cowbell®

Cyber Roundup Report 2024

An assessment of the threat landscape and what business leaders can do to become more secure

Introduction

Today, businesses are more interconnected than ever before, with data and cloud operations being the lifeblood of day-to-day operations. While this digital transformation offers significant opportunity for business growth and technological innovations it also brings with it unprecedented cyber risk.

The cybersecurity landscape is evolving at an unprecedented pace and not only are new threats popping up, but the integration of various AI models is also driving further development of the attacks. This can be from Open-source generative AI and large language models such as OpenAI's ChatGPT which are allowing executors to greatly improve the maturity and success of their attacks as well as AI that has been built specifically for threat actor groups.

The smarter AI becomes the more sophisticated attacks will be, and while AI providers are actively avoiding attempts to weaponize their technologies, attacks continue to increase in frequency and severity. Research has shown that adversaries seek to better understand and automate typical attack chain behaviors in a variety of use cases.

The tactics, techniques, procedures, and business models of ransomware operators keep evolving. While traditional ransomware focused primarily on the encryption and decryption of data, more recent campaigns have included espionage and threats to expose sensitive information, for extortion.

The attack surface for cybercriminals has widened dramatically and cybersecurity risks are no longer confined to large businesses. Public sector entities and critical infrastructure, including government, healthcare, and education, have been increasingly targeted by ransomware campaigns.

This report, based on Cowbell's comprehensive analysis of over 46 million small and medium-sized enterprises (SMEs) across the U.S., U.K., and Japan, offers valuable insights into how cyber risk manifests in different industries and why businesses of all sizes must take these risks seriously and adopt robust security strategies.

Executive Summary

The analysis reveals several critical findings

1. Supply chain attacks surged by five times (431%) between 2021 and 2023, indicating a growing vulnerability in interconnected business ecosystems.
2. The manufacturing sector emerges as the most at-risk, with cyber risk scores 11.7% below the global average – this is driven by its reliance on automation and the sensitivity of its intellectual property.
3. Public administration and educational services also face elevated risks, particularly from ransomware attacks, with a 70% increase in attacks on educational institutions over the past year.

The analysis also highlights the correlation between business size and cyber risk. Larger businesses, especially those with revenues exceeding $50 million, experience cyber incidents 2.5 times more frequently than other enterprises, largely due to their more complex operations and valuable data assets. This necessitates scalable and comprehensive cybersecurity strategies that can adapt to the growing complexity of larger organizations.

This report is divided into three parts: Key Findings, Implications for Business' and Actionable Steps for Business Leaders.

By onboarding these insights and implementing the recommended strategies, organizations can better protect themselves against the rising tide of cyber threats in an increasingly digital business landscape.

Part 1: Key Findings

Supply chain attacks gain momentum

Between 2021 and 2023, the volume of supply chain attacks has grown more than five times (431%), with further growth projected by 2025. These attacks are effective because they exploit the trust between interconnected organizations and their vendors or suppliers, and can potentially compromise multiple entities through a single breach.

The dramatic rise in supply chain attacks can be attributed to several factors:

- Increased digitization and interconnectivity of business operations.
- Growing complexity of supply chains, making them harder to secure.
- The potential for high-value targets through a single point of entry.
- The challenge of maintaining visibility and control over third-party security practices.

This trend highlights the need for robust third-party risk management.

KEY FACT:

supply chain attacks

UP 431%*

*2021-2023

Highest cyber risk: Manufacturing

According to the analysis, the manufacturing sector emerges as the most vulnerable to cyber threats, with risk scores 11.7% below the global average. This elevated risk is manifested in both the frequency and severity of cyber incidents, with manufacturers facing claims that are not only 1.6 times more frequent, but also 1.2 times more severe compared to the average across all sectors.

Key factors contributing to this heightened risk include:

- The sector's heavy reliance on automation and interconnected devices (Internet of Things).
- Presence of legacy systems and bespoke software that may lack modern security features.
- High sensitivity of data, including intellectual property and design plans.
- Increasing digitization of manufacturing processes without corresponding security measures.
- Complex supply chains that introduce potential points of vulnerability.

The combination of these factors creates a perfect storm of cyber risk for manufacturing companies, making them attractive targets for cybercriminals seeking to exploit valuable intellectual property or disrupt critical operations.

