CYBER PREDICTIONS REPORT 2024

CyberCube

Foreword

As we commence a new year, the future of the cyber (re)insurance market looks extremely promising.

The maturation of the cyber (re)insurance market is a strong theme in this report, which brings together some of our experts' views on the trends we're likely to see in the year ahead. The pathway is being laid for the cyber market to reach half a trillion in coverage in the years ahead with growth expected from all avenues.

More traditional reinsurance companies will start offering meaningful cyber reinsurance capacity in 2024 and continents such as Europe and Asia will increasingly identify cyber (re)insurance as an opportunity. There will also be further development of the insurance-linked securities (ILS) sector to create a long-term sustainable and thriving marketplace.

While there will be an increase in the frequency of cyber attacks fueled by the proliferation of Artificial Intelligence (AI), the insurance sector will work more closely with SMEs to address their needs. Insurers and the public sector will combine to strengthen societal resilience to major cyber events. For the broking sector, those companies that create a comprehensive cyber strategy will set themselves up for a successful 2024.

As cyber risks become more complex, we will all have a crucial role to play. CyberCube is aware there will be a pressing need for more sophisticated models. There will be a greater focus on data quality, and advancements in analytics will enable robust risk management.

These are just some of the predictions for 2024, expressed by CyberCube's wide range of experts. We hope you enjoy reading them.

Yvette Essen

Head of Content, Communications & Creative

Prediction: Additional reinsurers will enter the cyber reinsurance market in a meaningful way

Cyber insurance is one of the fastest growing lines of insurance to emerge in a generation, yet many traditional reinsurers have not seen cyber as an area of growth for them until recently. Three factors are driving the prediction that more traditional reinsurance companies will start offering meaningful cyber reinsurance capacity in 2024.

Firstly, cyber insurance analytics modeling has matured substantially. With the release of Portfolio Manager Version 5 by CyberCube in 2023, we now have many years of iteration on the modeling of cyber catastrophe risk and more consensus than ever before about the scenarios that matter.

Analysis of 94% of real-world systemic events and near misses over the last three years show a high or medium fit in the CyberCube catalog. When this is combined with CyberCube's attritional loss model being 1% point off the National Association of Insurance Commissioners (NAIC) filing rates, cyber modeling is at a stage that inspires confidence amongst reinsurers, at a time when many nat cat models are being deeply questioned.

Secondly, new tools are allowing reinsurers to better understand the quality of various cedent portfolios. Traditional approaches to providing capacity have relied heavily on a qualitative understanding of the underwriting capabilities of a potential cedent or MGA. CyberCube is turbocharging this with data-driven analysis that allows for quantitative comparisons of the underlying quality of risks in a portfolio, which further drives confidence.

Thirdly, it is increasingly clear cyber is a risk that is too big to ignore. As more Internet of Things (IoT) devices, data and artificial intelligence are rolled out in more sectors, cyber is reconfiguring the nature of risks in the global economy. As reinsurers look at traditional lines of insurance being transformed by internet-connected risk, as well as the opportunity to participate in a rich new line of insurance, those reinsurers who were hesitant to dip their toe in the waters of cyber will increasingly see the imperative to do so.

As new reinsurers start offering cyber in meaningful ways for the first time in 2024, this will contribute "many new trickles" of capacity, rather than a flood of reinsurance. Over time, 2024 will lay the groundwork for future growth of capital, supporting the future of what could become one of the largest lines of P&C reinsurance.

Pascal Milliare
Chief Executive Officer

Prediction: The insurance sector will work more closely with SMEs as they increasingly come under attack

A trend we're seeing is that it is not just large companies under attack. While larger companies tend to get most of the attention, the proliferation of attacks is focused around small and mid-sized entities, regardless of the sector.

These SMEs have much less knowledge of the intricacies of cyber security, and their staff have less experience in how to work with governments. They are also less sure about what they need to report in the event of a breach.

