The Computer Company, Inc.
IT Solutions Done Right

Cybersecurity for SMBs:

Why Your Business is at Risk & How to Stay Protected

Introduction

Cybercrime doesn't discriminate. It targets businesses of all sizes, and small businesses are increasingly feeling the heat. In fact, **43% of cyberattacks** target small and medium-sized businesses (SMBs), according to the U.S. National Cyber Security Alliance. Even worse, **60% of small businesses** that experience a breach close their doors within six months due to the financial fallout (Cisco).

The truth is cybercriminals don't care how big or small your business is. They care about access to sensitive data and vulnerabilities, and once they find them, the results can be devastating.

At The Computer Company (TCC), we believe in taking a proactive, preventative approach to cybersecurity, not just reacting to breaches after the fact. In this guide, we'll walk you through current cybersecurity risks for SMBs, the financial impact of an attack, and the solutions you need to protect your business.

Cybersecurity Risks for SMBs

What makes SMBs particularly attractive cybercrime targets is their limited security infrastructure. A lack of resources or expertise to implement and maintain strong cybersecurity systems leaves them exposed to cyber risks like ransomware, phishing, and insider threats. Here's what your business is up against:

01. Phishing Attacks

Phishing emails trick employees into sharing sensitive information like passwords and financial details. They look real, but they're designed to steal from you.

Phishing attacks reached their highest point in 2022, with more than 1.2 million attacks in the final quarter of the year alone (APWG).

02. Ransomware

Ransomware locks your files and demands money to release them. These attacks can bring your business to a halt.

The average ransom paid in 2023 was $568,705 (Coveware).

03. Malware

Malware can damage your systems and steal your data. It's often delivered via email or insecure software.

36% of SMBs dealt with malware infections in the past year (CISA).

Cybersecurity Risks for SMBs

04. Data Breaches

A breach puts sensitive information at risk and can lead to fines, legal trouble, and damage to your reputation.

The average cost of a data breach is $3.86 million for SMBs (Ponemon Institute).

05. Insider Threats

Employees or contractors with access to your systems can unintentionally (or intentionally) cause a security breach.

30% of data breaches come from within the company (Varonis).

Attacks are becoming more frequent, more expensive, and harder to recover from. The best way to protect your business isn't to wait for something to go wrong; it's to invest in security before disaster strikes.

Here are the main cybersecurity protections every business should have in place:

1. Managed Cybersecurity Services

You can't protect what you're not watching. Managed cybersecurity services provide 24/7 monitoring, real-time threat detection, and ongoing protection—so threats are stopped before they become a problem. **Why it matters: 60% of small businesses don't have a cybersecurity plan, even though they're a top target.** (Source: Verizon Data Breach Report)

2. Managed Detection and Response (MDR)

Hackers don't always announce themselves. Many breaches go unnoticed for months, giving attackers time to steal data or damage systems. MDR constantly monitors for suspicious activity and stops attacks as they happen. **Why it matters: On average, it takes 204 days to detect a cyberattack.** (Source: IBM Cost of a Data Breach Report)

3. Dark Web Monitoring

If your business's passwords or customer data are stolen, they often end up for sale on the dark web. Dark web monitoring scans these sites and alerts you if your information is exposed—so you can take action fast. **Why it matters: Over 24 billion usernames and passwords are circulating on the dark web right now.** (Source: Digital Shadows Report)

4. Penetration Testing

Hackers look for weak spots in your systems. Penetration testing simulates a real attack to find and fix security gaps before cybercriminals can exploit them. **Why it matters: 93% of company networks have vulnerabilities that hackers can break into.** (Positive Technologies Research)

5. Web Filtering & Spam Protection

Most cyberattacks start with a fake email or a malicious website. Web filtering and spam protection block harmful emails and websites before they can do damage. **Why it matters: 91% of cyberattacks start with a phishing email.** (Cybersecurity & Infrastructure Security Agency)

6. Business Continuity Planning

Cyberattacks, IT failures, and natural disasters can all disrupt business. A business continuity plan ensures you can recover quickly, minimizing downtime and financial loss. **Why it matters: 60% of small businesses shut down within six months of a cyberattack.** (National Cyber Security Alliance)

7. Security Awareness Training

Your employees are the first line of defense, but they're also the most common security risk. Security awareness training teaches them how to spot scams, avoid risky behavior, and keep company data safe. **Why it matters: 88% of data breaches are caused by human error.** (Stanford University Study)

Cybersecurity is an Investment, Not an Expense

The cost of an attack is far higher than the cost of prevention. Investing in cybersecurity now protects your business, your data, and your future.

The ROI of Strong Cybersecurity

Many SMBs see cybersecurity as an expense, but the reality is it saves money.
A strong security strategy prevents costly attacks, keeps operations running, and protects your reputation.

Avoiding Major Financial Losses

A single data breach can cost SMBs $120,000 to $150,000 (Aligned Insurance), and 60% of affected businesses shut down within six months (Cybersecurity Ventures). Investing in cybersecurity reduces
this risk.

Reducing Downtime & Productivity Loss

Ransomware can shut down operations for days, costing SMBs an average of $8,500 per hour (Datto). Proactive security measures like managed detection and response (MDR) and business continuity planning help prevent disruptions.

Avoiding Fines & Compliance Violations

Regulations like HIPAA and SOC carry heavy penalties. Non-compliance can mean fines in the millions (IBM Cost of a Data Breach Report). Cybersecurity solutions help businesses meet these requirements and avoid legal trouble.

Protecting Customer Trust

86% of customers say they would stop doing business with a company after a breach (PCI Security Standards Council). A strong security strategy helps maintain trust and keeps customers from leaving.

Lowering Insurance Costs

Cyber insurance providers offer up to 25% lower premiums to businesses with strong security in place (Marsh Cyber Risk Report). Investing in cybersecurity can lead to direct cost savings.

The Bottom Line

Cybersecurity is an investment that reduces risk, prevents losses, and keeps your business running. The cost of inaction is far greater than the cost of staying secure.

Building Your Cybersecurity Safety Net with The Computer Company

Cybersecurity is complex, especially for SMBs. That's why having a trusted security partner like TCC is a must.

Expertise Without the Overhead: With TCC, you get expert-level security without the cost of an in-house team.

Proactive Protection: We don't wait for problems. Our Managed Detection and Response and penetration testing catch issues before they disrupt your business.

Bespoke Solutions: We customize our services to fit your unique needs— whether it's dark web monitoring or business continuity planning.

24/7 Monitoring & Support: Our team is always watching and ready to respond, ensuring your systems are secure around the clock.

Compliance Made Simple: Stay on top of regulatory requirements with TCC's expertise in HIPAA, SOC, and other industry standards.

Partner with TCC today to secure your business and get the peace of mind you deserve. Contact us to learn more.

P: 800-418-2358 | E: info@computercompany.net