White Paper

Top 5 Cybersecurity Threats to U.S. Small Businesses

COX BUSINESS®

OUR FOCUS IS YOUR FUTURE℠

coxbusiness.com

Table of Contents

Executive Summary

Small businesses are facing a cybersecurity reality check. Once considered too small to target, today's tech-forward small businesses – especially in healthcare, legal and financial services – are now squarely in the crosshairs of increasingly sophisticated cybercriminals. These firms manage sensitive data, rely heavily on digital tools and often lack the layered cyber defense of larger enterprises. The result? A perfect storm of risk.

This whitepaper outlines the top five cybersecurity threats currently facing U.S.-based small businesses:

- ✓ Phishing & Social Engineering
- ✓ Ransomware
- ✓ Credential Stuffing
- ✓ Business Email Compromise
- ✓ Unpatched Software Vulnerabilities

Each threat is explored in depth, with practical insights into how these attacks unfold in small business environments.

We also examine the financial and operational impact of these threats, from ransom payments and compliance violations to lost revenue and reputational damage. The paper also highlights how AI and cryptocurrency are reshaping the threat landscape, enabling attackers to launch more frequent, targeted and untraceable campaigns.

Finally, we provide a security stack tailored to small businesses, offering actionable steps to strengthen cybersecurity posture across the perimeter, network, endpoint, application and data layers.

Whether you're an office manager, IT lead or business owner, this guide is designed to help you understand the risks, recognize the warning signs and take meaningful steps to protect your business, your clients and your reputation.

Top 5 Cybersecurity Threats to U.S. Small Businesses

01 Phishing & Social Engineering

Phishing and social engineering remain the most pervasive and dangerous threats to small businesses today. These attacks rely on deception rather than technical exploits by tricking employees into clicking malicious links, downloading infected attachments or revealing sensitive information. Social engineering tactics often involve impersonating trusted individuals or organizations, exploiting human psychology to bypass cyber defense tools.

The danger lies in how easily these attacks can compromise entire systems. A single click can lead to credential theft, ransomware deployment or unauthorized access to sensitive data. Small businesses, especially those in healthcare, legal, and financial services, are prime targets due to the high value of their data and the likelihood of quick response to seemingly urgent requests.

90%

Over 90% of successful cyberattacks begin with a phishing email.[1]

(Source: CISA, 2024)

For example, a receptionist at a small medical practice might receive an email that appears to come from their electronic health record (EHR) vendor. The message urges them to "verify account credentials" via a link that leads to a convincing but fraudulent login page. Once entered, the attacker gains access to patient records and internal systems.

02 Ransomware

Ransomware is one of the most financially devastating threats facing small businesses. This form of malware encrypts a company's data and demands payment, usually in cryptocurrency, for its release. The attack often begins with a phishing email or through an unpatched vulnerability, and once inside, it can spread rapidly across systems.

The consequences are severe. Operations grind to a halt, sensitive data may be permanently lost and businesses face the difficult decision of whether to pay the ransom. For small firms without robust backups or incident response plans, the pressure to pay is immense, especially in sectors like healthcare or accounting, where downtime can be catastrophic.

60%

Nearly 60% of small businesses hit by ransomware paid the ransom.[2]

(Source: National Cybersecurity Alliance, 2024)

Consider a small accounting firm that has suffered a ransomware attack and is locked out of its client files just days before tax season. The attackers demand $25,000 in Bitcoin to restore access. With deadlines looming and no viable backup, the firm pays the ransom, only to face additional costs in recovery, legal consultation and client notification.

03 Credential Stuffing

Credential stuffing is a highly automated attack that exploits the widespread habit of password reuse. Cybercriminals take usernames and passwords leaked from one breach and use bots to try them across hundreds of other platforms. If users have reused credentials, attackers can gain access to email accounts, cloud storage or financial systems with little resistance.

80%

Over 80% of hacking-related breaches involve stolen or reused credentials. [3]

(Source: NIST, 2023)

This threat is particularly dangerous because it often goes undetected. Unlike brute-force attacks, credential stuffing uses valid credentials, making it harder for security systems to flag the activity as suspicious. For small businesses, especially those without multi-factor authentication (MFA), the risk of compromise is high.

Imagine an attacker using credentials leaked from a breached fitness app to access a law firm's cloud-based document system. The same email and password combination works, giving the attacker access to confidential client files and internal communications.

04 Business Email Compromise (BEC)

Business Email Compromise is a targeted form of fraud where attackers impersonate executives, vendors or clients to trick employees into transferring funds or sensitive data. Unlike phishing, BEC attacks are often well-researched and highly personalized, making them difficult to detect.

