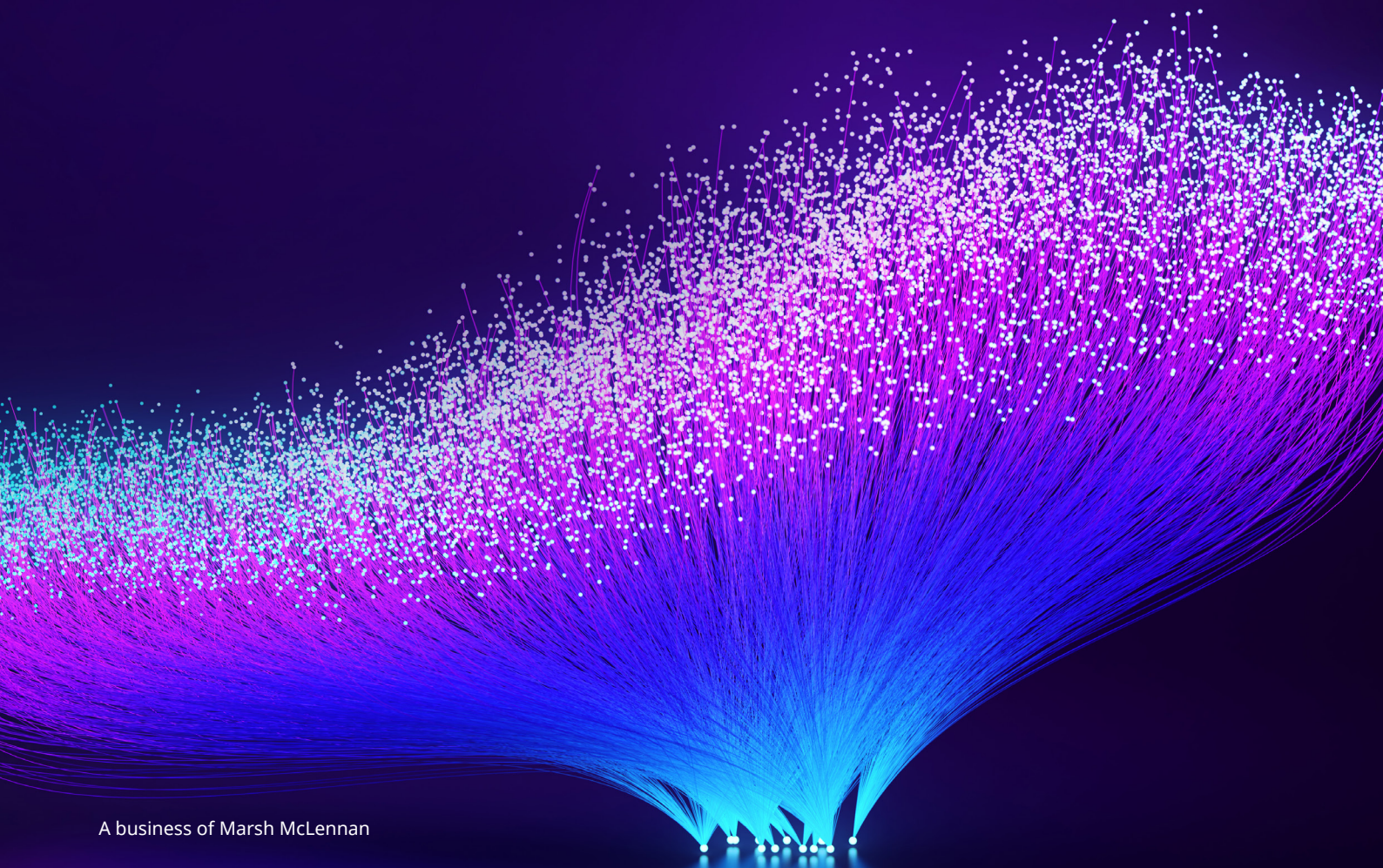
GuyCarpenter

Behind the Firewall:

2024 GLOBAL CYBER INDUSTRY INSIGHTS



A business of Marsh McLennan

CONTENTS

EXECUTIVE SUMMARY

In this report, we quantify the growth of the cyber market, which continues to evolve as a core class of insurance. Our approach consists of a comprehensive assessment of the size of the cyber industry by key regions, which, in turn, informs our view of the global cyber market.

As the market continues to expand, capacity providers, carriers, third-party services firms, and other members of the cyber ecosystem are contemplating new opportunities to grow without compromising performance. To support them on this journey, this study provides valuable insights on multiple dimensions of the cyber market.

In our previous report, our assessment looked at the US and non-US market segments. This year, we delve deeper into these segments and investigate the regional differences between North America (NA), Europe, Asia-Pacific (APAC) and the Rest of the World (ROW). This highlights the importance of grasping the geographic nuances of market development in key growth regions, and the underlying sensitivities that fuel their potential for growth.

After very large compound rate increases in 2021 and 2022, the market has stabilized while experiencing modest softening in certain areas. Rates flattened or decreased in 2023, continuing to adjust throughout 2024. This has culminated in a market that has expanded to an estimated USD 16.6 billion in 2024, with NA making up the majority at USD 10.5 billion, Europe at USD 3.9 billion, APAC at USD 1.7 billion and ROW at USD 0.5 billion. New growth to the industry is being driven by under-penetrated industry segments, developing regions and new products.

Alongside this growth, we are also investigating the aggregation potential these regions present through our vendor model partners. We see that divergence between models is partly driven by differences in interpretation of cyber events and how these can materialize. The modeled global aggregation loss potential for the industry varies from USD 20 billion to USD 46 billion for 2024 at the 1-in-200-year return period (RP), leading to a market loss ratio between 120% - 277%.

This emphasizes the contrasting perspectives among vendors in the face of escalating cyber activity and heightened geopolitical tensions globally, which have shifted the threat actor *modus operandi*. As a result, the cyber landscape has become more adversarial, causing actors to adopt emerging technology within their campaign operations. Organizations have responded accordingly and begun to deploy the same emerging technologies for defensive purposes against such campaigns.

Evolving tactics, techniques and procedures (TTPs) have impacted the cyber ecosystem for existing risks, as ransomware incidents remain a significant cause of losses worldwide, and vendors have prioritized developing models to detect and evaluate this threat. Besides malicious attacks, the threat of non-malicious accidental events persists, particularly with the dearth of vendor modeling capabilities behind it. Efforts are being made by the industry to improve visibility of systemic technology systems and what parallels can be drawn from malicious cyber events to discern a view. However, there is a difference in opinions regarding the extent to which these events result in losses. This highlights the importance of enhancing our collective comprehension of intangible cyber risks.

With a more granular lens through which to observe global cyber market dynamics and continued development across vendor model parameterization, Guy Carpenter is able to provide unique insights into the development of the peril as a whole and guide its clients in navigating these regions with confidence.

DECODING THE CYBER MARKET

Introduction

Our previous report, *Through the Looking Glass*, was written as the market was still acclimatizing to a resurgence of ransomware activity. Selective increases in claims frequency and severity, as well as isolated cases of back-year development, placed pressure on carriers to enhance underwriting and claims response in order to sustain profitability. In addition, the ever-present risk of cyber aggregation was felt in 2024 with a number of cyber "Kitty-Cats," defined as mid-sized catastrophe losses, including the CrowdStrike and CDK outages, which had relatively limited or sector-specific claims impacts.

