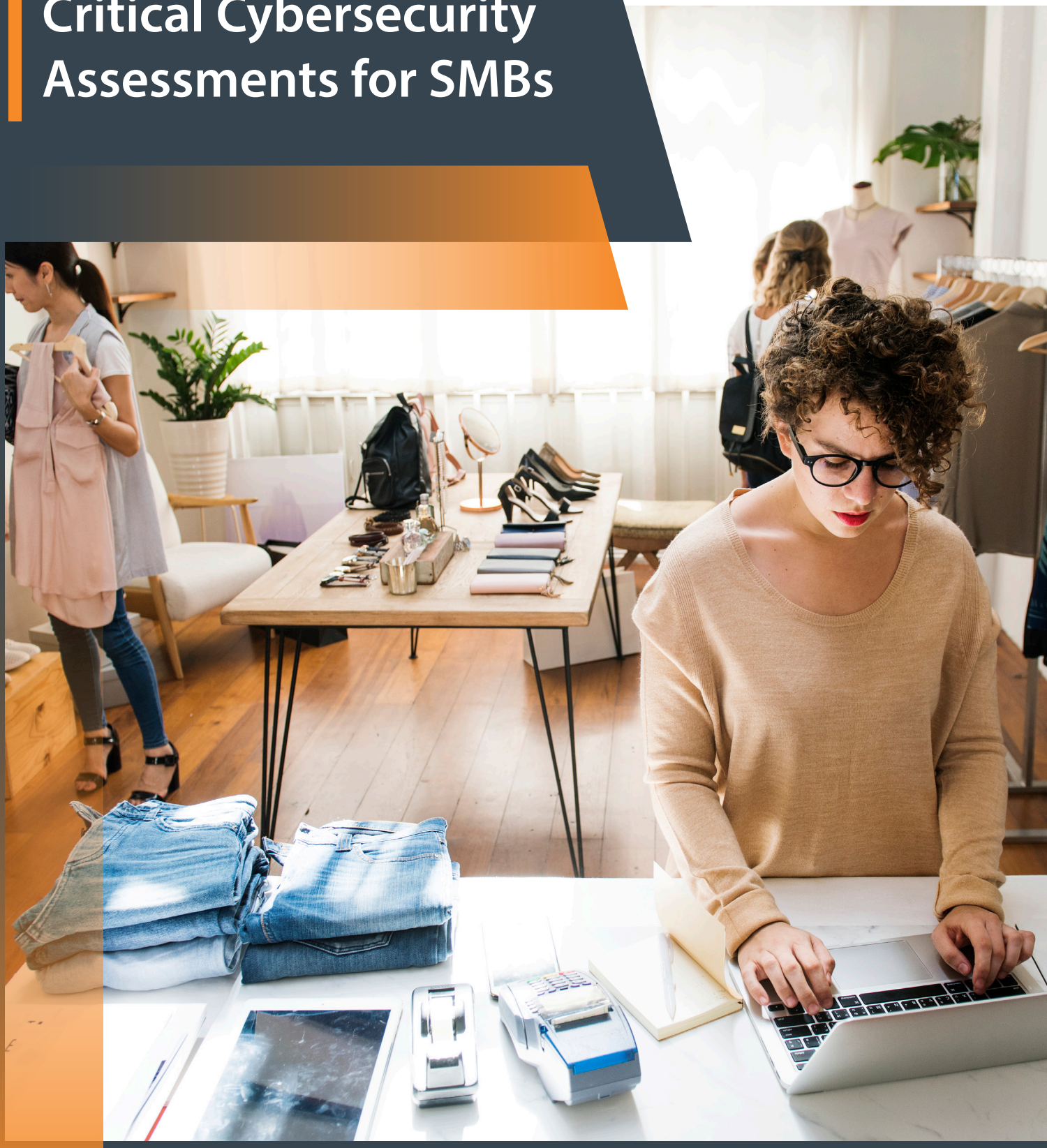
SECURANCE CONSULTING
Advantage of Insight AI

