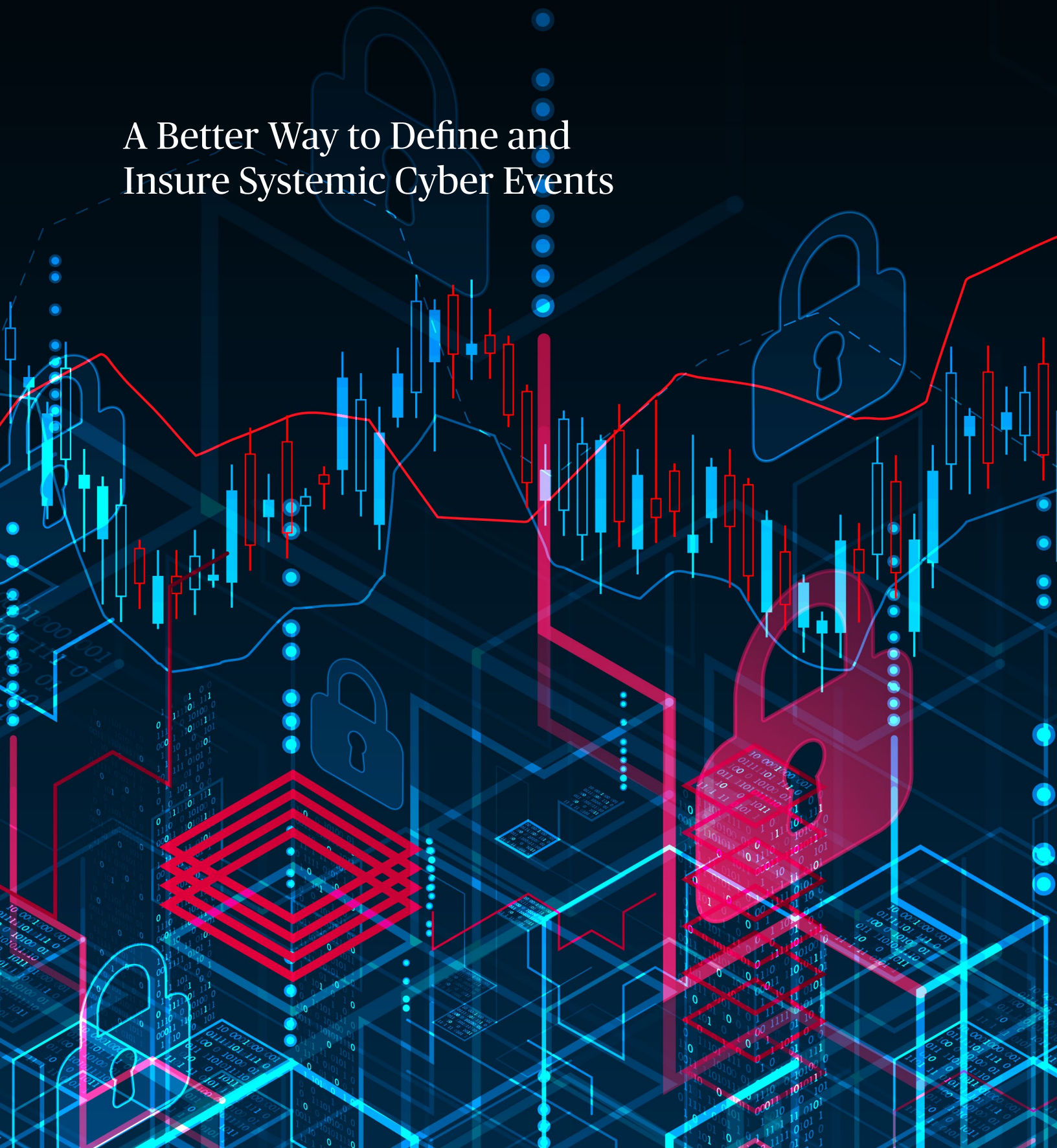
CHUBB®

A Better Way to Define and Insure Systemic Cyber Events



Introduction

The potential for a catastrophic cyber attack causing widespread damage at a significant cost is broadly discussed but not yet fully understood. As a result, most companies have been working to improve their cyber resilience, while the insurance industry has been developing solutions to manage these risks.

Despite these efforts, the ever-increasing reliance on technology by organizations and consumers, along with the interconnectivity of technologies and partners have created an environment in which cyber risks are expanding exponentially. Like a pandemic, a cyber-CAT event has no geographic boundaries or temporal limitations.

All stakeholders — including organizations at risk, governments, insurance carriers, brokers and the cyber security industry — need to develop and implement solutions that will maintain overall economic stability and societal resiliency while still providing organizations and individuals with the insurance protection they need.

