Catastrophic Cyber Risks – A Growing Concern

CHUBB

Cyber incidents can cause losses that are not limited by time or geography.

As the world digitizes, the frequency, severity and sophistication of cyber incidents are increasing along with the dependency on technology. Vulnerabilities and exposures are multiplying due to greater interconnectivity, creating systemic risks that are vast, growing and not easy to detect or control. Combining these systemic risk dimensions with potentially severe and widespread consequences creates the possibility for a cyber catastrophe.

Similar to pandemics, cyber incidents can cause losses that are not limited by time or geography. It's no longer theoretical – cyber criminals have already demonstrated their ability to disrupt supply chains for businesses around the world and cripple critical infrastructure, as with the recent attack that resulted in Colonial Pipeline shutting down its lines supplying fuel to the east coast of the U.S. With recent cyber incidents causing billions of dollars in economic losses, it's not difficult to imagine a catastrophic attack that could test the balance sheet capacity of the insurance industry.

Unlike previous sudden catastrophe events, we are witnessing the continuous escalation of cyber risks. This advance notice provides an opportunity to build cyber defences and economic safeguards before a catastrophe occurs.

Cyber Insurance Comes of Age

The steadily increasing adoption of cyber insurance means that more companies have protection but also that the cyber risk aggregation is expanding for the insurance industry.

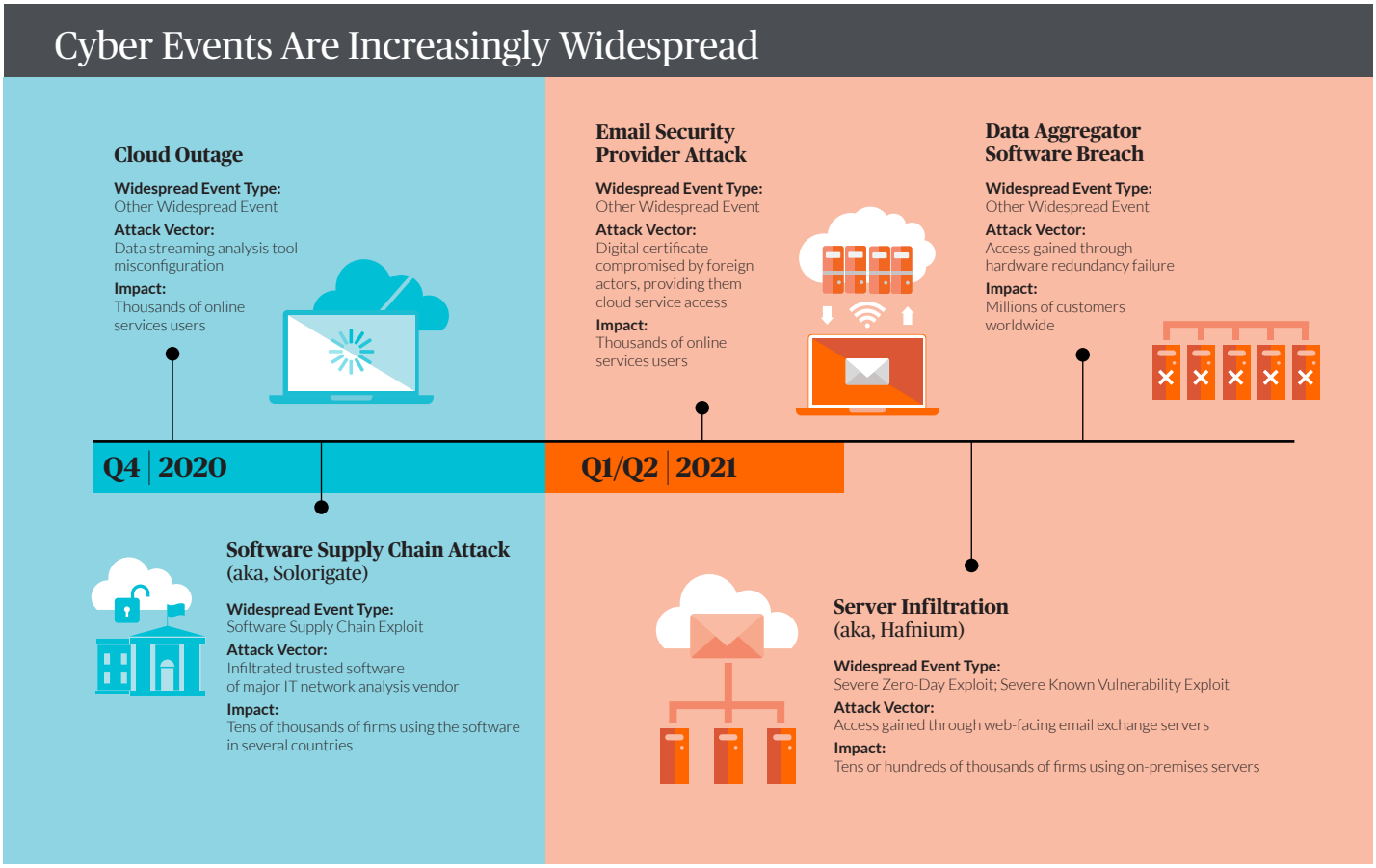
The promise of cyber insurance has been fully realized in recent years, with losses paid by insurers after significant cyber events serving to protect numerous organizations around the world.

