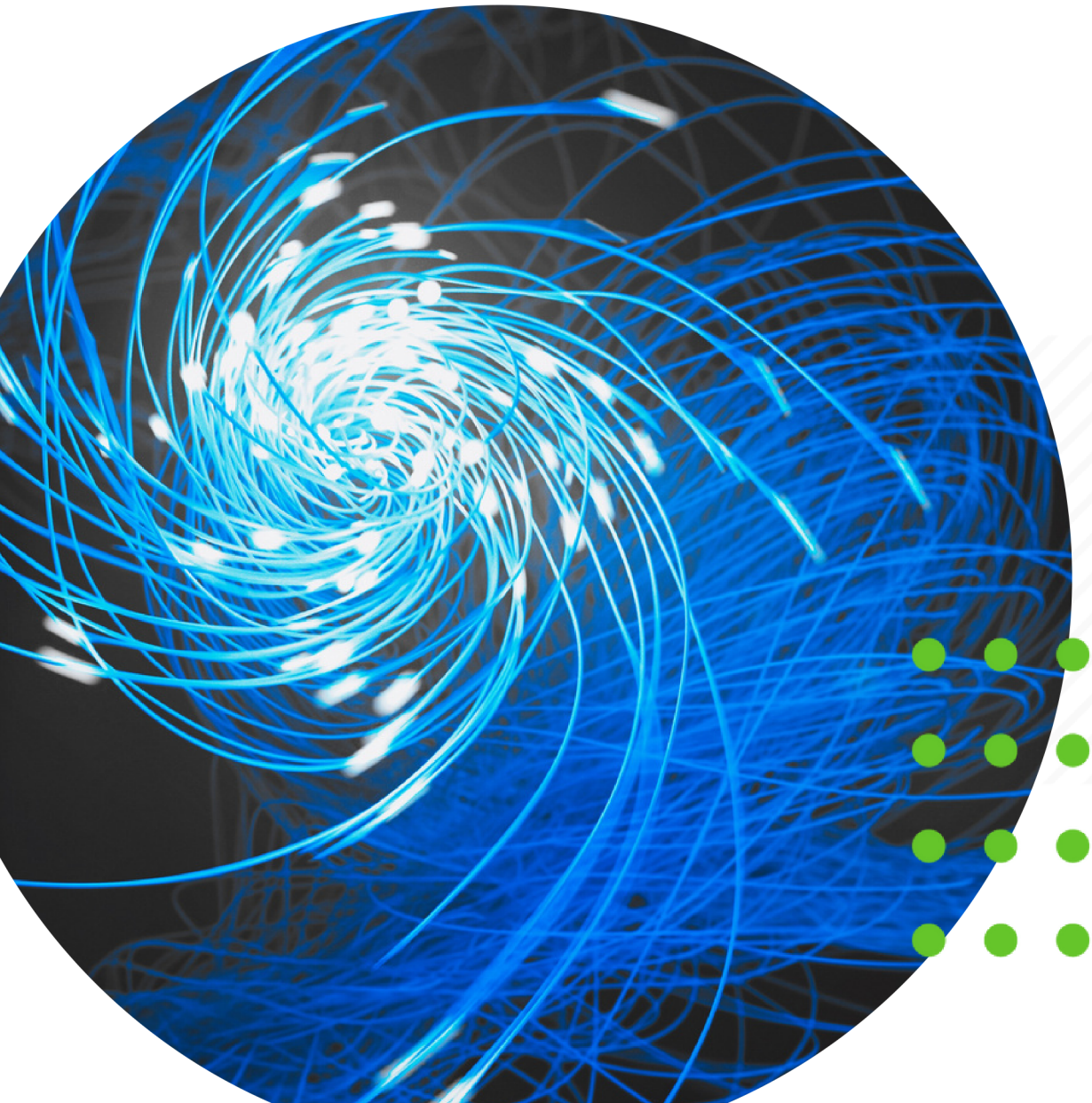
cowbell®

Modeling Catastrophic Cyber Events

The Leading Provider of Cyber Insurance for SMEs | cowbell.insure



V.DEC22

cowbell®

Table of Contents

A Path to Quantifying Catastrophic and Systemic Cyber Risk in SME market

Introduction

The U.S. economy's reliance on technology and digital processes has trickled downward from large enterprises and governments to small and medium-sized enterprises (SMEs). SMEs and private citizens alike are relying on a broad digital ecosystem as a core pillar of their daily lives.