Traditionally, attackers have focused on the bigger players, but the attackers are changing. We are seeing the evolution of technique and approach combined with the extensive exploitation of vulnerabilities in the software itself. There is a plethora of "fundamental" approaches, but with no single strategy that fully mitigates different approaches, SMEs can become targets.

Cyber insurance can be a really powerful tool for risk mitigation but we need the broader ecosystem to help us characterize it and understand it, including just how much risk we are assuming. One such strategy being implemented to address this is a change in the documentation that is now required from companies in regards to cyber security. This has resulted in a more comprehensive understanding of SME risk and demonstrates that we get better value functionality if we work more closely with organizations to address their cyber risk.

With the SME market becoming increasingly targeted, the insurance industry will need to work with companies even closer to create a more robust cyber risk mitigation strategy across the board.

> *"We are seeing the evolution of technique and approach combined with the extensive exploitation of vulnerabilities in the software itself."*

Admiral (ret.) Michael S. Rogers

Former Director of the NSA, Commander of U.S. Cyber Command & Board Member, CyberCube

Prediction: There will be an increase in the frequency of cyber attacks fueled by the proliferation of Artificial Intelligence

At CyberCube, we provide thought leadership to the insurance ecosystem on the evolution of the cyber threat landscape. One of the most important topics for the industry is to understand the implications of Artificial Intelligence (AI) on cyber risk. We expect an increase in the frequency of cyber attacks that will impact loss ratios in the cyber insurance industry over the coming years. Here are specific reasons driving this belief:

AI tools have enabled threat actors to improve the effectiveness of phishing campaigns by eliminating previously recognized indicators of phishing emails, such as grammatical and spelling errors.

As large language models (LLMs) are being deployed against proprietary data, we expect sensitive data to be targeted by threat actors using LLMs and associated infrastructure as conduits. We also expect that sensitive data will be leaked in unexpected ways, leading to an increase in data privacy violations.

Combining AI-generated source code with human-generated source code in software development opens up a new world of vulnerabilities. It has never been easier or faster to develop software with the emergence of AI co-pilots, but there is no promise of more secure software yet. This presents a window of opportunity for sophisticated, motivated threat actors to discover and exploit vulnerabilities in poorly secured software.

> *"One of the most important topics for the industry is to understand the implications of Artificial Intelligence (AI) on cyber risk."*

With this likely increase in the frequency of attacks owing to AI, the insurance industry needs to monitor the adoption of AI tools and developments in securing the AI stack in the near future. In the medium-to-long term, the industry needs to shape cyber policy language and appropriately price AI risk into policies.

Ashwin Kashyap
Co-founder and Chief Product Officer

Prediction: Insurers and the public sector will combine to strengthen societal resilience to major cyber events

The cyber insurance market continues to grow at a healthy pace — Munich Re has predicted the market will almost triple from around $12 billion today to $33 billion by 2027. However, there are still many enterprises without meaningful insurance cover. Insurance penetration rates for the cyber sector remain frustratingly low, especially outside of the US and Europe and in smaller businesses. For larger companies, capacity remains scarce and coverage restrictions create ambiguity over which cyber loss events may be covered by insurance.

While the cyber insurance market grows in value by billions of dollars, cyber crime is estimated to cost between $6-10 trillion annually, dwarfing the size of the insurance cover in place. In recent years, governments have initiated programs to partner with the private sector to improve enterprise cyber security, reduce the financial cost of cyber crime, and encourage deeper and broader risk transfer to the insurance industry.

In general, as the insurance market - and regulators - develop a deeper understanding of systemic cyber risk and the potential for catastrophic losses arising from cyber events, there will be a greater need for collaboration. The insurance market and supervisors need to focus more closely on risk assessment and portfolio management from the earliest risk transfer interactions to strengthen societal resilience to major cyber events.

In 2023, progress was made to develop an understanding of systemic cyber risk to economies. The US government, in particular, has managed a public process to understand what systemic cyber events might impact society and how the public and private sectors can partner to improve resilience. In November 2023, the US Treasury announced it had established consensus with the industry that a federal insurance response to cyber cat risk was warranted and will now move into the design of structures.

