5 steps SMBs must take to enhance their security

Being a small to medium sized business (SMB) doesn't mean you can't have enterprise-grade cybersecurity. In this guide, you will learn about five steps your SMB can take to level up its defences. And getting the most advanced cybersecurity isn't just about managing threats – it can give a real boost to your business – as we describe in more detail in the next guide in this series.

How would your SMB cope with a cyber incident? Are you confident that most breaches could be managed - or are there significant gaps in your defenses?

According to a World Economic Forum[1] survey in 2024, small and medium businesses are twice as likely as large enterprises to say they lack cyber resilience. What is more, large firms are pulling ahead with advanced security, while smaller firms are actually becoming less resilient. The study highlighted several challenges for SMBs when it comes to fending off attacks. These included a shortage of skills, challenges around aligning cyber and business strategy, the emergence of new kinds of threat, and the cost of accessing adequate security.

The good news is that all SMBs can elevate their cybersecurity using some of the most advanced technology and processes available – even if they don't have the budget or resources of a multinational corporation.

5 steps to level up your SMB's cybersecurity

If your company uses Microsoft's technology stack, you can rapidly implement the following five steps so your SMB meets the highest security standards.

1. Get a true picture of your security posture

You cannot improve your cybersecurity posture without an understanding of your current position. To do this, you need to conduct a complete audit of security settings around identity, devices, applications, data, and beyond.

And the Microsoft Secure Score makes this easy. Available for free within Microsoft Defender, it scans your network, connected devices, apps and settings to build a picture of your current security posture. The tool gives you a score from 0 to 100, giving you a clear indication of your current position. It also provides specific actions you can implement to improve your security right away. The more of these actions you take, the better your defenses will become.

2. Train, communicate and repeat

Human error remains the primary cause of cyber breaches today. According to a 2023 study[2], 74% of breaches involved some kind of employee action – such as clicking on a link in a phishing email.

The simplest and most effective way of reducing this kind of risk is through regular training and communication with employees. And you don't need a major enterprise's budget to do this. Simple steps include:

- Providing a short cybersecurity training module when onboarding new staff (particularly around strong passwords and spotting phishing emails).
- Integrating at least one cybersecurity training module into all employees' continuing professional development. Research[3] shows that even small amounts of training result in fewer breaches.
- Sharing cybersecurity tips in internal communications - simple, consistent messages about good security practice really pay dividends. One study[4] showed that, after receiving educational internal communications about phishing, employees were less likely to click on links in phishing emails.

3. Go beyond basic access control

Usernames and passwords form the foundations of access control. But in a world where employees are working remotely, using more advanced methods is essential.

One of the simplest things you can do is to set up Microsoft Authenticator. From your organization's Microsoft 365 admin account, you can 'switch on' this form of identity verification. Employees simply download the Microsoft Authenticator app to their smartphones and complete two-factor authentication when logging into your environment.

4. Use AI to monitor for threats

Monitoring for intrusions, detecting them and responding in time can be extremely challenging for SMB IT teams. But with Microsoft Defender, AI continually scans your environments for threats, providing alerts for IT staff to investigate, and helping them prioritize their workloads.

5. Configure permissions

One of the easiest ways to reduce the impact of a cyber-attack is by implementing consistent permissions controls. This means that, even if a malicious actor has entered your environment, they will be limited as to what they can see or download. With Microsoft Defender and Microsoft Purview, you can centralize policy management, enforcing consistent permissions across the business.

1 https://rb.gy/9u5l95 2 https://rb.gy/153mug 3 https://rb.gy/iq2wg3 4 https://rb.gy/dfs616

Level up your security with SoftwareOne Cyber 365

Need help implementing cybersecurity best practices? SoftwareOne's Cyber 365 offering gives you a comprehensive security solution tailored to your SMB's needs. The all-in-one service gives you the best of Microsoft's security products, with continual monitoring, robust protection, access, training and compliance included. That means you can have enterprise-grade security, and boost your defenses.

CONTACT US TODAY

Find out more at
www.softwareone.com

SoftwareOne AG | Headquarters
T. +41 44 832 41 69
E. info@softwareone.com