Because the digital economy is built on a web of interconnected systems and networks, it is also highly targeted by a range of isolated to state-sponsored cybercriminals who can launch disruptive, if not destructive, cyberattacks to obtain sensitive data or demand a ransom, amongst other forms of attacks.

Despite widespread discussions around the aggregation potential for a catastrophic or even broader systemic cyber event, no single cyber event has come close to rivaling the worst non-cyber systemic events (e.g., 2008 financial crisis, COVID-19). Nevertheless, the size and interconnectedness of the online ecosystem beg some important questions: how broad could these attacks be? Similarly, could they reach catastrophic proportions and how can we best prepare for and model such events?

SMEs are a critical component of our economy

SMEs make up 99.9% of all U.S. businesses (SBA) and are critically important to the health of the U.S. economy. They accounted for 62% of new jobs created between 1995 and 2020.

Systemic Cyber Risk vs Catastrophic Cyber Events

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 are the 2008 financial crisis or the COVID-19 pandemic. Not all systemic events are catastrophic in nature, but every systemic loss has the potential to grow to catastrophic levels of disruption. To date, there is yet to be a systemic cyber event of catastrophic level. While by some measures, the recent Log4J vulnerability could be categorized as systemic, the relatively slow speed of propagation combined with the technological ecosystem's ability to patch appear to have muted the possible disruption.

Systemic events can illustrate the degree to which cross-sector interdependence exists and test the overall resiliency of the system. Views of cyber systemic risk are of particular interest due to the interconnected nature of the cyber ecosystem. While the initial shock to the system could theoretically be small, the cyber interconnectedness can be concerning as far as potential reach of a single event over time. This reach also allows for an equal but opposing force in mitigation and repair of a possible vulnerability or breach. This is perhaps the most overlooked trait in analyzing cyber systemic risk. While all cyber systemic risks have the potential to be catastrophic, the cyber system has an unparalleled ability to react to and repair vulnerabilities before that happens.

What Systemic Cyber Risk is Not

It might be tempting to directly leverage catastrophic models already in place for other lines of insurance in evaluating the cyber catastrophe risk (systemic or otherwise). Most often, cyber catastrophes are lumped together with natural catastrophes. This is due to the maturity of both the natural catastrophe models as well as the risk transfer mechanisms. This is also an incorrect approach. The nature of the risk, the propagation vector, as well as the overall system make for a fundamentally different peril that merits a fundamentally different approach.

"Not all systemic events are catastrophic in nature, but every systemic loss has the potential to grow to catastrophic levels of disruption."

What Makes SMEs Different?

In analyzing systemic SME cyber risk, there are some unique considerations.

For one, the average SME is less likely to be a direct target. While the possibility of a disgruntled insider may exist, larger, more sophisticated, and more ideologically motivated threat actors are less likely to target small businesses. This is because individual enterprises of significant economic, social, and political influence or infrastructure fall largely outside of the scope of SMEs.

For the SME market segment, the degree to which enterprises may be at risk is a function of how a particular systemic event spreads. For that reason, the most significant measure of exposure is the quality and security of an organization's digital touchpoints.

The particular traits of this interconnectedness differ significantly from larger enterprises within the cyber ecosystem.