The threat level is high because BEC bypasses traditional security tools. There are no malicious links or attachments, just a convincing message that appears to come from someone the recipient trusts. The financial and reputational damage can be significant, especially for small firms that lack the resources to absorb such losses.

$2.4 billion

Business Email Compromise scams caused over $2.4 billion in losses in the U.S. in 2023. [4]

(Source: FBI IC3 Report, 2024)

For instance, a paralegal at a small law office receives an email that appears to come from the managing partner, requesting an urgent wire transfer to a new client account. The email is well-written, uses the partner's signature and references a real case. The transfer is made and $18,000 is gone before the fraud is discovered.

05 Unpatched Software Vulnerabilities

Unpatched software vulnerabilities are an often-overlooked threat. Known flaws in operating systems, applications and devices that have not been updated with the latest security patches leave businesses exposed. Cybercriminals actively scan for these weaknesses, often using sophisticated tactics to identify and exploit them.

60%

60% of breaches involved vulnerabilities for which a patch was available but not applied. [5]

(Source: Center for Internet Security, 2024)

The danger is that these vulnerabilities are well-documented and easily exploited. Once breached, attackers can install malware, exfiltrate data or move laterally across the network and steal credentials. Small businesses often delay updates due to concerns about downtime or compatibility, leaving them exposed.

Take the case of a small financial advisory firm that postpones updating its firewall firmware. Attackers exploit a known vulnerability to gain access to internal systems, bypassing authentication and accessing sensitive client data.

The Impact of Cyberattacks on Small Businesses

Cyberattacks are not just technical incidents, they are business crises. For small medical practices, law offices and financial services firms, a single breach can trigger a cascade of consequences like operational disruption, financial loss, legal exposure and long-term reputational damage. Unlike large enterprises, small businesses often lack the resources to absorb these shocks, making the impact disproportionately severe.

1. Financial Fallout

The direct costs of a cyberattack can be staggering. Ransomware demands alone can range from thousands to hundreds of thousands of dollars, depending on the size of the business and the sensitivity of the data. But the ransom is just the beginning. Recovery costs – including forensic investigations, system restoration, legal fees and customer notification – can easily exceed the ransom itself. In regulated industries like healthcare and finance, the financial burden is compounded by compliance penalties. A small medical practice that suffers a breach involving protected health information (PHI) may face fines under HIPAA, while a financial advisory firm could be penalized under SEC or FINRA regulations.

Consider a scenario where a small clinic is hit with ransomware that encrypts its patient scheduling and billing systems. The clinic pays $17,000 in cryptocurrency to regain access, but the total cost— including downtime, IT recovery and legal consultation— exceeds $75,000. The clinic also faces a HIPAA investigation and loses several long-term patients due to trust concerns.

2. Operational Disruption

Cyberattacks often bring business operations to a standstill. In small firms, even a short disruption can have cascading effects. Medical practices may be forced to cancel appointments, law offices may miss filing deadlines and accounting firms may be unable to access client records during tax season.

In this plausible example, a small law firm experiences a business email compromise that leads to the fraudulent transfer of $22,000. While the financial loss is significant, the greater impact is the week-long disruption as the firm shuts down systems, resets credentials and works with law enforcement and their bank to investigate the breach.

3. Reputational Damage

Trust is a cornerstone of professional services. When clients learn that their personal, legal or financial information has been compromised, the damage to a firm's reputation can be long-lasting. Negative press, online reviews and word-of-mouth can deter new clients and erode existing relationships.

Imagine that a small financial advisory firm experiences a credential stuffing attack that exposes client investment data. Although the breach is contained quickly, several clients move their accounts to larger firms with more robust security programs. The firm's online ratings drop and it takes over a year to rebuild its client base.

4. Legal and Regulatory Consequences

Small businesses in regulated industries are subject to strict data protection laws. A breach can trigger mandatory reporting requirements, audits and fines. In some cases, businesses may also face civil litigation from affected clients or patients.

Envision a situation in which a solo practitioner dentist fails to patch a known vulnerability in their practice management software. After a breach exposes patient records, the practice is fined $10,000 under HIPAA and is required to implement a corrective action plan, including staff training and third-party audits.

Why Small Businesses Are Especially Vulnerable

Despite their size, small businesses are increasingly targeted by cybercriminals. The misconception that "we're too small to be a target" is not only outdated, it's dangerous. In reality, small businesses often present an ideal combination of valuable data and weaker cyber defense, making them attractive entry points for attackers.

Weaker Security Posture
Most small businesses lack dedicated cybersecurity staff or formal security programs. Without in-house expertise, they often rely on general IT support or outsourced providers who may not specialize in threat prevention.