KEY FACT:

The **MANUFACTURING** sector emerges as the **MOST VULNERABLE** to cyber threats, with risk scores 11.7% below the global average.

Public administration and educational services: Latest high-risk industry

Public administration and educational services show risk scores 2 points lower than the global average, indicating higher cyber exposure. A notable trend is the 70% surge in attacks on educational institutions over the past year. These sectors face increased targeting due to urgent service restoration needs and limited cybersecurity budgets. Despite lower frequency, they experience 20-40% higher severity of claims than average.

Several factors contribute to the vulnerability of these sectors:

- Budget constraints often lead to outdated IT infrastructure and security measures.
- Large user bases with varying levels of cybersecurity awareness.
- Valuable personal and research data that attracts cybercriminals.
- The critical nature of services, increasing pressure to pay ransoms in case of attacks.

The higher severity of claims in these sectors reflects the potential for significant disruption and data loss when attacks do occur, highlighting the need for improved cybersecurity measures and incident response planning.

KEY FACT:

70% INCREASE in attacks on educational institutions in the past years

Healthcare and prof. services: High severity, lower frequency

The healthcare and professional services sectors present a different risk profile. Both experience lower-than-average claim frequency but face higher-than-average severity when incidents do occur. Specifically, the healthcare sector sees 20% lower frequency but 40% higher severity, while professional services experience 10% lower frequency but 15% higher severity. This is likely due to the sensitive nature of the data these sectors handle.

For healthcare, the high severity of attacks can be attributed to:

- Strict regulatory requirements and potential for hefty fines.
- The critical nature of patient data and potential for life-threatening disruptions.
- High costs associated with system downtime and data recovery.

In the case of professional services, the elevated severity of attacks could be due to:

- The confidential nature of client information.
- Potential for significant reputational damage.
- High value of intellectual property and strategic business information.

These findings emphasize the need for robust data protection measures and comprehensive incident response plans in these sectors, even if the frequency of attacks is lower than average.

Revenue impact on risk

The analysis reveals a clear correlation between a company's revenue and its cyber risk profile. Larger businesses, particularly those with annual revenues exceeding $50 million, face significantly higher cyber risks. On average, these organizations experience cyber incidents 2.5 times more frequently. In contrast, the smallest revenue band, comprising businesses with annual revenues under $10 million, experiences only 0.4 times the average claims frequency.

This disparity can be explained by several factors:

- Larger companies present a more attractive target due to their valuable data assets.
- Complex IT infrastructures in larger organizations create more potential entry points for attackers.
- Higher public profile of larger companies can make them targets for reputation-damaging attacks.
- Smaller companies may fly under the radar of sophisticated cybercriminal operations.

However, it is important to note that while smaller businesses face fewer attacks, they often lack the resources to implement robust cybersecurity measures or recover quickly from an incident. This means that while the frequency of attacks may be lower, the impact of a successful attack on a small business can be extremely severe.

KEY FACT:

Businesses with >$50m revenue are **2.5X MORE LIKELY** to face cyber incidents

Technological threats

The analysis has identified several technology categories that present significant cybersecurity risks. The top five risky technologies are:

Operating systems: As the foundation of all computer operations, operating systems naturally present a high risk. While modern operating systems have robust security features, they also have a significant number of documented vulnerabilities. Any exploit in an operating system can potentially lead to a complete system compromise.

Content management and collaboration tools: These have become increasingly important, especially with the rise of remote work. However, these platforms often have vulnerabilities that could allow attackers to tamper with content, leak data or gain unauthorized access.

Virtualization technologies: While offering great benefits in terms of resource utilization and flexibility, virtualization solutions introduce an additional layer of complexity that can create security vulnerabilities. If not managed properly, these can create single points of failure that affect multiple systems.

