



Cyber
Insurance
Academy

Systemic risk & cyber insurance

January 2023



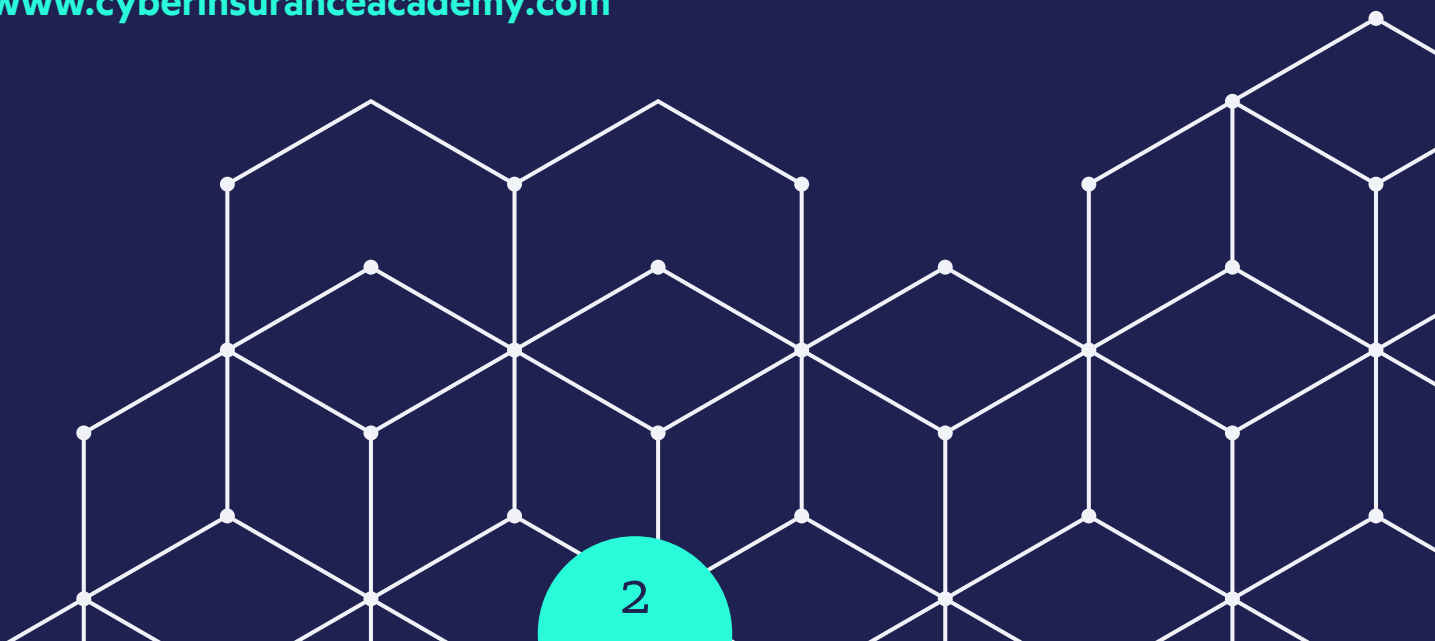


Managing systemic risk has been a core focus of cyber insurers for the past 24-48 months. Previously an elephant in the room, carriers are now waking up to the far-reaching, devastating effect of systemic cyber events on the health of their business.

This guide explains what systemic cyber events mean, how they operate in practice, and how cyber insurers can address this modern exposure.

The Cyber Insurance Academy is a 24/7 academy designed to build and expand cyber knowledge in the insurance sector. Our training is accredited by the Chartered Insurance Institute (CII).

www.cyberinsuranceacademy.com





Contents

What is Systemic Cyber Risk?	4
What Causes Systemic Cyber Risk?.....	5
Recent Systemic Cyber Events	8
How Systemic Risk Impacts The Insurance Market Today	9
Systemic Risk In Property	9
Limited Impact Events.....	10
Widespread Impact Events	11
Controlling Systemic Cyber Risk	14
Identifying Potentially Catastrophic Systemic Cyber Risks...	14
Pricing Systemic Risk.....	15
Improving Systemic Cyber Risk Resilience	16
The Policy	18



What is systemic cyber risk?

