CyberCube

# Cyber Predictions Report 2023


**Yvette Essen**

Head of Content, Communications & Creative, CyberCube


# Introduction

The start of a new year provides an ideal opportunity not just to reflect on the last 12 months, but also to prepare ourselves for the future. Many characteristics are likely to remain constant: a rise in the number of attacks, new targets being identified, and evolving threat actor tactics. Yet there will also be new areas of focus and trends to follow in 2023.

CyberCube prides itself on its deep bench of experts across all fields, including data science, security, threat intelligence, actuarial science, software engineering, and, of course, insurance. In this report, some of those great minds come together to share what they think will be the standout trends in 2023 to help you build a forward-looking view of risk.

Their predictions are wide-ranging, touching for example, on where we are in the underwriting cycle, how Artificial Intelligence (AI) will increasingly be utilized, the role of regulation and partnerships, and forecasting key developments in the insurance-linked securities (ILS) space. We hope you enjoy reading them.

# Pascal Milliare

Chief Executive Officer, CyberCube

## Prediction: Stronger partnerships will be forged as cyber market continues to grow

Cyber insurance has the potential to become one of the largest lines in the P&C insurance industry in the decades to come. However, that growth will only happen if there is a deep partnership across the value chain with a cross-section of industry participants.

The cyber insurance market is arguably no longer in its infancy. I predict that in 2023 the industry will work together in many different ways to help power the evolution of the cyber insurance market toward a more mature level, and deliver better value for the end customer.

In the coming year, underwriters and brokers will come under greater pressure to concentrate on value-added tasks, rather than spend their time on manual data entry or low-value screening. As we anticipate this shift in focus, CyberCube is collaborating with core technology systems providers used by our (re)insurance and broking clients to streamline our analytics and have them ingested into core systems through application programming interfaces (APIs).

The insurance community will also strengthen its ties with alternative capital providers to facilitate the growth of the insurance-linked securities (ILS) market. The reinsurance value chain will work together with ILS fund managers to bring new cyber reinsurance capacity to this market in 2023.

# Ashwin Kashyap

Co-founder & Chief Product Officer, CyberCube

## Prediction: Selective availability of capacity and a stronger focus on risk mitigation and cyber policy hygiene

I expect capacity to become available on a very selective basis because insurers and reinsurers are apprehensive about committing too much additional capital to grow their cyber business due to the fear of the unknown - and of large-scale cyber cat events in particular.

Market participants who want to allocate capacity towards cyber will need to develop a deeper understanding of cyber as a peril in 2023 , much like they have become comfortable with hurricanes and earthquakes. They will also need to gain greater trust in cyber models, which should present a credible reflection of reality.

The role of risk mitigation will also continue to increase in prominence. One of the redeeming characteristics of this line of business is that policyholders can improve their risk posture rather quickly and react to unfolding events by taking actions that can dramatically reduce the overall risk they present to an insurer. This is a lot harder to do in other lines of insurance, particularly property.

Consequently, there will be a standardization of policyholder cyber hygiene expectations from insurers. Cyber hygiene practices that insurers are likely to require include firmwide implementation of multi-factor authentication (MFA) and disabling Remote Desktop Services or having controls that require multiple levels of approval.

# Admiral (ret.) Michael S. Rogers

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

## Prediction: Insurers need to focus on how digitization can create supply chain issues

The insurance industry will need to focus on potential cyber supply chain issues as the world becomes more and more digitized. Our economic models and social structures are increasingly built around this idea of instantaneous connectivity that is never disrupted, which gives us bandwidth, connectivity, and stability. What will it mean if we continue to build this digitized world and yet its security and its capacity aren't always there?

This is being modeled out with supply chain issues. We have created an economic model whereby we believe we can drive our supply chains across the world, and will always have enough knowledge, insight, and unfettered connectivity. We thought we could generate enough capacity in terms of physical production at any given time, but COVID-19 has shown what happens when disruption arises to a far greater extent than anticipated.

