



## **The Impacts of Cyberattack on SMEs in the USA and Way to Accelerate Cybersecurity**

**Nazmul Hossain**

Peoples' Friendship University of Russia  
name after Patrice Lumumba

**Mahmud Hasan**

ECPI University, Virginia, USA

### **ABSTRACT**

We are at the 4<sup>th</sup> industrial revolution called industry 4.0. The world is turning from digitalization to automation. Technological advancement and adoption and utilization of changing pattern of technology is gaining the gear at all social, political, diplomatic, economic and commercial spheres including SMEs. Technological advancement is bringing speed, innovation and sophistication of products and services in SMEs in one hand and on the other hand, cyber hacking and various and changing pattern of cybercrimes are hampering the growth and development. The aim of the study is to analysis the impacts of cyberattacks on SME's productivity, growth and development in USA and potential way to accelerate the cyber security in the area. The study is mainly based on secondary sources of data including journals, research publications, scholarly articles, thesis papers etc. The finding of the study revealed that Banking and finance, healthcare, small manufacturing firms, retailers and E-commerce, public transport and infrastructure with less than 500 employees are the most vulnerable sectors for the Cyber-attack in the USA. The most commonly practiced cyberattacks are Phishing attacks, Ransomware, Malware, DDoS attacks, MitM etc. The Study suggests a number of cyber security measures including employee awareness and training program, creation of security policy and practice, know how to distinguish between fake antivirus offer and real notification and protect OT-IT system to prevent the damage.

**Keywords:** SMEs, Cyberattacks, Cybersecurity, Financial impacts, Artificial Intelligence.

### **INTRODUCTION**

In the science and technology based current digital-driven economic arena, cyber-attack emerges as a widespread threat for the business of all sizes. It's become more devastating for the SMEs than their largescale business counterpart (Babiceanu and Seker 2019; Choo 2011). The SMEs are increasingly being attacked in recent years as they are with limited resources and capabilities to take effective and sufficient measures in timely manner.

In the USA, SMEs faced 350% more social engineering attack than their largescale business counterparts in 2021. A 2024 survey found that 60% of SMEs view cyberthreats including phishing and ransomware as their biggest challenge, ahead of supply chain issues and potential pandemics. The impact of cyber crime and its level is increasing gradually due to business's

technology and online platform (Corllo et al., 2020; Deloitte, 2020). Cyberattack encompasses a range of activities ranging from hacking and data breaches to social engineering and ransomware attacks.

The study mainly focuses on examining the phenomenon of cyberattacks commonly affecting the SMEs in the USA drawing upon a comprehensive US database and suggest a number of effective measures to bring a potential breakthrough.

### THE MOST CYBERATTACKS AFFECTING SMES IN THE USA

Cyberattacks have become one of the most significant concerns for small and medium-sized enterprises (SMEs) in the USA. A 2024 survey found that 60% of SMEs view cyber threats, including phishing and ransomware, as their biggest challenge, ahead of supply chain issues and potential pandemics (StrongDM). SMEs are particularly vulnerable to these attacks due to limited resources in cybersecurity (U.S. Chamber of Commerce).

Additionally, with the rise in targeted attacks on small businesses, 47% of cyber breaches in the past year impacted businesses with fewer than 500 employees (StrongDM)(BDO). The most cyberattacks affecting SMEs in the USA are:

- **Phishing Attacks:** Phishing remains a major threat, with attackers sending deceptive emails to employees, tricking them into revealing sensitive information like login credentials. SMEs are highly vulnerable due to a lack of advanced email filtering systems and employee training (U.S. Chamber of Commerce) (BDO).
- **Ransomware:** Ransomware attacks are particularly damaging for SMEs, encrypting critical business data and demanding a ransom. Without strong backups or cybersecurity defenses, SMEs are often forced to pay the ransom to regain access, resulting in financial strain and loss of trust (StrongDM).
- **Malware:** Malware attacks are often used to infect a company's network via malicious software delivered through emails or compromised websites. Once installed, malware can steal sensitive data, spy on company activities, or disrupt operations entirely (BDO).
- **DDoS Attacks:** Distributed Denial of Service (DDoS) attacks overwhelm SME servers with traffic, causing service disruptions and loss of business. These attacks are relatively simple to execute but can have devastating effects on a small business's operational capacity and customer satisfaction (StrongDM).
- **Man-in-the-Middle (MitM) Attacks:** In these attacks, an attacker intercepts communication between two parties, typically over unsecured networks, to steal data or impersonate one of the parties. SMEs may lack the network security protocols necessary to detect and prevent these attacks (U.S. Chamber of Commerce).
- **Insider Threats:** Insider threats occur when a current or former employee intentionally or unintentionally compromises security by providing access to malicious actors or leaking sensitive information. SMEs often struggle to implement robust access control measures, making them vulnerable to this form of attack (BDO)(StrongDM).