In cybersecurity, systemic risk refers to



"The possibility that a single event on one small part of a digital system could cascade to other interconnected third parties sitting on that same system."

In other words, it is a single cyber event that impacts multiple insureds. For example, a successful cyberattack on one part of a digital business system could spread like wildfire to other parts of that business system and to other companies operating on it.

Systemic risk threatens to topple entire industries and economies and is not limited by time and geography. Eyeing up a significantly lucrative opportunity, hackers are taking advantage of this risk and are increasingly focusing their efforts on attacking complex interconnected systems.

What causes systemic cyber risk?

Global digitalization & cyber risk

Modern businesses are becoming increasingly dependent on technology for their operations. But this journey of digital transformation has, in turn, provided threat actors with significantly higher opportunities to exploit virtually undetectable vulnerabilities and exposures, free of the boundaries of time and space.



“The rapid growth of systemic risk is directly correlated to our increasing dependence on SaaS providers and is set to feature as a key, inherent cyber risk to any modern organization in the years to come.”

Recent years have seen a rise in the severity and frequency of attacks and have caused the market to harden. Ransomware incidents in particular have attracted headlines in recent years due to the severe costs they often impose on attack victims.

Catastrophic ransomware & malware attacks:

NotPetya

2017

Attackers exploited a tax software tool used mainly in Ukraine with malware. The attack then spread and affected many major organizations in Europe, the U.S., and elsewhere, resulting in around \$10 billion in losses.

WannaCry

2017

A ransomware attack impacted more than 200,000 computers around the world. Fortunately, there was already a patch available to stem the impact quickly.

However, it should be noted that email compromises and data breaches have also driven the frequency of cyber incidents, especially since remote working patterns have been more widely adopted.



"Insurance professionals need to understand the cascading effect of systemic risk, supported by accurate, reliable cyber catastrophe models."

Supply chain cyber risk

The dawn of the ransomware 'epidemic' marked the first major challenge to the fast-growing cyber insurance industry and the hardening of market conditions. But in addition to ransomware, the market has vied to gain control over the domino effect that one cyber event can have on many hundreds and thousands of insureds. This risk has risen as businesses have increasingly relied upon outsourced suppliers to deliver products, systems, and services. Given the breadth of business interruption coverage, it has been a crucial point of focus for many cyber carriers.

Catastrophic supply chain attacks:

Solarwinds

2020

Cyber attackers infiltrated the software of a major IT network analysis vendor, adding malicious code that went undetected for months and affected approximately 20,000 firms using the software in several countries.

Hafnium

2021

Alleged nation-state actors gained access to on-premises servers at potentially hundreds of thousands of firms by exploiting a zero-day vulnerability in commonly used software.

These events could have been considerably worse - here the attackers were motivated largely by espionage and financial gain rather than wreaking complete havoc and disruption. There is a very real possibility for an attack that could be both widespread and destructive, causing a cyber catastrophe that could go beyond disrupting supply chains and crippling critical infrastructure.

In order for the market to reach its full growth potential and unlock more capital, This growth in understanding is vital across the entire market - not just among the underwriters.

Recent systemic cyber events



The last 24 months have seen at least eight systemic cyber events that cyber catastrophe models would class as 'doomsday' events (in other words, events that create massive financial loss to the insurance sector).

The **2021 Log4j** crisis provided a key example of systemic cyber risk stemming from the modern-day business supply chain. Researchers discovered a severe vulnerability in a popular, open-source logging system called Log4j. The software is embedded in millions, if not billions, of consumer devices and business systems worldwide, meaning that cyber threat actors could take advantage of the massive potential attack surface to launch large-scale attacks with relative ease. As soon as alarms were raised, programmers tried to fix the issues to prevent what has been called Log4Shell attacks. While no cyber attacks have yet been attributed to the Log4j crisis, the crisis highlighted the potentially catastrophic impact of systemic cyber events.