What are the implications? It's about more than just the supply chain, which in some ways has become the poster child. Are we sure about the assumptions we've made about this world over the last 10 to 20 years in terms of our ability to operate in multiple domains in this physically dispersed world based on extensive virtual and network connectivity? Are those assumptions still valid? If they aren't, what are the implications for the future? I really think we will need to spend some time focusing on finding answers to those questions.

# Matthias Weber

Former Group Chief Underwriting Officer and member of the Group Executive Committee of Swiss Re, Board member, CyberCube

## Prediction: The insurance market cycle will stay alive

Are we experiencing a hard cyber insurance market? This apparently simple question is not that easy to answer. Cyber insurance is currently experiencing a supply-demand imbalance. As a result, prices for cyber insurance are moving up, policy terms are tightening, and demand for reinsurance is increasing. As a result, there is a widely held view that today's cyber insurance market is much firmer than it was a year ago. The cyber insurance market is "hardening".

But is this a truly "hard" market? Are cyber insurance premiums high enough for most insurance carriers to reap attractive levels of economic profit on top of their loss costs, expenses, taxes, and capital costs? We don't know, because a policy's future expected loss burden is not precisely known at the time when the policy is underwritten. In fact, the risk to the policy is likely to change while the policy is live. This risk of change is particularly pronounced with cyber insurance, as the weaponry of attackers and targeted attack surfaces expand quickly.

Hence, it will take some time until we know with certainty whether we are in a hard market as of today. And once we know, market softening might have started...