In the insurance industry, one barrier to long-term sustainability has been the lack of a consistent and clear definition of systemic cyber events. How can risk managers, brokers and insurers come to a common understanding of policy terms and conditions so that clients know what coverage they have, and insurers can meet the obligations of the client risks they assume?

In the following Q&A, Michael Kessler, Vice President, Chubb Group and Division President, Global Cyber Risk, discusses the evolving insurance market for widespread cyber risks, including common misperceptions and solutions.

Q&A With Michael Kessler

Q: What is systemic risk? How should it be defined?

A: The cyber insurance market lacks a clear definition of what constitutes "systemic risk." At Chubb, we define a "systemic" event in the cyber context as one that could inflict widespread harm to many customers due to shared elements or commonalities – often a single point of failure that is exploited. Put simply, it's a cyber incident that impacts multiple entities in a single act. One example of a systemic event is the exploitation of a vulnerability in a file transfer software utilized by thousands of businesses to deploy malware, exfiltrate data, or cause disruption in business. With so many clients exposed to loss by that single exploit, aggregate losses can be catastrophic.

DEFINING SYSTEMIC RISK:

A cyber incident that impacts multiple entities in a single act.

Q: How has the cyber insurance market responded to both the growing frequency of individual ransomware attacks versus systemic events?

A: In general, the market has been following shifts in the risk environment to keep pace with the change in loss costs due to both severity and frequency of ransomware events. The response to systemic risk has been less explicit.

Q: How do you and your team think about the evolving exposure to systemic risk?

A: At Chubb, we recognized three problems with respect to how the industry was addressing systemic cyber risk: 1) lack of coverage clarity for the insured, 2) inadequate pricing of the risk, and 3) insufficient focus on tracking and monitoring exposure.

THREE CHALLENGES:

- Lack of coverage clarity for the insured
- Inadequate pricing of the risk
- Insufficient focus on tracking and monitoring exposure

To address the first, we employed a clear definition of what constitutes a widespread cyber event. It clarifies that a systemic event is one that occurs via a single act and reinforces the broad potential impact of a single act that is unique to cyber risk. When policy wording is clear and certain, costly litigation can be mitigated and insurers can offer more capacity and consistency.

Second, we designed our policy so that the insured could see the pricing for systemic coverages transparently and make an active decision on what limits and retention to purchase in accordance with their risk tolerance. This is a familiar concept for insurance products, such as the provision of earthquake coverage separately from all other perils coverage in a property policy.

Third, we worked with modeling firms to align the event scenarios with the policy definitions to encourage a more consistent and laser focus on this exposure.

Q: What widespread events does Chubb's policy cover versus exclude?

A: Widespread events – excluding those involving war or infrastructure impairments – are covered and subject to the limit and retention that are purchased by the insured. No additional exclusions. If a widespread event occurs and there is no declaration of war or cause from infrastructure, businesses can rest assured they are covered. Cyber incidents that result from war or infrastructure impairment are excluded. Furthermore, war and infrastructure are clearly and objectively defined in the policy, so that the insured has contract certainty before an event occurs. There is no ambiguity because coverage is not dependent on subsequent assessment of the perpetrator of an attack (e.g., 'state sponsored' or 'state backed' attackers).

Q: What about the implications for reinsurance?

A: Reinsurance remains substantially a quota share market today, as it has been for many years. On the surface, that means insurers cede a share of the premium and an equal share of the losses to reinsurers. However, most contracts include a cap on reinsurers' losses, which leaves significant tail exposure with the cedant without the premium to pay those claims. A more efficient use of capital involves reinsurers covering cyber on an event excess of loss basis. This is similar to the model that works with catastrophe excess of loss reinsurance for property, which protects insurers from an accumulation of losses due to a single CAT event. This approach offers reinsurers greater margins for assuming tail volatility with the use of proportionately less capital. Reinsurers' ROEs increase and the overall cyber insurance market becomes more efficient. To evolve, the reinsurance market needs a clear definition of what a systemic cyber event is and a consistent approach to modeling frequency and severity of those events. Both the Chubb policy and one promulgated by Cyber AcuView, an industry consortium of the largest cyber insurers in the world, provide that clear definition of a systemic event, and modeling firms have vastly improved the quality and consistency of their models over the past 12 months.

THE VALUE OF CLARITY:

The quality and consistency of models have vastly improved over the past 12 months.

Q: What has been the reaction to the policy wording in the marketplace?

A: It has been almost two years since Chubb first introduced this language. Many clients understand what Chubb is doing and certainly support it. They realize the value of clarity in helping them make more informed risk management decisions. For example, a large business may opt to buy just the catastrophic coverages in the endorsement and self-insure the less-concerning financial exposures. A large company may decide to absorb lower dollar losses caused by a ransomware attack on its balance sheet and insure the risks they cannot control.