Ransomware activity continued to persist but evolved into double-extortion campaigns, which involved data exfiltration. This exacerbated an already deteriorated threat environment, which saw a significant rise in data theft events. Carriers are required to be increasingly nimble in underwriting strategies, as the threat landscape continues to evolve with cybercriminals quick to adapt their techniques to exploit organizations' ever-changing attack surfaces.

Cyber as a class of insurance borrows characteristics from both long-tail and short-tail classes while remaining distinct in nature to both. As such, this presents underwriters with a dynamic and reactive market, which requires real-time underwriting adjustments to manage exposure to emerging threats. Simultaneous increases in threat actor sophistication and security practices within companies create a tug-of-war—this attracts more scrutiny at all stages of the insurance process, from underwriting to risk management.

As loss drivers change, underwriters are increasingly likely to sublimit coverages, increase retentions and increase scrutiny around limit deployment. For example, an emerging focus on privacy regulation and litigation funding, which has brought scrutiny to wrongful collection of data as a coverage, is reinvigorating conversations around third-party liability. This could challenge the current perception of loss composition across the loss distribution.

THE SIZE AND SHAPE OF CYBER

2024 global premium estimate

Quantifying the size of the global cyber industry presents some challenges. Cyber exposure has historically fallen within both standalone and blended policies, with various levels of reporting transparency. Data capture is generally stronger in open-market products, with some visibility challenges in delegated portfolios. This is compounded by varying distribution networks for the cyber product across different territories, which requires careful consolidation, and temporal variation, which requires thoughtful consideration to provide a view at a specific time.

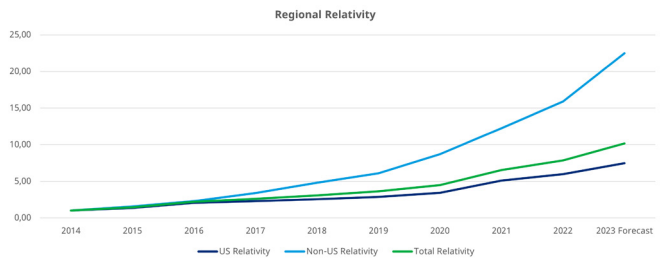
The methodology used to derive the premium estimate by Guy Carpenter has been designed to combat all these challenges. In addition, estimates have been compared against multiple sources that have released global or partial estimates. These sources—including Swiss Re, Munich Re, S&P reports and others—indicate that the 2024 cyber premium ranges from USD 16 billion to USD 17 billion and that the cyber market is showing significant change in its growth trajectory. To validate and form a view for 2024, Guy Carpenter analyzed the trends of the cyber market by region, size and sector to estimate the impact of factors such as 2024 rate changes and other shifting market dynamics. In our analysis, we leveraged our proprietary GC CyberExplorer® DataLake, an exposure cyber database that encompasses organizations, policy and losses information, across 130+ cyber clients globally alongside Marsh McLennan proprietary information. This allows us to derive our view for the cyber insurance market with deeper corroboration and validation.

Under the microscope—2024 premiums by region

As global cyber insurance premiums continue to increase, there has been a shift in the geographical distribution of the business. Although a significant portion of global premium still comes from carriers focused on NA, there has been a notable surge in growth in Europe and Asia. Driven by their success in the US, small and medium-sized enterprises (SMEs) specialists and insurtechs are now directing their expansion efforts toward the European markets to take advantage of this rapid growth. Our analysis of the market demonstrates that the greatest growth we observe on this class of business is driven by Europe, followed closely by APAC. For the latter, we are observing many startups and technology companies across Asia providing new data-centric solutions and, thus, promoting cyber in the region. This acceleration in growth is good news for global reinsurers' desire to diversify their exposure, which further helps unlock new capacity in the regions.

The reduced rate of growth observed in US cyber premiums should be interpreted as the market getting closer to its full potential, given its scale and maturity, as opposed to a decrease in appetite or capacity. Given the scale and relative maturity of the NA market, it is expected that the region exhibits a lower growth rate relative to Europe and Asia Pacific. The relativity in premium growth for the non-US regions highlights this acceleration in growth.

Figure 1: The growth of international and US written premiums by year, based on Guy Carpenter client reported incomes from 2014 through 2022



Source: Guy Carpenter

Guy Carpenter's client data reports a compound annual growth rate (CAGR) of 23% from 2014, which we have used to project to 2024.

To understand how the global market is developing, Guy Carpenter has analyzed the relative market share for the regions in question. These regions are split as follows: NA consists of US and Canada; Europe consists of UK and Continental Europe; APAC consists of Asia and Oceania; and ROW consists of South America, Africa and the Middle East.

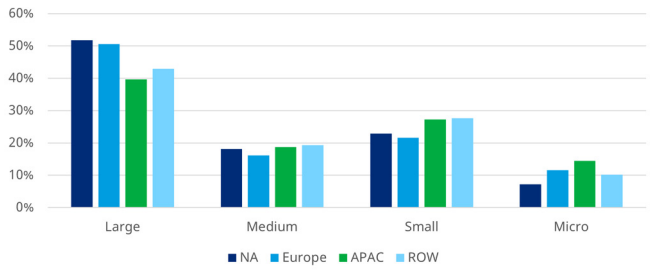
Table 1: Premium breakdown by region

Region	Proportion of global premium income
NA	63.44%
Europe	23.62%
APAC	10.02%
ROW	2.92%

Source: Guy Carpenter

The breakdown above is an expansion upon our previous report, which focused solely on 2 categories; the US and non-US markets. This report seeks to look at both the overall NA market and provide a granular breakdown of the non-US segment across Europe, APAC and ROW.

Figure 2: Size breakdown by premium %



Source: Guy Carpenter

Market evolution in key regions

NA

North America is the most mature segment of the cyber market and in some areas is experiencing high penetration, predominantly in the large corporate space, where the majority of organizations purchase cyber insurance. Penetration into smaller revenue bands, emerging industry sectors and personal lines business could be significant drivers of growth moving forward. Capacity is generally available from traditional insurers, with managing general agents (MGAs) continuing to bring new capital to the market. Driving the purchase of cyber cover is a combination of the increased awareness of cyber risks within the non-professional market and increasing dependence on technologies to enable business performance. This has led to an increase in cyber premiums stemming from large-risk business.

Europe

Pricing decreases and the increasing availability of cyber insurance with the entrance of insurtechs has made the European market more competitive. Growth has been observed particularly within the large-risk segment, as business continuity is increasingly dependent on cyber infrastructure. General Data Protection Regulation (GDPR) fines have increased year over year by 50% (DLA Piper, 2023), and upcoming proposed regulation in the EU continues to keep a focus on cyber exposures, although much of the motivation for purchasing is driven by first-party risk concerns. As with other markets, systemic risk and aggregation issues are a growing concern for European insurers, particularly with regard to infrastructure, vendor dependencies and war.

APAC

While cyber is a relatively mature product in the Pacific region, penetration in Asia continues to be low, with Marsh estimating it to be at 4-7%, driven mostly by mid-sized to large clients. Cyber take-up for SMEs in Asia is currently low but rapidly increasing, representing the highest growth rate. In response to the decreased experience with cyber products in Asia, underwriters are requiring strong risk controls from clients in order to access coverage. In particular, ransomware continues to be a focus for insurers, given the increased frequency. Insurers are willing to expand their coverage offering in the region, while the recent rate reductions and increased capacity have made it a favorable environment for buyers. Japan, India and Singapore remain key markets in the region, while China, Malaysia, Indonesia and South Korea trail closely behind in its growth development.

