The Risk of a Cyber Catastrophe

Solving for insurers' fear of the unknown

GRAY RHINO SERIES

Gallagher Re

Executive summary

- Business and insurance sector leaders are concerned about the prospect of a large-scale, systemic cyber attack—a “cyber catastrophe” risk.

- Cyber insurance is an evolving, rapidly growing market, but it has never had to deal with such a catastrophe. By comparison to markets in natural catastrophe risk, where disasters like hurricanes, wildfires, tornados and floods are regular occurrences, this makes a cyber cat event inherently difficult to model and price. The industry is hampered by a lack of tangible scenario data points, inconsistent or non-existent cyber catastrophe claims coding frameworks and an overarching high level of uncertainty.

- Cyber modeling remains in its relative infancy. There is substantial divergence in the modeling of larger scenarios, which does not inspire confidence among capital providers.

- In response, the (re)insurance sector is managing its exposures through appetite, pricing, tighter wordings and exclusions.

- Meanwhile, demand for cyber insurance continues to grow, and following triple-digit rate rises in the past three years, insurers can have more confidence they are pricing the risk correctly. But while the supply of capital is increasing in parts of the market, there remains a reluctance from capital providers to offer cost-effective and systemic solutions that solve for carriers’ true fear of the unknown.

- Corporates are also seeking routes to mitigate their risks. The cybersecurity industry has made considerable progress since 2017’s NotPetya attack in reducing vulnerability to attacks. New developments, such as the rise of artificial intelligence and the creation of new cybersecurity tools offer the prospect of better risk management. However, in the wrong hands, they could also pose questions for US and international security frameworks—keeping the market in a state of flux.

- Model providers are investing in improving their capabilities, but the (re)insurance industry will require more and better data from insured clients on their cyber vulnerabilities and loss experience to improve models—and hence—pricing.

- This may enable more granular coverage, for example, by differentiating between large corporations and SMEs—the former vulnerable to targeted attacks, while the latter want to insure their exposure to a longer-tail, system-wide event.

In January 2023, the World Economic Forum's (WEF) Managing Director, Jeremy Jurgens, shared the results of his organization's Cybersecurity Outlook[1] at Davos. 91% of the business leaders polled by WEF said that a far-reaching, catastrophic cyber event is at least somewhat likely in the next two years.

Clearly, it is a risk on the minds of CEOs and chief information security officers (CISOs). But the question that preoccupies the (re)insurance industry is: how much could it cost?

The prospect of a cyber catastrophe—or cyber cat—has been on the (re)insurance sector's worry list for a while. In 2022, Zurich Insurance's CEO, Mario Greco, declared that cyber attacks could become "uninsurable."[2] Greco appealed to governments to "set up private-public schemes to handle systemic cyber risks that have not yet been quantified, similar to those that exist in some jurisdictions for earthquakes or terror attacks."

Meanwhile, regulators are concerned that not enough businesses have cyber insurance coverage. In May, Lindy Cameron, Chief Executive of the UK's National Cyber Security Centre, told an audience of insurance executives[3] that "it has been said that only 200,000 of the 2.7 million businesses in the UK with a website buy stand-alone cyber insurance policies."

Cameron continued, "I'd love to believe that this was because it was covered as part of their wider business insurance. But I don't believe this is the case. This is partly due to a basic lack of understanding about cybersecurity—but the insurance industry also has a key role to play here."

Cyber remains a young risk class for the (re)insurance industry overall, and insurers are still working out what risks they are comfortable covering. Carriers are having to carefully manage their exposures, while model-builders are investing heavily in developing their offerings. New technologies, such as outside-in scanning, offer the prospect of more tailored underwriting. But is the sector ready to cover a truly systemic catastrophe?

