CROWDSTRIKE

Security Checklist for Small Businesses

In today's threat-filled business environment, small and medium-sized businesses (SMBs) must move beyond a "good enough" mindset when they think about cybersecurity. Malware, viruses, ransomware, phishing attempts and other eCrime techniques have evolved far beyond the reach of basic antivirus software, and the cybercriminals who use them are actively targeting SMBs.

Businesses must assess their current security posture to determine if they are good enough to protect their business, their mission-critical data, their intellectual property (IP) and their customer information from sophisticated, complex cyberattacks.

To help you evaluate your current security measures, use this simple 10-point checklist, and you'll be on the right path to protecting your business from cybercrime.

☐ **1. Perform an organizational security assessment.**

From mandatory employee badges to protecting the network that moves your data to and from your IT environment, assess every component of your IT environment — your hardware, software and physical security.

- Ask yourself: If an employee loses a laptop, can someone easily log in and access data?
- For remote employees, can other family members easily access games, email and the internet on their work laptop or desktop?
- How difficult is it for a person to walk into your business with no identification and have open access to your files, computers, servers and employees?

☐ **2. Prevent easy access.**

Do you have good password hygiene?

Are your employees required to use complex passwords that they must change every 30, 60 or 90 days? Have you considered implementing multifactor authentication (MFA), which requires a person to provide two or three different verification methods to gain access to company devices? Biometric identification provides superb protection when paired with a badge or password.

Is your business physically secure?

Do you require your employees to wear badges? Does your company use locks on their laptops? Are employees allowed only in areas of your business related to their job? Train your staff on tailgating and other ways bad actors may attempt to physically access your business.

☐ **3. Follow the data.**

Data is one of your most valuable assets. Whether it's in the form of customer lists, financial records, IP or contracts, you must ensure the safety of your data. Start by identifying everywhere data is entered into your systems and every location (virtual and physical) where your data is stored. Then determine if the data is currently protected.

The best way to protect your data is by deploying endpoint security. Modern endpoint security provides real-time threat detection, protection and an automated response if a data breach is detected. Managed detection and response (MDR), endpoint detection and response (EDR) and/or extended detection and response (XDR) technology is a must for protecting your data.

☐ **4. Encrypt your data.**

Data encryption is a fundamental building block of cybersecurity, ensuring that data cannot be read, stolen or altered either at rest or in transit. As more data moves online, data encryption plays an increasingly crucial role in cybersecurity.

☐ **5. Extend protection to the cloud.**

If you have moved your data to the cloud or have a hybrid cloud infrastructure, don't assume your data is safe. Ensure that all hardware, software and infrastructure that protect the cloud environment and its components — such as data, workloads, containers, virtual machines and APIs — are secure.

☐ **6. Secure remote access with a virtual private network (VPN).**

In a post-COVID-19 world, this is especially important. Do you have remote workers? Can you or your employees access your business applications and data from personal devices or on unsecure networks, such as those found in coffee shops and stores? Deploy a secure VPN to protect remote access to your IT infrastructure.

☐ **7. Automate patch updates.**

According to the U.S. Department of Homeland Security, an estimated 85% of all security breaches involve unpatched software. Ensure your IT team understands the risks associated with unpatched software, and ensure they implement patches as soon as they are released if your organization is unable to automate the process across your software.

☐ **8. Protect your endpoints.**

An endpoint is any device that can be connected to a network, including computers, laptops, mobile phones, tablets and servers. Ensure you have deployed endpoint security software such as MDR or EDR to protect your business from malicious activity.

☐ **9. Create a comprehensive incident response plan.**

An incident response plan is a document that outlines the actions an organization should take in the event of a data breach or security incident. Your incident response plan should be created with leaders across your business, reviewed frequently and reevaluated if an event occurs to determine its effectiveness.

☐ **10. Train your staff on cybersecurity best practices.**

Your employees play a large role in the defense of your organization. Train them periodically on password management, how to spot suspicious activity across their devices (texts, chat messages, emails and phone calls) and how to spot phishing attempts. Also review physical security measures that your employees should follow, such as locking their computers, handling hard copies of documents, logging in to work from unsecured networks and more.

Looking for assistance? Extend your team with CrowdStrike cybersecurity experts dedicated to protecting your business 24/7 with CrowdStrike Falcon® Complete MDR. This world-class managed detection and response service delivers an immediate and mature security program without the difficulty, burden and costs of building one internally.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike:

We stop breaches.

Learn more: https://www.crowdstrike.com/

Follow us: Blog | Twitter | LinkedIn | Facebook | Instagram

Start a free trial today: https://www.crowdstrike.com/free-trial-guide/.