Project Title :

Cybersecurity Risk Assessment Framework for Small Retail & Service Businesses (1–25 Employees)

Name : Sanjibani Paul

Institute : Chandigarh University

Semester : 3rd

Naviotech Solution Pvt. Ltd

Problem statement :

Small and Medium-sized Enterprises (SMEs) hold a significant share of the global business ecosystem, yet they are increasingly targeted by cybercriminals due to limited security maturity, insufficient financial and technical resources, and lack of skilled cybersecurity personnel. Although standard cybersecurity frameworks such as NIST CSF and ISO 27001/2 exist, they are overly complex, expensive, and resource-intensive for SMEs to understand, adopt, and implement effectively. As a result, SMEs often ignore large parts of these frameworks, adopt only minimal controls, or rely on a "fail-safe" approach instead of building resilience. These challenges create a high-risk environment in which SMEs face greater vulnerabilities to malware, phishing, and web-based cyberattacks, leading to financial losses, operational disruption, and reputational damage.

This research identifies the gap between existing frameworks and SME needs and highlights the urgent requirement for a simplified, scalable, and SME-tailored cybersecurity risk assessment framework that is practical, resource-efficient, and easy to implement.

Objective :

The primary objective of this research is to design and develop an SME-focused cybersecurity risk assessment framework and tool that addresses the limitations of existing frameworks and caters to the needs, constraints, and security maturity of SMEs.

The study aims to:

1. Identify and categorize the common cyber threats and vulnerabilities affecting SMEs, with emphasis on the most prevalent attack vectors: malware, phishing, and web-based attacks.
2. Analyze and compare existing well-known cybersecurity frameworks (NIST CSF and ISO 27001/2) to determine which elements are beneficial and which are unsuitable for SMEs due to complexity or resource requirements.
3. Develop a novel, simplified, and scalable cybersecurity framework tailored to SMEs, integrating promising concepts such as Threat-Based Risk Assessment, Least Cybersecurity Controls Implementation (LCCI), and Self-Determination Theory (SDT).
4. Create an interactive digital tool enabling SMEs to conduct cybersecurity self-assessment and receive customized, actionable recommendations.
5. Lay the foundation for future quantitative validation to measure framework effectiveness in real SME environments.

Target Audience :

Target Group	**Why the Paper is Relevant to Them**
SME Owners, Founders & Managers	Provides a clear, understandable framework and tool to assess and improve cybersecurity without requiring deep technical knowledge.
Cybersecurity Consultants & Practitioners	Offers a ready-made SME-oriented model that can be adopted or integrated into consulting services and awareness programs.
Policy Makers, Government Bodies & Regulators	Helps shape SME cybersecurity regulations, grants, incentives, and national strategies to build cyber resilience in the SME sector.
Academics & Researchers in Cybersecurity and Risk Management	Provides a foundation for further empirical research, framework validation, and development of educational modules.
SME IT Support Providers & Managed Service Providers (MSPs)	Equips them with a tailored framework that they can implement cost-effectively across multiple SME clients.

In Scope

The study includes:

- Development of a **cybersecurity risk assessment framework** tailored exclusively to SMEs.
- Analysis of **common cyber threats against SMEs**, especially:
    - Malware
    - Phishing
    - Web-based attacks
- Integration of **promising modern approaches** such as:
    - Threat-Based Risk Assessment
    - Least Cybersecurity Controls Implementation (LCCI)
    - Self-Determination Theory (SDT) for employee motivation

- Development of a **practical assessment tool** offering dynamic and interactive risk evaluation and recommendations.
- Guidance that is **scalable** based on SME resource constraints (e.g., tiered levels of cyber maturity).

Out of Scope :

The study excludes:

- Development of a full technical cybersecurity system or technological architecture beyond the assessment tool.
- Enterprise-level cybersecurity strategies and frameworks designed for large organizations.
- Detailed technical implementation of advanced cybersecurity controls such as:
    - AI-driven threat detection
    - SOC (Security Operations Centre) integration
    - Full incident response architecture
- Sector-specific cybersecurity regulations outside general SME application.
- Financial auditing of cybersecurity investments or return on security investment (ROSI).
- Comprehensive testing, field trials, or large-scale empirical deployment (acknowledged as future work).

Key Assumptions :

Assumption	**Explanation**
SMEs have limited cybersecurity expertise and financial resources	SMEs cannot implement expensive or highly technical frameworks; therefore, solutions must be simple, low-cost, and resource-friendly.
Management involvement is essential for cybersecurity success	SME leadership must recognize cybersecurity as a priority in order for implementation to succeed.
A simplified, tier-based approach is effective for SMEs	SMEs benefit from step-by-step, maturity-level-based controls that they can scale over time.

Assumption	Explanation
Employees are key contributors to cyber risk	Human error is a major vulnerability; motivational strategies like SDT can enhance awareness and proactive behavior.
Existing frameworks contain valuable elements	Although complex, NIST and ISO models offer proven concepts that can be adapted rather than reinvented.
Cyber threats will continue to increase for SMEs	The framework assumes a rising frequency of attacks, thus necessitating proactive, ongoing risk management.
A tool-based approach improves usability and adoption	SMEs are more likely to engage when an interactive tool simplifies the self-assessment and provides tailored guidance.