This represents a huge step towards building societal resilience to extreme systemic cyber attacks. It will encourage a sustainable private insurance market while providing clarity around the point at which the government steps in to cover residual losses suffered by businesses and citizens.

In 2024, other nations' governments will continue to watch with interest, to assess the applicability of the US research to their own economies.

Rebecca Bole

Head of Industry Engagement

Prediction: There will be a greater focus on data quality

Insurance companies are more heavily invested in cyber risk than ever before and are further embedding data and analytics into their workflows. Insurance companies are evaluating their exposures more closely as the market continues to mature and grow.

As part of their evaluations, insurance companies are going to place a greater focus on data quality. There are three areas they are likely to focus on:

1. Having confidence in the findings at the individual account level. Insurance carriers will seek assurance that their underwriters do not only understand the findings, but are also looking at appropriate, well-matched data, reflective of the risk they are insuring.
2. Predictive modeling - insurance companies want confidence that signals, scores, and models are predictive of loss experience. Underpinning this predictive relationship is the accuracy and quality of the data that is contributing to the analysis.
3. At the portfolio level, risks will need to be evaluated holistically and in abstraction. Primary carriers and reinsurers will want to not only understand modeled losses, but will also be on the lookout to enhance their portfolio diversification, and avoid adverse risk selection and other idiosyncratic findings in an underlying portfolio.

In light of these trends, CyberCube is working with (re)insurance carriers from the individual policy and account through to reinsurance evaluation to assist with risk selection, and portfolio exposure management.

> *"Insurance companies are evaluating their exposures more closely as the market continues to mature and grow."*

John Anderson

Principal Product Manager

Prediction: Market maturity and more advanced analytics will enable more robust risk management.

In 2024, I predict the cyber insurance market will show more signs of increased sophistication and will make deeper, more granular use of analytics to manage risk. This is due to both the growing maturity of the cyber insurance market and the continuing advancement of cyber analytics and modeling.

We see this in multiple facets:

- an increased take-up of cyber insurance across more industries
- standardization of coverage
- more market entrants/greater competition
- increasing regulatory involvement, contributing to market stability
- the development of more sophisticated risk assessment and underwriting processes.

As models and data have more proven power and sensible storylines, the leading practitioners will be looking for more cuts of model results to drive decision-making. This will enable them to know not only if they have accumulations to a cloud provider in their portfolio, but if they have accumulations to specific data centers.

This will also allow them to understand how their portfolio reacts to widespread malware, and how idiosyncrasies in their portfolio composition lead to different outcomes than the industry.

Supporting this level of analytics will take a certain technological commitment. API integration will allow not only the automation of existing workflows but creative sensitivity tests and subportfolio analysis. Portfolio steering and policy design will be more informed by analytics than ever.

Ultimately, this greater understanding resulting from more advanced cyber analytics will foster innovation and improved services across the industry. This will enable (re)insurers to offer a broader range of coverage options that match their own risk appetites and help (re)insurers more proactively address their portfolio of cyber risks.

Cody Stumpo

Senior Director of Product Management - Portfolio products

Prediction: Retail brokers will compile comprehensive strategies to grow their books

Cyber risk remains a dominant 21st centry risk, top of mind for reinsurers, insurers, and the enterprises that are their policyholders. While rate increases have stabilized, cyber insurance remains one of the best opportunities for insurance brokers to grow their business.

To capitalize on this growth opportunity, we expect to see more retail brokers put a comprehensive strategy together to more effectively cross-sell cyber insurance to their existing clients, up-sell higher limits at renewal, and win new business.

More brokers are beginning to realize that if executive leaders formalize a cyber growth strategy, they could see significant growth as a result. There are four areas we expect to see brokers focus on in 2024. These are:

Forming carrier panels and facilities for their client base: There will be more collaboration between brokers and their carrier partners, delivering favorable insurance coverage tailored to meet the needs of clients with similar exposures, but also budgets, leading to a more positive client-broker relationship.