Limited IT Budgets
Budget constraints often force small businesses to make trade-offs between operational needs and security investments. A strong security posture requires a multi-layered cyber defense strategy. Yet, endpoint protection, network monitoring secure backup and recovery solutions are frequently deferred or underfunded.

Valuable Data, Less Protection
Even the smallest medical practice or law office handles highly sensitive data like protected health information (PHI), financial records and legal documents that can be monetized on the dark web or used for extortion. Yet these businesses often lack the layered defenses needed to protect that data, making them disproportionately attractive to attackers.

High Likelihood of Ransom Payment
Small businesses are more likely to pay ransoms because they lack the resources to recover quickly on their own. This willingness to pay makes them repeat targets.

Use of Consumer-Grade Tools
Many small businesses rely on free or consumer-grade software that lacks enterprise-level security controls. The use of unmanaged or consumer-grade cloud services, often with default configurations and no centralized oversight, is a common practice amongst small businesses.

Insufficient Employee Training
Human error remains the leading cause of breaches. In small businesses, cybersecurity training is often irregular or nonexistent. As covered in this report, most breaches involve human error like falling for social engineering attacks, insufficient password management and misconfigured systems.

Recommended Small Business Security Stack

A strong cybersecurity posture doesn't require enterprise-level budgets – it requires a layered, strategic approach. For small businesses in healthcare, legal and financial services, the following security stack offers a practical framework to reduce risk, improve resilience and meet regulatory expectations.

5 Layers of Critical Protection

Perimeter: Block malicious websites

- Countless malicious websites are created every day. Get a solution that continuously updates to protect your business from the latest threats.
- Blocking access to inappropriate or unwanted content is also recommended as it can help maintain a professional work environment.

Network: Secure network access

- Make sure you have a strong firewall and change your network and WiFi passwords often. Strong passwords, or passphrases, should be 12 – 14 characters, alpha-numeric, include capitalized letters and special symbols (#, !, $, %, etc.).
- Maintain separate WiFi networks for employees and guests. WPA3 or WPA2 encryption is recommended to further secure WiFi networks.

Host: Endpoint protection

- Get antivirus and malware protection on all Internet-connected devices. This protection should also cover any devices used by employees while working remotely.
- Enforce strong password policies on all business devices, including regular password changes and lockout policies for failed attempts.

Application: Apply software patches

- Hackers exploit vulnerabilities in operating systems. Implement strict patch management policies to ensure your software is always up to date on all devices.
- Enforce Multi-Factor Authentication (MFA), require strong passwords for SaaS and web apps and rotate them periodically.

Data: Implement a backup plan

- Back up your business data to the cloud frequently. The best solutions will encrypt your data both in transit and rest. It also will scan backed up data for malware so it can be restored cleanly and quickly.
- Implement role-based access controls.

Small Steps, Big Protection – Make Cybersecurity a Priority Today

Despite their size, small businesses are increasingly targeted by cybercriminals. The misconception that "we're too small to be a target" is not only outdated, it's dangerous. In reality, small businesses often present an ideal combination of valuable data and weaker cyber defense, making them attractive entry points for attackers.

Cybersecurity is no longer a "nice to have" for small businesses— it's a business imperative. As this whitepaper has shown, the threat landscape is evolving rapidly, with phishing, ransomware, credential stuffing, business email compromise and unpatched software vulnerabilities posing serious risks to small businesses.

These threats are not theoretical. They are real, frequent and with the emergence of artificial intelligence and cryptocurrency, increasingly sophisticated. While small businesses may not have the resources of large enterprises, they are not powerless. By understanding the risks, investing in layered cyber defense and fostering a culture of security awareness, small firms can significantly reduce their exposure.

The good news is that many of the most effective defenses, like multi-factor authentication, patch management, strong password policies and employee training, are affordable and scalable. With the right strategy and trusted advisor, small businesses can protect their operations, their clients and their reputations in an increasingly hostile digital environment.

If you'd like to explore cybersecurity solutions tailored to your business, Cox Business is here to help. We offer multi-layered solutions to strengthen your security posture and keep you positioned for growth.

[1] Cybersecurity & Infrastructure Security Agency (CISA). "Phishing Guidance." 2024. https://www.cisa.gov

[2] National Cybersecurity Alliance. "Ransomware and Small Business." 2024. https://staysafeonline.org

[3] National Institute of Standards and Technology (NIST). "Password Guidelines and Credential Management." 2023. https://www.nist.gov

[4] Federal Bureau of Investigation (FBI). "Internet Crime Report 2023." 2024. https://www.ic3.gov

[5] Center for Internet Security (CIS). "Top Cybersecurity Controls for SMBs." 2024. https://www.cisecurity.org