Managed Service Providers (MSPs), which typically provide third-party infrastructure support to thousands of customers, have been a key area of aggregation. The attack on the MSP, Kaseya, is a good example of a systemic cyber event.

Kaseya

2021

The impact of a ransomware attack against a single company's software product cascaded across their client base, comprising more than 1,000 organizations, rendering them inoperable.

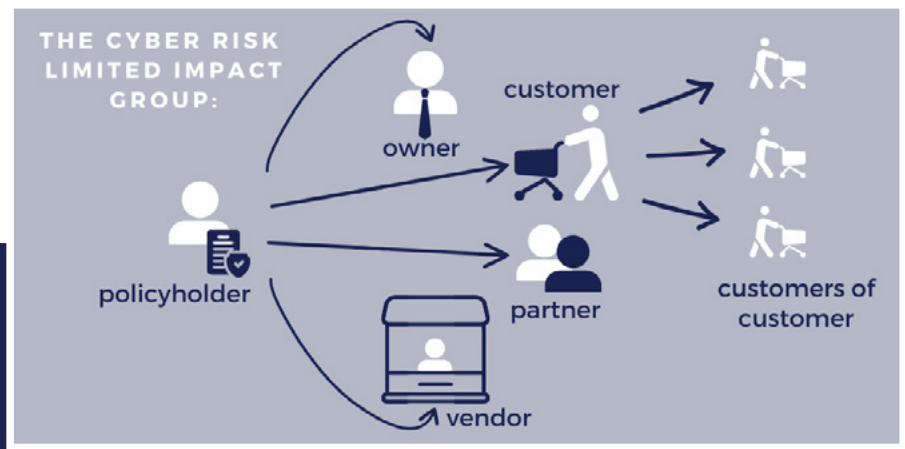
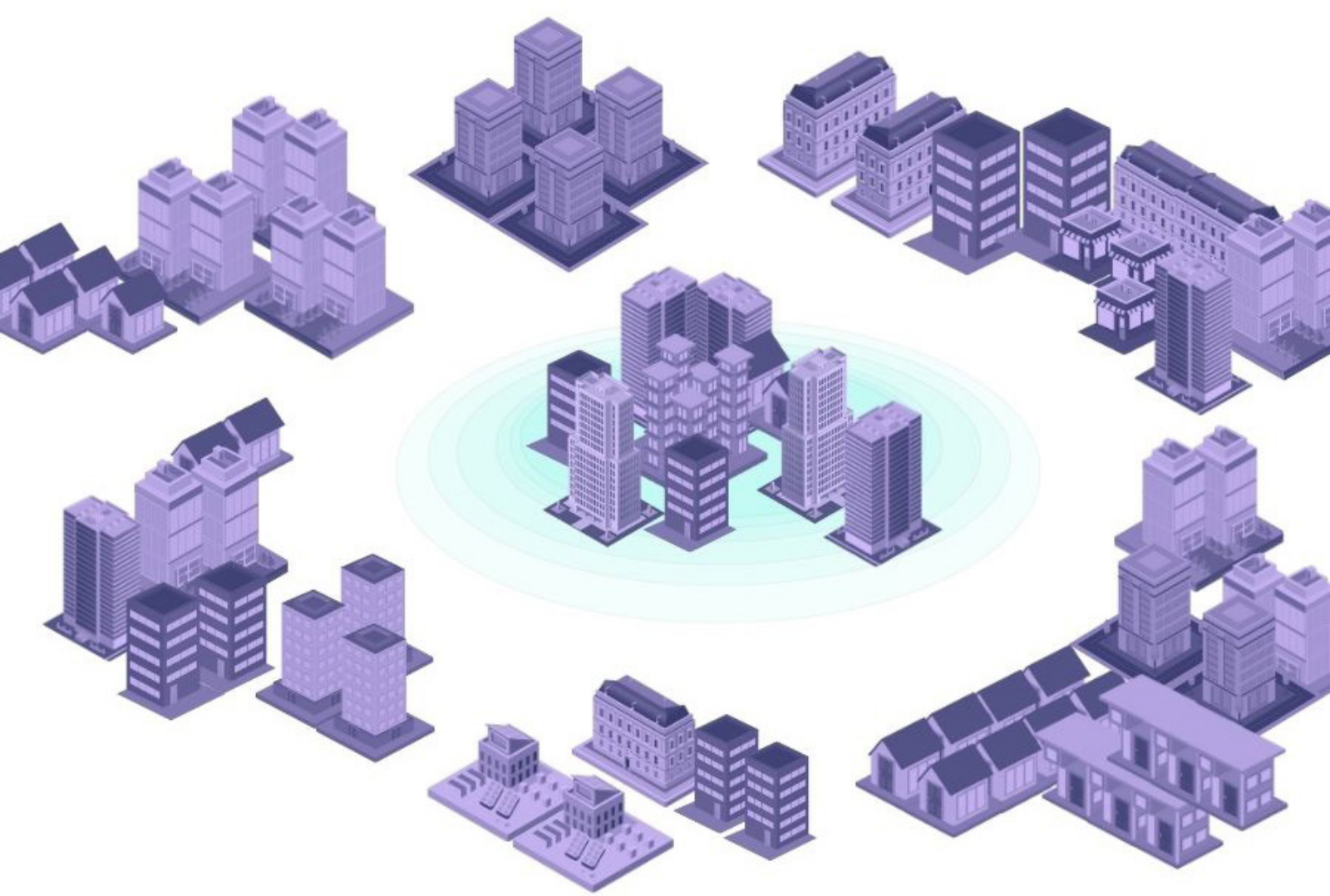
How systemic risk impacts the insurance market today

