HOUSE HOMELAND SECURITY COMMITTEE
SUBCOMMITTEE ON CYBERSECURITY AND INFRASTRUCTURE PROTECTION

Jack Kudale
Founder and CEO
Cowbell

Testimony on Sector Down: Ensuring Critical Infrastructure Resilience

June 27, 2024

I. Introduction

Chairman Garbarino, Ranking member Swalwell, and members of the committee thank you for the opportunity to testify today on cyber resiliency in the event of a major cyber event.

In 2019, I founded and launched Cowbell, a Cyber Insurance provider, powered by Artificial Intelligence, headquartered in the United States. Over the last 5 years, Cowbell has scaled from a small InsurTech to a leading provider of cyber insurance for small and medium-sized enterprises (SMEs). While we are first and foremost a cyber insurer, we take an active role in helping our policyholders decrease their cyber risk exposure by sharing our cybersecurity tools and expertise with them. Our continuous risk assessment of both our policyholders and the aggregate SME market equips our risks with best-in-class understanding and knowledge to mitigate and prevent potential loss. We employ nearly 165 people, including data scientists, software engineers, and cybersecurity and insurance industry professionals, who research the overall cybersecurity posture of the comprehensive SME ecosystem of risks.

The Cowbell team has supported cyber insurance and data initiatives for the U.S. Government since 2020. We actively participate in public-private partnerships, such as the Cybersecurity and Infrastructure Agency's (CISA) Cyber Infrastructure and Data Working Group (CIDAWG), through which we have worked over the past months with select industry partners to address concerns over data governance standards. We have engaged in ongoing discussions regarding the possibility of a Government Cyber Insurance Program through the Treasury's Federal Insurance Office (FIO) and the Office of the National Cybersecurity Director (ONCD) and we continue to be an outspoken voice in the field of SME cybersecurity risk and insurance. Cowbell is deeply committed to educating, securing, and insuring the cyber risk of small and medium-sized enterprises.

II. SMEs as Core Cybersecurity Risk

SMEs are one of the most underserved segments of the American economy when it comes to cybersecurity and cyber insurance. Any meaningful discussion surrounding the security of our critical infrastructure requires an understanding of the SME ecosystem. This segment represents over 99% of all businesses, 44% of the American GDP, and a potential major propagator of a widespread cyber contagion.

SMEs have the most to gain from basic cybersecurity measures; they hold the potential to either aggregate or extinguish a cyber catastrophe at scale via the most simple types of exploitations or software and hardware updates respectively. This is due to both the size and level of digital connectivity of the average SME. Unsophisticated types of vulnerabilities can aggregate simply due to a lack of basic awareness and security. Furthermore, an attack on an unsophisticated market poses indirect threats to every entity in the cyber ecosystem.

According to a World Economic Forum study,[1] 41% of all companies surveyed have been affected by a third-party cyber incident with small and medium-sized suppliers being increasingly targeted to later hack into their larger customers' systems. The expected rise in costs incurred by businesses globally due to software supply chain attacks is estimated to grow from US$46bn in 2023 to US$60bn in 2025[2].

The SME web of interconnected entities is critical to American economic stability. Moreover, it is perfectly positioned to form a core component of loss prevention if equipped with the appropriate tools for cyber risk.

III. Cyber Insurers as Risk Managers

Currently, the SME cybersecurity posture is widely varied. Understanding for a moment that the average company in the US has revenues of less than 5 million dollars, they can be forgiven for overlooking cybersecurity as core to their business. Nearly four out of five SMEs in the US are either uninsured or underinsured when it comes to cyber insurance.

Awareness, education, and standardization of cybersecurity hygiene are still lacking, most often in the small business segment. Additionally, awareness without sufficient guidance does not lead to appropriate action. A 2022 survey on small business cybersecurity trends highlighted that 51% of small businesses did not have any cybersecurity measures in place and that 59% of these businesses considered themselves too small to be targeted.[3]

---

[1]https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf
[2]https://www.juniperresearch.com/press/study-reveals-staggering-cost-of-software-supply/
[3]https://web.archive.org/web/20230322074906/https://digital.com/51-of-small-business-admit-to-leaving-customer-data-unsecure/

Cyber insurance providers such as ourselves are quickly becoming the most significant force in educating SME policyholders on basic cybersecurity. The degree to which these risks can change is key to their insurability. The risk profile of cyber insurance shoppers can be improved instantly through tech-enabled underwriting and purchasing processes.

IV. Insured vs Uninsured Market

Leveraging information from our risk pool, Cowbell teams have found notable differences in the cybersecurity hygiene of the average uninsured or first-time buyer of insurance vs the insured market. This poses a potentially compounding aggregation potential; the most uninsured entities are most overexposed. It also outlines a broader truth regarding insurance gaps: those with the least to lose stand to lose the most in the event of a cyber event.

Under these conditions, an increase in market penetration to the SME cyber insurance market pays dividends to the security of the overall cyber ecosystem. This is because every entity that is taught appropriate cyber hygiene is a break in the chain when it comes to cyber contagion and a reduction in aggregation potential for everyone. It is also what is most commonly missed in discussions about the size of the aggregate cyber exposure: every additional dollar of market coverage is insuring a diminished amount of systemic risk.