Safeguarding Success: Critical Cybersecurity Assessments for SMBs



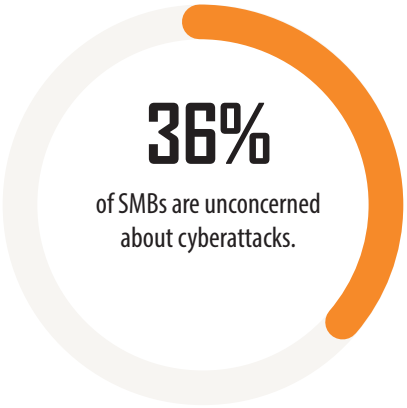
www.securanceconsulting.com

INTRODUCTION

In today's interconnected digital landscape, small and medium-sized businesses (SMBs) play a pivotal role in economic growth and innovation. However, the very characteristics that make these enterprises agile and dynamic also render them vulnerable targets for cybercrime. With minimal resources and limited dedicated cybersecurity personnel, SMBs face unique challenges in safeguarding their operations and sensitive data from malicious actors, making it imperative for them to prioritize and invest in robust cybersecurity measures. Implementing security best practices, conducting regular employee training, and leveraging affordable yet efficient cybersecurity tools can significantly enhance SMBs' resilience to a wide array of cyber threats. This proactive investment in cybersecurity not only protects SMBs against potential financial losses, but also fosters trust among customers, partners, and stakeholders, making it integral to the continued growth and sustainability of SMBs in the face of an ever-changing threat landscape.

2024 SMB Statistics[1]

An average of **$25,000** is lost by SMBs that have experienced a cyberattack.



WHY ARE SMBs A TARGET FOR CYBERCRIME?

Many SMBs assume that they are too small to experience a cyberattack, but this could not be further from the truth. In fact, SMBs face the brunt of many cyberattacks, with small businesses accounting for 46 percent of cyber breaches annually.[2] Below are the most common factors that make SMBs attractive targets for cybercriminals:

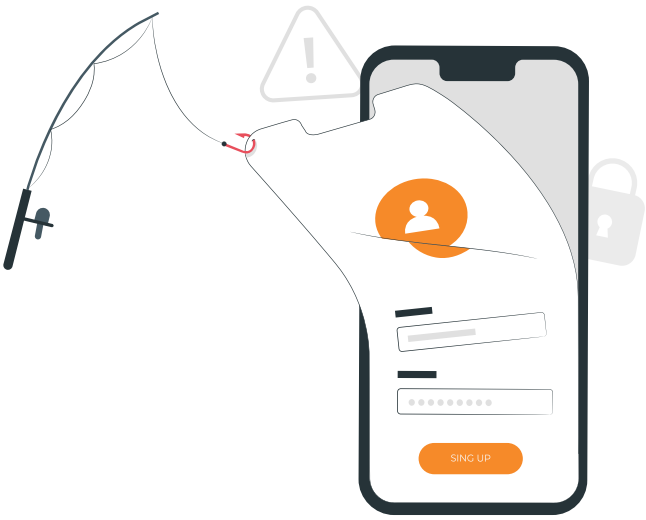
- **Limited resources**— SMBs have fewer financial and human resources dedicated to cybersecurity and lack the advanced cybersecurity infrastructure and protocols that larger enterprises can afford. These vulnerabilities make them easier targets for bad actors seeking to exploit weaknesses in software, networks, or employee awareness.
- **Valuable data**— Despite their size, SMBs possess valuable data, including customer information, financial records, and intellectual property, which cybercriminals can steal, extort, or resell on the dark web.
- **Supply chain weaknesses**— SMBs are often part of larger supply chains, and cybercriminals may target them as entry points to larger, more lucrative targets.

> Enterprise organizations have entire teams devoted to cybersecurity. At many small businesses, those efforts, if undertaken at all, are handled by someone who likely wears many other hats in the day-to-day operation of the business.[3]

- **Lack of security expertise**— Due to tight budgets, many SMBs do not have dedicated cybersecurity personnel or the expertise to implement and maintain robust security measures, making them more susceptible to common cyber threats, such as phishing and ransomware.
- **Inadequate employee training**— Cybercriminals frequently exploit human vulnerabilities through social engineering tactics like email phishing. There are affordable options for successful security awareness training, but many SMBs fail to take advantage of these due to competing priorities or a lack of awareness.
- **Quick financial gains**— Small businesses are more likely to pay ransoms in the event of a ransomware attack, as they may lack the resources to recover their data through other means. Bad actors exploit this vulnerability for quick financial gains. Even if an SMB does not pay the ransom, the hacker simply moves on to their next victim, while the business scrambles for a solution.

