TOUCAN TECHNOLOGY GROUP

EBOOK

Top Cybersecurity Threats for SMBs

toucan.tech

Small and medium-sized businesses (SMBs) are more exposed than ever.

According to the 2025 Verizon Data Breach Investigations Report (VDBIR), almost four times more SMBs were breached than large organizations. Granted, there are more small businesses than large businesses, but SMBs are attractive to attackers because of their limited cybersecurity resources, growing reliance on digital infrastructure, and often overlooked security vulnerabilities.

So, let's dive into the top cybersecurity threats facing SMBs in 2025 and how you can reduce your organization's risk.

Top Cybersecurity Threats for SMBs

Ransomware Attacks

Many organizations think ransomware is mainly targeted at large organizations. Think again.

The 2025 VDBIR found that ransomware-related incidents were 44% of overall breaches (up from 32% the previous year), and 88% of breaches caused by ransomware impacted SMBs, while only 39% of larger organizations had ransomware-related breaches.

In addition, modern ransomware attacks go beyond encrypting data and often involve double or triple extortion tactics, including data theft and public leakage threats. Without robust backup, detection, and response plans, many SMBs feel forced to pay ransoms to stay in business, which also fuels future attacks. In terms of financial and reputational damage, ransomware tops our list of top cybersecurity threats.

44% **of overall breaches were ransomware-related incidents (up from 32% last year).**

88% **of breaches caused by ransomware impacted SMBs.**

39% **of larger organizations had ransomware-related breaches.**

AI Makes Human Element & AI-Enhanced Social Engineering Breaches Easier for Attackers & Harder to Detect for Defenders

The human element was involved in 60% of all breaches, according to the 2025 VDBIR, with phishing, pretexting, and other social engineering tactics being the most common techniques.

While human error is always on the list of top cybersecurity threats, AI has dramatically increased the realism and reach of these attacks. Large language models and deepfake tools now create grammatically perfect phishing emails and impersonate trusted voices in live phone or video deepfake attacks. AI has made launching these attacks faster and easier for criminals and increasingly hard for users and systems to detect.

Third-Party and Software Supply Chain Attacks

30% **of all breaches involved a third-party vendor or service provider, and this number roughly doubled from the prior year, according to the 2025 VDBIR.**

From cloud providers to software vendors, if your partners' or their partners' security is breached, it can also cause a data breach at your organization. For example, the 2024 MOVEit breach impacted more than 2,700 organizations and exposed over 93 million personal records. More than 80% of the organizations that fell victim to the attack did not use the software but had third-party vendors that did. Breached suppliers are concerning enough, but it's not just malicious attacks that make third-party risk management so important.

Non-malicious vendor business interruptions like the widespread 2024 CrowdStrike outage that brought airlines, healthcare organizations and many other businesses to a sudden stop, showed that even reputable vendors make mistakes that can cause operational chaos and lost business.

Credential Theft and Abuse

Stolen credentials were used in 22% of breaches, **according to the 2025 VDBIR.**

Today's SMBs frequently rely on cloud platforms, email, and SaaS tools to provide fast, affordable, scalable solutions. However, this also creates numerous access points and configuration failure points that attackers can exploit. Credential stuffing, password reuse, social engineering, third-party vendor compromise, and dark web data leaks can expose these credentials. If you don't have a proactive cybersecurity plan in place, stolen credentials can enable attackers to slip in unnoticed and then expand their access to your entire network.

Vulnerability Exploitation

Closely following credential theft in the 2025 VDBIR was the 20% of breaches that were caused by vulnerability exploitation. This number was in large part driven by zero-day exploits that targeted edge devices and VPNs.

With limited patching resources, SMBs often fall behind on updates for routers, firewalls, and software. Attackers actively scan the internet for outdated systems with known vulnerabilities to exploit and are now leveraging AI to quickly write exploits for new vulnerabilities so they can immediately launch attacks.

20% of breaches that were caused by vulnerability exploitation

Additional Cybersecurity Risks to Watch

Cloud Misconfigurations

According to SentinelOne, about 23% of cloud security incidents are a result of simple cloud misconfigurations. These are often due to organizations misunderstanding the cloud's shared security model or leaving weak default security settings.

AI and Shadow IT

Unmanaged AI tools and unsanctioned software are spreading fast, opening unmonitored channels for data leakage and exposure.

IoT Devices

Smart devices from cameras to thermostats often ship with default credentials and lack patching mechanisms, making them easy backdoors for attackers.

Insider Threats

Malicious or careless insiders can cause major damage, especially in environments lacking monitoring or logging tools.

How to Reduce Your Risk

While we could write thousands of words on how to reduce your cybersecurity risks (but who has time to read that!), here's a quick chart of the top threats and security controls that can reduce your risk.

THREAT	MANAGED SERVICE MITIGATION
Ransomware	Endpoint detection and response (EDR), secure, regularly tested backups, immutable storage, and 24/7 monitoring
Phishing & Social Engineering	Security awareness training, phishing simulation tests, email filtering, and strong multi-factor authentication (MFA)
Credential Theft	Identity and access management (IAM), strong password manager/vault, security awareness training, and single sign-on (SSO) configuration
Third-Party Risks	Vendor risk scoring, contractual notification requirements, automated vendor monitoring, threat intelligence tracking, and access controls
Vulnerability Exploits	Regular patch management, continuous vulnerability scanning, IAM, and network segmentation or zero-trust architecture enforcement

In addition to implementing these controls, it's critical that your team regularly maintains, monitors, and updates them for continuously evolving threats and best practices. If this feels like a lot of work, managed IT services can reduce your expenses and ensure you have security experts managing your systems. A proactive cybersecurity prevention and detection program makes a big difference. In fact, the average cost of a data breach dropped by $258,629 for organizations that regularly provide cybersecurity awareness training and by $225,634 for organizations that have a trained incident response team. All of these prevention services and strategies can be affordably provided by a managed services provider since the costs are amortized across multiple companies.

Would you like additional help?

Call our Toucan Technology Group team! We're a local, family-owned IT managed services provider serving the greater Indianapolis area that offers comprehensive managed IT support (including breach detection and response) for up to 60% less than the cost of full-time, internal IT staff. If you already have an in-house IT team, we can also augment your team with specialized cybersecurity expertise or extra hands for projects and scaling needs.

TOUCAN
TECHNOLOGY
GROUP

Get a Free On-Site Cybersecurity Evaluation!

Contact us today for a free on-site cybersecurity evaluation for your greater Indianapolis business. We'll assess your current environment, identify exposure to the top cybersecurity threats, and offer a practical, affordable roadmap to protection!

Comprehensive, Affordable, and Scalable Managed IT Solutions for Indiana Businesses

43 Motif Blvd. Suite A
Brownsburg, IN 46112
(317) 376-4874

Contact Us **toucan.tech**