> "There are many challenges around the cyber market today and this is only going to intensify as the class grows. Gallagher Re has long held the view that cyber is going to become the most capital- and expertise-constrained class within the insurance industry. We have invested in a team which is uniquely equipped to help our partners navigate these challenges, some of which are described in this paper."
>
> Ian Newman
> Global Head of Cyber, Gallagher Re

What would a cyber catastrophe look like?

When considering the risk of cyber cat, the biggest problem for the industry is that we've never really experienced one. Because there has never been a truly systemic cyber disaster, there is no universally accepted definition for what might cause one and what form it might take—and no industry consensus on modeling the risks.

This makes for a stark contrast with natural catastrophes, such as hurricanes or earthquakes, where risks are much better known and modeled. And it creates a particular challenge for insurers in securing reinsurance capacity,[4] as capital providers in that market are grappling with the same uncertainty.

A shared understanding of what a cyber catastrophe could look like would be a useful starting point. This, in turn, needs to be translated into consistent claims reporting frameworks.

Gallagher Re has developed its own in-house "CyCat" wordings and has had success in attracting and retaining capacity on the basis of these wordings (see section below: **Cyber cat reinsurance**).

Ed Pocock, Gallagher Re's Head of Cyber Security, adds: "Essentially, [a cyber catastrophe] will interrupt the ability to conduct business, which in turn causes frustration. The duration will depend on the type of catastrophe. Traditional modeling divides cyber into three types of cats: data breach and the loss of data; outage and the inability to access data; and a lack of data integrity, where data becomes corrupted or unusable. The largest cyber cat events will contain elements of all three."

Paolo Cuomo, Executive Director, Strategic Advisory at Gallagher Re, takes a different tack. "If the world ends or descends into anarchy because of a cyber event, your organization is irrelevant...[but] you don't want an event in which your business is disproportionately affected. You won't be forgiven for that. That leads to Directors and Officers (D&O) claims. So, executives need to be asking the question—what's the likelihood that something will happen that we're less prepared to deal with?"

The consensus is that cyber catastrophes will be infrequent events, but severe and impacting a large population of users rapidly. (The slower a cyber cat progresses, the easier it is to interrupt its progress.) The banking and payment sectors are frequently cited as being likely to sit at the heart of any systemic cyber cat.

.

It has long been unclear who might intentionally launch a catastrophic cyber attack and why. While there have been small-scale and covert operations, nation-states seem unlikely to engage in large-scale cyberwar, according to Ed Pocock. The interconnectedness of the global economy would leave the attacking state almost as exposed to damage—albeit digital interdependence is somewhat decreasing. In any case, policies are quite likely to exclude explicit acts of war (see later section "How are insurers managing their exposures?").

Organized criminals are also unlikely candidates. In general, they prefer not to draw attention to themselves, and triggering a cyber catastrophe would make them the target of police and security services around the world.

The most likely origin of a systemic cyber event, therefore, is an accident, an unintended consequence of a smaller event, or a combination of two apparently unconnected events. These might include a piece of malware that proliferates out of control; the failure of a widely-used free data service, which has unexpected knock-on effects; or even the actions of "script kiddies"—the internet's version of teenage vandals.

This makes these events truly unanticipated and inherently hard to model—again, contrasting with weather-related risks such as hurricanes. A cyber cat could be something the industry has never seen before—challenging the assumptions of actuaries, modelers and cybersecurity teams alike.

But while the origin story of a cyber cat event remains vague and hypothetical, there's greater agreement on what could turn a known and manageable problem into a catastrophe.

For an event to threaten the system, it either has to knock out one of the internet's crucial pieces of centralized infrastructure or go uncontrollably viral.

A prolonged cloud outage is the first of the two most common suggestions—for example, the failure of Amazon Web Services or Microsoft Azure—rendering huge swaths of the business world inoperable.

The second is a new, virulent strain of malware, potentially a second cousin of NotPetya, one of the most destructive pieces of code in the last decade. Unexpected vulnerabilities in widely used software are a related risk (see the Log4j section in the box below). Companies can mitigate these risks with improved staff training on social engineering and phishing attacks, but thanks to the speed of software development, they will likely always remain material.

