MINOR PROJECT -1

Cybersecurity Risk Assessment Framework

A Comprehensive Model for Evaluating and Mitigating Risks in Small & Medium Enterprises (SMEs)

1. Common Cyber Risks in SMEs

Phishing Attacks

Deceptive emails aimed at stealing sensitive credentials. SMEs often lack advanced email filtering, making them prime targets.

Ransomware

Malicious software that encrypts data until a ransom is paid. Critical for SMEs without robust off-site backups.

Insider Threats

Risks originating from employees, whether malicious or due to negligence (e.g., weak passwords, accidental data sharing).

Unsecured Networks

Use of default router settings or public Wi-Fi for business operations, leading to potential data interception (Man-in-the-Middle).

2. Risk Assessment Model

NIST Cybersecurity Framework

- 1. IDENTIFY Assets
- 2. PROTECT Systems
- 3. DETECT Threats
- 4. RESPOND to Incidents
- 5. RECOVER Operations

Risk Evaluation Matrix

Impact / Likelihood	Low	Medium	High
Low	Acceptable	Monitor	Moderate
Medium	Monitor	Moderate	Critical
High	Moderate	Critical	Extreme

Risk Score = Probability of Occurrence × Potential Impact

3. Proposed Mitigation Strategies

Access Control (IAM)

Implement Multi-Factor Authentication (MFA) for all remote access and admin accounts. Apply the Principle of Least Privilege (PoLP).

Network Defense

Deploy Next-Generation Firewalls (NGFW) to filter traffic. Segment networks (e.g., Guest Wi-Fi vs. Corporate LAN) to limit lateral movement.

Human Firewall

Conduct regular security awareness training. Run simulated phishing campaigns to educate employees on recognizing social engineering.

Data Resilience

Follow the 3-2-1 backup rule: 3 copies of data, 2 different media types, 1 offsite copy. Test restoration procedures quarterly.

4. Model Validation: Case Studies

Case A: Retail SME (Before)

- **No Firewall:** Direct connection to ISP modem.
- **Shared Passwords:** Employees shared "admin123" for POS.
- **Data Loss:** No automated backups; risk of total loss.
- **Outcome:** High susceptibility to Ransomware and data theft. Risk Score: **Extreme**.

Case B: Tech Firm (After Implementation)

- **Perimeter Security:** Configured VPN with MFA for remote workers.
- **Endpoint Protection:** Installed EDR on all workstations.
- **Policies:** Enforced password rotation and role-based access.
- **Outcome:** Threats contained. Evaluation shows 90% risk reduction. Risk Score: **Low/Acceptable**.

5. Conclusion & Best Practices

Project Findings

SMEs are vulnerable primarily due to lack of budget and expertise, not lack of technology. A structured framework (NIST) combined with practical tools (MFA, Backups) effectively lowers the risk barrier.

Regular Audits

Conduct vulnerability scans annually.

Patch Management

Automate OS and software updates.

Security Culture

Make security everyone's responsibility.