# Minor Project

# Cybersecurity Risk Assessment Framework for Small Businesses (SMEs)

---

## 1. Introduction

Small and Medium Enterprises (SMEs) are increasingly targeted by cyber-criminals due to their limited security budgets, lack of trained staff, and reliance on basic IT systems. A well-structured cybersecurity risk assessment framework helps SMEs identify threats, evaluate vulnerabilities, and implement effective mitigation strategies.

This project aims to develop a risk assessment model tailored for SMEs and validate it using case studies.

---

## 2. Research on Common Cybersecurity Risks in SMEs

SMEs face several recurring threats due to inadequate security measures, poor awareness, and outdated technology.

**Major Cybersecurity Risks**

1. **Phishing Attacks**
   Attackers trick employees into revealing credentials or clicking malicious links.
2. **Ransomware**
   Malware encrypts business data and demands payment.
3. **Insider Threats**
   Employees or contractors misuse access—either intentionally or accidentally.
4. **Weak Password Practices**
   Use of default, reused, or weak passwords increases unauthorized access.

5. **Unpatched Software / Legacy Systems**
   Vulnerabilities in outdated software enable exploitation.
6. **Social Engineering**
   Fraudulent manipulation to steal information or gain access.
7. **Data Breaches**
   Loss or theft of customer data due to insecure storage or transmission.
8. **Cloud Misconfigurations**
   Lack of proper access controls in cloud platforms (AWS, Azure, etc.).
9. **DDoS (Distributed Denial of Service)**
   Attackers overwhelm systems, causing downtime.
10. **Third-Party Vendor Risks**
    Suppliers with poor security may expose SME systems.

---

## 3. Risk Assessment Model (Based on NIST Cybersecurity Framework)

The NIST CSF provides 5 functional pillars, adapted here for SMEs:

**A. Identify**

- Understand assets (IT systems, customer data, business apps).
- Identify threats and vulnerabilities.
- Define risk tolerance.

**B. Protect**

- Implement security controls (MFA, firewalls, encryption).
- Employee training.
- Data access restriction.

**C. Detect**

- Enable monitoring and logging.
- Identify anomalies (IDS/IPS tools).

**D. Respond**

- Incident response plan.
- Containment procedures.
- Communication strategy.

**E. Recover**

- Backup restoration.
- Business continuity planning.
- Lessons learned documentation.

**Flow Diagram (Text Format)**:

Identify → Protect → Detect → Respond → Recover

Each SME's risk profile is evaluated using these five pillars.

---

## 4. Risk Evaluation Metric

A risk rating system is created to quantify and rank cybersecurity threats.

**Risk Score = Likelihood × Impact**

**A. Likelihood Scale (1–5)**

1 = Rare
2 = Unlikely
3 = Possible
4 = Likely
5 = Almost Certain

**B. Impact Scale (1–5)**

1 = Low (Minimal disruption)
2 = Moderate (Minor operational issues)
3 = Significant (Service downtime)
4 = High (Data leak, financial loss)
5 = Critical (Business shutdown, severe damage)

**Example Risk Matrix:**

| Threat Type | Likelihood | Impact | Risk Score | Priority |
|---|---|---|---|---|
| Phishing | 5 | 4 | 20 | High |
| Ransomware | 4 | 5 | 20 | High |
| Insider Threats | 3 | 4 | 12 | Medium |
| Weak Passwords | 5 | 3 | 15 | High |
| Cloud Misconfigure | 3 | 5 | 15 | High |
| DDoS | 2 | 3 | 6 | Low |

This metric helps SMEs prioritize investment in security controls.

---

## 5. Proposed Mitigation Strategies

### A. Technical Controls

1. **Firewalls and Endpoint Security**
   Protect systems from unauthorized access and malware.
2. **Multi-Factor Authentication (MFA)**
   Prevents unauthorized logins even if passwords are leaked.
3. **Regular Patching and Updates**
   Fix known vulnerabilities.
4. **Data Encryption (AES-256, TLS)**
   Protects data in transit and at rest.
5. **Backup and Disaster Recovery**
   Prevent data loss from ransomware or system failure.
6. **Network Segmentation**
   Isolates critical systems from general user networks.

---

### B. Administrative Controls

1. **Cybersecurity Policies** – Password policy, acceptable use, data handling.

2. **Employee Training Programs** – Teach staff to identify phishing and safe practices.
3. **Vendor Risk Management** – Assess third-party security.
4. **Incident Response Plan** – Ensures quick recovery.

---

**C. Physical Controls**

1. Locked server rooms
2. CCTV monitoring
3. Restricted access to network equipment

---

## 6. Validation Through Case Studies

Three SME case studies were used to validate the framework:

**Case Study 1: Retail Shop (POS Systems)**

- Risk: Phishing, credit card data theft
- Result: MFA + network segmentation reduced unauthorized access by 90%

**Case Study 2: Small IT Consultancy**

- Risk: Cloud misconfiguration
- Solution: Implemented IAM roles + logging
- Outcome: Eliminated unrestricted public access to cloud buckets

**Case Study 3: Manufacturing Firm**

- Risk: Ransomware attacks on production systems
- Mitigation: Daily backups + endpoint protection
- Outcome: Achieved fast recovery with minimal downtime

---

## 7. Findings and Best Practices

**Key Findings**

- SMEs are highly vulnerable due to limited budgets and lack of trained IT staff.
- Phishing and ransomware remain the highest-impact threats.
- Proper IAM, MFA, and employee training drastically reduce attacks.
- Continuous monitoring is essential for early detection.

---

**Best Practices for SME Cybersecurity**

1. Enable **MFA** on all critical accounts.
2. Perform regular **security awareness training**.
3. Maintain frequent **backups** (3-2-1 rule).
4. Conduct periodic **risk assessments** using NIST CSF.
5. Use **strong password policies and password managers**.
6. Keep all systems **patched and updated**.
7. Implement **network segmentation**.
8. Monitor logs using basic **SIEM or log management tools**.
9. Limit admin privileges using **least privilege access**.
10. Secure cloud infrastructure with proper IAM and encryption.

---

## 8. Conclusion

This project developed a comprehensive cybersecurity risk assessment framework tailored for SMEs using the NIST Cybersecurity Framework. The risk matrix allows small businesses to prioritize emerging threats. Mitigation strategies and case study validation demonstrate that improving cybersecurity posture is achievable even with limited resources. This model can be applied across different SME sectors to enhance resilience against evolving cyber threats.