Investing in analytics and risk management services: Leveraging appropriate technologies will play a massive role in the overall cyber insurance sales and renewal strategy for brokers. By leveraging analytics and cyber risk assessment solutions, brokers can streamline operations, empowering their associates to be more effective. This will reduce time spent on administrative tasks such as building client presentations, and more time on higher value work such as advising clients and other relationship-building tasks.

Up-skilling or hiring cyber insurance specialists: Brokers will invest more in cyber insurance specialists who can lead the strategy for the company's growth efforts. Once a cyber practice is developed, this can help cascade the education and enablement for generalist producers and account managers so they can effectively discuss cyber insurance with their clients.

Setting performance metrics to track growth: Retail brokerages will invest more in tracking performance. Many brokers still have insureds that aren't carrying enough cyber insurance limits or aren't carrying it at all. To effectively grow this product line, a baseline view of the cyber book needs to be measured in order for brokers to build growth targets and performance metrics to track against.

Brokers that can create a comprehensive cyber strategy will set themselves up for a successful 2024.

Nate Brink
Head of Broker Partnerships

Prediction: The ILS market will continue to evolve

In 2023, we saw both the first private and public 144a cyber catastrophe bonds come to market. This was such a fascinating moment in the cyber insurance industry, specifically with the 144a cat bonds, witnessing the financial markets starting to put a price on systemic cyber event coverage.

The first public bond to transact, sponsored by AXIS, was named Long Walk as a nod towards proactively creating a path of sustainable access to capital for future needs. As we wait to see if and how other bonds in the market close and at what price, it will be exciting to see how that shapes the reinsurance and Insurance-Linked Securities (ILS) landscape in 2024.

The work done by stakeholders in 2023 created a strong foundation to see this market grow in 2024. The first public cat bonds were always an important test as they would bring together transparency and templates for structure, modeling, and pricing. One important structural piece was always how to define systemic cyber events. These transactions have to define how events will be classified as systemic, when they start, when they stop, and other structural items such as war and infrastructure exclusions. Seeing which structures the financial markets accept and how they price them can hopefully point towards a more consistent future state.

In order for the ILS market to continue to grow off the back of the work done in 2023 there will need to continue to be straightforward, clear structures that allow investors to continue to begin their participation while getting more comfortable with cyber as an asset. Continued collaboration from stakeholders throughout the value chain is crucial.

This topic presents more questions than answers for 2024. I predict in 2024 we will see further development of the cyber ILS market to create a long-term sustainable and thriving marketplace. Some key areas to watch include event-based reinsurance structures, how ILS capacity complements traditional capacity in this space, if new sponsors come to market in 2024, and how cat bond structures evolve as the market matures and investors provide feedback in both their words and their financial commitments.

Brittany Baker

VP of Solution Consulting

Prediction: Complex cyber risks will push for faster evolution and more sophisticated models

As the race between weapons and armors in the domain of cyber security continues and intensifies, we are seeing an increase in attack surfaces, complexity of attacks, the sophistication of threat actors as well as the tools and techniques they employ.

Correspondingly, the same is happening on the defense side — both reactively in response to new attacks and proactively through innovations in big data analytics, the use of Artificial Intelligence (AI) tools and other technologies to predict and prevent such attacks.

The industry requires a much deeper understanding of how cyber incidents can impact the business outcomes for enterprises. This will push cyber risk models to become a lot more nuanced in order to account for the multitude of variables that are necessary to quantify cyber risks. For instance, models should be able to incorporate new security signals that are being rapidly developed based on the evolution in cyber security driven by AI technologies. One such security signal may be an AI-supported analytics of network traffic, which could reveal valuable information about the security posture of an enterprise

Moreover, the increase in models' complexity will have to be balanced against the necessity to improve their flexibility. This is because the optionality and variability of model parameters will grow to reflect the sophistication and diversity of applicable cyber risks, which will require models to be adjusted more easily. For example, the ability to add new and modify existing model parameters will need to be baked into the model itself, making it more open and extensible.

