomware/malware* events are the key events of concern. When digging deeper into the vendor movements, the differentiating factor between the vendors is the footprint of affected insureds. Cyence and Moody's RMS have a moderately lower footprint in comparison to CyberCube, whereas the average severity per company between all 3 models is relatively similar. This results in the divergence that is observed for this event.

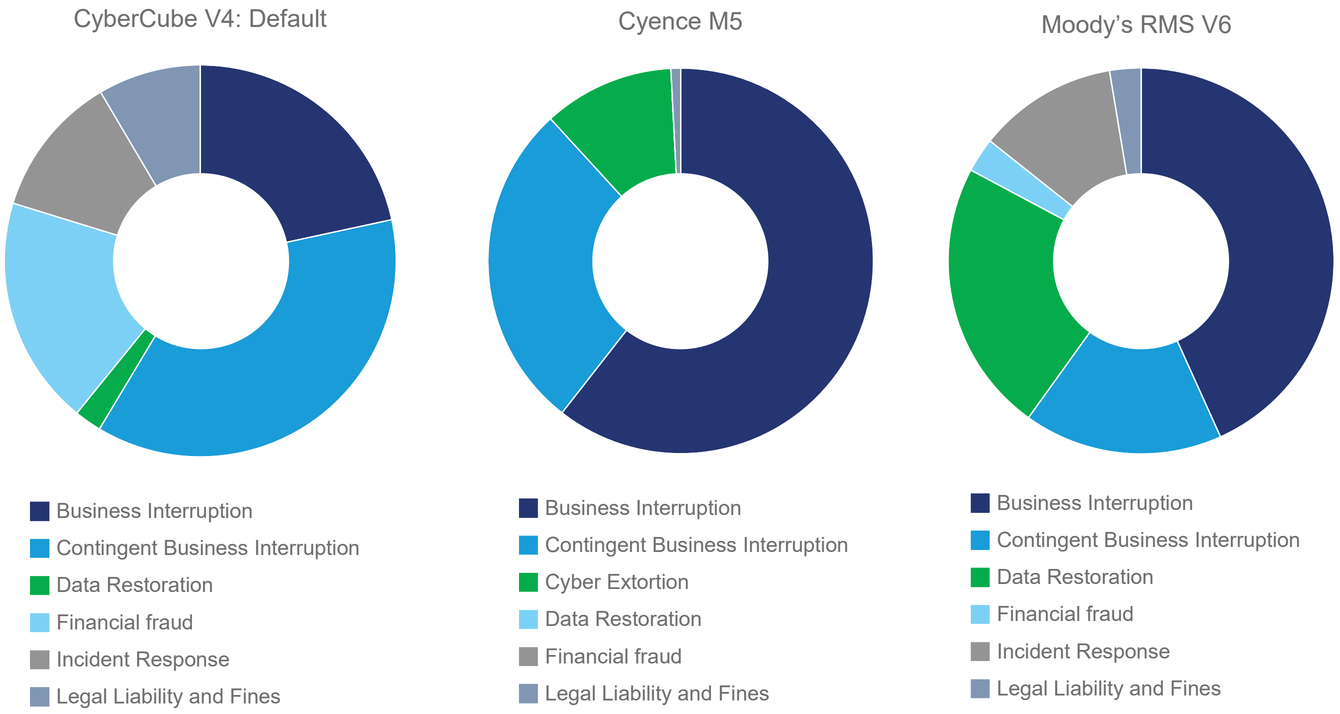
Cloud events yield relatively lower loss levels compared with ransomware/malware events. However, the vendor models understand the robust contingency measures built into cloud service providers through the adoption of multiple Availability Zones across corresponding regions. As such, any historical outage that has been observed across hyperscalars has thus far not been material beyond only a few hours. Given the technical challenges and lack of historical precedents, *cloud outage*-based events of a comparable severity to *ransomware* events are parameterized to occur far beyond the 200-year return period. On the modeling front, the footprint-severity parameters are in contrast to what is observed for *ransomware/malware*, as all 3 vendors exhibit very similar assumptions regarding footprint of insureds affected. The only differentiating factor between them is the average severity per company affected, where CyberCube exhibits the largest parameterization and Moody's RMS, the lowest.