.

Viral malware and widespread vulnerabilities

NotPetya

NotPetya is arguably the closest the world has come to a systemic cyber event and forms the foundation of many of today's cyber models. A variant of the Petya malware, NotPetya, was released in 2017, primarily against Ukrainian businesses via Ukrainian tax preparation software. It is believed to have been a Russia-backed attack.

Taking advantage of a vulnerability in Windows, NotPetya encrypted an infected machine's entire hard drive. Although it then displayed a ransom request, the virus seemed to be entirely destructive. Instructions on how to pay the ransom were attached to a fake, randomly generated Bitcoin address, meaning there was no way for the attackers to collect the funds.

The attack is estimated to have caused economic damage costing over USD10 billion (estimated insured loss of USD3B). Although a significant influence on today's models, much of the cyber market's exposure to NotPetya was non-affirmative, so a similar style of attack would now be excluded.

Log4j vulnerabilities

A series of vulnerabilities emerged in Log4j in November 2021. These vulnerabilities allowed remote code execution, meaning a threat actor exploiting them could potentially take over a server and exfiltrate or destroy data and connected systems. Log4j is an open-source logging tool found in online software repositories and is prevalent across widely adopted software and tools. These software repositories are used in a similar manner to how insurance wording experts take contract clauses from wording repositories and insert them into policy wordings.

A zero-day vulnerability,* it presented an immediate and widespread threat to multiple industries all over the world with external-facing services running Log4j. Since its discovery, there have been potentially millions of attempted attacks, with many cybersecurity experts expressing their concern. Jen Easterly, Director of the US Cybersecurity and Infrastructure Security Agency, reportedly[5] labeled the vulnerability as the most serious in her career. Despite being an unknown, patches were quickly developed for the Log4j vulnerability through collaboration across the cybersecurity industry. And whilst mass breaches have so far been averted, Microsoft is still viewing it as a high-risk situation.

*When threat actors can exploit a vulnerability before developers have detected it or had the chance to develop a fix.

Could the cloud burst?
Gallagher Re is close to announcing a partnership with an internationally renowned educational establishment with the objective of assessing the potential impacts of a major cloud computing failure.

Iain Willis, Research Director at the Gallagher Research Centre, said the project hoped to unlock more reinsurance capacity by increasing the degree of certainty about one of the most discussed major systemic events.

"One very exciting element of this project is to understand the respective vulnerabilities of the various cloud service providers," says Willis. "Cloud service providers have dozens of products and understanding how cyber attacks could potentially scale or propagate in space and time will be key to estimating realistic probable maximum losses."

So can we model the risk?

Iain Willis, Research Director at the Gallagher Research Centre (GRC), sees the need for further development of the models as a critical factor for capturing and understanding cyber risks. "Models that can capture a risk more precisely allow for the development of products and pragmatic pricing. The old adage that 'models make markets' tends to ring true. The concern currently would be that the divergence of existing model output shows the wide range of uncertainty in this peril. This is where research can really help," he said.

Currently, there are three industry-standard cyber models—Guidewire's Cyence, CyberCube and Moody's RMS Cyber Solutions. Three vendors, three ways of looking at the world and three outputs.

"These third-party tools are meant to quantify loss," says Justyna Pikinska, Global Head of Cyber Analytics at Gallagher Re. "They focus on cloud, data breach and ransomware, but each company sees cyber differently. Different data, different approaches and different outcomes. If we model the same portfolio in all three tools, we get divergent results."

The progenitor of cyber-cat modeling is natural catastrophe modeling, and cyber models are likely to follow a similar path of maturation.[6] But there are key differences.