TOP 5 RISKY TECHNOLOGIES

- Operating systems
- Content management and collaboration tools
- Virtualization technologies
- Server-side technologies
- Business tools and applications

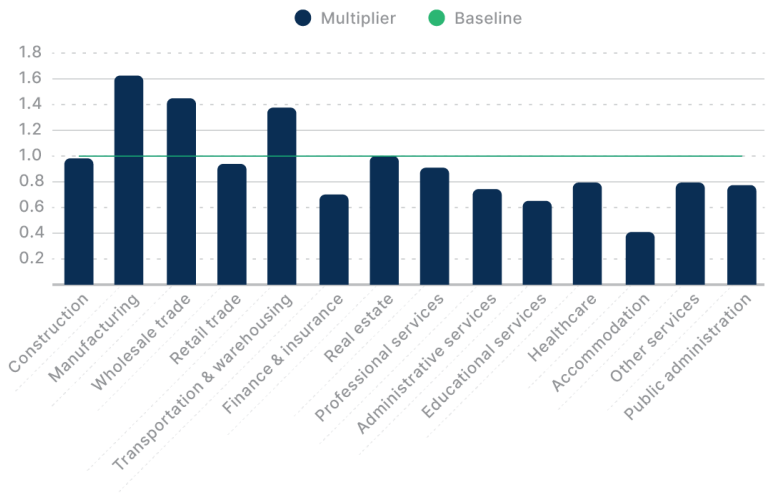
Server-side technologies: Databases and web/application servers are critical for data handling and processing. Exploits in these technologies can lead to severe data breaches and system disruptions, making them a prime target for attackers

Business tools and applications: These manage various critical operations and can thus be exploited to disrupt business processes and access sensitive data. The risk varies depending on the specific application, but the potential for disruption to core business functions makes this category particularly concerning.

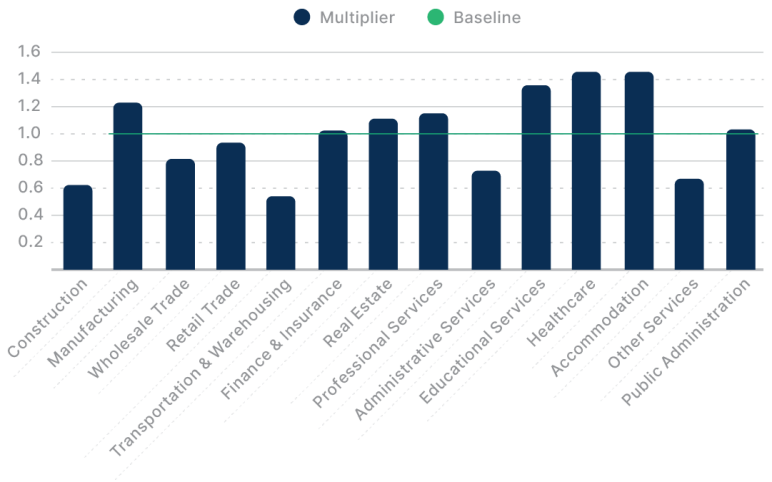
These technologies are fundamental to most business operations, which is precisely what makes them so risky. Their ubiquity and critical role in day-to-day functions mean that any vulnerabilities in these systems can have far-reaching consequences.

The cloud: Analysis relating to cloud provider usage found that businesses using Google Cloud report a 28% lower frequency of cyber incidents relative to other cloud users. In addition to a reduced frequency of incidents, Google Cloud exhibits the lowest severity of cyber incidents, while Microsoft Azure shows the highest.