Systemic risk in property

Systemic risk is not a new phenomenon in the insurance market; historically, it has been dealt with in property policies. Most property risks, like building fires and theft, have **limited impact**. Some, like earthquakes and floods, have **widespread impacts**. Insurers have treated these kinds of events differently because an event that impacts many policyholders at the same time could lead to accumulated losses, potentially to the point of exceeding the insurer's ability to pay claims.

Because of the potential financial impact which widespread catastrophic events can have on insurers, certain coverage in property insurance policies can only be purchased separately and with its own set of limits and retentions. This way, insurers are able to manage their exposure to catastrophic events and policyholders know they will be able to recover their insured losses in the event of a claim.

Like property insurers, cyber insurers already absorb a significant amount of systemic risk. However, many cyber insurers are currently struggling to identify the point at which their systemic risk tolerance should end in order to provide a sustainable solution to the market. Better training and understanding of technical, cybersecurity principles will enable insurers to apply, for example, exclusions to more intelligently manage their systemic cyber risk exposure, or for a cyber catastrophe reinsurance market to develop and cushion the impact of certain categories of events. Similarly to property, the cyber liability policy can consider two umbrella categories of events: Limited Impact Events and Widespread Events.



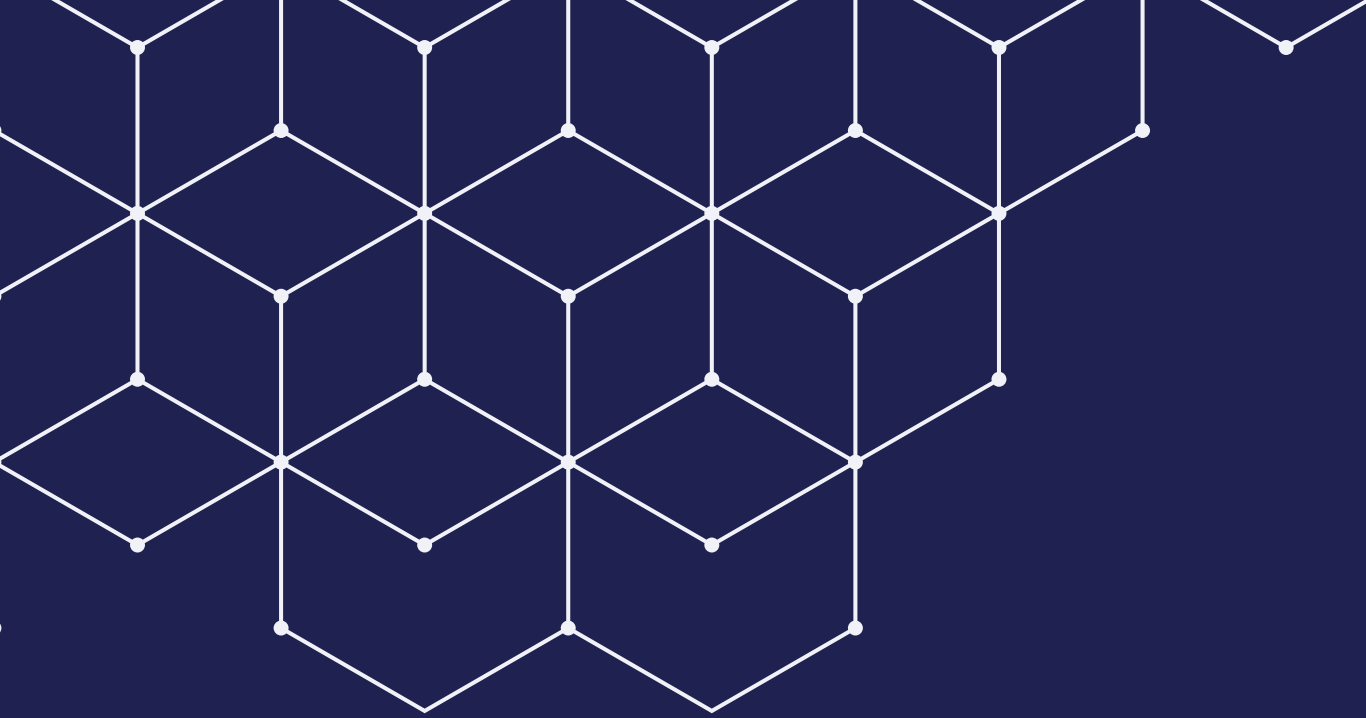
Limited impact events

These affect the policyholder and other entities that the policyholder has a defined relationship with (such as owners, vendors, partners, customers, and customers of customers). Together, they form what is known as a “Limited Impact Group”.

Widespread impact events

These affect businesses beyond the policyholder's Limited Impact Group. They can be carried out concurrently or automatically against a wide number of victims.






