# Cyber Systemic Risk/ Product Update:

## Broker FAQs

CHUBB

September 2024

Chubb is committed to continuing to lead the cyber insurance industry by providing direction and structure to help put it on a path to long-term sustainability.

Today, the frequency and severity of cyber events is causing many insurers, including Chubb, to evaluate their pricing, terms, and conditions. In recent months, multiple widespread cyber events have compromised targets ranging from software supply chain and email security vendors to data servers and infrastructure. The events involved several types of cyber attacks with the potential to escalate into catastrophic events.

As a result, Chubb is developing new and innovative solutions to manage these exposures. Chubb will continue to offer the core cyber coverages that our policyholders and distribution partners know and understand – however, we are also restructuring our terms and conditions around widespread events and partnering with industry associations and governments on different ways that might provide more informed coverage certainty for all parties.

## Impact on Cyber Brokers and Policyholders

Chubb anticipates our new solutions will provide distribution partners better long-term stability and growth within the cyber insurance market. Brokers will have an expanded opportunity to demonstrate their expertise for clients, including the ability to more clearly illustrate how much insurance is available for systemic exposures, customise the terms and conditions for client-specific exposures, and augment different coverages with value-added loss mitigation and risk advisory services. Chubb's new approach will leverage concepts familiar to most brokers and clients who are experienced with property insurance and property catastrophe insurance. Over time, a structured approach to quantifying catastrophic cyber risk should result in more cyber insurance capacity in the market.

# Cyber Risk Marketplace

**What is driving the current strategy changes for cyber insurance?**

Cyber incidents and threats are increasing and evolving. More than 18,000 new software vulnerabilities were published in 2020, nearly tripling from 2015, and continue to grow steadily.[1] Meanwhile, nearly 1.2 million new malware threats were identified in 2020, more than double the number from 2015.[2] While tactics such as ransomware have become more common and costly, business email compromise and data breaches continue to drive cyber incident frequency to some of the highest levels ever, especially with the increase in remote working arrangements. The increasing frequency and severity of such cyber events is pressuring insurers' attritional loss ratios, while systemic exposures with catastrophic potential grow ever more pervasive.


**Do other organisations share Chubb's viewpoint on the topic of systemic cyber risk?**

Yes, we believe that other organisations, governments, regulators, and rating agencies have observed the magnitude and urgency of this topic as well. In 2020, the U.S. Congress formed the Cyberspace Solarium Commission, chaired by Senator Angus King (I-ME) and Representative Mike Gallagher (R-WI). After a year-long study, the Commission concluded that the U.S. is at risk from a catastrophic cyber attack and is "dangerously insecure in cyber."[3]

In Europe, the European Union Agency for Cybersecurity (ENISA) was set up over 15 years ago to tackle the rising number of serious cyber incidents impacting public and private sector. Their new report published in April 2021 highlights that in light of today's cybersecurity threats, the global cybersecurity workforce would need to grow by 89% for organisations to defend their critical information and communications technology (ICT) assets effectively. In order to address this critical situation, national governments started to implement a number of programmes and policies.

In the UK, Defence Secretary Ben Wallace announced in October that the UK was building out a new digital warfare centre to bolster the UK's resilience to cyber attacks.

Additionally, the insurance ratings agency AM Best reported in June 2021 that "the prospects for the cyber insurance market are grim," noting "the far-reaching implications of the cascading effects of cyber risks and the lack of geographic or commercial boundaries" and concluding that insurers "whose risk management approach is deficient when it comes to cyber can find [themselves] subject to accumulation risk beyond [their] risk tolerance and could face rating pressure."[4]

**Please visit the links below to access observations from other organisations:**

- Executive Order on Improving the Nation's Cybersecurity (US Government): www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
- Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market (US Government Accountability Office): www.gao.gov/products/gao-21-477
- Cyber Insurance Rates Could Rise 50% in 2021 (MarshMcLennan Agency): www.marshmma.com/blog/cyber-insurance-rates-could-rise-50-in-2021
- Balancing Risk and Opportunity Through Better Decisions (Aon): www.aon.com/2021-cyber-security-risk-report/

### How does Chubb's strategy compare to the industry?

Most of the cyber insurance industry is focused on the narrower issues of ransomware and rate adequacy and is addressing these issues by lowering capacity, increasing rates, and making industry- or coverage-specific underwriting adjustments. While Chubb is taking similar actions, we are also drawing upon our decades of experience and significantly larger business scale to focus on the bigger-picture issue of systemic exposures. While other organisations have talked about the need for this within our industry, to date there's been little material action. It's likely that Chubb will lead the movement in this space.