While it may not be uncommon for a large enterprise or public institution to have locally housed data as well as teams dedicated to cybersecurity and best practices, small organizations often lack the appropriate resources, thereby making them more vulnerable and exposed on two fronts: data processed in-house or in cloud environments, and adequate configuration of systems for security best practices. It's also important to acknowledge that segments of the broader SME market might be lagging in the adoption of cyber insurance and the technologies to monitor and secure enterprise data.

The degree to which a systemic event can wreak havoc on the SME segment is therefore a direct function of the quality of enterprises' interconnections, as well as the overall malleability or speed to repair their digital touchpoints. Any accurate quantification of cyber systemic risk, particularly as it pertains to SMEs, requires a clear understanding of these characteristics

Paths to Modeling

Any meaningful analysis of SME systemic risks needs to start by considering the following traits of the underlying system and the enterprises that it comprises. In the case of SMEs, all three of these categories differ from the system of larger businesses in cyberspace.

1 Types of Threat Actors

- Cybercriminals,
- Nation-states,
- Insider threats.

2 Types of Systemic Cyber Losses

- Waterfall effect of cyber incidents in interconnected enterprises (supply chain)
- A systemic risk can trigger contagion

3 Cyber Pathways: Technological Mitigation

- Concentration
- Complexity and transparency

Types of Threat Actors

Before we can do any meaningful analysis on a systemic risk itself, it is important to consider the possible threat actors that would lead to a cyber event. The most common categorization for cyber risks are the following: **Cybercriminal**, **Hacktivist**, **Nation-State**, and **Insider Threat**.

All of these can potentially lead to a systemic event of catastrophic scale, yet the degree to which they may directly target specific market segments can make some of them less concerning to smaller enterprises.

> The indirect nature of certain threat actors allows time for individual enterprises to repair the vulnerability before a loss proliferates to SMEs and triggers catastrophic levels of loss aggregation.

	SME Exposure	Sophistication	Motivation
Hacktivist	Indirect	High	Ideological
Nation-State	Indirect	High	Political/Ideological
Insider	Direct	Low	Financial
Cybercriminal	Indirect / Direct	Varies	Financial

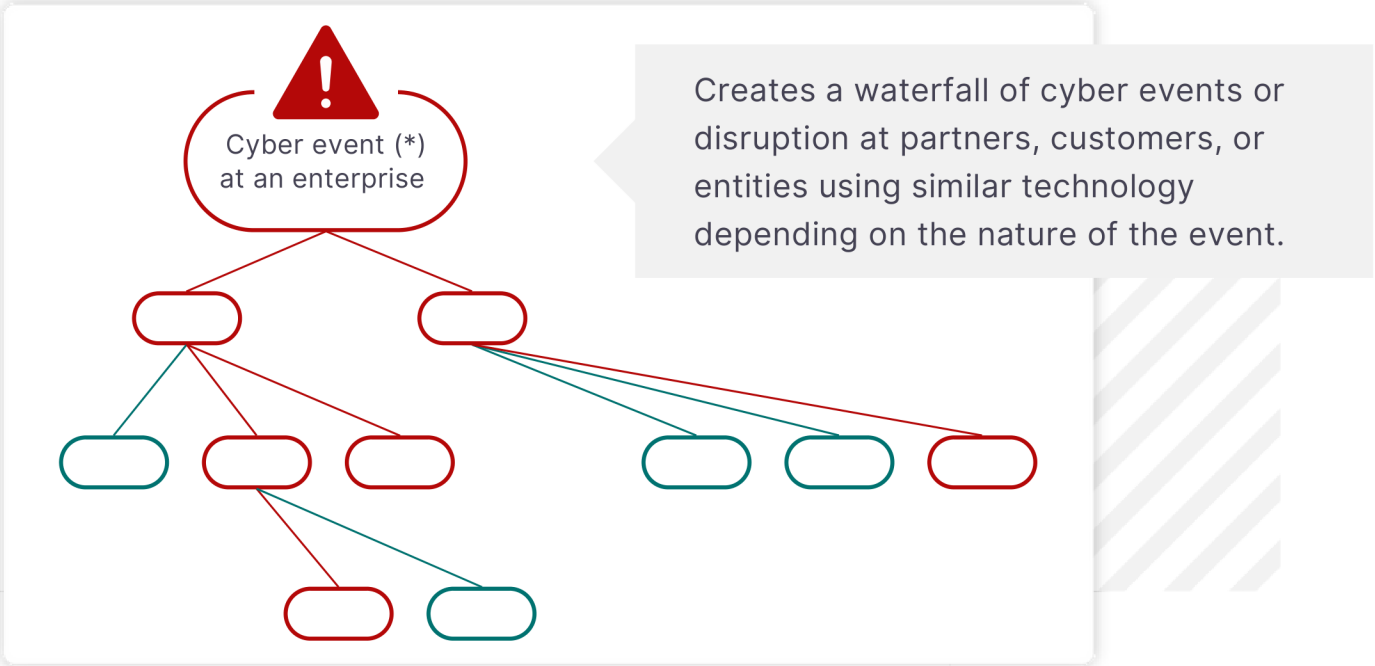
Portfolio exposures need to be assessed along two lines: sophistication and motivation. The more motivated a threat actor is to target a particular entity or market segment, the more sophisticated they need to be. In the case of SME, the vulnerabilities and threat actors of concern tend to be less sophisticated, seeking only to exploit the awareness and overall cybersecurity gaps that exist in a more underserved part of the cyber ecosystem.