The internet has become a crucial infrastructure in today's modern world - if an internet company suffered a cyber incident, the potential scale at which this incident could be felt is enormous. An outage at a trusted cloud computing firm, for example, could impact the business operations of thousands, even millions, of organizations at once.

Brokers or agents can work together with the policyholder to identify coverage options that meet their unique cyber exposure. The policyholder can then purchase the appropriate amount of Widespread Event coverage and retentions, so that, if they become affected, they will be able to recover their insured losses.

Against the backdrop of increasingly frequent, severe, and sophisticated cyber attacks, insuring in this way will ensure the long-term sustainability of the cyber insurance industry.



It is worth noting, however, that, in the context of property, insurers can expect the cost of supply of goods and labor to increase as the impact of a natural disaster widens (known as the “Demand Surge” theory). But, as things stand, this phenomenon does not impact the cyber market in the same way. The outcome of systemic cyber events so far suggests that losses do not increase with the number of organizations impacted. This is because there is often one universal decryption key provided to resolve the problem, or ethical white hackers may provide a free solution on the internet.

Controlling systemic cyber risk

Identifying potentially catastrophic systemic cyber risks

The adoption of cyber insurance has skyrocketed worldwide in recent years. In the space of 24 months, brokers have seen the product go from hard-to-sell to hard-to-buy, with smaller companies looking to shore up against threat actors. But with this increased demand for insurance, coupled with the rising severity and frequency of cyberattacks, insurers have been forced to carry greater aggregated cyber risk. We have listed key scenarios that could prompt a systemic event below.