"Nat cat models have the distinct advantage that their perils follow defined scientific laws with standardized scales of magnitude and intensity," says Simon Heather, Gallagher Re's Head of Cyber Cat Modeling. "Everyone can agree what a Category 5 hurricane looks like and can gather plenty of empirical data about peak wind speeds, pressure, tracks, genesis, etc. which are characteristics of all hurricanes. The same isn't true of a cyber event. We've no classification of event magnitude that is independent of loss impact, no real agreement on what a cat event looks like, and there are no standard features of all cyber events. This means that each model vendor must rely on their own event classifications, which often leads to broad differences in model frameworks and outputs."

According to Adam Banas, a Cyber Consultant at Gallagher Re, there are other challenges too: "Users don't necessarily know which model is most accurate as results often differ greatly between them. If they are converging, it's a result of a concerted effort to understand the models and how they treat the specific nature of the underlying portfolio."

Heather says: "I think we will see some convergence—or at least a reduction in divergence. But that's not a given."

"One of the reasons we can't guarantee convergence are the 'unknown unknowns'. There are none of those in nat cats but in cyber everyone's worried about them. Every time a new piece of software comes out, there are new unknown unknowns. It's an irreducible uncertainty."

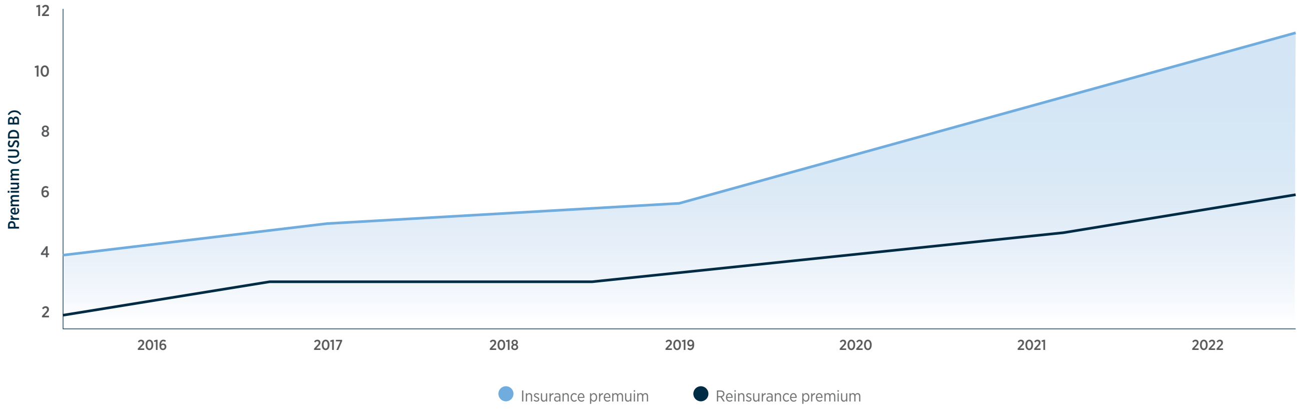
"One of the reasons we can't guarantee convergence is the irreducible uncertainty in cyber systems due to undiscovered vulnerabilities that attackers could utilize, and every new software or technology increases this uncertainty. There is much less of this type of uncertainty in nat cats, which allows for more model convergence."

The divergence and immaturity of cyber modeling is one of the key drivers behind the chronic shortage of capacity in the cyber reinsurance market.

Overall, capacity has been increasing. Gallagher's cyber capacity report in May took total premiums written in the market as a proxy for the volume of capital flowing in to back them, and found reinsurance premiums rose from around USD2B in 2016 to USD6B in 2022.

But this still falls well short of the potential reinsurance demand from carriers, who have been incentivized to take on more cyber risk by rapidly rising policy rates in recent years. Gallagher's report found the insurance market has now largely corrected following ransomware losses in 2019—20. In the US, the average cyber policy rate has jumped by about 180% since 2019, according to figures from the Council of Insurance Agents & Brokers.[7] Such rate rises, together with improvements in portfolio optimization and more stringent underwriting, have resulted in "a greater number of carriers looking to take on additional cyber exposure and premium," the report concluded.

