A PRACTICAL GUIDE FOR SMALL & MEDIUM ENTERPRISES

Cybersecurity Risk Assessment Framework

Developing Actionable Models for SMEs

Security. Simplicity. Sustainability.

The Context: Why SMEs are Prime Targets

Small and Medium Enterprises are often seen as "low-hanging fruit" by attackers. While large corporations have dedicated security budgets, SMEs face unique challenges:

- **Limited Resources:** Lack of dedicated IT staff and restrictive security budgets.
- **Dependence on Digital:** Heavy reliance on cloud services, digital payments, and e-commerce platforms.
- **Focus on Growth:** Security is often perceived as an overhead, not a business enabler.
- **The Result:** Data breaches, regulatory fines, and business-ending financial loss.

Common SME Cyber Risks

Phishing & Social Engineering

Exploiting untrained employees for credential theft.

Weak Access Control

Default passwords, shared accounts, and no MFA.

Ransomware

Encryption of critical data due to unpatched systems.

We propose using the **NIST Cybersecurity Framework (CSF)** due to its simplicity, scalability, and focus on practical steps, making it ideal for resource-constrained SMEs.

Identify

Understand assets, risks, and vulnerabilities.

Protect

Develop and implement safeguards.

Detect

Monitor for anomalies and incidents.

Respond

Take action regarding detected incidents.

Recover

Maintain plans for resilience and restoration.

Practical Application for SMEs:

The **Identify** phase is the most critical for an SME, establishing a risk baseline before investing in protective measures.

- Focus first on **Inventory and Asset Management** (What data do we have?).

Risk Evaluation Metric: Likelihood vs. Impact

Threats are ranked by multiplying the **Likelihood** (how often it might occur) by the **Impact** (potential damage to the business). This prioritizes mitigation efforts toward high-risk areas.

Risk Scenario		Likelihood (1-5)	Impact (1-5)	Risk Score (L x I)	Priority
1. Phishing & Credential Theft (No MFA)	Easy to deploy; staff untrained.	**5 (Very Likely)**	4 (Significant Financial Loss)	**20**	**Critical**
2. Ransomware Infection	Common automated attacks; data is critical.	4 (Likely)	**5 (Business Disrupting/Total Loss)**	**20**	**Critical**
3. DDoS Attack on Website	Requires specific targeting; may block sales.	2 (Unlikely)	3 (Loss of Sales/Reputation)	6	Low

*The highest scores (15-25) are **Critical Risk** and require immediate mitigation efforts.*

Mitigation Strategies: Technical Controls

Identity & Access Management

- **Mandatory Multi-Factor Authentication (MFA):** Essential for all administrative and user accounts.
- **Principle of Least Privilege (PoLP):** Give users only the minimum access needed for their job role.
- **Strong Password Policy:** Enforce length and complexity, ban common passwords.

Network & Endpoint Protection

- **Next-Gen Firewall:** Implement a firewall with Intrusion Prevention System (IPS).
- **Endpoint Detection and Response (EDR):** Replace basic antivirus with an EDR solution on all devices.
- **Automated Patch Management:** Ensure all operating systems and software are automatically updated.

Mitigation Strategies: Human & Operational Controls

Training & Awareness

- **Regular Phishing Simulation:** Monthly, unannounced tests to drill users on identifying threats.
- **Annual Security Training:** Comprehensive training on password hygiene, ransomware, and reporting procedures.
- **Clear Reporting Channel:** Establish a non-punitive "Report Phishing" button in the email client.

Data Backup & Recovery

- **3-2-1 Backup Rule:** Maintain three copies of data, on two different media types, with one copy offsite (cloud).
- **Immutable Backups:** Ensure backups cannot be modified or deleted by a ransomware attack.
- **Test Recovery Plan:** Periodically test the ability to restore critical systems from backup.

Case Study & Documentation: Retail SME

Case Study: Local E-Commerce Shop

Initial State: Shared admin account, no MFA, reliance on free antivirus, 100% cloud hosting (AWS).

Assessment (NIST - Identify):

- ✓ Critical Risk: Phishing (Score 20)
- ✓ High Risk: Cloud Misconfiguration (Score 15)

Validation: The model successfully identified **Phishing** and **Access Control** as the highest priority risks, aligning with the actual vulnerabilities demonstrated in the initial security audit.

Documentation & Best Practices

The final deliverables must include:

- ✓ **Policy Document:** Simplified security policy (e.g., password and MFA mandate).
- ✓ **Asset Register:** A list of all hardware, software, and data locations.
- ✓ **Actionable Roadmap:** A prioritized list of mitigation steps based on the Risk Score (e.g., implement MFA first).
- ✓ **Incident Response Plan:** A basic step-by-step guide for what to do during a breach or ransomware attack.

Summary and Future Vision

The Path to SME Cybersecurity Resilience

Cybersecurity for SMEs is not about becoming unbreachable, but about becoming an **undesirable target** by raising the effort required for an attack.

By implementing the **NIST-based framework**, prioritizing threats using the **Likelihood x Impact** matrix, and focusing on **MFA and employee training**, SMEs can achieve a strong security posture affordably.

Start with the basics: MFA and Training.

Questions?

Thank You