Australia and New Zealand continue to be key markets across the Pacific, while other more emerging territories continue to display interest in developing this line of business, particularly in those territories that already have a well-established property/casualty market. This is led by increased awareness around the peril as well as stricter regulatory requirements.

ROW

We are seeing cyber take-up rates slowly increase in Latin America and the Middle East, which indicates that the markets are still maturing. There is growing interest among insurers and reinsurers to diversify their books into these territories, as cyber insurance is gaining more traction due to recent cyber attacks.

This is also due to a number of initiatives from governmental and private/public bodies actively looking to invest in building digital infrastructure. Examples include how the IFC (International Finance Cooperation) is looking to invest in data center infrastructure across Latin America and how the GCC (Gulf Cooperation Council) is leaning heavily into digital infrastructure and high-tech industries.

While these initiatives are very promising for the cyber insurance market, the lack of standardization means insurers are presented with the complex challenge to tailor solutions for the region, which can potentially make purchasing cover for buyers more costly. Moreover, personal lines has seen significant growth via banks, as the product can be embedded, which has also proved positive. As a region, ROW has potential to grow and establish cyber insurance as a mainstream product as its regulatory environment develops and demand flourishes.

Under the microscope—2024 premiums by industry

The composition of buyers of cyber insurance remains consistent globally, with the financials, manufacturing, IT, professional services, healthcare and retail sectors being the main buyers across all geographies. The data below breaking down premiums by organization size and industry is proprietary data based on the GC CyberExplorer® DataLake. The firmographic breakdown of the industries by premium share within that region are as follows:

Table 2: Cyber premiums percentages by industry and region

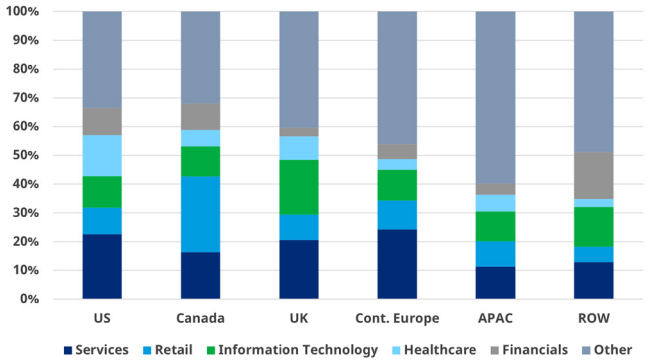
Top 6 Industries	NA	Europe	APAC	ROW
Financials	11%	15%	15%	18%
Healthcare	11%	2%	4%	2%
Information Technology	19%	11%	7%	7%
Manufacturing	10%	14%	15%	9%
Retail	13%	9%	11%	8%
Services	11%	12%	11%	8%
Other	25%	37%	36%	48%

Source: Guy Carpenter

- NA exhibits the largest share of premium across regions by far in the healthcare sector because of its well-established healthcare insurance industry. This encompasses not just hospitals but other medical service providers and equipment/device manufacturers, thus making it a key area of risk concentration for the region.
- NA features the highest premium share in the IT sector, driven as a result of the US comprising almost 70% of the world's largest IT companies.
- Europe and APAC drive premiums for manufacturing in comparison to NA; this is unsurprising, as the manufacturing sector is larger in those regions, with APAC alone comprising over 40% of the global manufacturing economy.
- Financials proves to be an important entry point for cyber insurance across the ROW; financials are regulated more strictly, thus promoting strong cyber awareness within ROW.
- Industry data capture tends to be better in the US, leading to a smaller share of premium allocated to "unlisted" or "unknown" industries.

The developed nature of the NA and European markets leads to increased premium contribution from large risks, whereas APAC and ROW feature more of a contribution from SMEs. It should be noted that non-NA/EU exposures have lower thresholds for large versus SME companies due to local market currency disparities, thus skewing the demographic classification.

Figure 3: Premium composition by region and industry



Source: Guy Carpenter

THE GLOBAL CYBER ACCUMULATION POTENTIAL

Introduction

Understanding how cyber exposure accumulates is a key vector toward the sustainability of the cyber market. It is critical to understand and manage the tail risk contained within cyber portfolios to ensure sustainable growth. As the cyber market has grown, the tools used to model losses have continued to improve alongside it. Catastrophe losses remain a dominant consideration for portfolio management, indicating the need to interrogate, understand and refine modeling assumptions. This report is a continuation of our previous *Through the Looking Glass* report concerning vendor risk views and provides both an update on expected industry losses and understanding of changes to the market.

Man-made perils have inherent variation and complexity in contrast to natural catastrophes. Due to the continuing evolution of cyber hazards and risks with updating technology, where there are differences in attack vectors, there is a range of approaches to modeling the losses. While claims experience is growing, especially for individual claims, there is a conspicuous absence of catastrophic cyber claims.

As part of our assessment of the global cyber accumulation potential, we provide an analysis of market losses predicted by the 3 vendor models with the longest pedigree in this class: CyberCube, Guidewire Cyence and Moody's. Each vendor has a unique approach to modeling cyber catastrophe events, with a continually evolving and bespoke view of the risk. For this study, the evaluation of a global cyber accumulation used only the aggregation components of the vendor models. Our methodology is comparable to the previous industry study report; this multivendor, year-on-year approach allows this study to have a stronger foundation for comparison.

The results of this study highlight that the quantum of losses between models diverge. Due to the lack of historical cyber catastrophe experience, as vendors' view of the cyber threat landscape evolves and they gain access to additional cybersecurity information, modeled losses diverge in the far tail. The lack of cyber catastrophe experience, unlike natural catastrophe experience, leads to difficult empirical calibration of models and heavy reliance on expert judgment when parameterizing these models. Rather than focusing in on the loss values themselves, we look at the reasoning behind the divergence.

Modeling a global industry loss

Headline views

As per our previous study, we leveraged Guy Carpenter's proprietary exposure database (GC CyberExplorer® DataLake) to model a global industry cyber loss. This extensive database currently encompasses 8.5 million cyber policies, representing USD 6.2 billion of gross written premium as of 2023. The GC CyberExplorer® DataLake represents a robust and reliable base for our industry loss study. Our modeling approach accounts for 3 main items:

1. Examining cyber policies to form a view on the exclusions that exist in the cyber market. To achieve this, we analyzed cyber policies across the varied regions included in this study and identified the coverages offered, their sublimits where applicable, and exclusions.

Cyber model stability and convergence are essential for the long-term growth of the cyber insurance industry. Achieving this is challenging due to the lack of catastrophic claims experience and the ever-evolving nature of cyber attack vectors and response tactics. Given the former, expert opinion will continue to drive differences among commercial models. The latter may be an ever-present reality, perpetuating the need for vendors to update their models frequently. With that said, each year we don't witness a major cyber event tells us something too. So in any scenario, the models are at least getting better over time. Studies such as this paper examining catastrophe tail risk, both over time and among providers, are critical for guiding decisions on how models should be considered when managing cyber insurance policies and portfolios.