Premium growth in insurance and reinsurance as a proxy for capital influx



Source: Gallagher Re, NAIC, S&P Global and Swiss Re Institute calculations.

Increased modeling credibility will be important for unlocking more capacity and bringing in new capital providers to the reinsurance market, including through nontraditional routes, such as insurance-linked securities.

There are reasons to be optimistic on this front. The report pointed out that both well-established vendors, such as RMS, and cyber-specific new entrants like CyberCube and Guidewire have been investing "heavily" in improving their capabilities.

How are insurers managing their exposures?

Confronted with a rapidly evolving market—and models whose outputs can vary widely—the insurance sector currently uses traditional underwriting measures to manage its exposure. They must be nimble.

"The cyber market has an incredible ability to pivot and is super-reactive to emerging trends," says Adam Banas, as he lists the exclusions and warranties cyber insurers are increasingly relying upon. "Critical infrastructure such as internet service providers (ISPs) like BT as well as cables and satellites are not covered. Ransom payment cover has at times been removed or sublimited in many cases."

Prompted by the Ukraine crisis, Lloyd's of London recently introduced cyber-specific war exclusions for state-backed events[8] to a mixed reception. "The bulletin may have been too prescriptive," Banas concludes. Another challenge is attribution, Banas says, which is a particular problem for cyberwar exclusions as it may be far from clear who is behind an attack.

Jennifer Braney, Cyber Consultancy Lead at Gallagher Re, says: "Exclusions for war, state-sponsored cyber operations and systemic exposure in general will continue to develop, as carriers and regulators focus on market sustainability. This means that some state-sponsored scenarios may be excluded depending on the specifics of the situation, the coverage in the policy wordings and developments in legal precedent."

Some have applied sublimits to cyber cat events. Should a cloud outage extend for more than three days, or a new strain of malware run riot, a policyholder's purchased limit of, say, USD10M could be reduced to USD2M by a sublimit.

Banas explains the rationale: "In a big systemic event, most losses come from businesses that are essentially cannon fodder. What that means is that you're unlikely to be as badly affected as you would be by a targeted attack. The damage will be less material."

Meanwhile, some players are adopting another tactic borrowed from a more mature class—property cat—and diversifying their portfolios of exposures by geography.

This approach works well in cyber, as the internet itself is becoming more regionalized. 2017's NotPetya malware attack led to the creation of digital borders within networks so that CISOs could reduce the risk of contamination. Cloud providers' operations are also split into geographic zones—US East and West, Ireland and the Nordics, for example. An outage will generally only affect one or more data centre in these zones. Content delivery networks—a network of interconnected servers that speed up webpage loading—are also relatively regional in their construction. In addition, some regions and countries have been isolated from the full effects of ransomware attacks because of their languages—Japan, for instance.

Local time is another factor that creates inherent regionalization. The first 12 hours of a cyber attack are the most critical. If that attack is launched in North America late in the day, by the time Europe wakes up and switches on its laptops, news of the attack will be highly visible and defenses may already be available.

Cyber cat reinsurance

The past few years have seen substantial demand from insurers to cede cyber risk to reinsurers. In 2022, close to 50% of all premium written was ceded to the reinsurance community, having risen steadily from 40% in 2019.[9]

While these percentage levels of cession may fall back in the years ahead as insurers grow more comfortable with the class, in absolute terms, the amounts are likely to continue to grow as the market does. And as with any insurance class, a key reason to buy reinsurance is to cover your tail-risk—your catastrophe risk.

Gallagher Re's view is that in developing Cyber Reinsurance Event definitions, we need to be broad enough to cover all types of cyber perils and scenarios, although some reinsurers aim to reduce coverage to specific named perils.

