Project :

MINOR PROJECT 1

Cybersecurity Risk Assessment Framework for Small Retail Businesses

Name: Sanjibani Paul

Course & Semester: B.Tech CSE , 3rd Semester

University Name: Chandigarh University

Submission Month & Year: November, 2025

INDEX

1. ABSTRACT

This project focuses on developing a simple and effective Cybersecurity Risk Assessment Framework tailored for small retail and service businesses with 1–25 employees. Small businesses often lack the knowledge, budget, and resources to protect themselves from cyber threats. As a result, they are highly vulnerable to cyberattacks such as phishing, data breaches, Wi-Fi intrusion, and ransomware.

The objective of this project is to create a practical risk assessment model that small business owners can easily adopt without technical expertise. The framework includes five key stages: data gathering, threat identification, risk scoring, treatment planning, and implementation. The project also includes checklists, scoring techniques, a risk register, and a risk treatment plan to help small businesses evaluate and improve their cybersecurity posture.

To demonstrate the effectiveness of the framework, a simulated assessment was conducted for a sample small café business. The assessment identified critical risks such as shared staff accounts, lack of MFA, unsecure Wi-Fi, outdated POS software, and weak backup practices. Corrective actions were proposed to reduce cyber risks within 30 days.

This framework contributes as a beginner-friendly cybersecurity model for small businesses and can be further enhanced for real-world use.

2. INTRODUCTION

In today's digital age, cybersecurity has become essential for all types of businesses, including small retail and service businesses. Even though small businesses may not store large amounts of data like big companies, they are still major targets for cybercriminals because they usually have weaker security controls, limited budgets, and low awareness about cyber threats. Small retail and service businesses such as cafés, salons, bakeries, stationery shops, and small service centres rely on basic IT systems like Wi-Fi, Point of Sale (POS) systems, mobile phones, and laptops for daily operations. However, they often ignore cybersecurity practices such as strong passwords, secure Wi-Fi networks, data backups, and regular software updates. This makes them vulnerable to cyberattacks such as phishing, malware, identity theft, online payment fraud, and data loss.

To solve this problem, this project presents a simple and beginner-friendly Cybersecurity Risk Assessment Framework designed specially for small retail and service businesses with 1–25 employees. The framework helps business owners identify risks, understand threats, and apply basic cybersecurity measures to protect their business.

This project provides a step-by-step approach that includes data collection, threat assessment, risk scoring, risk register creation, treatment planning, and implementation with simple checklists and easy methods. A simulated case study was also conducted to demonstrate the use of the framework on a small business.

3. BUSINESS PROFILE AND SCOPE

2.1 Business Profile

For this project, a simulated case study was conducted for a small café business to demonstrate the use of the Cybersecurity Risk Assessment Framework. The selected business details are as follows:

- **Business Name:** Sweet Bean Café
- **Location:** Chandigarh – Sector 34
- **Type of Business:** Retail Food & Beverage Service
- **Number of Employees:** 6
- **Operational Systems Used:** 1 POS system, 1 laptop, 3 staff mobile phones, 2 CCTV cameras, and a Wi-Fi network
- **IT Support:** No full-time IT staff; occasional support from a local technician

The café depends on digital systems for daily operations such as billing, online orders, payments, and customer communication. Due to limited knowledge of cybersecurity, the business has several weaknesses that can lead to security risks. Therefore, a cybersecurity assessment was carried out using the proposed framework.

2.2 Scope of the Assessment

The scope of the cybersecurity assessment includes the evaluation of key digital assets and security practices used in the business. The assessment covers:

- Wi-Fi Network Security
- Device and System Security (POS, Laptop, Mobile Devices)
- User Access and Password Management
- Data Backup and Recovery Practices
- Awareness of Cyber Threats and Staff Training

The assessment does not include large-scale enterprise systems or advanced cybersecurity tools. The focus is only on basic security controls suitable for small businesses with limited technical expertise and budget.