Stephen Clark, Sr. Director of Product Management, Guidewire Cyence

2. Reviewing the cyber product, across the regions analyzed, in the light of the cyber scenarios contemplated by the 3 leading cyber vendor models.
3. Calibrating scenario selection and model settings to ensure a normalized modeled basis between the vendors for the best representative view of the risk.

Using the USD 16.6 billion industry premium estimate and policy details from the Guy Carpenter CyberExplorer® DataLake, a set of portfolios was constructed to model geographical segments of the industry and extrapolated up to represent the global premium. This methodology allowed considerations for the geographical exposure mix, the rate environment in prior years and the portfolio record size to be taken into consideration. In extension to our previous studies, we distinguish between US and non-US regions and decomposed the exposures to estimate the individual losses stemming from key regions. In the table below, we represent the losses predicted by each model across the Global, NA, Europe, APAC and ROW market segments.

Table 3: Accumulation potential by region (in USD)

Return Period	CyberCube V5.5	Cyence M7	Moody's V8
Global			
50	24,896m	9,265m	6,749m
200	45,625m	24,069m	20,103m
NA			
50	15,450m	5,698m	3,809m
200	29,335m	15,600m	13,507m
Europe			
50	4,124m	2,390m	2,043m
200	7,786m	5,818m	4,225m
APAC			
50	5,603m	1,001m	1,939m
200	8,909m	2,304m	5,120m
Rest of World			
50	440m	175m	163m
200	783m	412m	348m

Source: Guy Carpenter

Table 3 further highlights the variation across the main vendor models, at a global and regional level across the lower return periods and the extreme tail. As expected, the largest contributor of losses relates to the NA segment (69% of the global loss) followed by Europe (15% of the global loss). This is in line with our understanding of the market dynamics and evolution of the cyber insurance industry as discussed above.

In our prior study, the 2023 update for the *Through the Looking Glass* report, we estimated global cyber losses to range between USD 15.6 billion and USD 33.4 billion at the 1-in-200-year RP. This contrasts with our updated analysis, which results in an estimated global cyber industry loss of between USD 20.1 billion and USD 45.6 billion for the same return period. This year's study shows that the modeled outputs have increased across all return periods and the extreme tail due to a combination of a change in exposure year on year and the updates introduced by the newer versions of the vendor models. Market dynamics have shifted with an increased proportion of larger companies purchasing more cover across the board at relatively lower deductible levels. This growth in sum insured alongside a turbulent and ever-changing threat landscape has contributed to the development in vendor model losses.

Analysis for *Through the Looking Glass* was run on CyberCube V4, Cyence M5 and Moody's V6, whereas this year's report has been conducted on CyberCube V5.5, Cyence M7 and Moody's V8. These vendors had an intermediate version, which we also had to navigate. This meant accounting for changes in model settings and ensuring they were normalized for consistency across all vendors. This entailed in toggling business interruption/contingent business interruption (BI/CBI) coverage to be calculated on a profit-margin basis, as this is a key driver of loss, as well as ensuring security controls were captured correctly across measures, such as backup policy and patching cadence. Doing so enabled the study to be carried out in the most consistent and representative manner.

We observe a deterioration in results across the entire curve. This may be counterintuitive given that the (re)insurance industry has yet to suffer a catastrophic cyber event. Instead, these results suggest that the past cyber events provided insights on how threat actors became more sophisticated against insured organizations that keep improving their cyber security posture.

Divergence in modeled losses stems from differences in the average event footprint considered by the vendors, combined with a contribution from variance in the event frequency. 2023-24 was an eventful period that saw threat actors particularly active in exploiting managed service provider (MSP) zero-day vulnerabilities. Such events prove lucrative for threat actors, given the potential footprint for aggregation, producing an uptick in ransomware claims frequency. In response to the cyber threat landscape moving away from traditional ransomware toward double extortion, vendor models had to adapt their views for both footprint and severity.

Expert opinion continues to make a substantial impact on both the specifics of the perils modeled and on the modeled spread of events between insureds. As such, by requiring constant adaptation to reflect the cyber threat landscape, all models remain untested in terms of large-scale catastrophe events. Without a volume of claims experience to calibrate from, the models diverge in predicted average footprints—and therefore diverge in terms of quantum of losses.

Views in key regions

In this analysis, we modeled cyber losses across the different vendors and noted the divergence in views for each of the regions modeled.

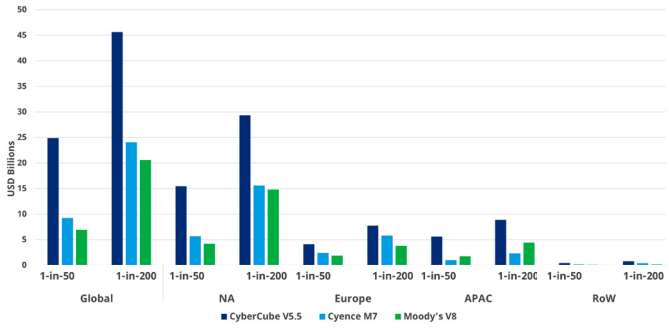
To understand this divergence, there are 3 aspects to consider:

1. The firmographic and technographic risk profile of the designated region. This refers to the type of organizations targeted by malicious actors alongside the technology and software relied upon by such organizations. This will have an impact on the modeled outputs for regions relying upon niche, local technologies rather than on larger international technologies.
2. The cyber security posture and resilience across the different jurisdictions alongside the regulatory requirements implemented within the regions. This has an impact on how organizations may recover and respond to a cyber event, in turn affecting the financial loss.
3. The regional cyber threat landscape. This includes the threat actors that are attracted by the organizations in question, common motives and the types of cyber crime that may be perpetrated against such organizations. This will impact the magnitude of the losses in the instance of a cyber event.

Based on our analysis, we observed that the vendors account for the differences between the regions and how typical companies within these regions would react to cyber events (for example, based on their internal incident response training, the availability and expertise of local incident response groups and the likelihood for offline backups to exist).

This leads to regional variations in both how losses emerge and in the relative magnitude of the loss. For example, we expect the losses stemming from a company within APAC to be lower compared to a European counterpart. The level of variation differs between vendors. Analysis of these variations, however, reveals that the extent of the variation is insufficient to accurately represent the costs of cyber events in the designated regions. This demonstrates the need for further calibration and research to adjust the assumptions implemented within the vendor models.