# Jon Laux

VP of Analytics, CyberCube

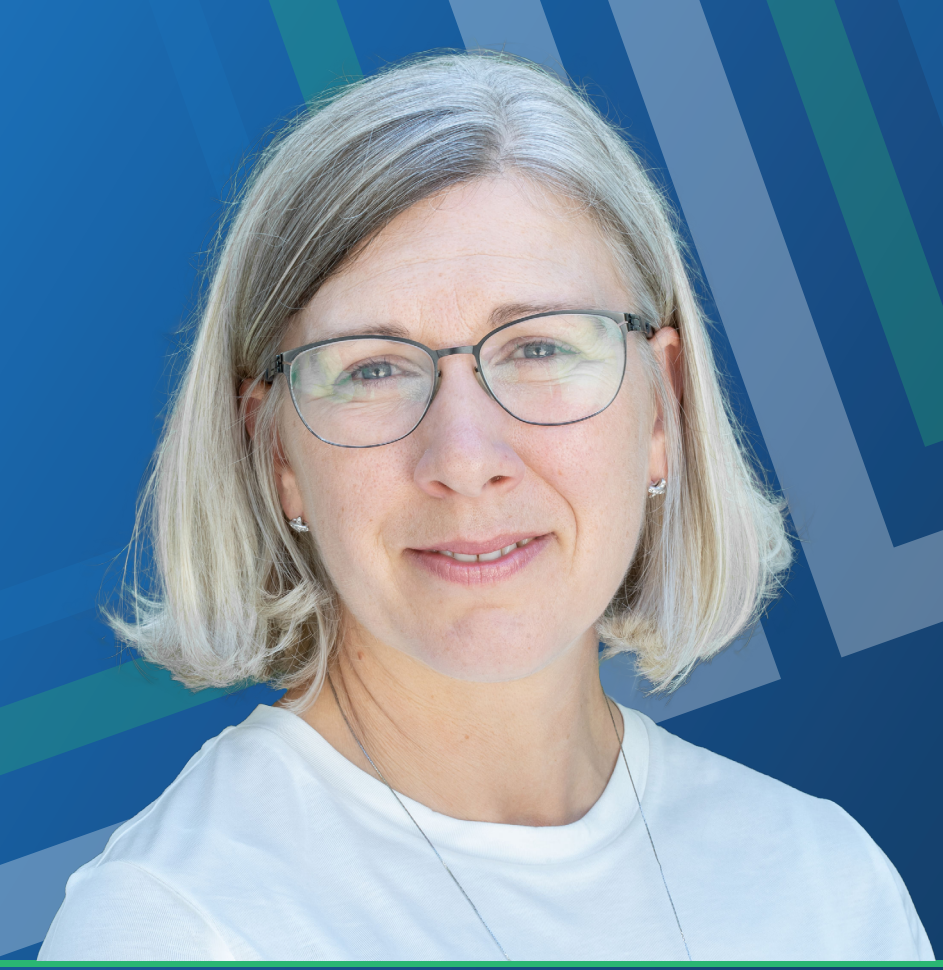

## Prediction: Heightened rate levels invite greater market capacity and shift (re)insurer's focus to defining tail risk

Cyber rates have risen dramatically in 2022, in some cases doubling, as insurers recalibrated from claims relating largely to ransomware. In 2023, rates will continue going up, but the pace of increase will slow to levels more comparable to other lines of business. The heightened rate levels will invite greater market capacity and shift (re)insurers' focus on defining tail risk.

There are some signs that we are approaching the peak of the hard market. Building insurance towers is easier, and quotes are generally available on all program layers. Some of the capacity that has been sitting on the sidelines in recent years is now reentering the market, with participants keen to be included in programs. Reinsurance capacity has become more constrained in recent years, but we expect conditions to ease as the rate rises in the primary market flow through. Additionally, reinsurance participants will have opportunities to become more creative, for example, by structuring event cover as well as aggregate stop loss cover.

From a portfolio perspective, the primary concern for insurers will be on the extreme tail as books have grown significantly. Increasingly, (re)insurers and brokers are under internal pressure to explain why their cyber strategies are sound, and they will need to perform a wide array of benchmarking, sensitivity, and real-time analyses for cyber risks to support their plans.

With this in mind, CyberCube recently launched the world's first set of detailed Exposure Databases. These aim to provide a foundation for cyber risk models to help insurers better understand the segments they are covering – or could be covering – and to give the (re)insurance community, collectively, a clearer view of the big picture around what's driving cyber exposures. We will be making further enhancements to our Exposure Databases and our suite of products in 2023 to help support the market.




**Rebecca Bole**

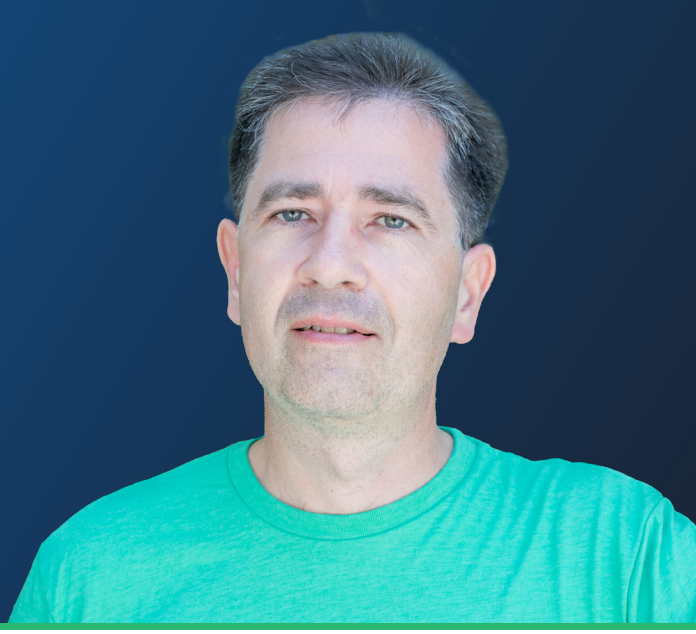
Head of Industry Engagement, CyberCube


# Prediction: Regulatory stress tests developed: As data is submitted, regulatory action may be taken

In 2022, we saw regulators start to gather data on insurers' cyber insurance aggregation risk - taking the research that has been ongoing these past years to a practical level. Many regulators are aware of the systemic nature of cyber risk and the potential for catastrophic losses arising from cyber attacks. As insurers' cyber exposures grow, more regulators are taking concrete steps to understand the scenarios that might lead to a catastrophic loss better and to seek data from the market on the financial impact of these scenarios on insurers' balance sheets. In 2022, notable activity featured:

- Lloyd's including three new Realistic Disaster Scenarios for data collection, which were jointly produced by Guy Carpenter and CyberCube.
- The Bank of England's Prudential Regulatory Authority launching four cyber stress tests into the market.
- Europe's insurance regulatory body, EIOPA, beginning a consultation on its proposed cyber insurance stress tests in November.
- The U.S. Treasury's Federal Insurance Office starting a consultation into the potential for a public-private partnership on providing financial relief for extreme catastrophic cyber events.