COMMON ATTACK METHODS

Cybercrime continues to grow every year, and the threat landscape is constantly changing, making it difficult for SMBs to stay ahead of malicious actors. Awareness of common cyberattack methods is an important first step in defending your organization. Below are some of the most prevalent cyber threats today.

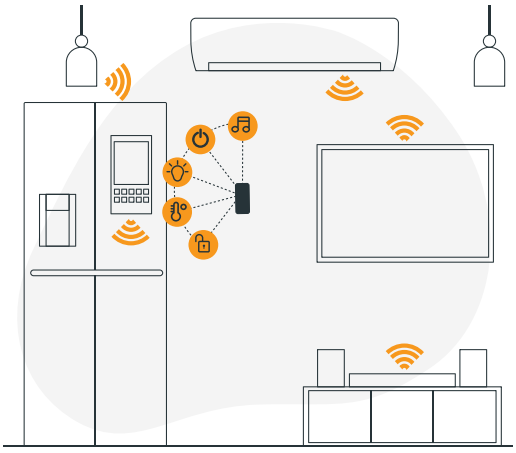


Social Engineering

Social engineering is a technique used by cybercriminals to trick individuals into breaching security practices. Social engineers use fraudulent emails, text messages, phone calls, and websites to convince users that they are trustworthy. Often, they are after critical data and assets, such as login information, financials, personal information, and money. Human error is the number-one culprit in successful social engineering attacks. In fact, employees of small businesses experience 350 percent more social engineering attacks than those at larger enterprises.[4]

Ransomware

Ransomware is a type of malicious software, or malware, that prevents organizations from accessing computer files, systems, or networks and demands that a ransom be paid for their return. There are other forms of malware, such as spyware, Trojan horses, and keyloggers, but ransomware continues to be the most prevalent. SMBs are frequently targeted by ransomware groups because they are more likely to pay the ransom in the event of a successful breach.



Internet of Things (IoT) Leaks

The IoT describes a network of physical devices that can transfer data to one another. Organizations of all sizes are implementing IoT devices across the business to increase interconnectedness and streamline operations, but this growing network of technologies can present doorways to sensitive information, data, and other systems, especially if the devices are not properly configured and secured.