2.3 Objectives of the Project

The main objectives of this project are:

- To develop a simple Cybersecurity Risk Assessment Framework for small retail and service businesses
- To identify and evaluate common cyber risks faced by small businesses
- To provide practical and low-cost solutions to reduce cyber risks
- To demonstrate the framework through a simulated real-world case study

4.THREAT SUMMARY

Small retail and service businesses face multiple cyber threats due to limited security awareness, lack of IT staff, and the use of common digital tools such as Wi-Fi, mobile phones, and POS systems. The table below summarises the most common cyber threats relevant to such businesses.

4.1 Common Cyber Threats for Small Businesses

Category	Threat	Description
Network Security	Wi-Fi Hacking	Attackers break into weak or unsecured Wi-Fi networks to access business systems.
Device Security	Malware & Ransomware	Malicious software that locks or damages systems and demands payment to restore access.
User Accounts	Phishing & Credential Theft	Fake emails or messages used to steal passwords or banking details.
Data Security	Data Loss	Loss of important business data due to system failure, accidental deletion, or cyberattack.
Access Control	Unauthorized Access	Shared or weak passwords can lead to misuse of systems or data theft by internal or external users.
Payment & POS	POS System Attack	Outdated POS systems can be exploited to steal payment or customer information.
Human Factor	Social Engineering	Staff are tricked into sharing passwords, clicking unsafe

Category	Threat	Description
		links, or installing harmful software.

4.2 Potential Impact on Small Businesses

Cyberattacks can have direct and long-term effects on small businesses. The major impacts include:

- Loss of customer data or payment information
- Financial losses due to fraud or ransomware
- Business downtime leading to revenue loss
- Damage to business reputation and customer trust
- Legal or compliance issues related to data privacy

4.3 Need for a Risk Assessment Framework

Due to limited security knowledge and low budget, small businesses often do not implement cybersecurity measures. A simple and structured framework is required to:

- Identify possible cyber threats
- Evaluate the level of risk
- Take corrective action to prevent attacks

The proposed framework in this project provides a beginner-friendly approach to help small businesses improve cybersecurity with minimal cost and effort.

5. FRAMEWORK DESIGN

The proposed Cybersecurity Risk Assessment Framework is designed to help small retail and service businesses evaluate their cybersecurity posture in a simple and structured manner. The framework consists of **five key stages**, starting from information gathering to implementation of security measures.