Jennifer Braney says: "Fundamentally, event definitions seek to link back all aggregating loss from that event to either a common originating cause, or a series of related acts or incidents. A time limit may also be applied to the period of claims aggregation, depending on the breadth of aggregation language in the event definition.

"Gallagher Re has developed two in-house 'Cyber Cat' wordings to cover the two broad types of aggregating language and has had success in attracting and retaining capacity in the traditional and alternative markets on the basis of these wordings."

In addition, the development of the nascent market in cyber catastrophe bonds also offers a fresh source of capacity for cedants.

Beazley launched one of the market's first cyber catastrophe bonds in January 2023.[10] It provides the firm with one year of indemnity reinsurance protection against all cyber perils if Beazley's losses from an event exceed USD300 million, the insurer said.[11] The catastrophe bond attaches at a level of catastrophic loss not previously experienced by the market. Gallagher Securities acted as the sole structurer and placement agent for this landmark transaction.

Can new technologies improve the market's view of risk?

Gallagher Re has been studying the potential for new technology to improve cyber insurers' view of risk for some time and published an in-depth study[12] into one particular development last year—outside-in scanning technologies.

A divide has opened up in the cyber market between larger traditional insurers and a group of new arrivals; primarily US tech-based managing general agents (MGAs) who use outside-in scanning technologies to assess their policyholders' vulnerabilities. Instead of asking a client to respond to a lengthy questionnaire about their security posture, this new breed of MGAs uses technology to rapidly scan the client's internet-facing surface and then makes underwriting decisions based on the results of the scan.

After a zero-day event, carriers can also use this tech to identify potentially exposed clients and help them patch or protect themselves, before losses emerge.

Some of these new MGAs have achieved impressive growth and published data to show that their policyholders are less likely to have a cyber event. Justyna Pikinska has mixed views: "Outside-in scanning can prevent some of the claims. At Gallagher Re, we've looked into this technology and work closely with multiple data providers. It's very helpful for SMEs purchasing a low limit of cover but does not necessarily show you all the results, particularly when considering targeted attacks on larger companies. If a malicious attacker wants to go after [a large corporate], they will find a way."

Other new technologies may help insured companies beef up their cyber defenses, such as so-called self-healing systems.[13] This new breed of network, incorporating machine learning and other AI tools, is designed to identify errors or faults within itself and potentially repair them without human intervention.

The system achieves this through monitoring to quickly gauge deviations from standard configuration settings and either repair or re-install the affected component. Industry commentator Forrester Research has recommended them, and many in the IT community are optimistic about their potential to defend against cyber attacks.

AI could help to defend against cyber attacks—or make them worse

Since ChatGPT was unveiled in November 2022, hackers have been busy. Already, large language models are being deployed by bad actors to write phishing emails, analyze code to find vulnerabilities or even to write malicious code.

As noted above, markets such as Japan have historically experienced fewer claims from phishing attacks due to the difficulties that fraudsters have in convincingly translating their attack emails, but large language models are facilitating better translations. With AI still in its infancy, its potential to disrupt the cyber market and cybersecurity appears almost unlimited.

“AI is very exciting—a new paradigm,” says Pocock. “But we’re going to see a lot of catastrophizing. It does lower the bar for threat actors to launch a broader range of attacks with less manual dependency, phishing being a good example.”

That said, AI is a double-edged sword. If attackers can use it, so can defenders. “The balance of power doesn’t change if you have good defenses,” says Heather. One example would be the much-increased ability of anti-virus software to detect intruders using AI to identify their behavior, rather than the traditional approach of identifying signatures.

> “There will be points over the next five years when threat actors have the edge, other times when good guys do. However, AI will not change the fundamental nature of the cyber cat or its likelihood.”
>
> Ed Pocock
> Head of Cyber Security, Gallagher Re

Problems may emerge if there is a mismatch between attackers and defenders, however—and this is most likely amongst small and medium enterprises (SMEs). “SMEs are more vulnerable,” says Heather. “They often don’t have an understanding of AI—a lot of the time, IT security is not their focus.”