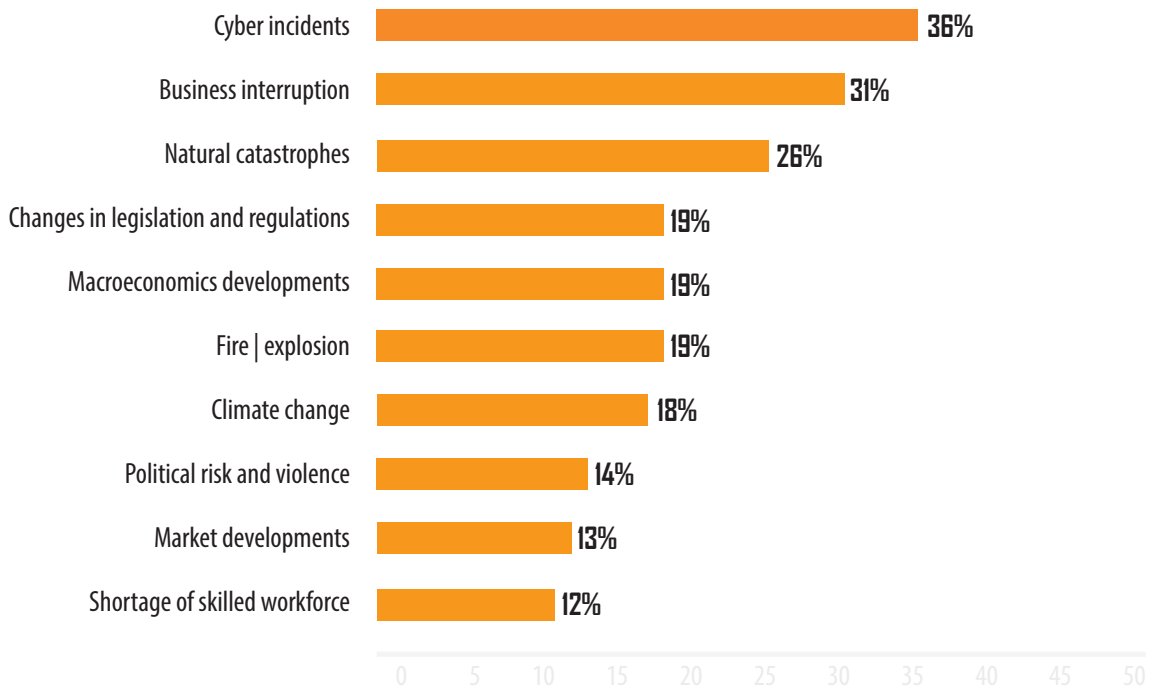
Insider Threats

Insider threats involve negligent or disgruntled employees who sabotage business operations by accessing and leaking sensitive information to the dark web.

Advanced Persistent Threats (APTs)

APTs are a longer form of attack where a hacker penetrates a system and remains on the organization's network for an extended period of time to extort money or data. APTs are covert and stealthy, making them difficult to detect and prevent.[5]

The most important business risks in in 2024[6]



CRITICAL ASSESSMENTS FOR SMBs

Data breaches and cyberattacks are on the rise globally, and no company is immune to them, regardless of size or industry. Unfortunately, for SMBs, the consequences of these attacks can be devastating, to the point of putting the organization out of business. Investing in the right cybersecurity tools and expertise is far less expensive than dealing with the potential fallout from a successful cyberattack. Consider these critical assessments for your business:

Social Engineering Campaigns

Make your employees the first line of defense against cybercrime by fostering a culture of security awareness. This can include frequently reminding staff about security best practices, implementing routine security awareness training, and conducting regular phishing (email), vishing (phone calls), and smishing (SMS messages) simulations. Educating employees about these risks can better equip them to recognize and prevent potential security breaches.

External | Internal Network Vulnerability Assessments and Penetration Tests

Both external and internal vulnerability assessments and penetration tests provide valuable insights into an organization's security posture, helping to prioritize remediation efforts and improve overall cyber resilience. The external assessment focuses on the perimeter of the network that is accessible from the Internet, including external-facing servers, websites, and any other services exposed to the outside world. The internal assessment focuses on the internal network infrastructure and assets, including servers, databases, workstations, and other devices.

Firewall Configuration Review

Firewalls act as a barrier between a trusted internal network and untrusted external networks, monitoring and controlling incoming and outgoing network traffic based on predetermined security rules. A firewall configuration review analyzes the firewall's rule sets, policies, and configurations to ensure they align with the organization's security objectives. Regular firewall configuration reviews will help your organization to identify and rectify potential vulnerabilities or misconfigurations that could be exploited by attackers.

Privileged User Access Review

Privileged users typically include system administrators, network administrators, and other personnel who require elevated access to perform their duties. The goal of this review is to ensure that privileged access is granted based on the principle of least privilege, meaning users have the minimum level of access necessary to perform their job functions. Routine privileged user access reviews are a critical component of access management and overall cybersecurity hygiene. They help organizations reduce the risk of insider threats, unauthorized access, and potential misuse of privileged accounts, contributing to a more secure and controlled IT environment.

Develop, Review, and Test an Incident Response Plan (IRP)

The question is no longer if, but when, a cyberattack or data breach will impact your business. By developing an IRP, your organization will be prepared to minimize the spread of an attack and therefore reduce costs, time, and stress in the event of a successful breach. An effective IRP will be comprehensive and include a clear chain of command, contact information, and detailed procedures for addressing incidents. Even if you already have an IRP in place, annual reviews are necessary to keep the plan relevant and forward-facing. Testing the plan by performing tabletop exercises is even more crucial so that you know if your plan actually works.[7]

> Even when operating with small staffs and budgets—and often, no IT professionals—small-business owners cannot overlook cybersecurity. These businesses need a partner that thinks of cybersecurity holistically, not as a check-the-box solution.[8]

There are a number of approaches your organization can take when it comes to cybersecurity, depending on your budget, security requirements, and compliance obligations. Managing cybersecurity completely in house is one option, but that is a challenge all on its own for SMBs due to limitations in resources, expertise, and scale.