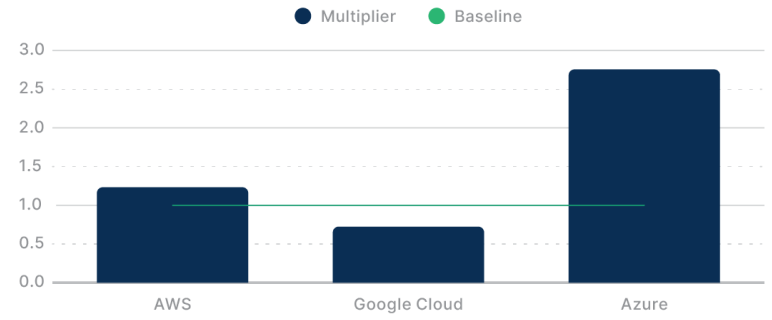
CLAIM FREQUENCY RELATIVITY



CLAIM SEVERITY RELATIVITY

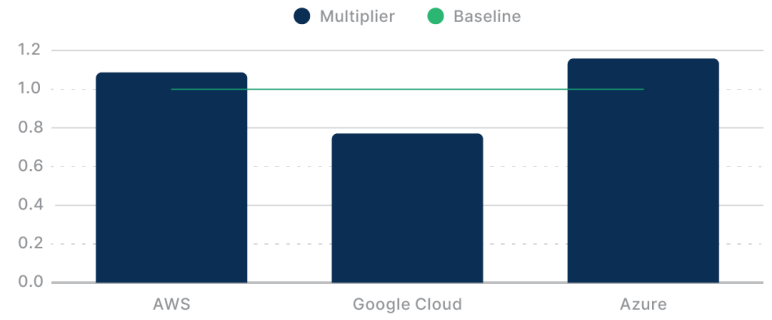


CLAIM FREQUENCY RELATIVITY FOR CLOUD



CLAIM SEVERITY RELATIVITY FOR CLOUD

(Six Months Development)



Part 2: Implications for Business

The insights obtained from the analysis have several implications for businesses across various sectors – understanding them is crucial for developing effective cybersecurity strategies and protecting against evolving threats.

Here, we summarize the major implications for SMEs to consider.

Industry-specific cybersecurity strategies are crucial

Each sector faces unique challenges and vulnerabilities which require tailored approaches to cyber risk management.

Manufacturing companies must prioritize updating legacy systems and improving patching protocols to address their specific vulnerabilities. They should also focus on securing their intellectual property and implementing robust network segmentation to protect critical operational technology.

Public administration and education sectors, meanwhile, should focus on strengthening their defenses against ransomware attacks. This includes implementing comprehensive backup strategies, enhancing email security to prevent phishing attacks, and providing regular cybersecurity awareness training to staff and students.

Healthcare organizations need to maintain stringent data protection measures due to the sensitivity of patient data and the potential for severe reputational damage in case of a breach. This involves implementing strong encryption for data at rest and in transit, ensuring compliance with healthcare-specific regulations, and developing robust incident response plans that minimize disruption to patient care.

Rising importance of cyber risk management

As cyber risks grow more severe, investment in advanced cybersecurity measures is no longer optional – it is a necessity. Businesses should implement prompt patching systems, conduct regular vulnerability assessments, and adopt industry-specific best practices for data protection.

What does comprehensive cyber risk management look like?
Key focus areas should include:

- Regular security audits and penetration testing.
- Implementation of multi-factor authentication across all systems.
- Development of a robust incident response plan.
- Employee training on cybersecurity best practices.
- Adoption of a zero-trust security model.

Small businesses are not immune

Despite facing fewer attacks on average, small businesses often lack proper cyber hygiene, making them attractive targets for cybercriminals.

It is therefore crucial for small business owners to understand that their size doesn't make them invisible to attackers. Implementing basic security measures, such as regular software updates, employee training on phishing awareness, and robust password policies, can significantly improve a small business's security posture.

Small businesses should also consider:

- Implementing basic endpoint protection solutions.
- Regularly backing up critical data.
- Utilizing cloud services that offer built-in security features.
- Developing an incident response plan tailored to their resources.

Cyber risk: Revenue size matters

Larger businesses, particularly those with revenues over $50 million, need to recognize their increased risk exposure and respond accordingly.

This might involve investing heavily in cybersecurity infrastructure, including robust backup systems, advanced threat detection tools, and comprehensive employee training programs. Large organizations should also develop and regularly test incident response plans to ensure they can quickly and effectively respond to cyber incidents.

Supply chain vulnerabilities are growing

The dramatic rise in supply chain attacks highlights the need for businesses to look beyond their own networks when assessing cybersecurity.

Companies must ensure that their partners and suppliers maintain strong cybersecurity practices. This could entail implementing rigorous third-party risk assessment procedures, regularly auditing the security posture of key suppliers, and developing contingency plans for potential supply chain disruptions.

Technology risk management is critical

The security of fundamental systems, such as operating systems and server-side technologies, is especially important given the technology categories associated with high risk.

Regular updates, patch management, and security hardening of these critical systems should be a top priority. For content management and collaboration tools, implementing strong access controls and encryption is crucial.