Severe known vulnerability exploits

Software vulnerabilities are discovered on a regular basis and require patches in order to avoid being exploited. Companies that do not address severe, known software vulnerabilities are key targets for threat actors and carry high risk.

Severe zero-day exploits

Zero-day software vulnerabilities have not yet been discovered and are therefore unpatched and potentially severe. It is therefore easy for hackers, who secretly know about these vulnerabilities, to exploit them. Even companies with robust cyber hygiene may face exposure to zero-day attacks.

Software supply chain exploits

Here, malicious actors, normally state-sponsored, infiltrate trusted digital systems and enter, like a Trojan horse, into an organization's network. They are expected to continue and accelerate as geopolitical hostilities grow.

Infrastructure outages

The 2021 Colonial Pipeline incident demonstrated how attackers could use ransomware to cause major infrastructure outages, affecting key services and the millions of citizens who rely on them. Infrastructure outages can be the result of a cyberattack, but also of system failures, human and programming errors, and non-malicious cyber incidents.

Pricing systemic risk

Underwriters are supported by cyber catastrophe models that have been developed over the last five-to-ten years. However, these models must be recalibrated constantly in order to meet what is a very dynamic and emerging risk. Ultimately, however, these models provide insurers with the ability to understand the aggregation in their portfolio and to gauge what their financial losses would look like in a given scenario, which is then priced back into the premiums charged to the clients.

Improving systemic cyber risk resilience

Once key systemic cyber risks are identified, resources must be committed to improving cyber resilience.

While there is some tolerance to systemic cyber risk in the market, policy carriers and other insurance professionals must understand the aspects of this type of catastrophic cyber exposure in order to provide adequate protection to their clients, while maintaining healthy capital reserves. In addition, insurance professionals must invest in client education, guiding them through best practices for tackling their increasing exposures, addressing the systemic risks in their business operations, and preparing for a potential cyber catastrophe.

Due diligence

Thorough due diligence should be undertaken on any third-party IT providers and cyber security defenses must be designed around them. Organizations should also comb through their contracts to assess any indemnities for which they, or the third party, may be liable.

Market cooperation

The threat of catastrophic cyber events will require increased collaboration between the private and public sectors on disclosure and reporting requirements following cyber incidents. This will improve the quality and quantity of actuarial data available to underwriters and carriers and will allow for better-priced, better-structured liability policies. Governmental cooperation with insurers on the evolving cyber threats at hand will enable a more stable and sustainable cyber insurance market and, ultimately, a stronger economy, should attackers seek to exploit systemic risk and cause widespread destruction.

Continuous underwriting

Cyber carriers are increasingly focusing efforts on continual, passive monitoring of businesses they insure via non-invasive testing, and advise their insureds of risks and events on a frequent and ongoing basis to prevent attacks from happening in the first place. Clients appreciate this value proposition and the proactivity of the market, particularly as this will help to reduce premiums long-term. However, articulating and responding to this complex and quickly-evolving risk is challenging; carriers implementing continuous underwriting into their policies must leverage technology to gather this supporting information.

Minimum requirements

Cyber underwriters previously wrote on an exposure basis, looking at the loss following a cyber event and the methods of containment needed to stop it. The rise in ransomware events shifted this focus to applying cybersecurity controls and boosting cybersecurity hygiene to prevent attacks from happening altogether. Without these controls and safety measures, the insured will not be covered.

Risk aggregation

Cloud service providers are part of every modern business. If parts of a hosting provider experience downtime, then all the companies in that hosting region will experience business interruption that could potentially be covered by their policy.

It is therefore important for cyber carriers to ensure that their book has a healthy distribution across providers and regions. In fact, insurers should maintain close contact with cloud providers such as AWS, Microsoft, and Google, to deepen their technical understanding of how these providers structure their cloud products, their regional zones, and uptime ratings. In turn, insurers can incorporate their cloud services into their books and offer coverage in a sustainable manner.

The policy

Insurers must be proactive in adjusting their offerings to suit the changing market needs. It is important to note that, when talking about systemic cyber risk, it is the outcome that the insurer cannot sustain, rather than the trigger of the event (such as a ransomware event itself or a critical vulnerability).

