MSP360

MANAGE. SUPPORT. PROTECT.

WHITEPAPER

Strengthening SMB Cybersecurity with the Essential Eight Framework

1-866-4-MSP360
1-415-301-7773

sales@msp360.com

6425 Living Place Suite 200
Pittsburgh, PA 15206

msp360.com

Small and Medium Businesses (SMBs) are increasingly under siege from cybercriminals. In 2024, 61% of SMBs reported experiencing a cyberattack within the past year[1], with phishing and ransomware ranking among the most pervasive threats. These attacks aren't just frequent; they come with a hefty price tag. The average cost of a data breach for an SMB now exceeds $4 million[2], encompassing downtime, remediation expenses, and reputational fallout. Exacerbating the issue, 47% of SMBs acknowledge lacking adequate resources to effectively manage cybersecurity, leaving them exposed to increasingly advanced attacks[3].

Cybercriminals view SMBs as easy targets due to their limited IT resources and lack of robust cybersecurity measures. The escalating threat landscape underscores the urgency for SMBs to adopt a structured and actionable framework such as *The Essential Eight* to organize and focus the work of bolstering their cyber defenses.

What is the Essential Eight?

The Essential Eight is a cybersecurity framework developed by the Australian Cyber Security Centre (ACSC). Originally designed to protect Australian businesses and government agencies, the framework has universal relevance. It comprises eight carefully selected strategies aimed at mitigating cyber risks and enhancing organizational resilience against attacks.

Despite its origin, the Essential Eight addresses cybersecurity fundamentals that apply globally. And for SMBs, it offers a clear and actionable guide to reducing vulnerabilities and improving security without requiring extensive resources or specialized expertise.

The Essential Eight's pragmatic approach is particularly valuable for SMBs, providing a simple and prioritized roadmap to address cyber threats in a systematic and achievable manner.

Essential Eight's Cyber Risk Mitigation Strategies

The Essential Eight framework is built around eight core strategies that should be implemented by SMBs, each addressing a critical aspect of cybersecurity:

1. Implementing Application Control

Application control restricts the execution of unauthorized programs, ensuring only approved software can run within the environment. This proactive approach significantly reduces the risk of malware infections by preventing unknown or malicious code from executing. By implementing whitelisting tools and policies, SMBs can create a robust first line of defense.

1 Crowdstrike, Cybersecurity Survival Guide for Small and Medium Businesses (2024)
2 IBM, Cost of a Data Breach Report (2024)
3 StationX, Cyberattacks on Small Business Trends (2024)

2. Patching Applications

Keeping applications up-to-date is crucial for closing vulnerabilities that attackers exploit. Patch management involves regularly applying vendor-released updates to eliminate known risks. By automating patch distribution and prioritizing critical updates, SMBs can prevent attackers from leveraging outdated software as an entry point.

3. Configuring Microsoft Office Macro Settings

Macros are often used by cybercriminals to deliver malware through seemingly legitimate documents. Configuring macro settings to disable them by default or allow only digitally signed macros minimizes this threat. SMBs benefit from reduced exposure to phishing attacks and malicious document-based exploits.

4. Hardening User Applications

Hardening user applications involves disabling exploitable features, such as Flash or Java, that are rarely needed but commonly targeted. This approach reduces the attack surface, making it harder for cybercriminals to exploit vulnerabilities in web browsers and other applications. Regular audits of enabled features ensure ongoing compliance.

5. Restricting Administrative Privileges

Limiting administrative access prevents attackers from exploiting privileged accounts to gain deeper control over systems. By enforcing the principle of least privilege and implementing just-in-time access, SMBs can contain potential breaches and reduce the likelihood of widespread damage.

6. Patching Operating Systems

Operating system patches address vulnerabilities that, if left unpatched, can lead to serious compromises. By establishing a structured patching schedule and deploying updates promptly, SMBs can protect against a wide range of threats targeting outdated OS components.