With 80% of the SME market still uninsured and overexposed, these entities need to understand that cyber risk is business risk, and SME risk is a cyber aggregation risk.

V. Understanding the Downstream Impact of Cyber Events

Cowbell and cyber insurance providers have unique visibility into the downstream impact of cyber incidents, where cyber meets financial, human, and physical consequences. Cowbell especially gains such visibility when working with secondary victims of supply chain attacks.

Supply chain attacks seek to damage an organization and its customers through a single breach of one entity. Since 2021, the number of U.S. entities affected by supply chain attacks has increased year over year. In 2021 521 U.S. organizations reported impact due to a supply chain attack.[1] In 2022 this figure tripled to 1,543 and increased again in 2023 to 2,769. Research firm Gartner predicts that by 2025 45% of all organizations will have experienced operational impact due to a software supply chain attack.[2]

Visibility into the downstream impact of cyber events can allow cyber insurers to understand:

- Incident types

- Nature of impact
- Amount of losses
- Types of losses
- Types of damages
- Downtime
- Recovery time
- Impacted policyholders' size, sector, location
- Relationship between impacted policyholders and breached organization
- If impacted policyholders had a backup vendor
- If impacted policyholders had a business continuity plan
- If there was lateral movement from the breached organization onto the systems of impacted policyholders
- Amount of policyholder data held by the breached entity

VI. Current State of the Cyber Insurance Market

The global cyber insurance market has reached a size of US$14bn in 2023 and is estimated to increase to around US$29bn by 2027[4]. Showing significant growth potential, the market is driven by the awareness of the increasing frequency and sophistication of cyber-attacks, including the potential financial repercussions, as well as by stricter state and national regulatory requirements. Further growth factors continue to be the ongoing digital transformation and technological advances in all sectors and concrete requirements to be satisfied by business partners within the supply chain. This overall trend illustrates the importance of cyber insurance as a core component of cyber risk management. However, large companies still account for the majority of premiums; small and medium-sized enterprises bear most of their cyber risks on their own.

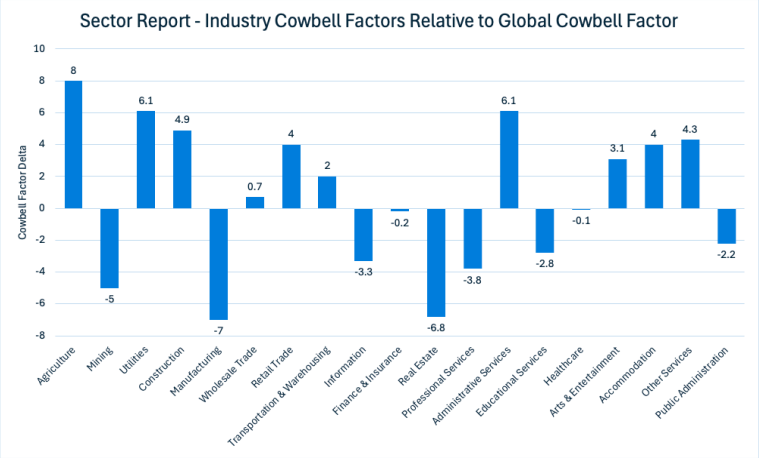
Market growth projections for the SME cyber market have not kept pace with the larger corporations. This is outlined by the WEF Cybersecurity Outlook, demonstrating that while more high-revenue companies are maturing into leaders in cyber resilience, more low-revenue organizations are losing overall cyber resiliency rather than gaining it.[5]

VII. SMEs, Cyber Insurance, and Critical Infrastructure

Cowbell is committed to protecting and advocating for the underserved, underrepresented market that is the SME market. SMEs are the backbone of the U.S. economy and if they are vulnerable, the national economy and all entities associated with critical infrastructure are vulnerable. In the case of a systemic risk that would lead to a catastrophic event, a significant percentage of the SME market is extremely vulnerable.

[4]https://www.munichre.com/en/insights/cyber/global-cyber-risk-and-insurance-survey.html
[5]https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf

The illustration below shows the SME sector report using patented technology[6] - Cowbell Factors - comparing major industries' aggregate cyber risk postures to each other.



Source: Cowbell

Today's hearing should serve as an urgent call to collective action for our valued SMEs. Specifically:

1. Classification of SMEs as a subset of any cyber preparedness measures
2. Increased calls for the SME ecosystem, particularly entities that remain uninsured, to become cyber-resilient
3. Harmonization of SME cybersecurity and data governance best practices

Cyber Insurers have constructed a viable framework for cyber resilience. However, the limitations to both penetration and total risk-bearing market capacity merit special attention. The damage from catastrophic events could either exceed or fall squarely outside of the scope of the current insured market. Insurers, particularly those in the SME space, face a major challenge in closing this gap between economic and insured losses. Given the dynamic growth of risks in a digital world, higher insurance penetration for cyber risks is the ultimate goal. In securing our most valuable SMEs from the digital threats they face, we can collectively offer increased resiliency to the economy and society.

Thank you for the opportunity to testify today, I look forward to your questions and our continued discussion.

###

[6]US PTO 11,870,800 Issued Jan 9, 2024 and US PTO 11,888,861 Issued Jan 30, 2024