Cybersecurity Risk Assessment Framework for Small Businesses

1. Introduction

Small and medium-sized enterprises (SMEs) face a growing number of cyber threats but often lack the resources, expertise, and infrastructure of large corporations. Approximately 60% of small businesses go out of business within six months of a major cyberattack. This document presents a practical and user-friendly cybersecurity risk assessment model specifically designed for SMEs.

2. Threat Categories

A. Technical Threats:

- Malware and ransomware
- Network breaches and DDoS attacks
- Unpatched software and system vulnerabilities

B. Human/Social Threats:

- Phishing and social engineering
- Insider threats (intentional or accidental)
- Weak passwords and poor credential management

C. Business Continuity Risks:

- Data loss due to hardware failures
- Failed or outdated backups
- Unclear or missing disaster recovery plans

3. SME Risk Scoring Matrix

The model uses a qualitative matrix to evaluate each risk based on Likelihood and Impact. Assign a Likelihood (Low/Medium/High) and an Impact (Low/Medium/High) for each threat. Use the matrix to determine the overall risk level.

4. Assessment Workflow

Step 1: Identify Key Assets

- Inventory digital assets (email, databases, POS, etc.)

Step 2: Map Threats to Assets

- Consider technical, human, and continuity risks

Step 3: Score Likelihood & Impact

- Rate threats qualitatively

Step 4: Use the Risk Matrix

- Classify as Low, Medium, High, or Critical

Step 5: Prioritize & Mitigate

- Address Critical and High risks first

5. Mitigation Strategies

Technical Threats:

- Patch software regularly
- Install antivirus/EDR
- Use firewalls

Human/Social Threats:

- Train staff
- Use MFA
- Monitor user activities

Business Continuity:

- Automate backups

- Test recovery monthly

- Create & test DR plans

6. Use Case Scenarios

Healthcare Clinic:

- Critical Risk from ransomware via phishing

- Mitigation: backups, training, anti-malware

Retail Store:

- High Risk from SQL injection/card theft

- Mitigation: patching, HTTPS, secure payments

Logistics Firm:

- High Risk from credential phishing

- Mitigation: MFA, monitoring, password manager

7. Best Practices for SMEs

- Use MFA on all key accounts

- Enforce strong passwords

- Conduct quarterly staff training

- Automate and test backups

- Use antivirus, firewall, and encryption

- Maintain incident response plan

- Reassess risks twice a year

8. Conclusion

This model provides SMEs with a simple, actionable way to assess and prioritize cybersecurity risks.

It balances technical, human, and operational concerns, offering a roadmap to resilience.

Infographic: Risk Matrix Example