Today, the core coverages – incident response expense, first-party cyber risk, third-party cyber liability, and professional liability/errors and omissions – provide important risk transfer and risk management solutions for organizations of all sizes and industries. In addition, cyber risk management services offered by carriers have been valuable in helping companies mitigate risk and improve their technology defences on the front end, while incident response teams have proven effective in bringing companies back online sooner following a cyber event.

The steadily increasing adoption of cyber insurance – now estimated at nearly 4 million policies for U.S.-domiciled and non-U.S. surplus lines insurers and approaching 50 percent of U.S. businesses covered, according to a Government Accountability Office report from May 2021[1] – means that more companies have protection but also that the cyber risk aggregation is expanding for the insurance industry.

At the same time, companies have also improved their cyber resilience over the last several years. In 2020, 53 percent of IT and security professionals surveyed around the world reported that their organizations had achieved a high level of cyber resilience, compared to 35 percent in 2015.[2]

While cyber insurance is clearly playing an increasingly important role in managing the cyber exposure for organizations, the ability of insurers to absorb the total loss potential long term is less certain.



Escalating Risks and 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.

Despite organizations being more aware of cyber risk and its consequences, cyber incidents and threats are only increasing and evolving.

More than 18,000 new software vulnerabilities were published in 2020, nearly tripling from 2015 and continuing to grow steadily.[3] Meanwhile, nearly 1.2 million new malware threats were identified in 2020, more than double the number from 2015.[4] Among successful security breaches in 2020, 85 percent involved a human element, such as social engineering schemes.[5]

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 during the COVID-19 pandemic and the extensive remote working arrangements that have resulted.

Cyber events are also having a 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. Well over 100,000 organizations from all over the world were affected by these events.

In one of these events, known as Solorigate, it was revealed that a massive supply chain attack where malicious code was embedded in an update of a trusted network analysis software had gone unnoticed for nearly eight months, affecting roughly 20,000 companies and government agencies.

In another event, a group of alleged nation-state actors and criminal syndicates known as Hafnium exploited a then-unknown (“zero-day”) vulnerability in a common software to gain access to on-premises servers at potentially hundreds of thousands of firms.

High-Profile Incidents Raise Tension

When will we see a truly catastrophic cyber event that's both widespread and destructive?

Even as pervasive and costly as the Solorigate and Hafnium events were, they could have been much worse. It appears that the primary motive in each of these events was espionage, but if the intent had been to steal or destroy critical data or other information, the economic consequences could have easily multiplied. According to Kevin Mandia, CEO of cybersecurity firm FireEye, in testimony to the Senate Intelligence Committee, the threat actors behind the Solorigate attack had the access required and the capability required should they have wanted to be disruptive.[6]

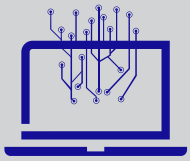
To further illustrate, in 2017 the NotPetya attack exploited a tax software tool called M.E.Doc used almost exclusively in Ukraine, but the malware then spread indiscriminately and ultimately impacted many major corporations based in Europe, the U.S., and elsewhere, resulting in an estimated $10 billion in losses. Some companies victimized by the NotPetya attack suffered losses exceeding $100 million. If this type of destructive malware would have been deployed in the Solorigate or Hafnium attacks, the combined economic damages could have been exponentially larger than the NotPetya event.