Part 3: Action Points for Business Leaders

To address the evolving cyber threat landscape effectively, business leaders should consider implementing the following five action points.

1 – Conduct regular cyber risk assessments

SMEs need to prioritize the implementation of regular, comprehensive cyber risk assessments. These assessments should be tailored to the specific threats and vulnerabilities faced by their industry. Utilizing tools like Cowbell Factors can provide valuable benchmarks against industry peers, offering insights into areas where the organization may be lagging or excelling in its cybersecurity efforts.

Major components of an effective cyber risk assessment include:

- Identifying critical assets and data.
- Evaluating current security controls.
- Assessing potential threats and vulnerabilities.
- Determining the potential impact of various cyber incidents.
- Prioritizing risks based on likelihood and potential impact.

2 – Provision cybersecurity training for employees

Human error remains one of the most significant vulnerabilities in any organization's cybersecurity defenses. To address this, business leaders should invest in comprehensive, ongoing cybersecurity training programs for all employees. These programs should be role-specific, recognizing that different positions within the organization may face different types of cyber threats. Phishing awareness should be a key focus, especially for small businesses that may be more vulnerable to this type of attack.

Effective cybersecurity training should cover:

- Recognizing and reporting phishing attempts.
- Safe browsing and email practices.
- Proper handling of sensitive data.
- Password security and the use of multi-factor authentication.
- Social engineering awareness.
- Secure remote work practices

3 – Strengthen incident response and backup systems

Having a robust incident response plan is crucial in today's threat landscape. This plan should clearly outline the steps to be taken in the event of a cyberattack, including who is responsible for what actions. Equally important is the implementation of comprehensive backup systems – these need to be regular, automated, and stored offline or in a segmented network to protect against ransomware attacks.

Key elements of an effective incident response plan include:

- Clear roles and responsibilities for the incident response team.
- Procedures for containing and mitigating the impact of an attack.
- Communication protocols for internal and external stakeholders.
- Steps for preserving evidence for potential legal proceedings.
- Processes for post-incident analysis and improvement.

4 – Improve due diligence across the supply chain

Given the surge in supply chain attacks, businesses need to extend their cybersecurity efforts beyond their own networks.

This involves implementing rigorous vetting processes for third-party vendors and regularly auditing the security posture of key suppliers. Develop a comprehensive third-party risk management program that includes security questionnaires, on-site assessments (where appropriate), and continuous monitoring of critical vendors.

5 – Prioritize technology risk management

After the research identified several high-risk technology categories, business leaders need to prioritize the security of these critical systems.

Key actions should include implementing a robust patch management program to ensure all systems, especially operating systems and server-side technologies, are up to date with the latest security patches. For content management and collaboration tools, implement strong access controls, encryption, and regular security audits.

By implementing these five action points, business leaders can significantly enhance their organization's cyber resilience. However, it is equally important to remember that cybersecurity is not a one-time effort – it needs to be treated as an ongoing process that receives continuous attention and adaptation to new threats.

Conclusion

The cybersecurity landscape for SMEs is becoming increasingly complex and threatening. As this report demonstrates, cyber risks vary significantly across industries and company sizes, necessitating tailored approaches to cybersecurity.

The surge in supply chain attacks, rising by five times (431%) from 2021 to 2023, highlights the interconnected nature of modern business risks. The manufacturing sector's position as the most vulnerable to cyber threats serves as a wake-up call for an industry undergoing rapid digital transformation. Meanwhile, the correlation between company size and cyber risk underscores the need for larger organizations to be particularly vigilant.

By understanding these trends and implementing the recommended action points, business leaders can take significant steps toward improving their organization's cyber resilience. As the threat landscape continues to evolve, staying informed and proactive in cybersecurity efforts will be crucial for the long-term success and security of businesses across all sectors.

For more detailed information and industry-specific insights, please visit cowbell.insure.

FIVE CRITICAL CYBER ACTIONS FOR SMES

- ✔ Conduct regular cyber risk assessments
- ✔ Provision cybersecurity training for employees
- ✔ Strengthen incident response and backup systems
- ✔ Improve due diligence across the supply chain
- ✔ Prioritize technology risk management

cowbell®

support@cowbellcyber.ai | (833) 633-8666 | **cowbell.insure**

US0059 1124