Data theft events are those where we observe the most divergence among the vendors with CyberCube being the most significant of the 3. Cyence and Moody's RMS interpret the event as the least material of this subset in the 200-year return period, whereas CyberCube's interpretation proves larger than cloud events. The latter parameterizes a multitude of data theft scenarios compared with Cyence and Moody's RMS—each of which vary in its technographic parameterization. The scenario narratives that CyberCube deploys are much broader in its consideration of a wide range of data breach events and triggers. This lends to a debate on what is considered a true data breach catastrophe event among the vendor models.

Furthermore, CyberCube's scenario parameterization takes into account specific data breach cost fallouts such as financial fraud, which is one of the most significant loss contributors. While Moody's RMS does model financial fraud, it is parameterized significantly lower

> **"THERE IS A NEED FOR A STRONG DATA-DRIVEN FOUNDATION TO GROW CAPACITY. THIS ENCOMPASSES BOTH DATA SIGNALS RELATED TO EXPOSURE AS WELL AS LEARNING FROM PRECEDENTS AND EXPERIENCE TO REFINE MODELS. MODEL STABILITY WILL PROVE THE FOUNDATION FOR GROWING THE MARKET TO REACH ITS TRUE POTENTIAL,"**
>
> **Charles Clarke, Group Vice President, Guidewire Analytics Sales & Advisory**

Figure 11: Breakdown by Cost Components



Source: Guy Carpenter

than CyberCube. Conversely, Cyence does not explicitly model the component. These factors are what creates the divergence in views across the vendors for data breach events.

Cost component drivers

Similar to the scenario framework, Guy Carpenter has a framework to assess vendor model cost components. The definitions of the model cost components vary between the vendors, which makes direct comparisons challenging. By allocating the losses to defined categories, the models can be more easily compared and contrasted.

Previously in the 2019 study, business interruption costs were the largest single component of the insured loss for *cloud* and *ransomware* scenarios, with the contribution ranging from 49% to 94% at the 200-year event. Since then, there has been a marked realization of the impacts that supply chains and third-party dependencies can have on a company, and this has been reflected by the models. Business interruption still plays a driving factor in the losses, but contingent business interruption now contributes from 16% to 37% of a 1-in-200-year event.

The exhibits above show the breakdown of a global 200-year event by the top 6 cost components for each of the vendors.

Interpretation

From the modeling results, there is still a notable and significant diversion between the default outputs from the vendor models. When we analyze this more deeply, the variation is most noteworthy for ransomware and cloud scenarios. This is expected in the scenario tails, where assumptions and modeling methodology drive the outcomes.

Historical precedents and counterfactuals provide a valuable way to validate vendor modeling results. They can inform the suitability of vendor models and provide insight into relevance of scenario parameterization. That being said, careful consideration is required in how these interpretations are derived. The cyber market has yet to observe events akin to a 200-year return period, but despite this, there is a degree of convergence between the vendor model at this range of the exceedance probability. In contrast, there is a plethora of data points to inform the lower return period view but the modeled results shows significant divergence. It is apparent that there is still some degree of expert judgment that influences the modeling in lower return periods.

In contrast to its footprint presented in our 2019 report, the cyber industry has developed much more globally. This is reflected in the significant contribution of modeled loss that has emerged, although there remains large scope for further uptake and insurance penetration.