Figure 4: Cyber loss breakdown by region



Source: Guy Carpenter

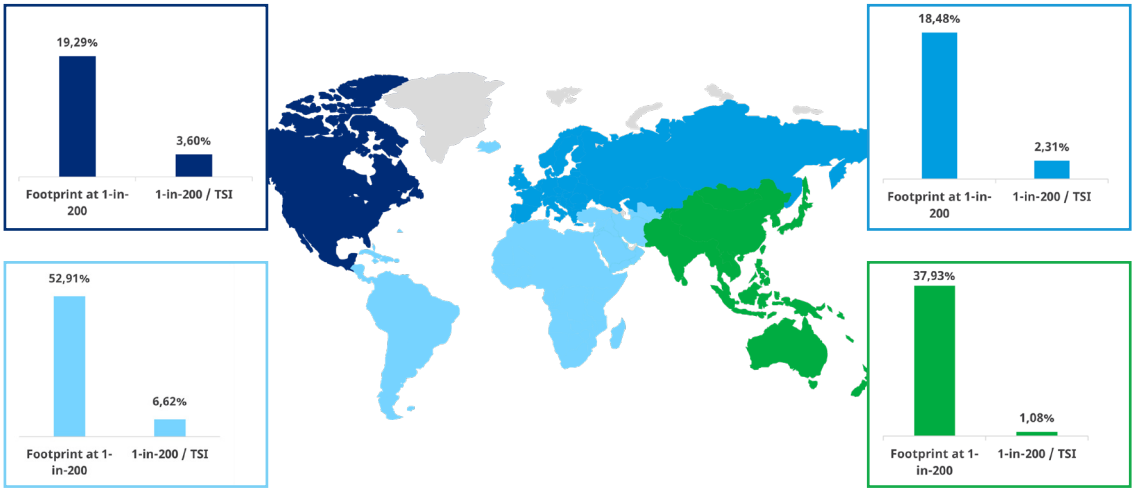
Moody's recognizes the need for cutting-edge research and analytics to address challenges brought by widespread cloud events and how to model these, business interruption loss refinement, and capturing multi-client attack scenarios. By leveraging our modeling expertise and collaborating with specialist cyber writers and technology partners, we aim to address tough challenges and navigate the complexities of the evolving cyber risk landscape and continue to support the cyber market grow and develop new opportunities.

Damini Mago, Associate Director, Product - Cyber Modeling & Analytics, Moody's

Figure 5: 1-in-200 cyber event footprint and loss to TSI percentages by vendor

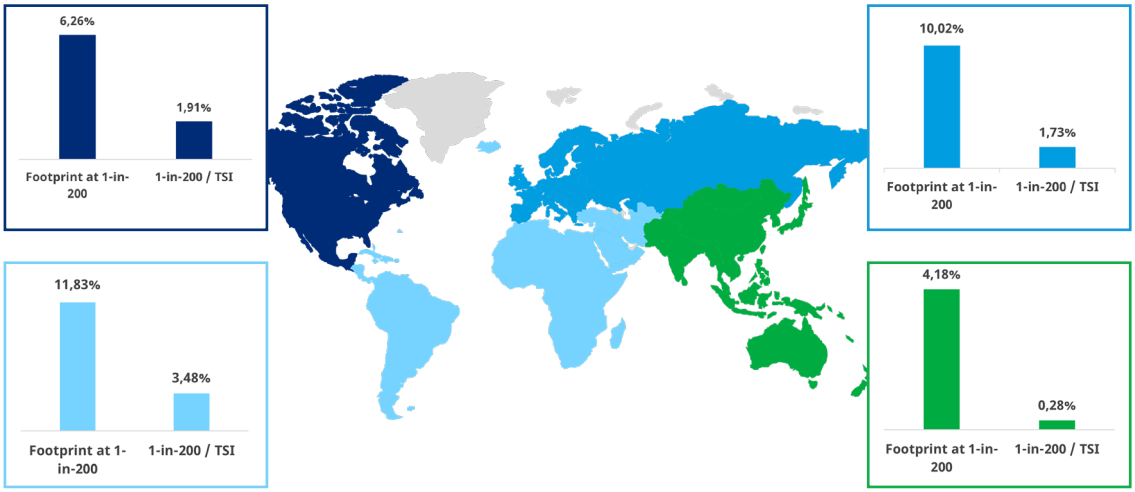
CyberCube V5.5

This shows the percentage of companies affected, by region, at the 1-in-200 RP, and the 1-in-200 loss as a percentage of the TSI of the region.



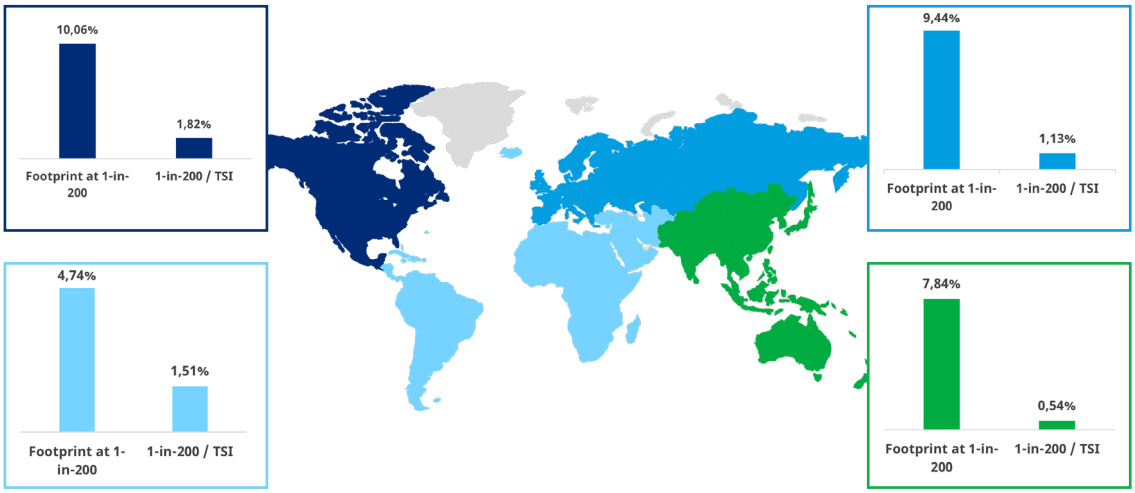
Cyence M7

This shows the percentage of companies affected, by region, at the 1-in-200 RP, and the 1-in-200 loss as a percentage of the TSI of the region.



Moody's V8

This shows the percentage of companies affected, by region, at the 1-in-200 RP, and the 1-in-200 loss as a percentage of the TSI of the region.



Source: Guy Carpenter

This is an example of the footprint and 1-in-200 year value—there is a representation of the footprint of a 1-in-200 event with respects to all companies within the region, and the 1-in-200 loss as a percentage of the TSI.

Breaking down the global industry loss

In our previous study, we identified the cloud, data theft and ransomware/malware scenarios as the key scenarios driving the curve. Unsurprisingly, the same scenarios emerge as key event drivers in this study. When assessing the quantum of loss generated, we observe a consensus among the vendor models in terms of cyber events driving the tail.

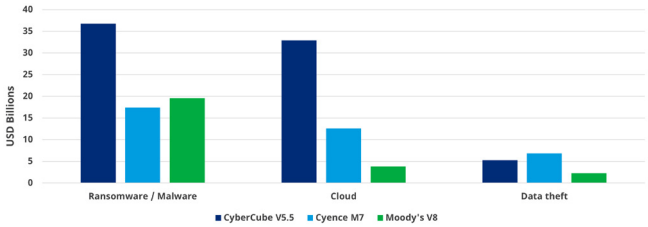
Global industry loss – event drivers

Ransomware/malware events remain the main driver of losses. Our understanding of the cyber threat landscape shows that ransomware/malware events remain a key concern for the industry, reinforcing this result. This proves to be consistent across all individual regions. When analyzing the movements observed across vendor models, we narrowed it down to a difference in frequency of ransomware/malware events and their associated footprint.

Cloud events still yield lower losses compared to ransomware/malware events. Vendor models show a greater divergence for this type of events, with CyberCube predicting global catastrophic cloud losses of a comparable severity to a ransomware/malware event while Moody's shows the lowest parameterization. Given the lack of historical precedents and how cloud service providers are adopted by organizations, the difference in views across the vendor models is understandable. The vendor community continues to contemplate additional information and factors to improve their parameterization of cloud events.