That same year, the WannaCry ransomware attack hit more than 200,000 computers worldwide. Fortunately, it used a known vulnerability that already had a patch available, so most users were immune to it. However, like the Hafnium example provided previously, the impact could have been much more widespread and severe if it had exploited a zero-day vulnerability instead.

To date, we've witnessed widespread events (e.g., Solorigate, Hafnium) and destructive events (e.g., NotPetya, WannaCry) – but losses from these events have been manageable so far. With such vast loss potential building, when will we see a truly catastrophic cyber event that's both widespread and destructive?

Potential Catastrophic Cyber Risks

The ever-increasing reliance on technology by organizations and consumers as well as the interconnectivity of technologies and partners have created an environment in which the severity of cyber events can expand exponentially. The following types of events, particularly in combination, have been identified as having the potential to be catastrophic.



Severe Known Vulnerability Exploits:

On average, roughly 50 new software vulnerabilities are published every day. If patches aren't applied, these can be exploited. Approximately 15 percent are severe, in that they are easy to exploit, can be deployed remotely with limited access privileges, and cause significant adverse impact.[7] Since severe vulnerabilities are widely known and can be identified on the networks of potential victims through common internet scanning techniques, companies that fail to address severe software vulnerabilities are at high risk of being victimized.

Severe Zero-Day Exploits:

Zero-day software vulnerabilities are known by cyber criminals but not yet by anyone else. These are particularly concerning because some are easily exploitable, potentially severe, and often lack protection. Put another way, even companies with well-run cyber risk management programs may be exposed to zero-day attacks.

Software Supply Chain Exploits:

Software supply chain attacks are effectively a Trojan horse that allows bad actors to enter systems through trusted, certified software. The Solorigate operation demonstrated a high degree of sophistication by the adversaries in exploiting common software development practices in use across the technology industry. These attacks, many of which appear to be directed or sponsored by state actors, are expected to continue and potentially accelerate. Geopolitical friction, particularly between the West and its adversaries, will continue to exacerbate the threat of these events going forward.

Infrastructure Outages:

Attacks and other cyber incidents involving infrastructure can have widespread consequences. For example, in the May 2021 attack on Colonial Pipeline, the gasoline supply company serving the east coast of the U.S., foreign cyber criminals leveraged an infrastructure outage through a ransomware attack, compounding the impact. As a result, the pipeline was shut down for several days, causing gas shortages affecting 45 percent of America's fuel supply to millions of citizens and businesses in several states. Infrastructure outage risk is unique in that it can occur from a cyber attack, but also through system failures, human errors, programming errors, or other non-malicious types of cyber incidents.

Other Widespread Events:

There are certain types of cyber attacks that can be carried out concurrently or automatically against a wide number of victims. The Internet and some telecommunications services have risen to the level of critical societal infrastructure, taking the potential risk of failure to an enormous scale. In some cases, a telecom company may be the only provider for a major or mid-size city. In other cases, some large cloud computing firms are so widely used that a widespread outage would impact the business operations of thousands or millions of different companies at the same time. Any such attack capable of mass deployment could cause a catastrophic cyber event.

Ransomware Encounters:

While not necessarily catastrophic in nature, ransomware attacks, which hold targeted organizations' or individuals' electronic files or information hostage until a fee is paid, are now being carried out with industrialized efficiency. Typical demands, which began in the thousands of dollars, have now skyrocketed well into the tens of millions, with criminals targeting organizations of all sizes.

Strengthening Cyber Resilience

It's more critical than ever for organizations to improve preparations for a potential cyber catastrophe.

With cyber exposures increasing – either through the nature of operations and IT environments, failure of common infrastructure, or bad actors exploiting vulnerabilities – it's more critical than ever for organizations to improve preparations for a potential cyber catastrophe.

A great place to start is understanding the specific exposures each organization may face through the lens of the potential catastrophic cyber events outlined in this paper, then committing necessary resources to improving cyber defences and resiliency. Shared IT vendors represent a significant systemic risk to organizations, so extensive due diligence should be conducted on these vendors and redundancy and resiliency should be built around them, in addition to examining the indemnity language in contracts to assess how risk is being transferred.