Evolution from Beyond the Clouds

Since the 2019 study, the cyber threat landscape has evolved, and the causes for concern have advanced alongside:

- **Increased reliance on cloud services:** In 2023, businesses are likely to be even more reliant on cloud services than they were in 2019.
- **Greater interconnectivity:** The increased interconnectivity of systems and devices in 2023 means that a cyber attack on a leading cloud-service provider could have even wider-reaching effects.
- **Advancements in cyber attack techniques**: In 2023, cyber attackers are likely to have access to more advanced techniques and tools for carrying out attacks.
- **Regulatory environment:** In 2023, there may be more stringent regulatory requirements for cyber risk management and reporting, which could result in greater scrutiny of insurers and reinsurers in the event of a cyber attack.
- **Changes in insurance market dynamics:** The cyber insurance market is expected to continue growing in 2023, with more insurers and reinsurers entering the market. The evolution of this market increases the ability of a systemic event to have a significant impact to the balance sheets of insurers and reinsurers.

As well as threat landscape movements, clearly the shift in the exposure and the modelling approaches has had a big impact. The significant compounded underlying rate increases that have moved through the industry has depressed tail-side metrics in loss ratio terms. Finally, models themselves have revised their view of the risk over the last 4 years, generally down based on the learnings from experience.

Proxies with other classes

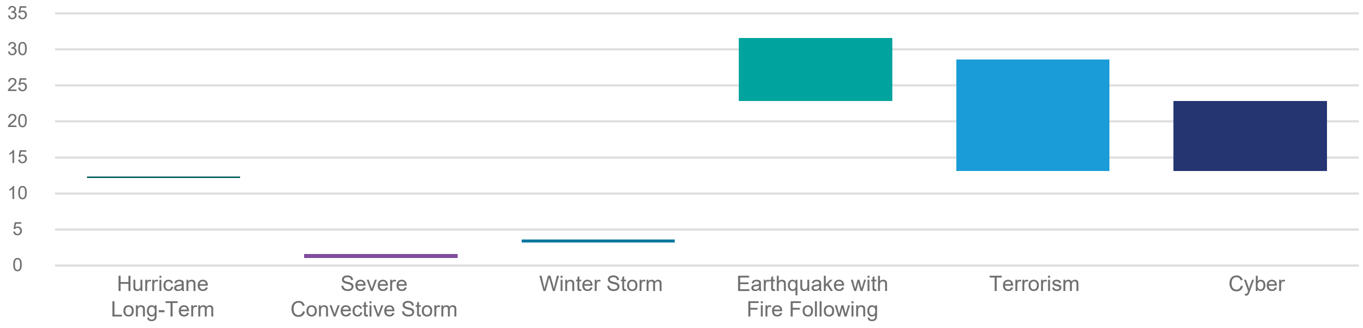
To put cyber as a class of business into context within the insurance market, we can compare the variation in other catastrophe perils across vendor models. This helps give valuable context for the classes' interpretation for potential capacity providers.

The cyber scenario ratios are not as convergent as the hurricane and storm scenarios. However, these are scenarios with a high frequency of events and long-gathered data on exposure. Instead, they are more in line with earthquake and terrorism, where the frequency of large, historic events is much lower. As time passes, it is likely this range will narrow further.

> **"AS CYBERCUBE LOOKS TO NEW MODEL VERSIONS, WE REFLECT ON A GROWING GLOBAL CYBER MARKET AND A PRESSING NEED TO BRING NEW CAPITAL INTO THE SECTOR. DIVERSIFYING THE SOURCES OF CAPITAL FROM TRADITIONAL (RE)-INSURANCE TO CAPITAL MARKET CHANNELS WILL HELP ACHIEVE A RESILIENT, LONG-TERM CYBER INSURANCE INDUSTRY,"**
>
> **Ashwin Kashyap, Chief Product Officer, CyberCube**

As we reflect on this, we see cyber sits firmly within the range of a class with an extended tail and a high degree of uncertainty, but not in the realms of unfamiliarity for insurers, reinsurers and investors. While precedents and modeling evolve, the relative convergence or divergence between the models will be closely followed, which will bring comfort to sources of potential capacity for the future.