These types of attacks highlight the importance of investing in cybersecurity for SMEs, as they are increasingly becoming targets of sophisticated cybercriminals due to their often-limited security infrastructure.

## TYPES OF SMES COMMONLY TARGETED BY CYBERATTACKS

Small and medium-sized enterprises (SMEs) are increasingly targeted by cybercriminals due to their limited cybersecurity defenses and the sensitive data they handle. Financial institutions, for example, manage personal banking data, making them vulnerable to phishing and ransomware attacks (Cyber Defense Magazine). Healthcare providers experience an average of 1,684 attacks per week, with ransomware being particularly disruptive (World Economic Forum) (ClearDATA). In sectors like manufacturing and transportation, cyberattacks exploit operational technology systems, causing widespread supply chain disruptions (Industrial Cyber). E-commerce SMEs face significant risks from data breaches and phishing (BigCommerce). Here's some SMEs commonly targeted by cyberattackers:

- **Financial Institutions (e.g., Banks):** SMEs in the financial sector are prime targets for cyberattacks due to the sensitive data they manage, including personal banking information and financial transactions. These businesses often experience attacks such as phishing and ransomware, which can severely disrupt operations and lead to significant financial losses. Continuous security measures and training are essential to protect against evolving threats like ransomware and phishing (Cyber Defense Magazine).
- **Healthcare Providers:** Healthcare-related SMEs are highly targeted by cyberattacks due to the sensitive personal and medical data they hold. In 2023, healthcare ranked as the third most attacked sector, with an alarming average of 1,684 attacks per week. Ransomware is particularly disruptive, often crippling healthcare services and risking patient safety. Implementing zero-trust security models is critical to safeguarding these organizations (World Economic Forum) (ClearDATA) (American Council on Science and Health).
- **Small Manufacturing Firms:** Manufacturing SMEs are vulnerable to cyberattacks, especially in sectors like transportation, due to their reliance on operational technology (OT) systems. These attacks, including ransomware, target the interconnectivity between OT and IT systems. As these systems are increasingly digitized, the risks grow. Addressing these vulnerabilities requires collaboration between government bodies, industries, and cybersecurity experts. Strategies like network segmentation, real-time monitoring, and robust access controls are crucial to mitigate these threats (Industrial Cyber).
- **Retailers and E-commerce SMEs:** E-commerce SMEs face significant risks from cyberattacks, including data breaches, phishing, and malware. These businesses handle sensitive customer information, such as credit card details, making them prime targets for cybercriminals. Large-scale breaches in recent years, such as those at Target and Home Depot, highlight the importance of robust security measures for all online retailers (BigCommerce).
- **Public Transport and Infrastructure SMEs:** SMEs involved in public transportation and critical infrastructure are increasingly at risk due to their reliance on digital systems. Cyberattacks targeting these sectors, especially Distributed Denial of Service (DDoS) attacks, can cause significant operational disruptions. With the digitalization of transport systems, stronger cybersecurity measures are urgently needed to protect these vital services (World Economic Forum).

### COMMON WAYS CYBER ATTACKERS TARGET SMES

Cyber attackers frequently target small and medium-sized enterprises (SMEs) using various tactics that exploit both technical vulnerabilities and human error. Here's the Common Ways Cyber Attackers Target SMEs-

- **Email Phishing:** Phishing is one of the most common cyberattack tactics targeting businesses, especially through emails. Cybercriminals use deceptive emails to trick recipients into revealing sensitive information or clicking malicious links. The attacker's goal is to impersonate trusted organizations, such as banks or government institutions, to gain access to private data. Phishing continues to evolve and remains a significant threat, often leading to data breaches and financial fraud (SentinelOne).
- **Exploiting Weak Passwords:** Weak passwords remain a significant security risk for both individuals and organizations. Short, simple, or predictable passwords are easily exploited by cybercriminals through methods like brute force attacks or dictionary attacks. A single compromised password can lead to unauthorized access, account takeovers, and widespread data breaches. Strong password policies, including multifactor authentication (MFA) and unique passwords for different accounts, are essential in mitigating these risks (Jetpack).
- **Exploiting Vulnerabilities in Software:** Unpatched software remains one of the most significant security risks for organizations. Cybercriminals often exploit known vulnerabilities in outdated software to gain unauthorized access, steal sensitive data, or disrupt operations. These vulnerabilities, if left unaddressed, increase the likelihood of successful attacks like ransomware and data breaches. Regular patching and a systematic approach to vulnerability management are essential to mitigate these risks and ensure compliance with security standards (Splashtop).
- **Social Engineering:** Social engineering attacks manipulate human behavior to trick victims into divulging sensitive information or performing actions that compromise security. Attackers often use psychological tactics, such as impersonating trusted individuals or organizations, to gain the victim's trust. Common forms include phishing, pretexting, and baiting, with phishing being the most prevalent. These attacks are dangerous because they exploit human error rather than technical vulnerabilities, making them harder to detect and prevent (Imperva).
- **Supply Chain Attacks:** SMEs are increasingly targeted by supply chain attacks, where cybercriminals exploit vulnerabilities in smaller companies to gain access to larger organizations in the supply chain. These attacks are effective because SMEs often have weaker cybersecurity defenses, making them the weakest link. Cybercriminals use these attacks to compromise critical infrastructure and sensitive data, often bypassing stronger security measures at larger firms by infiltrating through their smaller partners (Insights | Integrity360).