As data is returned on these stress test scenarios, regulators will gain a better understanding of the financial implications of a catastrophic event. As cyber becomes a larger part of underwriters' exposures, regulators are likely to take action to ensure tighter governance of the sector.




# Max Sokolov

Sr. Director, Software Engineering, CyberCube


## Prediction: AI adoption will accelerate

The adoption of artificial intelligence (AI) both on offensive and defensive sides of cyber security will accelerate in 2023. AI is becoming increasingly important in the evolution of both cyber attacks and defending against various threats as it helps analyze huge volumes of information, detect patterns, and boosts the automation of operations.

On the offensive side, the following trends are likely to become more pronounced:

1. To increase dwell time in a compromised environment without being detected, attackers will employ a set of AI-based techniques to improve detection evasion.
2. The cost optimization (in terms of both time and money) of well-known and established attack mechanisms like mass generation of phishing emails and websites, as well as improved efficiency of brute force password hacking.
3. AI tools will likely allow malicious actors to better identify weak spots in enterprise defenses and the most valuable targets for the attack. For example, using AI to identify the most vulnerable computer systems and networks, as well as the most negligent and careless individuals, will provide a faster and more accurate list of candidate targets to focus on. Similarly, accurate and rapid categorization of company assets (e.g. computers, personal mailboxes, persons with the highest access privileges, etc.) will help attackers move faster and with improved precision.
4. The personalization of attacks (e.g. highly tuned phishing emails) will expand to increase the probability of success.

In order to combat the evolving and emerging offensive trends cited above, defensive systems must adopt AI to improve:

1. The speed and accuracy of categorization and protection of assets based on their potential breach value.
2. Detection of user and software behavior to identify anomalies and distinguish malicious behavioral patterns from benign ones.
3. Accuracy and the automation of the log analysis to increase the signal-to-noise ratio for security engineers during mass-scale attacks.

## John Anderson

Principal Product Manager, CyberCube

# Prediction: Greater focus on using predictive data and cat loss metrics

Cyber analytics and financial modeling for the insurance industry continue to evolve and mature at a rapid pace year over year, with the past year being no exception.

Insurance carriers will have an increased focus on finding "predictive" data and analytics solutions in the year ahead. They will need to curate data that can provide lift for their underwriters and will otherwise emphasize the power of correlation between data and the likelihood of an incident, as well as pushing for data that can model for the severity of that incident.

The utilization of nat cat loss metrics will play an even greater role at a time when carriers will also be making advances in leveraging cat metrics in their underwriting decisions. Over the past 12+ months, there have been advances in terms of carrier forms addressing aggregation through policy terms and conditions. As carriers seek to get to grips with their potential accumulation risks, they will be increasingly interested in using cat loss exceedance probability metrics within underwriting guidelines. Understanding what a company's marginal risk impact is with regard to a wider portfolio will be a powerful tool for the most sophisticated insurance carriers.

In light of both of these trends, we've recently launched Account Manager version 4.0, which offers single-company cat loss metrics and builds upon new studies on security signals, and their correlation to incidents and the market. In the coming year, we plan to enhance Account Manager further, focusing on predictive modeling, marginal risk impact solutions, and refinements to signals and telemetry, to achieve even stronger correlation.

## Cody Stumpo

Sr. Director of Product Management, CyberCube

# Prediction: Carriers to focus on Defining Events

I envisage a lot of carriers exploring how to limit accumulation risk through event definition in 2023. Before going to market with new products, they will need to understand the impact of various possible wordings excluding or sublimiting widespread events on both price-informing metrics like portfolio Average Annual Loss and capital-informing metrics like portfolio Return Period Losses.

While Version 4 of CyberCube's Portfolio Manager can already do much of this testing, that's why in 2023 we will be supercharging Portfolio Manager Version 5's ability to help the market define this critical area. We think our clients will be able to make the case to their insureds that widespread event coverage forms a relatively small part of their protection; but is significant to the cyber insurance industry's ability to expand.