### Can advanced cyber underwriting techniques mitigate the risk of cyber catastrophes?

Chubb has a dedicated team of cyber risk engineers and underwriters, and we are introducing new threat analysis and AI tools within our underwriting processes. Additionally, we provide our cyber policyholders access to a comprehensive suite of loss prevention and mitigation services. Our proactive investment in these areas has resulted in Chubb's cyber underwriting results outperforming the broader cyber insurance industry.[5] Despite these significant investments, many cyber threats are engineered specifically to evade internal controls and best practices. No underwriting or loss prevention control can completely eliminate the risk of cyber catastrophes.

### What is a systemic cyber exposure? How is Chubb defining this term?

In our view, "systemic" refers to an exposure that has the potential to affect many clients due to commonalities or shared elements of exposure, whereas "catastrophic" refers to a systemic risk that actually manifests into severe or large losses for many policyholders.

### What catastrophic cyber risks have emerged in recent years?

The ever-increasing reliance on technology by organisations and consumers as well as the interconnectivity of technologies and partners have created an environment in which cyber risks can expand exponentially. Cyber events are also having more widespread impact. Over a 100-day span from December 2020 to March 2021, several major attacks compromised targets ranging from software supply chain and email security vendors, to data servers and municipal infrastructure. In total, well over 100,000 organisations around the world were affected by these events, resulting in disruptions for millions of customers and citizens, as well as substantial economic losses. As an example, the Solorigate software supply chain attack, where malicious code was embedded in an update of a trusted network analysis software, affected 20,000 companies and government agencies. This event could have been much worse if the intent had been to steal or destroy critical data or other information.

## The following types of risks, particularly in combination, have been identified as having the potential to escalate into catastrophic events:

**Severe Known Vulnerability Exploits:**

Some known software vulnerabilities that are not patched can be severe, in that they are easy to exploit, can be deployed remotely with limited access privileges, and can cause significant adverse impact.[6]

**Severe Zero-Day Exploits:**

Certain software vulnerabilities that are known by cyber criminals but not yet by anyone else can be easily exploited, are potentially severe, and often lack protection.

**Software Supply Chain Exploits:**

These attacks are effectively a Trojan horse that allows bad actors to enter systems through trusted, certified software.

**Infrastructure Outages:**

Critical societal infrastructure, such as electrical grids and telecommunications services, face potential risk of failure on an enormous scale, whether due to a cyber attack or non-malicious cyber incidents, including system failures, human errors, or programming errors. The attack earlier this year on Colonial Pipeline, the gasoline supply company serving the east coast of the U.S., leveraged an infrastructure outage through a ransomware attack that caused gas shortages for millions of citizens and businesses in several states.

**Other Widespread Events:**

Certain types of cyber attacks can be carried out concurrently or automatically against a wide number of victims, ultimately causing a catastrophic cyber event. The Internet and some telecommunications services have risen to the level of critical societal infrastructure, and some large cloud computing firms are so widely used that an outage would impact the operations of thousands or millions of companies.

**Ransomware Encounters:**

While not necessarily systemic in nature, ransomware attacks, which hold targeted organisations' or individuals' electronic files or information hostage until a fee is paid, are now being carried out with industrialised efficiency, with ransom demands continually escalating. Some destructive attacks may masquerade as ransomware, such as the NotPetya and WannaCry events.

# Chubb's Cyber Product Offering

**The cyber insurance market has been discussing ransomware for years. Is Chubb looking at it differently now?**

We have been analysing ransomware trends for several years and, as these trends have evolved, so have our underwriting strategies. To help manage the risks, we have responded with changes to underwriting strategy (e.g., avoiding certain classes or businesses that lack certain controls), retentions, limits, and coinsurance. Chubb is also applying signal-based underwriting for these risks, which analyses weighted factors and risk signals obtained from various internal and external sources to help us identify risk factors for clients and prospects. Chubb's new cyber product offerings will offer even more ways to configure sublimits, coinsurance, and retentions for ransomware encounters across multiple insuring agreements.

**How many systemic cyber risk claims has Chubb received so far?**

Over the past nine months, Chubb has received hundreds of cyber notices associated with major widespread cyber events.