### ECONOMIC IMPACTS OF CYBERATTACKS ON SMES IN THE USA

In the USA cyberattacks on SMEs are very common and growing together with the acceleration of the cost of attacks. In 2023, about 73% of US small company owners claimed having been the victim of a cyberattack. Even with the historically high volume of assaults, 85% of executives said they felt equipped to deal with a cyber disaster.

Regretfully, too few businesses really adhere to cybersecurity best practices. Cybersecurity

control adoption rates are still modest (20–34%). This poor adoption of cybersecurity measures by SMEs leaves them vulnerable to increasingly sophisticated cyber crime and accelerating the cost.

According to the Global Financial Report 2024, there is a growing likelihood of significant losses resulting from cyberattacks in the United States. Such losses can put a company's solvency in jeopardy and possibly lead to funding issues. Since 2017, the magnitude of these catastrophic losses has increased to \$2.5 billion, more than quadrupling. Furthermore, indirect losses are far larger and include things like reputational harm and security enhancements.

The banking industry is particularly vulnerable to cyberattacks. Due to the volume of sensitive data and transactions they manage, financial organizations are frequently the target of criminals looking to steal money or cause disruptions to the economy. Almost one-fifth of all attacks are directed on financial companies, with banks being the most vulnerable.

If the cyberattacks continue to rise at the current rate, small firms may face severe financial consequences. By 2025, damages are expected to have increased to \$10.5 trillion, a 300% rise from 2015 levels.

And most remarkably, 55% of people in the U.S. would be less likely to continue doing business with companies that are breached according to the report of Small Business Cybersecurity Statistic 2024 (Komron Rahmonbek 2024).

### **BEST LOW-COST SOLUTIONS FOR SMES TO PREVENT CYBERATTACKS**

Small and medium-sized enterprises (SMEs) are increasingly vulnerable to cyberattacks due to limited resources for cybersecurity. To protect against these growing threats, SMEs must adopt effective and affordable cybersecurity strategies. Below are some low-cost solutions SMEs can implement to enhance their cybersecurity defenses.

#### **Implement Multi-Factor Authentication (MFA)**

Multi-factor authentication (MFA) adds an additional layer of security by requiring users to provide two or more verification factors before accessing a system. This reduces the risk of unauthorized access from stolen credentials, making it a highly effective and low-cost solution for SMEs to secure sensitive data (StrongDM, 2024).

#### **Invest in Reliable Antivirus and Endpoint Security**

Antivirus and endpoint security solutions offer real-time protection against malware, ransomware, and phishing attacks. These tools provide continuous monitoring and threat detection across all devices and networks within the organization. Solutions such as Bitdefender or Kaspersky offer affordable packages designed for small businesses, ensuring comprehensive protection at a reasonable cost (BDO, 2023).

#### **Use Secure Cloud Backup Solutions**

Backing up data is critical to ensure that SMEs can recover in the event of a cyberattack, particularly ransomware. A cloud-based backup service that encrypts data and stores it securely provides an affordable and efficient solution. Services like Backblaze and iDrive offer

reliable, low-cost options for SMEs to maintain data integrity and business continuity after an attack (U.S. Chamber of Commerce, 2023).

### **Adopt a Managed Security Service Provider (MSSP)**

For SMEs without dedicated cybersecurity staff, partnering with a Managed Security Service Provider (MSSP) offers a cost-effective way to monitor and manage security. MSSPs provide 24/7 monitoring, threat detection, and incident response, enabling SMEs to benefit from professional cybersecurity services without the high cost of an in-house team (Cyber Defense Magazine, 2023).

### **Conduct Regular Employee Cybersecurity Training**

Human error remains a leading cause of data breaches, particularly in SMEs. Regular training programs can help employees recognize phishing emails, suspicious links, and other common cyber threats. Affordable platforms like KnowBe4 offer cybersecurity training modules designed specifically for small businesses, helping to raise awareness and reduce vulnerabilities (SentinelOne, 2023).