7. Utilizing Multi-Factor Authentication (MFA)

MFA adds a layer of verification by requiring users to present multiple forms of authentication. This greatly reduces the risk of unauthorized access, even if passwords are compromised. SMBs can enhance security by mandating MFA for all users, starting with privileged accounts.

8. Ensuring Regular Backups

Frequent and secure backups are critical for recovering from ransomware attacks or system failures. SMBs should implement automated backup schedules, store copies offsite, and regularly test recovery processes to ensure data integrity and minimize downtime.

Each of these strategies contributes to a holistic defense, addressing common vulnerabilities and providing SMBs with robust protection against evolving threats. But The Essential Eight doesn't just stop with recommending that SMBs put these strategies into practice; they go much further to help you determine the maturity level of your implementation.

Maturing the State of SMB Cybersecurity

The Essential Eight framework introduces three maturity levels to guide organizations in progressively enhancing their cybersecurity capabilities. However, before advancing through these levels, SMBs must assess their current state of each strategy—a process supported by the Essential Eight's specific assessment guidance.

Assessing the Current State

The Essential Eight provides a structured assessment process to help organizations identify gaps and prioritize improvements. For example, an SMB implementing Multi-Factor Authentication (MFA) might evaluate their current maturity as follows:

- **Maturity Level 1:** MFA is enabled for administrative accounts only.
- **Maturity Level 2:** MFA is extended to all privileged accounts.
- **Maturity Level 3:** MFA is required for all users accessing any system.

This progression illustrates how detailed assessments inform maturity growth, ensuring that cybersecurity measures evolve to meet increasing threats. While the example above is simplistic in nature, The Essential Eight framework provides detailed assessment recommendations for each of the eight security strategies.

SMBs can use the assessments across all eight strategies to understand their baseline, identify areas of improvement, and align their goals with desired maturity levels.

Linking Assessment to Implementation

The results of these assessments guide SMBs in prioritizing actions and allocating resources effectively. For each strategy, the maturity levels provide a roadmap for implementation. The table below summarizes the outcomes for each strategy across maturity levels:

Mitigation Strategy	Maturity Level 1	Maturity Level 2	Maturity Level 3
Application Control	Whitelist known applications	Dynamically adjust based on usage	Enforce strict rules and adapt as needed
Patch Applications	Apply patches within 30 days	Apply patches within two weeks	Apply critical patches within 48 hours
Macro Settings	Disable macros by default	Only allow macros from trusted locations	Strict macro controls with monitoring
User App Hardening	Disable unnecessary features	Proactively disable exploitable elements	Regular audits to ensure compliance
Admin Privileges	Limit access to a few users	Regularly review admin rights	Enforce just-in-time access
Patch OS	Monthly patch updates	Patches applied within two weeks	Apply critical patches within 48 hours
MFA	MFA for admin accounts	MFA for all privileged accounts	MFA for all users
Backups	Weekly backups stored offsite	Daily backups with verification	Continuous backups with rapid recovery

Improving SMB Security with The Essential Eight

The Essential Eight framework offers SMBs a practical and effective blueprint for strengthening their cybersecurity defenses. As cyberattacks grow more frequent and sophisticated, the framework's strategies empower SMBs to proactively mitigate risks and safeguard critical data and systems.

By implementing the Essential Eight, even at the initial maturity level, SMBs can make meaningful progress in defending against common threats. Advancing through the framework provides robust protection and positions organizations to withstand even the most sophisticated cyberattacks.

In today's evolving threat landscape, SMBs cannot afford to ignore cybersecurity. The Essential Eight equips businesses with the tools and guidance necessary to secure operations, protect data, and maintain stakeholder trust. Starting the journey now ensures a safer and more resilient future.

About MSP360

Established in 2011 by a group of IT professionals, MSP360™ provides simple and reliable cutting-edge Backup and IT management solutions for MSPs and IT departments worldwide.

MSP360™ platform combines the number one easy-to-use backup solution to deliver best-in-class data protection, secure remote access software to provide support to customers or team members, and painless RMM to handle all aspects of IT infrastructures, all under a single pane of glass.