5.1 Framework Overview

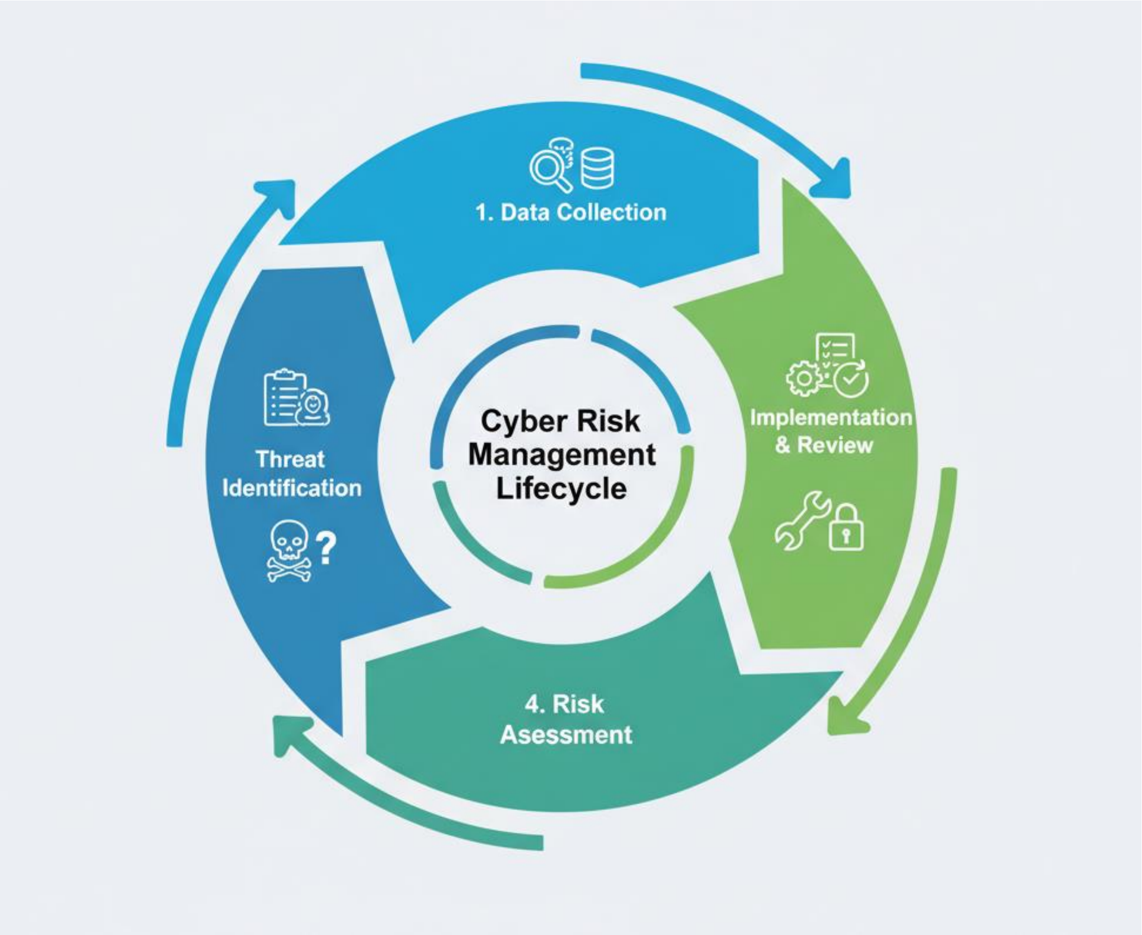
The framework follows a step-by-step approach:

1. **Data Collection** – Gather information about business assets, devices, user access, and existing security practices.
2. **Threat Identification** – Identify the possible cyber threats and vulnerabilities related to the business.

3. **Risk Assessment & Scoring** – Analyse the likelihood and impact of each risk using a simple scoring method.
4. **Risk Treatment Planning** – Define actions to reduce or eliminate the identified risks.
5. **Implementation & Review** – Apply the corrective actions and review improvements.

This framework is easy to use and does not require technical expertise, making it suitable for small business owners.

5.2 Framework Diagram



5.3 Tools and Documents Used in the Framework

The following tools and documents were used while applying the framework:

Stage	**Document/Tool Used**
Data Collection	Interview Checklist, Consent Form
Threat Identification	Threat Summary Table
Risk Scoring	Likelihood & Impact Scoring Sheet
Risk Assessment	Risk Register (Excel Sheet)
Risk Treatment	Risk Treatment Plan
Implementation	Evidence Screenshots & Follow-up Review

5.4 Benefits of the Framework

- Simple and beginner-friendly
- Cost-effective and suitable for small shops/businesses
- Helps identify risks early
- Provides step-by-step actions to improve security
- Can be adapted for any small business sector

6. RISK ASSESSMENT METHOD

The risk assessment process helps in identifying, analysing, and prioritising cyber risks that may affect the business. A simple scoring system was used to assess the likelihood and impact of each risk, making it easy for small business owners to understand.

6.1 Data Collection Approach

The first step was to gather information about the business, devices, network, and current security practices. This was done using:

- **Interview Checklist** to collect details about IT usage, access control, backup practices, and awareness levels
- **Consent Form** to seek permission for assessment
- **Technical Checklist** to inspect Wi-Fi security, POS, devices, and backup settings

This step helped in understanding the existing security posture of the business.