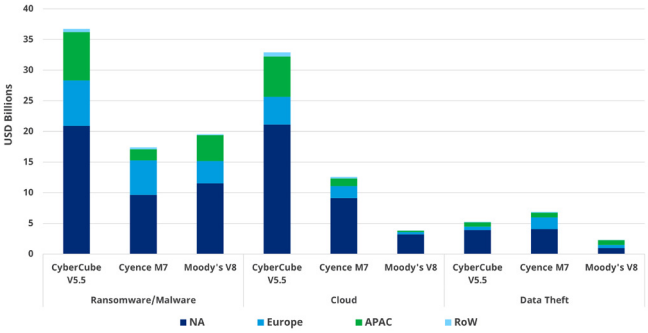
Data theft events are the third-greatest contributors of losses across the 3 vendor models. The view is still consistent that this is the least material of the "big 3" scenarios. Given the numerous historical precedents, it is clear why the 3 vendor models are relatively aligned on their view of data theft in comparison to cloud and ransomware/malware.

Figure 6: 1-in-200 cyber loss breakdown by event type



Source: Guy Carpenter

Figure 7: 1-in-200 cyber event type breakdown by region



Source: Guy Carpenter

Global industry loss–cost components

Vendors differ in terms of methodology, scenarios and parameterization, but also vary in how they define the cost components that may be triggered in the instance of catastrophic cyber events. Previously, in our 2023 study, we established that business interruption and contingent business interruption costs were a driving factor in the modeled losses. This view remains true, with vendors deeming that, in the event of cyber catastrophe, affected companies will suffer a loss of income either directly or through the cascading impact of their third-party dependencies. We estimate these contributions to range from 13% to 46% and 17% to 35% for business interruption and contingent business interruption respectively of 1-in-200-year event.

The exhibits in Figure 8 show the breakdown, on average, of a global cyber event by the top 6 coverages.

In this figure, the dominant cost component varies between vendors in the global view. Three key coverages are apparent: business interruption (BI), contingent business interruption (CBI) and incident response (IR). Breaking down contributions by coverage is essential, as losses flow via different mechanisms depending on the cyber event faced. Under a ransomware/malware event, the potential for a catastrophic accumulation event is only present when the attack is perpetrated against a common vulnerability. When threat actors exploit these shared technologies, it hampers connected companies,

leading to substantial losses in business interruption that affect multiple companies simultaneously.

In the case of a severe cloud outage event, a common denominator cloud provider is affected, resulting in significant downtime for all hosted processes from connected users. Accumulation potential stems from the volume of connected companies to the cloud provider being unable to perform their main business activities—whether that is as an online retailer or being unable to access key files from cloud storage. Given that many companies rely on such technologies, and few possess backup providers for such occurrences, they cannot remediate following the downtime event, leading to significant CBI losses from such events.

Large accumulation potentials are driven by events that affect large numbers of companies simultaneously, or by coverages that trigger across a broad set of perils—in the case of IR, the contribution is generated due to the frequency of the coverage triggering. IR consists of 2 parts—a forensic-investigation component and a data-recovery component. With most catastrophic cyber events, one or both requirements are triggered. This leads to significant losses stemming from IR claims.

Cost component variation by region

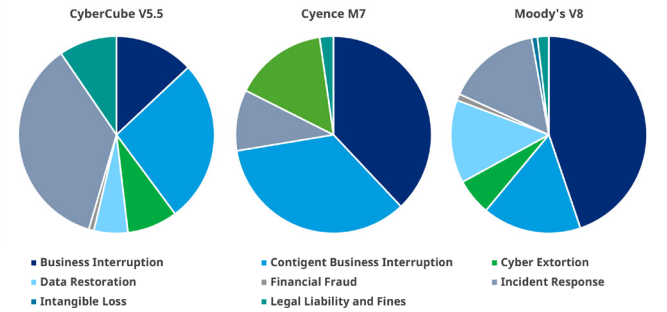
NA has the most mature cyber market, and the coverages offered in the region reflect that maturity. In general, most coverages are offered across policies with limited restrictions on items like CBI and ransomware.

The European region sees a more conservative approach to some cost components. For example, CBI offerings tend to be far more limited in scope and may require named Cloud Service Providers (CSPs) to be affected to recover in some cases. Europe tends to have a conservative approach to coverages for GDPR fines as well, given the legal ambiguity around recoverability of those fines.

APAC tends to have an even more restrictive offering around BI and CBI. In many cases, there is also no coverage for ransom payments, further impacting the nature of losses the region may experience in the event of a cyber catastrophe.

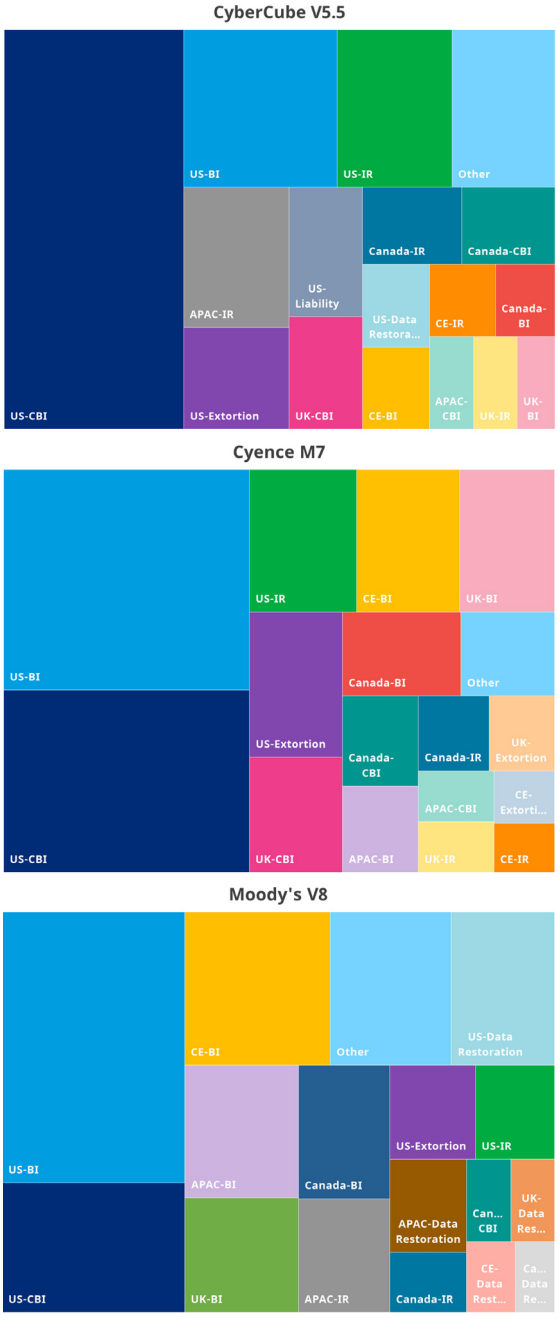
These nuances in the coverages applied can influence the quantum and nature of the losses experienced when modeling cyber catastrophes. This will be most pronounced in the tail, especially in the event of a ransomware or cloud event. These events would be experienced very differently from an insured loss point of view dependent on region.