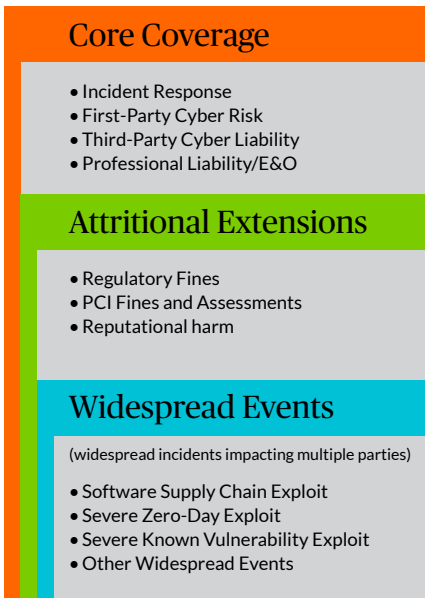
**Why are we continuing to see so many changes in the cyber market? Has the insurance industry experienced similar upheavals with other lines of business?**

Cyber insurance has only really matured as a segment in recent years, and even now, it is still very much an evolving line of coverage. At the same time, cyber risks are dynamic and escalating rapidly in complexity and severity. Historically, the property insurance market experienced shocks from sudden events of unprecedented scale, such as the 1906 San Francisco earthquake and the September 11th terrorist attacks. Solutions were developed in the aftermath of those events which provided more clarity around named perils and made separate coverages available for catastrophic risks. With cyber insurance, we have an opportunity to act now to improve overall product design and also to possibly create solutions with governments, which can provide stability for the insurance market and coverage certainty for clients.

**Will Chubb continue to offer the same cyber coverages that you offer now?**

The same core coverages that we currently offer – incident response expense, first-party cyber risk, third-party cyber liability, and professional liability – will continue to be available. In addition, Chubb is making a distinction between Limited Impact Events and Widespread Events. We anticipate that our core products will accommodate an estimated 90 percent of historical losses under the standard Limited Impact Event coverages.

Chubb will underwrite for significant attritional risks, but will also offer additional coverages for systemic exposures with widespread and catastrophic potential as extensions to the main cyber insurance product, allowing us to offer these coverages in a more structured, sustainable way. These will be referred to collectively as Widespread Event coverages, and will be inclusive of the several sub-components outlined in the policy. Widespread Events and each sub-component will be subject to a specific limit, retention, and co-insurance amount. This is similar to the way property insurance has addressed catastrophic risks such as floods and earthquakes for well over a century.




**What types of coverage extensions should we anticipate?**

Chubb will incorporate many coverage enhancements within its core cyber insurance product that previously were only extended via endorsement. These include attritional extensions such as regulatory fines, Payment Card Industry (PCI) fines and assessments, reputational harm, deceptive transfer fraud, preventative shutdown, and more. Chubb also will offer separate coverage extensions to accommodate Widespread Events, such as software supply chain exploits, severe zero-day exploits, and severe known vulnerability exploits. The graphic on the left provides an overview of this breakdown. Clients and prospects will need to work with their broker to determine the unique cyber risks they may face from their operations and IT environment, and then select the coverage extensions that make the most sense for them.

**Is Chubb's pricing going to change for cyber coverages?**

Pricing will continue to reflect each client's specific coverage needs and risk profile. Where jurisdictional approval is required to issue insurance on an admitted basis, an updated rate filing will be made, and we will underwrite and price business according to such approved rate filings.

**When will these product changes go into effect?**

Chubb has already been using this new approach on large accounts, and we will expand to other market segments in the coming months. It is critical to begin working with your clients' risk managers well in advance of their renewals to identify their specific risks and explore the coverage extensions that will provide the right protection for them. Deployment of the new approach on an admitted basis will be dependent on geography and state-specific filings, which are expected to commence with effective dates starting in January 2022.

**Will there be a sales document we can attach to the form to explain the benefits?**

Yes, a product summary is available for download.

# Underwriting Process

**What can I do to plan for these changes? Will resources be provided to me to help guide my discussions with clients and prospects?**

In addition to reading and understanding these FAQs, we encourage you to take advantage of any training and webinars that will be offered by Chubb. Materials such as whitepapers, webinars, and videos will be made available throughout the year that you can share with your policyholders. Please visit chubb.com/uk/cyber or contact your Chubb cyber underwriter for more information.