## Natalie Chin

Senior Principal Product Manager, CyberCube


# Prediction: Brokers to demonstrate their value proposition as rates stabilize

Cyber risk remains a dominant twenty-first-century risk, top of mind for reinsurers, insurers, and the enterprises that are their policyholders. Brokers are, of course, the linchpin in this insurance relationship.

The cyber insurance marketplace remains volatile heading into 2023, but in a different sense than in 2021/2022. There were a couple of years of seemingly unending rate increases to right-size insurers' cyber books and account for unprecedented ransomware attacks.
Another upcoming shift in the market environment is some stabilization in premiums, especially with new entrants helping to increase capacity. It's by no means a return to the soft market we saw pre-2020, but it does mean brokers need to solidify their value proposition yet again.

The first step they can take is upskilling their associates' knowledge of the changing cyber threat landscape to increase cyber insurance adoption from their existing client base. We often hear from brokers that only 10-20% of their clients are buying cyber insurance today. While they are seeing more and more success with larger clients, brokers can bring more resources to these clients by offering analytics and having access to cyber experts.

The other area in which I see brokers having an opportunity to differentiate in cyber is helping clients increase their insurability. CyberCube is launching a second product for brokers called the Prep Module aimed at helping brokers do exactly that. This new solution will provide clients with a better roadmap to buying and renewing their cyber insurance policies by keeping them informed and prepared to address the security issues that matter to their insurability. Underwriters are leveraging this type of data when selecting and pricing risk today. So now brokers will be able to supply their clients with the answers they need and give them more time to take action on them.


**Brittany Baker**

VP of Solution Consulting, CyberCube


# Prediction: The ILS cyber market will see real traction

Cyber risk as a new asset class for the insurance-linked securities (ILS) market has been a topic for discussion for several years. The current state of the insurance market has set the stage for real traction in cyber ILS in 2023.

Demand for cyber insurance has generally outstripped the supply the insurance industry has the capacity or appetite to support. Enterprises of all sizes struggled in 2022 to find the coverage they require at affordable rates - or any cover at all. Cyber managing general agents (MGAs) have seen large funding rounds, but their growth has been limited due to this capacity crunch. Traditional primary carriers are also struggling to find reinsurance treaties that satisfy their capital needs to keep up with their growth projections.

On the investment side, the nat cat ILS market returns have been badly hit over the last few years which has increased the desire to present new asset classes to investors in a way that wasn't necessarily required previously. Cyber has started to make its way into the mandates of different funds and groups, which are building up a solid technical understanding of cyber risk.

While there have been a few private cyber ILS transactions in the past, the industry is still waiting for the first 144a cat bond. 2023 is ripe for this to occur due to more sophisticated modeling, the development of industry exposure databases, and an increased understanding of cyber risk across the necessary stakeholders.

In order for the cyber risk ILS market to really take off, the first 144a cat bond will need to have certain characteristics. It must be simple and repeatable - if it's too complex or niche, then the industry will still be left waiting. It will need to clearly define the covered perils and their event definitions - if other investors still see vague definitions or all perils, they will remain on the sideline. Modeling and reporting agents have to prove they are up to the task - some may have experience in the nat cat world but others will be new to the game and will need to prove their value to the financial markets.

## Ross Wirth

Head of Client Management &
Technology Services, CyberCube

# Prediction: The popularity and maturity of cyber will continue to increase

Visibility and awareness of cyber risk will increase through 2023, as risk officers and risk managers broaden their definitions of risk. Cyber offerings will continue to mature, both as standalone coverage and embedded in traditional contracts. We will continue to transition from Property & Casualty to Property, Casualty & Cyber.

In response to the growth of cyber, we will see market leaders across the insurance value chain increasing the maturity of their offerings and how these are delivered across the enterprise and to the market.

Market leaders will embed cyber across their business units and offerings, rather than treating it as a separate vertical requiring standalone go-to-market capabilities and distribution. They will become increasingly sophisticated in how they standardize risk definitions and apply data consistently.They will also need to focus on ensuring a strong link between their understanding of individual risks and their portfolio aggregations.