To sum up, in 2024, it is likely that the rapid growth and evolution of cyber risks' complexity will require a significant increase in the sophistication and flexibility of models to better account for and quantify the changes in cyber risk dynamics.

> *"The increase in models' complexity will have to be balanced against the necessity to improve their flexibility."*

Max Sokolov

Sr. Director, Software Engineering

Prediction: The pathway is being laid to create half a trillion of cyber coverage

Cyber is likely to grow into a large market over the next 15 years. Catastrophe risk in the capital markets exceeds $100 billion and cyber has the potential to become just as large over the next two decades.

Growth projections for this sector have been consistently ambitious and just as consistently met. Multiple reinsurers and brokers have projected that the market will approach $25 billion in 2025. Continued growth at a 37% compound growth rate — consistent with the last decade — will take the market there.

Estimates from brokers and carriers for 2030 range from $45-60 billion. Jefferies proactively projects direct written premiums of $480 billion by 2040, representing 19% of industry premiums at that point. Let's reflect on the mighty convergences that will unfold over that period. As the world becomes more automated, the risk will become more cyber-driven. Maybe the most important insured sector at stake is auto - particularly if autonomous auto is heavily shared and fleeted. The increasing reach of the Internet of Things will drive cyber premiums. Terror and cyber are converging and that will be a driver as well.

While cyber coverage is becoming more necessary, it is also more costly at the same time.

> *"Companies will band together into associations that provide some risk and mitigation practice sharing, likely by industry and at captive layers."*

Coverage may increasingly come with a package of services including inspection, defense and monitoring.

While there are no large cyber newcos – yet – there are at least a dozen important MGAs that obtain capacity from incumbent carriers. I expect that some of these MGAs will ultimately become divisions of such carriers and that others will develop proprietary capacity — between those goalposts, significant dedicated capacity will develop in the sector.

Reinsurance market growth will be necessary as primary insurers typically cede 50-60% of premiums. The capital markets are off to

a good start. Deal experience to date has been good. Unlike the cat sector in which every deal in the first decade needed to be freshly sold into the generalist market, the cyber sector enjoys an audience of over 50 insurance-linked funds, for each of which cyber risk is absolutely diversifying.

Finally, there is work in progress in governments around the world to provide some high-level "security" support to the cyber sector. Government facilities have almost universally been responsive rather than proactive (Pool Re to Birmingham, Citizens & Cat Fund to Andrew, the CEA to Northridge & Loma Prieta). Our cyber-Andrew will be the midwife for our cyber-TRIA.

> *"Cyber is growing quickly enough that the 25-year journey of the cat sector will need to be compressed by a few years."*

But this is not the industry's first rodeo. A decade of careful work has generated a $12 billion premium sector that makes money and whose accumulation risks are cautiously watched. That is a good start.

Mike Millette

Managing Partner at Hudson Structured Capital Management Ltd, Board Member, CyberCube

DOWNLOAD NOW

DOWNLOAD NOW

DOWNLOAD NOW

Awards in 2023

InsuranceERM awards - Cyber risk solution of the year

InsuranceERM awards - Stress scenarios software of the year

Axco Global Insurance Awards

America’s Best Startup Employers 2023 - Forbes

Global Excellence Awards

InsuranceERM Americas Awards 2023 - Cyber solution of the year

InsuranceERM Americas Awards 2023 - Analytics solution of the year

Insurance Business UK’s 5-Star Diversity, Equity & Inclusion report

CBInsights Survey

Top 10 cyber insurance startups and insurtechs

ITC DIA Europe Top 100

United States’s 101 Top CEO’s in the InsurTech Space

10 Cyber Insurtech Companies Driving Innovation for the Industry

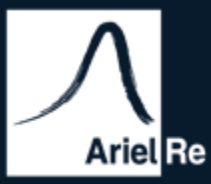
Cyber Security Awards 2023

Inside P&C awards - InsureTech Product of the Year

Inside P&C awards - Women in Insurance (Highly Commended)

Tracxn - “Emerging Startup Awards 2023”