Figure 8: Mean loss breakdown by coverage



Source: Guy Carpenter

Figure 9: Mean loss breakdown by coverage and region



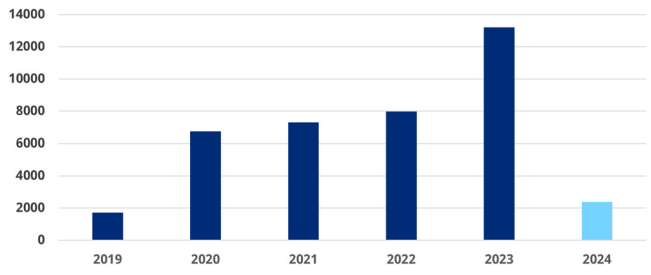
Source: Guy Carpenter

Shown on the previous page are the contributions to the global average annual loss (AAL) by cost component and region, by each vendor model. The bottom 20 cost-components by region for each model are reflected in the "Other" category. Examples of components included here are Continental European CBI, ROW liability and APAC extortion costs. Across all vendors, US insureds dominate predictions, and BI is the most significant cost component that generates losses. Regional differences are apparent, such as within the disproportionately large APAC-IR component within the CyberCube V5.5 global AAL. This indicates that regional differentiation must be taken into consideration when modeling losses within a portfolio to understand why certain vendor models respond in the way they do. Vendor modeling is not regionally agnostic—the choice of model can affect the dynamics of the losses, dependent on the region to which it is applied.

Events in retrospect

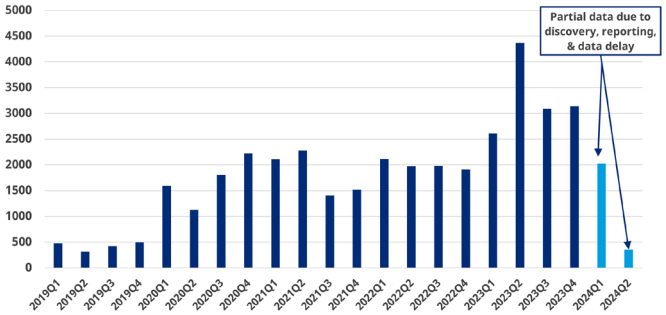
2023 and 2024 were eventful years that saw threat actors particularly active in ransomware campaigns. This is evident through the numerous incidents observed across the years, indicating frequency has increased. However, this uptick in frequency has not necessarily exhibited a mirrored increase in severity to date. Improvements in insureds' security hygiene and awareness have forced cyber threat actors to turn away from ransoms in exchange for data return and have pushed toward a new era of data exfiltration. In over 90% of ransomware incidents in Q3 2023, claimants reported elements of exfiltration and data compromise. The combination of traditional ransomware, alongside the threat of extracted data, is known as "double extortion" and has emerged as a key consideration for incident responders.

Figure 10: Ransomware event count by year



Source: Marsh McLennan Cyber Risk Intelligence Centre

Figure 11: Total ransomware event count by quarter



Source: Marsh McLennan Cyber Risk Intelligence Center

Such double-extortion campaigns have been successful, as threat actors have increasingly targeted systemic third-party vulnerabilities. These actors are becoming familiar with the downstream effects of targeting crucial technology dependencies and how lucrative capitalizing on the potential accumulation can be. Consequently, ransomware groups have been active in targeting zero-day vulnerabilities across systems to varying levels of success. Some of the most significant attacks across 2023-24 are mentioned:

Table 4: Main malicious cyber events

2023-24	MOVEit	Change Healthcare	CDK Global
Date	May 2023	Feb 2024	June 2024
Technology type	Secure file transfer software	Healthcare payment exchange platform	Auto dealer CRM SaaS tool
CVE	CVE-2023-34362	CVE-2024-1708, CVE–2024-1709	NA
Threat actor type	RaaS Groups	RaaS Group	Ransomware group
Campaign type	Ransomware, data exfiltration	Ransomware	Ransomware
Organisations affected	Approx. 2,620	Approx. 63,000	Approx. 15k
Insured loss	Preliminary estimate of $500m	Preliminary estimate of $50m	NA
Loss driver	Incident response and data recovery	Extortion	CBI

Source: Guy Carpenter

These events demonstrate how an accumulation cyber event can materialize, propagate and affect multiple risks. Not only do these past events corroborate that malicious and ransomware attacks remain the most common risk, they also demonstrate that non-malicious events should be considered and monitored. For instance, the potential global fallout from widespread IT failure has the potential to be damaging, but less than its malicious counterpart was, as was highlighted in the recent CrowdStrike outage.

Considered one of the largest IT outages in history, a flawed software update from security vendor CrowdStrike resulted in widespread failures across more than 8 million Windows machines worldwide. This incident occurred on July 19, 2024, leading to affected devices displaying the notorious "blue screen of death."

In many respects, the outage echoed the fears of people concerned with software issues leading to such widespread system failure. Luckily, the losses did not escalate as much as the market initially anticipated, as 90% of systems were restored within the first 12 hours of the event. This broadly falls within the waiting period observed across the market, thus capping the realized loss. This event highlighted the market's resilience, as organizations and enterprises have invested in their security posture and adopted improved cyber hygiene practices. Having stronger security controls in place is what allows companies to purchase cover and strengthen their cyber risk management programs. Guy Carpenter anticipates this trend to continue to develop going forward, but also encourages the vendor models to appropriate their service offering around such non-malicious events, as this is currently not the case.

The cyber insurance market can continue to improve how it anticipates such events and mitigates their effects. In this regard, vendor models partners will assist in the quantification and parameterization of such attacks, and help users understand the accumulation potential in the following ways:

- **Identifying technology dependencies**: Continuing development in identifying systemic technology dependencies will be imperative in providing a tangible way for the industry to view systemic cyber. Doing so will ensure a robust approach to mapping systemic cyber systems and their potential accumulation footprint. Furthermore, this will improve risk selection and ensure an extra layer of transparency in decision-making across the value-chain for all stakeholders.
- **Assessing information security resilience**: Determining the accumulation footprint, however, is only one half of the equation. The other half involves determining the impact of such events and how material they may be with respect to the insured's infosec protocols and technological resilience. Calibrating potential losses based on a company's resilience through protocols such as implementation of backups, 2FA/MFA versus SSO (2-factor authentication/multi-factor authentication versus single-sign-on), patching cadence and so on, will prove valuable in guiding a view for potential accumulation impact.
- **Designing incident-relevant scenarios**: Given the lack of historical events in the cyber space, any insight that can be appropriately gleaned from an incident will be useful in building a forward-looking view of the risk. That is why being able to curate and design scenarios representative of recent events will prove a strong way to validate a view of the peril and ensure its relevance.
- **Evaluating modeled losses retrospectively**: As accumulation events continue to occur, assessing the scale of the potential loss and its materiality retrospectively will indicate a view for the loss curve. If a tail-view of an event can be extrapolated appropriately, through the correct tools and parameters, this can help inform the catastrophe potential of an event in real time.
- **Exploring relativities between cascading events**: The cyber peril manifests itself in many different forms across the CIA Triad (confidentiality, integrity and availability). These principles provide a clear framework to understand the implications of different cyber events. While many events occur, implicating each of these facets individually, there are some that can span across more than one principle, thus indicating that they are not mutually exclusive. Understanding how different events can influence occurrences will be a valuable next step for the industry in modeling accumulation potential. An example of this would be how certain data-breach events could potentially contribute to numerous ransomware campaigns and vice versa, depending on the technology system affected. Building a view around such cascading events will prove insightful.