As product lines expand and market leaders mature their offerings, they will explore additional sources of capacity. Expanded reinsurance and accessing broader investment vehicles via Insurance-Linked Securities will provide the required capital.

Existing players will partner with new entrants to provide liquidity to match market demand. These instruments will be well-defined vehicles that will start small and then grow as measures become standardized and shared across the market. One thing is for sure: 2023 promises to be another fast-paced year for cyber, with continued dramatic growth!

**Michael Millette**

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

# Prediction: Increasing use of mature cyber models to make meaningful business decisions

## Cyber Risk Model Maturity

Making sure that the models work is a regular part of our board discussions at CyberCube. We review model validation analysis – reviewing the model's ability to predict risk levels and provide useful pricing information to our clients. Cyber risk can evolve quickly, and models require regular updating. That said, the results anticipated by the CyberCube models align nicely with real-life observations. Below we highlight some performance insights from three different sets of models.

**Loss Ratio Models:** The current version of the model anticipated a mean 2021 loss ratio of 61% for the industry. NAIC filings indicate that the industry saw 65%. When we assess the distribution of results, the match to the industry is remarkable:

| | Percentile Distribution | | | | |
|---|---|---|---|---|---|
| Source | *5th* | *25th* | *50th* | *75th* | *95th* |
| CyberCube | 8% | 28% | 51% | 82% | 139% |
| NAIC Filings | 10% | 36% | 62% | 87% | 137% |

**Catastrophe Risk Models:** We have cataloged 42 notable cyber catastrophe events over the three years ending in April 2022. It is notable that 37 of these (88%) had a medium or high fit with a scenario in the CyberCube event catalog. We do not believe peer models picked up as many events as closely.

**Cyber Risk Selection Models:** Over the last year, we have published three reports analyzing the effectiveness of our security signals for risk selection. Our findings have been consistent and steadily improving. We find that companies showing at least one of our critical signals are six times more likely than average to suffer a cyber attack. For some of our signals, companies are 20 times more likely than average. The models are strong, and serve as a powerful pricing tool for the industry.

These findings are a really powerful testament of the models' maturity and power to inform meaningful business decisions. CyberCube started with a deep data set inherited from Symantec and has added to it every year with all the data from a customer base that includes many of the leading brokers, insurers and reinsurers in the industry. It is exciting to see the insights we can provide with the benefit of this abundant data.

# Notable Research in 2022

[Regional cyber conflicts could spark new threats in 2022: CyberCube]

[Insurers and reinsurers should stress test threat of Russian cyber attacks]

[CyberCube report highlights criminal cyber threat actors and their motivations]

[CyberCube supports new Insurance Institute of London book on cyber insurance]

[Ukraine cyber war fall-out and ransomware trends areas of focus in new CyberCube research]

[Russia's sovereign internet creates security risks with implications for cyber (re)insurance while war in Ukraine develops]

# Partnerships in 2022

# Product announcements in 2022

**CyberCube updates Portfolio Manager to reflect evolving cyber trends**

**CyberCube launches world's first Exposure Databases to enrich cyber modeling**

**CyberCube enables proactive cyber cat management at point of underwriting with latest Account Manager release**

# Awards and Recognitions in 2022

Break Out Awards **- Business Insurance**

Stress scenarios software of the year **- InsuranceERM**

**DIA** Top 250

Emerging Startups 2022: Top Insurance IT Startups **- Tracxn**

Insurtech 50: The most promising insurtech startups of 2022 **- CB Insights**

Parametric Insurance in 2022: the 150+ companies to watch **- InsTech**

California's 101 Top CEOs in the Computer Space **- Best Startup**

Insurtech 100 **- Fintech Global**

Top 25 Insurtechs **- Intelligent Insure**r

# Corporate News

**CyberCube Announces $50 Million in Growth Capital Financing to Further Advance Cyber Risk Analytics**

**Editorial Content:** Yvette Essen, Head of Content, Communications & Creative
**Design:** Muhammad Ahmad, Graphic Designer

CyberCube