Partnerships in 2023



Press releases in 2023

The insurance market will see greater partnerships with ILS fund managers as it transitions to Property, Casualty & Cyber

CyberCube's Portfolio Manager model utilized for first cyber cat bond

Accretive Insurance Solutions Utilizes CyberCube's Broking Manager to Drive Risk Transfer Decisions

CyberCube identifies potential targets in VMware ransomware campaign

Lockton Re cyber report says now is the time for cyber ILS

CyberCube enables brokers to better prepare clients for cyber insurance placements

CyberCube highlights areas of focus for the cyber insurance and broking community

Peak Re chooses CyberCube to underpin global cyber risk expansion

The Plexus Groupe selects CyberCube to quantify cyber risk decisions

Leading insurer Aviva teams up with CyberCube for suite of cyber solutions and services

Cytora and CyberCube partner to provide insurance underwriters with greater insight into cyber risks

CyberCube supports U.S. Risk Insurance Group in quantifying cyber risk financial exposure

Bishopsgate selects CyberCube's Broking Manager to gain competitive advantage

Prudent Insurance Brokers Join Forces with CyberCube

Press releases in 2023

The insurance market will see greater partnerships with ILS fund managers as it transitions to Property, Casualty & Cyber

CyberCube's Portfolio Manager model utilized for first cyber cat bond

Accretive Insurance Solutions Utilizes CyberCube's Broking Manager to Drive Risk Transfer Decisions

CyberCube identifies potential targets in VMware ransomware campaign

Lockton Re cyber report says now is the time for cyber ILS

CyberCube enables brokers to better prepare clients for cyber insurance placements

CyberCube highlights areas of focus for the cyber insurance and broking community

Peak Re chooses CyberCube to underpin global cyber risk expansion

The Plexus Groupe selects CyberCube to quantify cyber risk decisions

Leading insurer Aviva teams up with CyberCube for suite of cyber solutions and services

Cytora and CyberCube partner to provide insurance underwriters with greater insight into cyber risks

CyberCube supports U.S. Risk Insurance Group in quantifying cyber risk financial exposure

Bishopsgate selects CyberCube's Broking Manager to gain competitive advantage

Prudent Insurance Brokers Join Forces with CyberCube

Economy shows resilience to recent cyber attacks, but major events remain a risk

CyberCube's Broking Manager to empower BFL CANADA clients to make better cyber decisions

Fermat broadens relationship with CyberCube through license of Industry Exposure Database

MOVEit attacks shine light on the cyber (re)insurance industry's blind spots

Lockton Re expands CyberCube partnership with Industry Exposure Database

Ariel Re adds CyberCube's Exposure Databases and APIs to its suite of analytical tools

CyberCube report: Nation-state cyber hot zones offer a view into the future of cyber war

Cyber supply chain risks highlighted by IUA and CyberCube report

Toa Re selects CyberCube to strengthen its risk management capabilities

AXIS Closes Market's First 144A Cyber Catastrophe Bond

mShift partners up with CyberCube to automate the delivery of cyber insurance analytics

CyberCube launches marginal risk analysis capabilities at the point of underwriting with the latest Account Manager release

Videos in 2023

CyberCube's Event Briefing: ESXi Args attack on VMWare

CyberCube's Global Threat Briefing H1 2023

AI and the cyber threat landscape What to expect

CyberCube analysis: Identifying cyber vulnerabilities in French companies

Reflecting trends in CyberCube's Portfolio Manager Version 5 with Jon Laux

CyberCube's Portfolio Manager Version 5 - What Changed?

CyberCube delivers the world's leading cyber risk analytics for the (re)insurance industry, with over two-thirds of the global cyber (re)insurance market relying on its best-in-class data and analytics to power their cyber insurance growth. CyberCube's cloud-based solutions help (re)insurance organizations quantify cyber risk to facilitate insurance placement, underwriting, and risk aggregation management.

Editorial Content

Yvette Essen, Head of Content, Communications & Creative

Designer

Muhammad Ahmad, Graphic Designer

www.cybcube.com