# Quoting Process

**Are there certain underwriting considerations that will inform the systemic coverage and pricing that Chubb offers?**

Yes. Several factors will inform the systemic coverage and pricing offered by Chubb, including the organisation's critical dependencies, contractual protections with service providers, cyber security hygiene and controls, and incident response/resilience planning and testing.

**What is the change to the pricing structure of Widespread Event coverage?**

Chubb is committed to providing transparency to all clients and will offer separate pricing, limit, and retention options for systemic coverage.

# Policy Form

**What coverage is being excluded in Chubb's new cyber products?**

Coverage for Widespread Events is not being excluded. It is being structured in a way to transparently provide capacity for underwritten events. Insureds have the option to purchase coverage for Widespread Events, but it is not required.

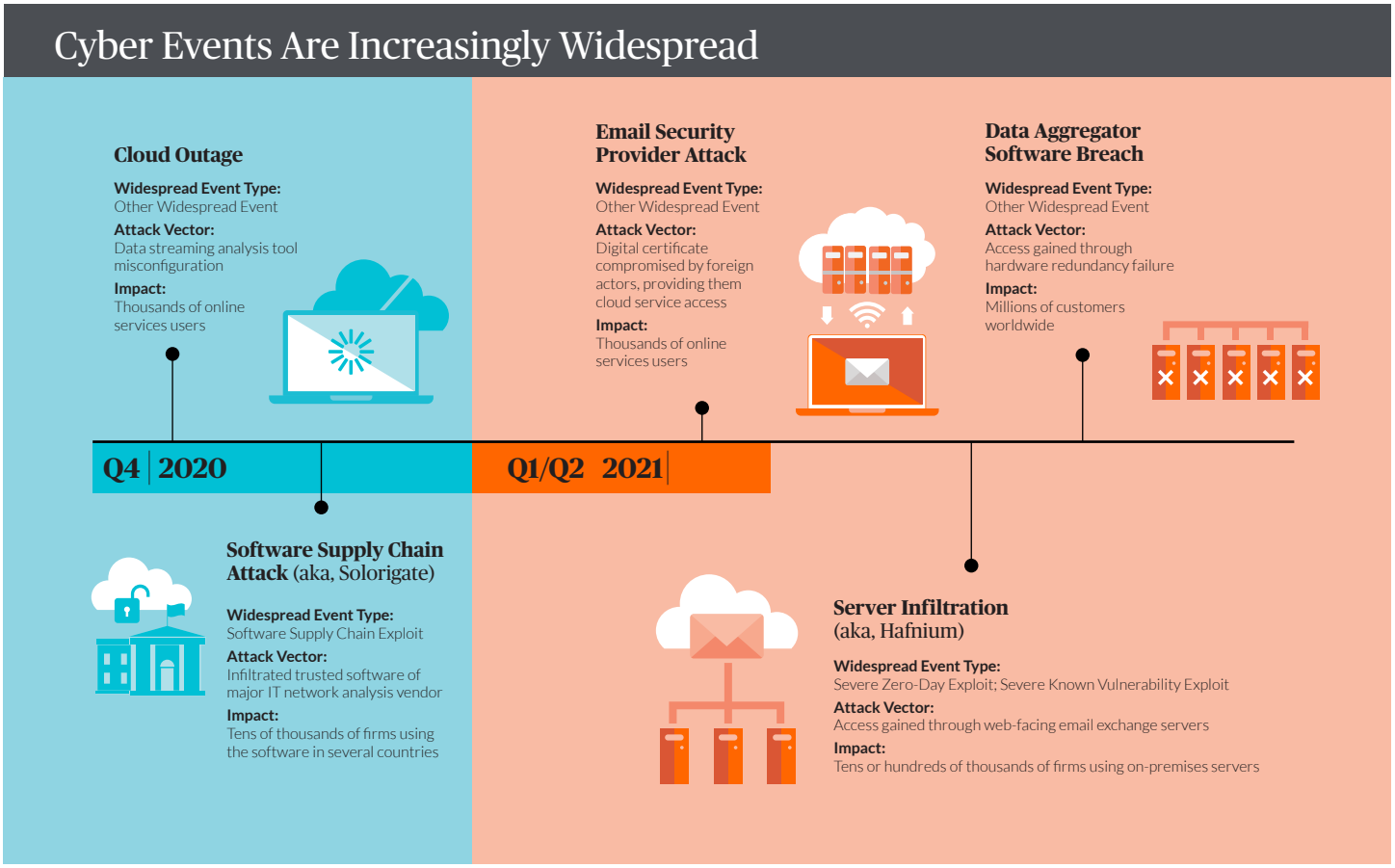
**Where are Limited Impact Event and Widespread Event concepts described in the policy?**

The first page of the policy states that Cyber Incidents will be categorised as either a Limited Impact Event or a Widespread Event; those definitions are outlined in Section II of the policy. Additional key definitions used within these concepts include Widespread Trigger and Limited Impact Group, among others.