### **Utilize Network Segmentation**

Network segmentation involves dividing a network into smaller, isolated segments, which can limit the impact of a potential cyberattack. This strategy helps SMEs protect sensitive data by preventing unauthorized users from accessing entire networks. Implementing segmentation is an effective low-cost measure to safeguard critical assets (Imperva, 2023).

### **Deploy a Virtual Private Network (VPN)**

Using a Virtual Private Network (VPN) ensures that all data transmitted over the internet is encrypted, safeguarding it from interception or unauthorized access. VPNs are especially useful for remote workers or employees accessing company systems from unsecured networks. Solutions like NordVPN and ExpressVPN provide affordable, secure connections, helping SMEs maintain data privacy (Integrity360, 2023).

SMEs can significantly strengthen their cybersecurity posture by implementing these cost-effective solutions. From multi-factor authentication to network segmentation and employee training, these strategies help protect against the growing number of cyberattacks targeting small businesses, ensuring that critical assets and data remain secure.

### **References**

- [1] BDO. (2023). Top 10 Cybersecurity Threats to Businesses in 2023. BDO. <https://www.bdo.com/insights/digital/top-10-cybersecurity-threats-to-businesses-in-2023>
- [2] Strong DM. (2024). 35 Alarming Small Business Cybersecurity Statistics for 2024. StrongDM. <https://www.strongdm.com/blog/small-business-cyber-security-statistics>
- [3] U.S. Chamber of Commerce. (2023). New Survey Finds Small Businesses Think Cyberattacks Are Biggest Threat. U.S. Chamber of Commerce. <https://www.uschamber.com/small-business/new-survey-finds-small-businesses-think-cyberattacks-are-biggest-threat>
- [4] Cyber Defense Magazine. (2023). The Biggest Cyber Threats for the Financial Industry in 2023. Cyber Defense Magazine. <https://www.cyberdefensemagazine.com/the-biggest-cyber-threats-for-the-financial-industry-in-2023/>

- [5] World Economic Forum. (2023). A rise in healthcare cyber attacks calls for zero trust. World Economic Forum. <https://www.weforum.org/agenda/2023/05/cyber-attacks-on-healthcare-rise-zero-trust/>
- [6] ClearDATA. (2023). Cybersecurity Threats in Healthcare: 2023 Threat Report. ClearDATA. <https://www.cleardata.com/resources/2023-healthcare-threat-report/>
- [7] American Council on Science and Health. (2023). Cybersecurity in Health Care: Critical to Patients, Medical Providers. ACSH. <https://www.acsh.org/news/2023/05/11/cybersecurity-health-care-critical-patients-medical-providers-17042>
- [8] BigCommerce. (2023). Ecommerce Data Breaches: Costs of Security Mismanagement. BigCommerce. <https://www.bigcommerce.com/articles/ecommerce/ecommerce-data-breaches/>
- [9] World Economic Forum. (2023). Why cybersecurity risks matter and how to raise security. World Economic Forum. <https://www.weforum.org/agenda/2023/03/why-cybersecurity-in-manufacturing-matters-to-us-all/>
- [10] Industrial Cyber. (2023). Addressing OT Cybersecurity Threats in Transportation Sector Through Enhanced Strategies & Collaboration. Industrial Cyber. <https://industrialcyber.co/features/addressing-ot-cybersecurity-threats-in-transportation-sector-through-enhanced-strategies-collaboration/>
- [11] SentinelOne. (2023). What is Smishing (SMS Phishing)? Examples & Tactics. SentinelOne. <https://www.sentinelone.com/cybersecurity-101/cybersecurity/what-is-smishing/>
- [12] Jetpack. (2023). How Weak Passwords Expose You to Serious Security Risks. Jetpack. <https://jetpack.com/blog/weak-passwords/>
- [13] Splashtop. (2023). Risks & Vulnerabilities of Unpatched Software. Splashtop. <https://www.splashtop.com/blog/risks-and-vulnerabilities-of-unpatched-software>
- [14] Imperva. (2023). What is Social Engineering | Attack Techniques & Prevention Methods. Imperva. <https://www.imperva.com/learn/application-security/social-engineering-attack/>
- [15] Integrity360. (2023). SMEs in the Crosshairs: Why do Hackers Target Small-to-Medium Sized Enterprises?. Integrity360. <https://insights.integrity360.com/smes-in-the-crosshairs-why-do-hackers-target-small-to-medium-sized-enterprises>
- [16] Komron Rahmonbek 2024. 35 Alarming Small Business Cybersecurity Statistics for 2024. Feb 1, 2024. <https://www.strongdm.com/blog/small-business-cyber-security-statistics>