The way forward: Better data, better models and a more granular market

In a young market with far less loss experience to draw upon, greater disclosure and transparency among the cyber community would be welcomed by the (re)insurance industry.

At present, the regulatory environment tends to compel organizations to disclose only when they have fallen victim to a data breach. In the US, a positive step was last year's Cyber Incident Reporting for Critical Infrastructure Act, which requires companies that are attacked to report significant cyber incidents and offers them protection in order to incentivize them to report.[14]

But the Gallagher Re team believes that the focus for disclosure should not be solely on successful attacks. There is value in being open about near-misses.

> "The cyber insurance industry needs to have much better knowledge and data to share and address the risk collectively."
>
> Adam Banas
> Cyber Consultant, Gallagher Re

Governments and regulators have also been pressing for data-sharing. In her address to the industry in May,[15] Lindy Cameron of the UK National Cyber Security Centre said: "The lack of aggregated data sharing across the industry on the scale and impact of incidents is hampering the maturity of the market, and the models on which cyber insurance is priced."

She added: "I recognize that aggregated insurance data is a valuable commodity. This makes sharing data difficult for you. However, I urge you to collaborate with us and with each other to make best use of aggregated data, in order to help us understand the true scale and impact of cyber incidents."

With greater disclosure and sharing of data, more effective models and a larger body of data residing outside the models will come.

More granular data may also help the insurance industry better characterize the different risks facing different parts of the market. In particular, the exposure to cyber cat risk may be very different among SMEs and so-called nano businesses.

At present, the insurance industry treats smaller businesses as simply a miniaturized version of a large business. But in cyber terms, SMEs are an entirely different species. "I think it's bold to assume the SME market will behave like larger firms. SMEs are a blind spot for current models," says Heather.

Currently, 65% of global cyber premium comes from companies with revenues greater than USD 1B, according to figures from Gallagher Re's Cyber Industry Exposure Database. This is the type of business most likely to be targeted by a bespoke attack. However, at least 86% of all policies are for SMEs with revenues less than USD 10M, businesses highly likely to fall prey to an automated attack—or be drawn into a systemic event.

There is a growing argument for dividing the cyber market into two—one market and product suite for large players, a second for SMEs. This is reinforced by the idea that SMEs may be more vulnerable to AI-powered attacks than their larger counterparts and may find outside-in scanning techniques more pragmatic.

If the cyber market does bifurcate on the basis of policyholder size, modelers would need to focus more keenly on the differences between large and small companies, and appropriate parameterization to reflect them.

Pocock believes a diversification of models would be positive for the market. "The upshot of diversity of modeling is a good thing. Cyber is young, so if we all do it the same way, there's a risk of us having a collective delusion."

For Heather, there's another modeling challenge the industry needs to meet—the (re)insurance sector's reliance on nat cats as a basis for modeling cyber cats.

"We need a new approach not wholly based on established practices. We need to dislocate cyber from the familiarity of nat cat model frameworks," Heather says. "Cyber events behave more like a pandemic than an earthquake or hurricane."

When a nat cat and a cyber cat are compared side by side, many important differences emerge. The duration of a cyber cat may be much longer; nat cats behave predictably, cyber cats do not and can have peaks and troughs of claims; and cyber is a class in which the policyholder's behavior has a far greater impact on the nature of their risk. Consider a hurricane; a property owner cannot move the property out of the path of the storm. In cyber, a CISO can effectively isolate their business from an emerging threat.

Banas argues that cyber should be seen through the lens of financial lines (FL). “A lot of the contractual language around event-based reinsurance is coming from FL because it is the other ultimate systemic risk. In FL, one failure can lead to another failure and another. It doesn’t have the confines of time and space, and it’s much more difficult to tie individual losses together to one event. When does it start? When does it end?”

