# Cybersecurity Risk Assessment Framework for Small Businesses (SMEs)

## 1. Introduction

Small and Medium Enterprises (SMEs) increasingly rely on digital infrastructure for operations, customer engagement, and financial transactions. However, limited budgets, lack of skilled cybersecurity staff, and low awareness make SMEs prime targets for cyberattacks. According to industry observations, threats such as phishing, ransomware, insider misuse, and insecure networks disproportionately affect SMEs, often leading to financial loss, reputational damage, and regulatory non-compliance.

This project aims to design a **practical cybersecurity risk assessment framework for SMEs**, aligned with the **NIST Cybersecurity Framework (CSF)**, to identify, evaluate, and mitigate cyber risks. The framework is validated through case-based analysis and simulated phishing attack scenarios.

---

## 2. Objectives of the Study

- Identify common cybersecurity risks faced by SMEs
- Develop a structured risk assessment model using NIST CSF
- Create a quantitative risk evaluation metric
- Propose feasible mitigation strategies for SMEs
- Validate the framework using simulated case studies
- Document lessons learned and preventive best practices

---

## 3. Methodology

The methodology followed in this project consists of the following steps:

### 3.1 Risk Identification

A literature review and industry reports were analyzed to identify common SME cybersecurity threats: - Phishing and social engineering attacks - Ransomware and malware infections - Insider threats (intentional or accidental) - Weak authentication and password reuse - Unpatched software and outdated systems - Insecure Wi-Fi and network configurations

### 3.2 Risk Assessment Framework (NIST CSF)

The **NIST Cybersecurity Framework** was used as the base model. It consists of five core functions: 1. **Identify** – Asset management, risk assessment 2. **Protect** – Access control, awareness training 3. **Detect** – Monitoring, anomaly detection 4. **Respond** – Incident response planning 5. **Recover** – Backup and recovery mechanisms

This framework was adapted for SME-scale operations with minimal complexity.

### 3.3 Risk Evaluation Metric

Each risk was evaluated using a **Risk Score formula**:

**Risk Score = Likelihood × Impact**

| Scale | Likelihood | Impact |
|---|---|---|
| 1 | Rare | Negligible |
| 2 | Unlikely | Minor |
| 3 | Possible | Moderate |
| 4 | Likely | Major |
| 5 | Almost Certain | Severe |

Risk Levels: - 1–5: Low Risk - 6–12: Medium Risk - 13–25: High Risk

---

## 4. Case Studies and Validation

### Case Study 1: Small Retail Business

- Threat: Phishing email impersonating bank support
- Vulnerability: No employee security awareness training
- Risk Score: Likelihood (4) × Impact (4) = 16 (High Risk)

### Case Study 2: SME IT Services Firm

- Threat: Ransomware via email attachment
- Vulnerability: No endpoint protection, outdated OS
- Risk Score: Likelihood (3) × Impact (5) = 15 (High Risk)

### Case Study 3: Local Manufacturing Unit

- Threat: Insider data leakage
- Vulnerability: No access control policies
- Risk Score: Likelihood (3) × Impact (4) = 12 (Medium Risk)

These cases validate that the framework effectively identifies and prioritizes SME cyber risks.

---

## 5. Simulated Phishing Attack Experiment

### 5.1 Experiment Setup

- Created a **fake login page** resembling a common email service
- Designed a **phishing email** with urgent language
- Sent the email to test users in a controlled environment

### 5.2 Observations

- Users clicked the phishing link due to urgency cues
- Credentials were entered on fake login page
- No user verified the sender authenticity

## 6. Results

| Parameter | Observation |
|---|---|
| Email Open Rate | High |
| Link Click Rate | Moderate to High |
| Credential Submission | Significant |
| Awareness Level | Low |

The results show that phishing remains one of the most effective attack vectors against SMEs.

## 7. Lessons Learned

- Human factors are the weakest link in SME security
- Lack of training increases phishing success
- Simple controls (MFA, email filtering) drastically reduce risk
- SMEs need affordable and easy-to-deploy security solutions

## 8. Mitigation and Preventive Measures

### Technical Controls

- Firewall and IDS/IPS deployment
- Multi-Factor Authentication (MFA)
- Endpoint protection and antivirus
- Regular patch management
- Secure email gateways

### Administrative Controls

- Employee cybersecurity awareness training
- Strong password and access control policies
- Incident response plan
- Regular risk assessments

### Physical Controls

- Restricted access to critical systems
- Secure server rooms and devices

## 9. Best Practices for SMEs

- Follow NIST CSF baseline controls
- Conduct periodic phishing simulations
- Maintain offline and cloud backups
- Enforce least-privilege access
- Monitor logs and alerts regularly

## 10. Conclusion

This project demonstrates that a structured cybersecurity risk assessment framework, tailored for SMEs, can significantly improve their security posture. By combining NIST CSF principles with a simple risk scoring model, SMEs can prioritize threats and implement cost-effective mitigation strategies. Continuous awareness training and proactive risk management are critical for long-term cybersecurity resilience.

## 11. Screenshots (To Be Attached)

- Fake login page screenshot
- Phishing email screenshot
- Click statistics dashboard

## 12. References

- NIST Cybersecurity Framework
- OWASP Top 10
- ENISA SME Cybersecurity Reports