Outsourcing cybersecurity can be a cost-effective option for SMBs. Cybersecurity as a Service (CSaaS), a subscription model in which a third party provides the expertise, resources, and services to meet a company's security needs, is increasingly popular with businesses that need to protect their data, customers, and reputation at an affordable rate. CSaaS packages typically include critical assessments such as those listed above, and may also cover monitoring and incident response. With CSaaS, some companies take an "all in" approach with one vendor, while others choose to outsource some or most of their security tasks, while retaining others internally.

CSaaS subscriptions differ by vendor, but they can typically be customized to fit an organization's needs. Generally, a CSaaS package should cover security at every layer of the technology infrastructure: networks, applications, platforms, data, and cloud services.

Questions to Ask When Evaluating CSaaS Vendors

Cybersecurity requires a sophisticated level of resources and personnel that many SMBs do not have and cannot afford to maintain internally. A CSaaS subscription can be a great option for small businesses that need critical security services at an affordable rate. When vetting a third-party vendor, consider asking the following questions to determine if they fit your organization's needs.[9]

1. Which aspects of cybersecurity are still my responsibility, even with a third-party managing them?
2. How much of my threat attack surface is protected by your services?
3. How much experience | knowledge does your team offer?
4. Can you customize your CSaaS solutions to meet my business needs?
5. What kinds of reports will I receive from you and how often?
6. How do your services integrate with the security tools and platforms I already have in my environment?
7. How do you secure my data at rest and in motion?
8. Which security standards and regulations do you follow?
9. How do you ensure that your services will not disrupt my environment?
10. What core benefits should I expect from this service?

> Time is the new currency in cybersecurity, both for the defenders and the attackers. Early detection and fast response can significantly reduce the impact of a breach. Security teams must focus their efforts on threat detection and response approaches that promote speed and efficiency in the face of cyberattacks.[10]

CONCLUSION

Small Business, Big Impacts

The cybersecurity landscape presents both challenges and opportunities for growth, innovation, and interconnectedness in the small business sector. Though limited resources make them attractive targets, SMBs can establish robust defenses by investing wisely in cost-effective solutions that fit their unique needs. As technology continues to advance, the commitment to cybersecurity not only safeguards sensitive data and operations, but also positions SMBs for success in the digital era.

Securance Consulting has built a reputation helping businesses across a variety of industries manage risk and compliance, enhance cybersecurity, and improve operations. To receive more information about how our CSaaS package can help your organization, **contact us** today.

ABOUT SECURANCE

Securance has more than two decades of experience helping organizations combat evolved cyber threats, build effective risk management programs, align with compliance standards, and increase operational efficiency. Our comprehensive approach integrates proven methodologies, dependable expertise, and each customer's unique requirements to maximize the benefits and long-term value of each assessment.

SOURCES

1. https://www.getastra.com/blog/security-audit/small-business-cyber-attack-statistics/
2. https://www.strongdm.com/blog/small-business-cyber-security-statistics
3. https://www.wired.com/sponsored/story/why-small-businesses-need-to-take-cybersecurity-seriously/
4. https://www.thealternativeboard.com/blog/social-engineering-your-employees-might-be-your-biggest-security-risk#:~:text=According%20to%20recent%20cybersecurity%20statistics,than%20those%20at%20larger%20enterprises
5. https://online.uttyler.edu/degrees/business/mba/cyber-security/cyber-crime-target-small-businesses/
6. https://www.strategic-risk-global.com/catastrophe-risk/top-tips-for-managing-the-biggest-risks-facing-businesses-in-2024/1450928.article
7. https://www.trustntm.com/the-ultimate-cybersecurity-checklist-for-small-businesses/
8. https://www.forbes.com/sites/forbestechcouncil/2023/10/12/small-business-cybersecurity-20-effective-tips-from-tech-experts/?sh=bea0052cd32f
9. https://www.sophos.com/en-us/cybersecurity-explained/what-is-cybersecurity-as-a-service-csaas?x-clickref=1011ly5hWKcQ&affiliate=1101l15926
10. https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs

Safeguarding Success: Critical Cybersecurity Assessments for SMBs

SECURANCE CONSULTING
Advantage of Insight AI

13916 Monroes Business Park, Suite 102, Tampa, FL 33635 • 877.578.0215
www.securanceconsulting.com