cowbell®

Cyber Round-Up Q1 2023

A Review of Potentially Catastrophic Cyber Events

Table of Contents

Every quarter, Cowbell releases a *Cyber Round-Up* report with analysis of data, market trends, and general commentary on the state of cybersecurity and the cyber insurance market.

Introduction

In Cowbell's whitepaper, "Modeling Catastrophic Cyber Events," we define catastrophic and systemic cyber risk in the small and medium-sized enterprise (SME) market. Cowbell's approach to catastrophe (cat) modeling hinges on an understanding of systemic risk. A systemic risk is the possibility that a single event or development might trigger widespread failures or disruptions spanning multiple organizations, sectors, or nations.

Recent systemic events (albeit not cyber events) include the 2008 financial crisis and the COVID-19 pandemic. Not all systemic events are catastrophic in nature, but every systemic loss has the potential to escalate to catastrophic levels of disruption. To date, no systemic cyber event has resulted in catastrophic losses, despite the potential for catastrophic losses to occur in events we have had to date.

Currently, four out of five SMEs are uninsured or underinsured. This presents a large gap in adoption of cyber insurance. If a systemic cyber event of a catastrophic level were to occur, the SME ecosystem could suffer severe consequences. To a certain extent, systemic risk can be disconnected from catastrophic cyber risk.

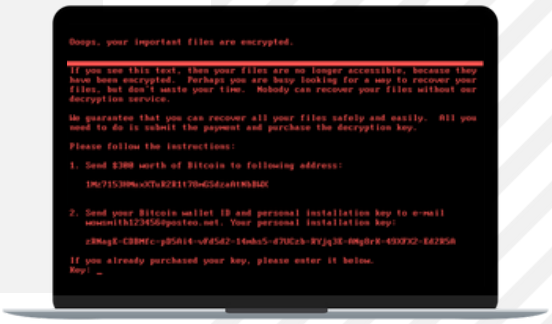
In recent history, there have been events that could have reached catastrophic levels, but did not. They have also been relatively infrequent. In this report, we will highlight two well-known examples as case studies: NotPetya and Log4J.

Case Study 1: NotPetya

In 2017, the NotPetya cyberattack first targeted Ukrainian critical infrastructure and then spread rapidly, including to the U.S. The malware was able to spread rapidly in part because of the easy access to the exploit, unpatched systems, and misappropriated credentials. In total, damages amounted to $10 billion, about double the monetary cost of damages caused by WannaCry, a cyberattack that occurred in the same year.

However, there was a disconnect between cyber headlines and actual losses. According to a GallagherRe report, events like NotPetya in 2017 yielded headlines, such as “NotPetya, the most devastating cyberattack in history,” but it “didn’t produce losses on the scale anticipated due to a number of disaggregating factors. These headlines were, at the time, often accompanied by doom-laden declarations questioning the very insurability of Cyber risk and understandably concerned a whole swath of the market.”

The fact that the NotPetya malware was able to spread around the world due to unpatched systems means that better patching policies are needed to increase resilience and cyber defenses.



> The malware was able to spread rapidly in part because of the easy access to the exploit, unpatched systems, and misappropriated credentials.

Case Study 2: Log4J

Less than five years after the NotPetya cyberattack, the Apache Log4J vulnerability was discovered in 2021. This is a good example to understand systemic risk as it was a vulnerability on a very broadly used component of software (Apache). Since Log4J is so widely used, this vulnerability affects countless individuals, businesses, and organizations. One can be directly or indirectly affected as a result of using a software with Log4J or being involved with a third party that uses a software with Log4J. Patching, or lack thereof, is also to blame for the extent to which this vulnerability wreaked havoc.

While by some measures, the Log4J vulnerability could have been categorized as systemic risk (there were millions of attempts per hour to exploit the vulnerability), the relatively slow speed of propagation combined with the technological ecosystem's ability to efficiently respond and patch seemingly mitigated the possible disruption. It is clear that the industry has made substantial progress in response time between the NotPetya cyberattack in 2017 and the Log4J vulnerability in 2021.

The industry has made substantial progress in response time between the NotPetya cyberattack in 2017 and the Log4J vulnerability in 2021.

Patching, or lack thereof, is also to blame for the extent to which this vulnerability wreaked havoc.

Conclusion

Going forward, the response time of the entire ecosystem (businesses, cybersecurity industry, governmental entities) needs to improve even more because there are always new technologies and therefore new patches. The importance of effective patching cannot be emphasized enough. The cloud can speed up the process of patching across a large group of users, but cloud computing comes with its own set of challenges and underlying risks.

The industry as a whole is doing a better job of working together to act and respond quicker to vulnerabilities. Cyber insurance plays an important role in improving this response time. At Cowbell, our dedicated risk engineering team monitors threats in real-time and notifies policyholders about identified vulnerabilities and exposures. Beyond this notification, our policyholders have access to risk engineers for one-on-one calls to help improve their risk profile, making them more resilient.

Reach out to Cowbell today!

- cowbell.insure
- cowbell
- cowbellcyber
- cowbellcyber

Cowbell is signaling a new era in cyber insurance by harnessing technology and data to provide small and medium-sized enterprises (SMEs) with advanced warning of cyber risk exposures bundled with cyber insurance coverage adaptable to today's and tomorrow's threats. In its unique AI-based approach to risk selection and pricing, Cowbell's continuous underwriting platform, powered by Cowbell Factors, compresses the insurance process from submission to issue to less than 5 minutes.

cowbell®

Cyber Round-Up Q1 2023

A Review of Potentially Catastrophic Cyber Events

Cowbell's quarterly data reports are created to provide real-life, relevant data surrounding cyber insurance security for small and medium-sized enterprises.

With these reports, we want to help businesses as well as U.S. insurance agents and brokers understand how to prepare effectively to avoid or respond to a cyber incident.

We hope that you will be able to use these reports and the information they contain to expand your education surrounding cyber insurance, and its value, and as a way to educate employees on the importance of cybersecurity awareness.