Coverages

Today, core coverages include incident response expenses, first-party cyber risks, third-party cyber liability, professional liability, and cyber risk management services (Technology, PR, and legal). Whilst these provide important risk transfer solutions for cyber-savvy organizations, the cyber insurance product has not yet reached peak maturity and cannot sufficiently address the constantly evolving cyber risk.

It is likely that coverages will be modeled closely on property insurance for policies covering catastrophic events. Coverage for catastrophic cyber events should be clearly delineated from the general coverages available, producing more transparent pricing, maintaining coverage availability, sharpening underwriting, and improving client retention.

Waiting periods

The average downtime experienced in 2022 stayed relatively stable at around less than a week. That is lower than figures from 2020-21, where the downtime following a ransomware event stood at eleven days. However, in light of the potentially catastrophic fallout following systemic events, waiting periods on most cyber policies today (typically lasting less than a day) do not offer insurers sufficient protection against over-exposure to systemic events and they are subsequently likely to consider extending these waiting periods for such events.

Exclusions

Some key contractual wording includes:

Infrastructure exclusions

These will protect capital against internet failure risk.

Natural perils exclusions

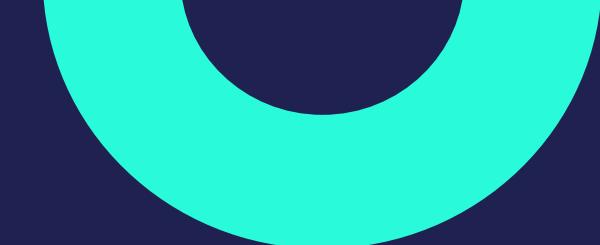
These protect against natural events that cause widespread downtime (such as a hurricane that hits the entirety of the US's East Coast, causing a total blackout in that region).

War exclusions


It has been widely reported that Lloyds of London has recently mandated the inclusion of war exclusion clauses starting in March 2023. This is because state-backed attacks are a subset of systemic risk, and not, as is commonly misunderstood, in response to the war in Ukraine.

For an exclusion to apply, the carrier must prove that the event would fall within the category of cyber warfare. It is worth noting that these exclusions have been legally fraught and have rarely been relied on by insurers, so much so that we have yet to see the war exclusion clause applied where coverage is actually denied. The 2014 Sony attacks, for example, were attributed to North Korean cyber warfare but the insurance market still paid out under the policy.

However, the market has undergone substantial change since 2014, and the new war exclusions are in place to bring much-needed clarity.



The insufficient understanding of systemic modeling in the market has ultimately led to a dearth of much-needed capacity and unstable pricing that does not accurately reflect the investment a business has made in its security measures and overall cyber hygiene. To increase profitability in this age of business interruption, the cyber insurance market needs more data - data that we did not have access to five years ago in the dawn of Ransomware-as-a-Service and when pricing was lower. To unlock more capital in the market and allow it to scale, we must accurately and appropriately address our systemic exposures.



The Cyber Insurance Academy is a 24/7, online academy for insurance professionals who truly want to stand out. We combine specialist, multidisciplinary, and professional expertise, with CII-accredited education and training programs on all things cyber insurance and emerging risk. We pull insights from every corner of the insurance sector, with our community of over 500 cyber insurance professionals from over 40 countries.

Learn more at [our website](#) and on [LinkedIn](#).

To enquire about our accredited cyber insurance courses, please email support@cyberinsuranceacademy.com. Our team would be happy to help you.

The information in this guide is correct as of 01 January 2023. We pride ourselves on bringing complex technical concepts down to earth with content that you can trust, but, given the rapid pace of change in the cyber insurance sector, some or all of the facts in this guide may become outdated.

www.cyberinsuranceacademy.com



Bringing Cyber Insurance **Down To Earth**

www.cyberinsuranceacademy.com

 @CyberInsuranceAcademy

 @CyberInsAcademy

 @CyberInsAcademy