This is an important trait of the SME ecosystem in the case of loss mitigation. Threat actors are oftenmore indirect and less sophisticated. This is to say that the vulnerability of these enterprises can change significantly as they deploy best practices. The scope of exposure is also a direct function of the quality of their processes in implementing and improving cyber hygiene in real-time. Continuous monitoring and quantification of these processes within a broader system can be a significant marker of the degree to which the ecosystem can react, mitigate, or outright circumvent a catastrophic event.

Types of Systemic Cyber Losses[1]

Once an event has occurred, the manner in which it spreads through the system can be classified into three categories: supply chain, contagion, and in special cases, a hybrid of the two. Though similar, these types of losses differ fundamentally in how wider disruption may amplify within the system. This also means that the appropriate and available means of loss mitigation will differ as well, thereby impacting modeled views of loss propagation, aggregation, and overall disruption to the system.

Waterfall Effect of Cyber Incidents in Interconnected Enterprises (Supply Chain)



[1] "Systemic Cyber Risk: A Primer", Carnegie Endowment for International Peace, March 2022 https://carnegieendowment.org/2022/03/07/systemic-cyber-risk-primer-pub-86531

A problem affecting a single component of the overall system triggers a chain reaction impacting a cascading range of dependent entities within the broader system.

A Systemic Risk Can Trigger Contagion

Identical copies of a system component can fail simultaneously or in rapid succession. One failure creates systemic effects without a cascading supply chain event.

The impact of systemic risk described above can combine where an incident spreads throughout an ecosystem of large and small enterprises and triggers business disruption which in turn results in a contagion affecting several critical components of numerous enterprises.

Cyber Pathways: Technological Mitigation

The pathway and speed of both contagions and chain reactions will be highly dependent on a set number of variables that should be quantified. While not every pathway or vulnerability can always be known or identified, the resiliency of the overall system is a significant predictor of how widespread and disruptive a future vulnerability or event could become.

Concentration

In the online ecosystem, a net consolidation around certain technologies, software providers and third-party vendors has led to aggregation points that should be monitored and quantified.

This consolidation can provide organizational efficiencies, particularly for SMEs seeking to leverage the broader ecosystem, but they also can create single points of failure and modes of propagation for systemic loss. Conversely, these efficiencies also scale the ability to respond, mitigate, and repair if leveraged efficiently in the context of cybersecurity.