Organizations should also take full advantage of the expertise offered by their insurance broker or agent and their cyber insurance carrier. While IT, risk management, and business continuity teams may have confidence in their cyber protection and incident response measures, no organization can ever be fully protected from all potential cyber incidents – especially catastrophic ones.

Many insurance carriers offer a range of pre-incident services to help organizations improve their cyber defence posture, such as response readiness assessments, security performance benchmarking, network vulnerability testing, and common attack simulations. Organizations also should be prepared to respond when a cyber incident occurs. An insurer's incident response team of experts can help contain the damage from such events and help restore an organization to full operations as soon as possible. These services could make the difference between merely surviving a major cyber event and moving forward with confidence.

Advancing Solutions

Cyber insurance, like property insurance, has exposure to catastrophic events.

From a global perspective, catastrophic cyber events have the potential to bring commerce to a halt and cripple critical infrastructure. Much as with the coronavirus pandemic, this requires the government and private sector to work together on important topics, such as the disclosure and reporting of cyber incidents to improve consistency of data and the establishment of legal frameworks to deter and punish cyber criminals.

The increase in both frequency and severity of cyber incidents is causing insurers to reevaluate their pricing and terms and conditions. Providing a stable market for cyber insurance while accounting for the potential scale of catastrophic risk will require new solutions, such as a partnership with the government, as well as in the product offerings of individual insurers. For the insurance industry, the challenge becomes how to craft policies that offer coverage certainty, provide meaningful protection, and help manage both attritional and catastrophic cyber events for clients and insurers.

Insurers have historically insured property for catastrophic events, such as floods and earthquakes, as separate coverage parts to both transparently price for and monitor those exposures. This process has helped maintain overall market stability and coverage availability. For example, while many of the major earthquake, flood, and hurricane events of the last half century have been material earnings events for the property and casualty insurance industry, they have rarely led to carrier insolvencies. As a result, the insurance industry has remained resilient and stable for policyholders – even in the aftermath of catastrophic events.

Cyber insurance, like property insurance, has exposure to catastrophic events, and so the cyber insurance industry may need to respond in the same manner as the property insurance industry. The industry must be proactive in offering coverage for catastrophic events separately from core coverages. Coverage for catastrophic events would not be excluded, but rather be more clearly delineated, ensuring that separate coverage is priced for transparently, and subject to appropriate underwriting, coverage limits, and client retentions. This approach will enable the cyber insurance industry to continue to provide innovative solutions for policyholders, while ensuring the long-term sustainability of the market.

About the Author

Michael Kessler is a Vice President of Chubb Group and the Division President of Chubb's Global Cyber Risk Practice. In this role, he oversees all facets of the business including strategy, product and business development, underwriting and service operations, and overall profit and loss performance. Mr. Kessler has nearly 30 years of experience in insurance and actuarial consulting and previously served as Chubb's Chief Reinsurance Officer (2016 – 2021) and Chief Actuary for its International insurance business (2008 – 2016). Mr. Kessler holds a Bachelor of Arts in Mathematics from Cornell University. He is a Member of the American Academy of Actuaries and a Fellow of the Casualty Actuarial Society.

Endnotes

1. Cyber Insurance: Insurers and Policyholders Face Challenges in an Evolving Market (2021). Retrieved from www.gao.gov/products/gao-21-477
2. Cyber Resilient Organization Report (2020). Retrieved from www.ibm.com/security/digital-assets/soar/cyber-resilient-organization-report/#/
3. National Institute of Standards and Technology's National Vulnerability Database. Accessed at https://nvd.nist.gov/vuln/search
4. AV-TEST Institute (2021). Accessed at www.av-test.org/en/statistics/malware/
5. Verizon 2021 Data Breach Investigations Report (2021). Retrieved from https://enterprise.verizon.com/resources/reports/2021/2021-data-breach-investigations-report.pdf
6. U.S. Senate Select Committee on Intelligence (2021). Accessed at www.intelligence.senate.gov/hearings/open-hearing-hearing-hack-us-networks-foreign-adversary
7. NIST Security Vulnerability Trends in 2020: An Analysis (2021). Retrieved from 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 30,000 people worldwide. Additional information can be found at www.chubb.com.

To learn more about Chubb's industry-leading cyber risk management experience and expertise, visit www.chubb.com/ca or email cyber@chubb.com.

Chubb. Insured.℠