Q: Do you think Chubb's approach should be adopted more broadly?

MODEL FOR THE INDUSTRY:

More uniform coverages and insuring agreements with potentially different limits, deductibles and pricing, would accrue significant benefits for buyers and reinsurers.

A: Chubb is one of the leading providers of cyber insurance globally. We have underwritten cyber exposures for policyholders for more than two decades. We're focused on being a leader in order to break through any barriers. We will continue to use our underwriting experience, data, and insights to develop solutions to help meet this growing risk. We are confident our model can provide meaningful protections for our clients and serve as a model for other insurers to follow. By offering more uniform coverages and insuring agreements with potentially different limits, deductibles and pricing, significant benefits would accrue for buyers and reinsurers.

Catastrophic risks multiply

The potential for a systemic cyber event to cause catastrophic loss is alarming and growing. During 2022, the number of malware attacks across the world was nearly two-fifths higher than the total volume in 2021, reaching an all-time high in Q4 2022, when an average of 1,168 weekly attacks per organization was reported.[1]

More than 25,000 software vulnerabilities were discovered in 2022, the highest reported annual figure to date.[2] A vulnerability is a flaw or weakness in software that can be exploited by malware. In April, May and June 2023, the National Institute of Standards and Technology tallied 6,991 new software vulnerabilities, 1,027 of which were categorized as "critical."[3]

Estimates of a systemic event causing catastrophic losses indicate that the cost would exceed the aggregate capacity of the global insurance market.[4] A report by the Government Accountability Office (GAO) described these events as cyber incidents that "spill over from the initial target to economically linked firms, thereby magnifying the damage." The GAO report estimated the potential loss from a single systemic cyber event as ranging from $2.8 billion to $1 trillion.[5]

Chubb's Approach to Cyber Enterprise Risk Management

A sustainable approach to insuring a broad array of cyber events, including Widespread Events

Three prongs to Chubb's Cyber ERM:

- Loss Mitigation Services – access to the tools and resources needed to address and gauge key areas of cyber security risks before an event occurs.
- Incident Response Services – a diverse team of experts in the legal, computer forensics, notification, call center, public relations, fraud consultation, credit monitoring, and identity restoration service areas to help limit exposure to a loss when an event occurs.
- Risk Transfer – broad and sustainable insurance coverage backed by the financial strength of Chubb.

Competitive advantages

- Leading provider of cyber risk solutions since first product was launched in 1998.
- Innovative, highly customizable risk solutions to address clients' unique needs, regardless of size, industry or type of risk.
- No minimum premiums. Premiums scale for all sizes of risks based on the scope of coverage and limits.
- Cyber crime coverage by endorsement or provided under separate policies from Chubb's industry-leading Fidelity and Crime products.
- Cyber Incident Response Expenses, with expansive consumer-based solutions that are more robust than minimum regulatory requirements.
- Online quoting and real-time policy issuance for eligible small risks. Referred risks will receive fast turnarounds from your Chubb underwriter.
- Innovative coverage designed to address evolving regulatory, legal, and cyber security standards and built to consider future changes.
- Easy-to-read form is aligned with the flow of a typical cyber incident in order to aid decision-making throughout.
- Coverage Territory applicable worldwide to address continued evolution of hosting and data storage.

Widespread event endorsement

- Widespread Event Endorsement addresses events with widespread impact, affecting parties with no relationship to the insured. Similar to how flood and earthquake risks are addressed in property policies – coverage, limits, retentions – and coinsurance can be tailored for all Widespread Events, or by specific peril:
  - Widespread Severe Vulnerability Exploits
  - Widespread Severe Zero-Day Exploits
  - Widespread Software Supply Chain Exploits
  - All other Widespread Events
- Ransomware Encounter Endorsement addresses the increasing risk of ransomware by allowing for a tailored set of coverage, limit, retention and coinsurance to apply uniformly across all cyber coverages.
- Neglected Software Exploit Endorsement recognizes and rewards good software patching hygiene by providing full coverage for 45 days, and then for software that remains unpatched beyond 45 days, gradually re-weights risk sharing between the Insured and Insurer as time passes.

[1] Check Point. Global Cyber-Attack Volume Surges 38 percent in 2022. Jan. 9, 2023.
[2] Tenable Research. Mind the Gap: A Closer Look at the Vulnerabilities Disclosed in 2022.
[3] NIST National Vulnerability Database. As reported by the Wall Street Journal, June 20, 2023
[4] Marsh. Cyber Insurance Market Overview, Fourth Quarter 2021.
[5] U.S. Government Accountability Office. Potential Federal Insurance Response to Catastrophic Cyber Incidents. Sept. 29, 2022