A portfolio seeking to analyze their systemic exposure would need to analyze both how this concentration might increase exposure and how it could allow for a faster and more scalable response.

Complexity and Transparency

In the case of systemic vulnerability that could be exploited, the overall complexity of the vulnerable software is relevant to the potential for systemic loss. Not all software dependencies are readily known, disclosed, or in some cases even understood.

For SMEs with less sophisticated in-house cybersecurity professionals, the level to which the software they use is codependent must be considered. This requires a deep understanding of the software, which may be private to the uninformed public.

The intellectual property of software can make some of these codependencies unknown to the public. This means that understanding the quality of an SME's digital connection to the broader system requires highly specialized knowledge of private pieces of the digital infrastructure, oftentimes unavailable to smaller enterprises that elect to forgo basic cybersecurity measures.

In the absence of a quantifiable measure of an enterprise's connection to the cyber ecosystem, the systemic SME risk is amplified significantly. Yet these interconnections can, in fact, be monitored, not only reducing the systemic exposure but also making it much more quantifiable and conducive to modeling through the mining of digitally housed data points.

More importantly, the degree to which the broader network of cybersecurity professionals and technologically-driven insurers within the ecosystem are equipped with appropriate data points is a significant measure of the overall resiliency of the system. The more complex the interconnections, the more effective the cybersecurity and tech-enabled insurance providers are in reducing systemic vulnerabilities and losses before they reach catastrophic levels.

Securing the SME Market Through Augmented Underwriting

While recent campaigns and reporting requirements have spread cybersecurity awareness, a troubling gap remains. In the case of larger infrastructure and organizations, government measures like General Data Protection Regulation (GDPR) in the E.U. and the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) in the U.S. have increased the focus on cybersecurity to a degree, yet SMEs and individuals remain relatively underserved and undereducated when it comes to cybersecurity best practices.

Systemic vulnerabilities, particularly in the case of the SME market segment can be significantly reduced through a combination of improved awareness, improved cybersecurity, and improved cyber insurance. Unfortunately, market penetration continues to leave this market underserved.

The cyber insurance market and insurtech companies, in particular, have expanded their product offerings to include cybersecurity training, scanning, and risk engineering, acting in many ways as a “CISO for hire” for organizations that lack the appropriate resources internally. In evaluating systemic risk, the vulnerability of the broader system is paramount. A secure cyber ecosystem can only be achieved by closing the awareness, security, and insurance gaps that remain within the SME cyber ecosystem.

With a risk pool of 30 million U.S. SMEs (92% of the U.S. market), Cowbell has gained significant insights into the broader systemic risk of the SME cyber ecosystem, for both insured and uninsured entities, but monitoring is only one piece of the picture.

A more resilient system overall can only be achieved through broader leverage of relevant data, communicated back to individual enterprises, in real-time, with necessary repairs deployed systematically and with speed and efficiency. This not only increases the protection but allows for further and ever-increasing accuracy of systemic resiliency. This resiliency is significant when the appropriate data and cybersecurity measures are properly and systematically deployed.

Conclusion

The cyber insurance industry has come a long way in its understanding of catastrophic cyber risk and its insurability. In order to address the gaps in both insurance and cybersecurity, insurers need to take a proactive role, serving as both security consultants as well as insurers, thereby establishing clear and quantifiable risk-sharing mechanisms between policyholders, private insurers, and the government, and increasing the overall resilience of the cyber ecosystem.

With a more clearly defined risk, more educated market, and more proactive technology-driven underwriting, the protection gaps can be narrowed by keeping pace with the growing demand, and the most vulnerable parts of the digital ecosystem and broader economy can be protected.

The Leader in Cyber Insurance for SMEs

Cowbell delivers standalone and individualized cyber insurance to small and medium-sized enterprises. Cowbell's cyber policies include continuous risk assessment, access to risk engineers for advice, cybersecurity awareness training for employees, and more.