For policies that provide the same limits, retentions, and coinsurance across all types of Widespread Events, it is not important to differentiate between the four sub-categories of Widespread Events. However, if there are differentiated limits, retentions, or coinsurance, then the following Widespread Event sub-category definitions should be reviewed:

- Widespread Severe Known Vulnerability Exploit
- Widespread Severe Zero-Day Exploit
- Widespread Software Supply Chain Exploit
- All Other Widespread Events

Section X of the policy addresses "Duties in the Event of a Cyber Incident" and describes in detail how the policyholder and Chubb will collaborate in the event of a Cyber Incident. This includes information about the timing and methods for determining whether a Cyber Incident is a Limited Impact Event or a Widespread Event. As always, the policy should be read in its entirety.




### Can you provide examples of any actual historical examples of Widespread Events?

Examples of recent widespread events are depicted in the graphic above.

### How does coinsurance work? Can you provide an example?

The coinsurance applicable to Widespread Events, Ransomware Encounters, and Neglected Software Exploits is a "loss-reducing" coinsurance, which means that the policyholder's coinsurance does not erode the limits of insurance. Rather, responsibility for each loss is apportioned between the insured and the insurer, and the insurer's portion is then subject to the applicable limit for that risk.

For example, if the policy has a Sub-Limit of 5 % of the $10 million aggregate policy limit for a Widespread Event, the Insurer's maximum liability for any Widespread Event losses under that Widespread Event Sub-Limit would be $500,000 (i.e., 5% of $10 million).

If coverage for a Widespread Event is subject to 50% coinsurance, then a $1 million loss event would be apportioned between the insured and the insurer 50/50, and the Widespread Event Sub-Limit would then be exhausted because the insurer would have paid the entire available $500,000 Sub-Limit.

Alternatively, a $500,000 Widespread Event loss would also be apportioned 50/50, but because the insurer would only pay $250,000 in this situation, there would be $250,000 remaining under the Widespread Event Sub-Limit for future events.

# Endnotes


1. National Institute of Standards and Technology's National Vulnerability Database. Accessed at https://nvd.nist.gov/vuln/search
2. AV-TEST Institute (2021). Accessed at www.av-test.org/en/statistics/malware/
3. Federal Commission Warns Dangerously Insecure U.S. At Risk of 'Catastrophic' Cyber Attack (2020). Accessed at www.forbes.com/sites/daveywinder/2020/03/14/make-america-safe-again-federal-commission-warns-us-at-risk-of-catastrophic-cyber-attack/?sh=244402e34d27
4. Ransomware and Aggregation Issues Call for New Approaches to Cyber Risk (2021). Accessed at www.insurancejournal.com/research/research/ransomware-and-aggregation-issues-call-for-new-approaches-to-cyber-risk/
5. Ibid.
6. NIST Security Vulnerability Trends in 2020: An Analysis (2021). Accessed at www.redscan.com/media/Redscan_NIST-Vulnerability-Analysis-2020_v1.0.pdf

## About Chubb

Chubb is the world's largest publicly traded property and casualty insurance company. With operations in 54 countries and territories, Chubb provides commercial and personal property and casualty insurance, personal accident and supplemental health insurance, reinsurance and life insurance to a diverse group of clients. As an underwriting company, we assess, assume and manage risk with insight and discipline. We service and pay our claims fairly and promptly. The company is also defined by its extensive product and service offerings, broad distribution capabilities, exceptional financial strength and local operations globally. Parent company Chubb Limited is listed on the New York Stock Exchange (NYSE: CB) and is a component of the S&P 500 index. Chubb maintains executive offices in Zurich, New York, London, Paris and other locations, and employs more than 31,000 people worldwide. Additional information can be found at www.chubb.com.

To learn more about Chubb's cyber risk management experience and expertise, visit chubb.com/uk/cyber