Finally, there’s the overwhelming challenge of people—the employees whose behavior has such an overwhelming impact on an organization’s security. The most realistic option is improved education and training, coupled with automated detection and response systems.

But in the midst of this swirling change, solid foundations are being created. The pool of data around cyber risk continues to grow. The industry has learned from historic events and developed safeguards that did not exist even five years ago.

Jennifer Braney says: “It seems like the cyber market gets a lot more scrutiny than some casualty-flavored classes of business. We don’t hear about the latest model developments or the expected size of the loss for the next global financial crisis, for instance. I think this is largely down to a lack of understanding of cyber and because we haven’t seen a cyber systemic event before.

“The lesson there is for the whole market to upskill on cyber and at the same time question ourselves on how we are able to get comfort around the fear of unknowns in other lines of business.”

Contributing authors

Adam Banas
Cyber Consultant, Gallagher Re

Jennifer Braney
Cyber Consultancy Lead, Gallagher Re

Paolo Cuomo
Executive Director, Strategic Advisory, Gallagher Re

Simon Heather
Head of Cyber Cat Modeling, Gallagher Re

Justyna Pikinska

Global Head of Cyber Analytics, Gallagher Re

Ed Pocock
Head of Cyber Security, Gallagher Re

Iain Willis
Research Director, Gallagher Research Centre

[1] 2023 Global Cybersecurity Outlook, WEF
[2] Cyber attacks set to become ‘uninsurable’, says Zurich chief, *Financial Times*, December 2022
[3] Lindy Cameron at BIBA Conference 2023, National Cyber Security Centre, May 2023
[4] See Gallagher Re’s recent report, The vital role of capital in cyber (re)insurance, May 2023
[5] CISA warns ‘most serious’ Log4j vulnerability likely to affect hundreds of millions of devices, Cyberscoop.com, December 2021
[6] Evaluation of cyber models, Gallagher Re, 2022
[7] See also: the CIAB’s Commercial Property/Casualty Market Index for Q1 2023, p.6
[8] Market Bulletin: State backed cyber-attack exclusions, Lloyd’s of London, August 2022
[9] The vital role of capital in cyber (re)insurance, Gallagher Re, May 2023
[10] Beazley secures $45m cyber cat bond with Fermat Capital a backer, Artemis.bm, January 2023
[11] Beazley launches market’s first cyber catastrophe bond, Beazley, January 2023
[12] Looking from the Outside-In: Can taking the threat actors’ viewpoint help insurers?, Gallagher Re, April 2022
[13] Self-Healing Cybersecurity Systems: A Pipe Dream or Reality?, *Security Week*, June 2021
[14] Cyber breach reporting to be required by law for better cyber defense, PwC
[15] Lindy Cameron at BIBA Conference 2023, National Cyber Security Centre, May 2023

Learn more about our client-focused, collaborative approach.
Connect with us today at **GallagherRe.com**.

It’s the *way* we do it.

Gallagher Re

Gallagher Re is a business unit that includes a number of subsidiaries and affiliates of Arthur J. Gallagher & Co. which are engaged in the reinsurance intermediary and advisory business. All references to Gallagher Re below, to the extent relevant, include the parent and applicable affiliate companies of Gallagher Re. Nothing herein constitutes or should be construed as constituting legal or any other form of professional advice. This document is for general information only, is not intended to be relied upon, and action based on or in connection with anything contained herein should not be taken without first obtaining specific advice from a suitably qualified professional. The provision of any services by Gallagher Re will be subject to the agreement of contractual terms and conditions acceptable to all parties. Gallagher Re is a trading name of Arthur J. Gallagher (UK) Limited, which is authorised and regulated by the Financial Conduct Authority. Registered Office: The Walbrook Building, 25 Walbrook, London EC4N 8AW. Registered in England and Wales. Company Number: 1193013. www.ajg.com/uk. GRE6249