Figure 12: 200 Tail to Mean Ratio



Source: Guy Carpenter

CONCLUSIONS

From its nascent beginnings as a bolt-on to technology errors & omissions to the first-party coverages that emerged and subsequently evolved over the past decade, it is apparent that the cyber market has become a much more significant constituent of the global insurance industry. At no time in the past has it had as much critical mass as it has now, and there are no signs of slowing down. Although penetration levels are still lower outside of the US and Europe, the class is growing in its global footprint. Over the next 10 years we are likely to see a greater convergence toward the more even split between the US and the rest of the world than we see in other classes.

Modeling platforms such as those referenced in this report continue to grapple with the potential for accumulation losses. The class of business now stands comparable to specialty classes in premium but is dwarfed by ubiquitous exposures such as property. However, the nature of relatively geographically-focused perils that constrains the downside impact for property perils is not the same in cyber. The industry needs reliable models that are invested in the class, and to hone and improve their offerings for the good of end users. This is the case both at the academic extremes of 1-in-200-year losses, as well as in lower return periods where modeling needs to have more of an empirical foundation.

As we examine the tail-side metrics set out in this report, we do well to consider carefully the context. Here, we set out 1-in-200-year occurrence exceedance probability metrics that range from USD 16 billion to USD 33 billion. These are very meaningful numbers that far exceed what has been experienced in the class. To date, the market has observed a multi-billion dollar loss in NotPetya, but the bulk of its USD 3 billion total did not fall on the cyber market. However, the rate of growth of these projections is notably lower than the growth of the premium base, as we see when we compare this with our 2019 report. This speaks to the evolution of the product, exposure and modeling methodologies. These factors should all be encouraging signals for stakeholders contemplating engaging this profitable class.

The improvements to data quality and nimbleness of the cyber models are instrumental in continuing to attract capital to the cyber market. As the models continue to evolve, reinsurance buyers and sellers will be able to hone in on what truly differentiates each portfolio and more accurately identify, price and trade key catastrophe risk. As structures evolve to laser out catastrophe events, reinsurance buyers will have more choice in how they manage their portfolios and the diversity that arises from divergent buying strategies will expand the opportunities for capital to flow into the market, thus feeding its ongoing growth.

We can see how far the market has come to broaden into the global product line we have today, however we are at a crossroads. In order to unlock the broader potential of the class and take the next step necessary to close the penetration gap, we need to solve the capacity crunch together. This means efficiently matching up risk and capital across the transaction chain, from insurance and reinsurance products to retrocession. Innovating the shop window of cyber products is a key step, and this can be achieved on the shoulders of a maturing modeling foundation that builds the necessary trust.

There is no question that hypothetical losses from a significant cyber event would impact the market, as this report demonstrates. However, given the industry's resilience to significantly greater losses from other classes, in most cases these should not be insurmountable. Industry leaders and insurance entrepreneurs recognize this and spy opportunities for continued growth and performance in this sector. As we contemplate what lies ahead, the focus must continue to be on further activating this valuable product category with commensurate traditional and alternative capacity. We do well to recall that our customers' risk is our business, and herein lies the opportunity.

THE IMPROVEMENTS TO DATA QUALITY AND NIMBLENESS OF THE CYBER MODELS ARE INSTRUMENTAL IN CONTINUING TO ATTRACT CAPITAL TO THE CYBER MARKET.

Appendix

The scope of the study was global standalone and packaged policies. The loss estimates in this report are an attempt to quantify a cyber catastrophe loss quanta across the globe. The loss estimates do not represent losses arising from non-affirmative cyber coverage.

In addition, the study looked at the industry as a whole. However, this masks the fact that individual carriers with different policy wordings, different portfolios of companies, for example, industry mix and company size, and different underwriting strategies, will have very different losses from these catastrophic events. To understand the impact of these scenarios on a particular book of business, modeling needs to be run on that book of business. The natural catastrophe and terror results are based on the US industry exposure set in Moody's RMS Risklink v21 and AIR v8.