- **Appropriating event wordings and policy language**: Providing a distilled view of losses through the appropriation of relevant wordings and/or exclusions enables users to customize results accordingly. Efforts should be directed toward modeling wordings in the most representative way possible to enable cedents and reinsurers to customize their view of risk. As the cyber catastrophe reinsurance market grows, Guy Carpenter has worked to compile a repository of scenarios to reflect event definitions and exclusionary language to tailor modeled results most accurately to both prospective and retrospective events to **determine potential recoveries and further refine cedent risk tolerance**.

The points above should serve as a guide and indicate the direction toward which developments should be made. Doing so will greatly expand the lens through which accumulation events are viewed and drive robustness in our approach to tackle this issue. The market is already observing steps in this direction, which indicates a positive trend in development. Efforts will continue to improve as stakeholders get involved and continue to collaborate.

On the horizon

The cyber threat landscape is continuously evolving. As businesses' cybersecurity posture is increasingly improving, threat actors remain on the hunt for new vulnerabilities or entry points relying on increasingly sophisticated methods and mechanisms. Thus, systemic cyber remains an area of concern with:

- **Increased reliance on cloud services**: Businesses relying on cloud services has increased by 14% since 2020 due to increased reliance for remote-working during the COVID-19 pandemic. Regardless of the size, region or the industry to which organizations belong, cloud-service providers are embedded within these organizations' business model, making them vulnerable in a targeted cyber attack.
- **Advancements in cyber attack techniques**: In 2025, threat actors will carry on their search for zero-day vulnerabilities and leverage advancements in technology (e.g., generative AI) to weaponize and deliver their attacks.
- **Regulatory environment**: 2025 may see more stringent regulatory requirements for cyber risk management and reporting, where (re)insurers may be mandated to demonstrate and justify their cyber view of risk with regard to systemic cyber with supporting arguments.
- **Changes in market dynamics**: Cyber remains a class that will continue to grow over the course of 2025, with new players expected to enter the space in both established and emerging markets, which will in turn increase the potential severity of a systemic cyber event.

Drawing on its position within the cyber reinsurance market, Guy Carpenter has leveraged the potential of the GC CyberExplorer® DataLake to form a view of the cyber industry loss. This has highlighted the differences between the regions to better understand the global results.

Although cyber is a peril without borders, the results demonstrate a salient point, namely that insurance is cultural. Losses representative of one region differ from another for many of the reasons discussed in this study. Future cyber modeling, including vendor models, ought to continue considering the nuances and characteristics of the cyber market in different geographies to predict losses that may emerge from systemic cyber events accurately.

As the cyber insurance market becomes increasingly global in nature, CyberCube continues to invest in data, analytics and models to help our clients unlock the opportunity ahead of us. Since the last report, our model has been used across the value chain to help unlock capital and create sophisticated portfolio strategies. 2025 will be our biggest year yet in terms of product development and we aim to give our clients even more capabilities to understand and manage Cyber Cat Risk.

Ashwin Kashyap, Chief Product Officer, CyberCube

CONCLUSION

Cyber remains an exciting line of business. Few lines of business see the same pace of evolution, whether from the threat landscape or the underwriting of the class. As technology advances and reliance on cyber processes grows, threat actors also become more sophisticated, driving the expansion of the cyber market. One notable trend is the increasing penetration and growth of cyber insurance outside of NA. This can be attributed to growing confidence in writing cyber products in various markets, as well as the emergence of Insurtechs and cyber writers focusing on SMEs. This expansion is likely indicative of the future trajectory of the market.

Global accumulation potential modeling reveals significant potential losses, with 1-in-200-year occurrence losses estimated between USD 20 billion and USD 46 billion. This represents a deterioration in expectations compared to the previous year, as different vendors rely on assumptions from industry experts due to the lack of comparable cyber catastrophe events. Consequently, there is a divergence in the estimated quantum of loss.

Despite variations in loss estimates, there is convergence among vendors regarding the types of perils and the nature of losses. Ransomware/malware and cloud events consistently dominate the modeled losses across all vendors. Additionally, business interruption (BI), contingent business interruption (CBI) and incident response (IR) contribute significantly to the overall losses.

Furthermore, regional analysis reveals differences in coverages offered, which can impact the generated losses. As the cyber market continues to mature, these nuances may provide a competitive advantage for certain providers over others.

Looking ahead, fundamental changes are expected in the threat landscape and underwriting processes due to the integration of artificial intelligence (AI). AI will play a crucial role in enhancing risk assessment, threat detection and response capabilities, revolutionizing the cyber insurance industry, but also empowering threat actors in ways currently not contemplated.

Due to a lack of available empirical evidence, vendor models will rely on assumptions to assess some of the risks and impacts of cyber events. This has led to an increase in magnitude for the worst-case scenarios as models have been updated over time, based on the latest information about threat actors and the vendors' improved understanding of the potential for cyber catastrophes. However, it is reasonable to apply a degree of caution when using those estimates since many of these events have not yet materialized.

By examining past cyber aggregation events such as the CrowdStrike, CDK, Change Healthcare and MOVEit events, one can argue that the impact of these events did not reach the severity levels that a conservative viewpoint might suggest. Threat actors often face limitations in their ability to exploit vulnerabilities on a large scale, thwarted by resource constraints. Additionally, they aim to secure a reasonable payoff without attracting excessive attention from regulatory or governmental entities.

Furthermore, the models' simulations of severe events in the tail end, such as large-scale ransomware attacks or significant service outages in critical infrastructure, are likely only feasible for the most sophisticated actors with support from governments. The exposures resulting from these events are managed and reduced through exclusions.

GUY CARPENTER CAN PROVIDE EXPERT GUIDANCE ON HOW TO CREATE A CUSTOMIZED RISK PERSPECTIVE BY UTILIZING ONE OR MORE VENDOR MODELS. OUR EXTENSIVE EXPERIENCE AND DEEP UNDERSTANDING OF THE MARKET EXPOSURE DATA, INDUSTRY LOSS EXPERIENCE AND EXPERT ASSESSMENT OF THE CYBER CATASTROPHE LANDSCAPE ENABLE US TO OFFER VALUABLE INSIGHTS. THIS APPROACH ALLOWS OUR CLIENTS TO EFFECTIVELY QUANTIFY AND CONSEQUENTLY MANAGE CYBER RISK EXPOSURES OVER TIME.

Appendix

The scope of the study is cyber policies written by global and regional cyber carriers. The loss estimates in this report are an attempt to quantify a cyber catastrophe loss across the globe and provide insights around the regional breakdown of such loss. 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.

Contacts

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

Souki Chahid
Head of Cyber Analytics – UK & International
souki.chahid@guycarp.com

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

Jess Fung
Head of Cyber Analytics – North America
jess.fung@guycarp.com

GuyCarpenter

About Guy Carpenter

Guy Carpenter, a business of Marsh McLennan (NYSE: MMC), is a leading global risk advisory and reinsurance specialist and broker. Marsh McLennan is a global leader in risk, strategy and people, advising clients in 130 countries across four businesses: Marsh, Guy Carpenter, Mercer and Oliver Wyman. With annual revenue of $23 billion and more than 85,000 colleagues, Marsh McLennan helps build the confidence to thrive through the power of perspective. For more information, visit guycarp.com, or follow on LinkedIn and X.

A business of Marsh McLennan