Contacts

Anthony Cordonnier

Global Co-head of Cyber
Anthony.Cordonnier@guycarp.com

Erica Davis

Global Co-head of Cyber
Erica.Davis@guycarp.com

Additional contributors:

Afsar Ali

Jess Fung

Siobhan O'Brien

Jamie Pocock

Grace Seigle

Bimal Shah

Disclaimers

This report, and the analyses, models and predictions contained herein ("Information"), includes data compiled using proprietary computer risk assessment technology of Risk Management Solutions, Inc. ("RMS"). Such Information constitutes RMS confidential and proprietary information and trade secrets. The technology and data used in providing this Information is based on the scientific data, mathematical and empirical models, and encoded experience of scientists and specialists (including without limitation: earthquake engineers, wind engineers, structural engineers, geologists, seismologists, meteorologists, geotechnical specialists, mathematicians and cyber security experts). As with any model of physical systems, particularly those with low frequencies of occurrence and potentially high severity outcomes, the actual losses from catastrophic events may differ from the results of simulation analyses. Furthermore, the accuracy of predictions depends largely on the accuracy and quality of the data used in the analyses and models. The Information is provided under license to Guy Carpenter & Company, LLC ("Guy Carpenter") and is either Guy Carpenter's or RMS's proprietary and confidential information. The recipient of this Information is further advised that RMS is not engaged in the insurance, reinsurance, or related industries, and that the Information provided is not intended to constitute professional advice. IN NO EVENT SHALL RMS (OR ITS PARENT, SUBSIDIARY, OR OTHER AFFILIATED COMPANIES) BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES WITH RESPECT TO ANY DECISIONS OR ADVICE MADE OR GIVEN AS A RESULT OF THE CONTENTS OF THIS INFORMATION OR USE THEREOF.

The data and analysis provided by Guy Carpenter herein or in connection herewith are provided "as is," without warranty of any kind whether express or implied. The analysis is based upon data provided by the company or obtained from external sources, the accuracy of which has not been independently verified by Guy Carpenter. Neither Guy Carpenter, its affiliates nor their officers, directors, agents, modellers, or subcontractors (collectively, "providers") guarantee or warrant the correctness, completeness, currentness, merchantability or fitness for a particular purpose of such data and analysis. The data and analysis is intended to be used solely for the purpose of the company internal evaluation and the company shall not disclose the analysis to any third party, except its reinsurers, auditors, rating agencies and regulators, without Guy Carpenter's prior written consent. In the event that the company discloses the data and analysis or any portion thereof, to any permissible third party, the company shall adopt the data and analysis as its own. In no event will any provider be liable for loss of profits or any other indirect, special, incidental and/or consequential damage of any kind howsoever incurred or designated, arising from any use of the data and analysis provided herein or in connection herewith.

Statements or analysis concerning or incorporating tax, accounting or legal matters should be understood to be general observations or applications based, solely on our experience as reinsurance brokers and risk consultants and may not be relied upon as tax, accounting or legal advice, which we are not authorized to provide. All such matters should be reviewed with the client's own qualified advisors in these areas.

GuyCarpenter

About Guy Carpenter

Guy Carpenter & Company, LLC is a leading global risk and reinsurance specialist with more than 3,400 professionals in over 60 offices around the world. Guy Carpenter delivers a powerful combination of broking expertise, trusted strategic advisory services and industry-leading analytics to help clients adapt to emerging opportunities and achieve profitable growth. Guy Carpenter is a business of Marsh McLennan (NYSE: MMC), the world's leading professional services firm in the areas of risk, strategy and people. The Company's 83,000 colleagues advise clients in 130 countries. With annual revenue of nearly $20 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses including Marsh, Mercer, and Oliver Wyman. For more information, visit www.guycarp.com and follow us on LinkedIn and Twitter @GuyCarpenter.

©2023 Guy Carpenter & Company, LLC. l 1166 Avenue of the Americas, New York, NY 10036 l +1 (917) 937-3000 A business of Marsh McLennan