6.2 Risk Scoring Method

A simple **Likelihood–Impact scoring model** was used to evaluate each risk. Both Likelihood and Impact were rated on a scale of **1 to 4**, as shown below:

Score	**Likelihood Level**	**Description**
1	Rare	Very unlikely to occur
2	Possible	Could occur occasionally
3	Likely	Expected to occur
4	Very Likely	High chance of occurrence

Score	**Impact Level**	**Description**
1	Low	Minimal effect on operations
2	Medium	Noticeable impact but manageable
3	High	Significant disruption or financial loss
4	Critical	Major damage, financial or reputational loss

6.3 Calculation of Risk Scores

The following formulas were used to calculate risk scores:

- **Raw Risk = Likelihood × Impact**
- **Residual Risk = Raw Risk × (1 − Controls Effectiveness)**

Where **Controls Effectiveness** is measured on a scale of 0 to 1 (example: 0.10 = 10% effective).

This helped in prioritising the risks based on the level of threat to the business.

6.4 Risk Register

A Risk Register was prepared to record all identified risks along with their likelihood, impact, existing controls, recommended actions, and priority level. The risk register helps in tracking risk treatment progress.

The risk register includes:

- Risk ID
- Asset

- Threat
- Vulnerability
- Likelihood & Impact score
- Raw and Residual Risk
- Priority Level
- Recommended Action

7. RISK REGISTER FINDINGS

Based on the assessment of the Sweet Bean Café, a total of ten (10) cybersecurity risks were identified. Each risk was analysed using the Likelihood–Impact model, and a risk score was calculated to determine the priority level. The table below summarizes the key risks identified during the assessment.

7.1 Summary of Key Risks Identified

Risk ID	Risk Description	Priority Level
1	Shared staff user accounts	High
2	Single Wi-Fi network for guests and staff	Critical
3	No Multi-Factor Authentication (MFA)	Critical
4	Outdated POS software	High
5	Backups not tested for recovery	High
6	Weak Wi-Fi password	Medium
7	No cybersecurity awareness training for staff	High
8	Free/low-level antivirus only	Medium
9	Backup stored only on café premises	Low
10	CCTV access not secured	Medium

7.2 Analysis of Results

From the risk register, it is clear that the business has several areas of high and critical risk that require immediate attention.

- **Critical Risks** such as lack of Wi-Fi separation and no MFA can lead to major data breaches and financial loss if exploited.
- **High Risks** like outdated POS software and weak backup methods can severely affect the business if a cyber incident occurs.
- **Medium and Low Risks** are less urgent but should be addressed as part of continuous improvement.

7.3 Risk Prioritization

The risks were prioritised based on **residual risk score**, after considering the effectiveness of existing controls. A summary of the prioritization approach:

- **Critical Risks** must be fixed within 7 days
- **High Risks** should be addressed within 15 days
- **Medium Risks** should be resolved within 25 days
- **Low Risks** can be treated within 30 days

This prioritization helps the business plan risk mitigation efforts effectively.

8. RISK TREATMENT PLAN AND IMPLEMENTATION

A Risk Treatment Plan was created to reduce or eliminate the identified cybersecurity risks. The plan includes recommended actions, responsible persons, and target dates for completion. This ensures that risks are addressed in a structured manner.

8.1 Risk Treatment Plan

The table below summarises the treatment actions planned for each risk:

Risk ID	Risk Description	Action to be Taken
1	Shared staff user accounts	Create separate user accounts for all staff
2	Single Wi-Fi for guests and staff	Create separate Guest and Staff Wi-Fi networks
3	No MFA enabled	Enable MFA on email, banking, and POS accounts

Risk ID	Risk Description	Action to be Taken
4	Outdated POS software	Update POS software and enable auto-updates
5	Backups not tested	Schedule regular backups & test restoration monthly
6	Weak Wi-Fi password	Set a strong password and change every 3 months
7	No staff cybersecurity training	Conduct basic cybersecurity awareness training
8	Free antivirus only	Upgrade to better antivirus or security plan
9	Backup stored on-site only	Store backup on cloud or off-site location
10	CCTV not secured	Change default ports & enable secure access

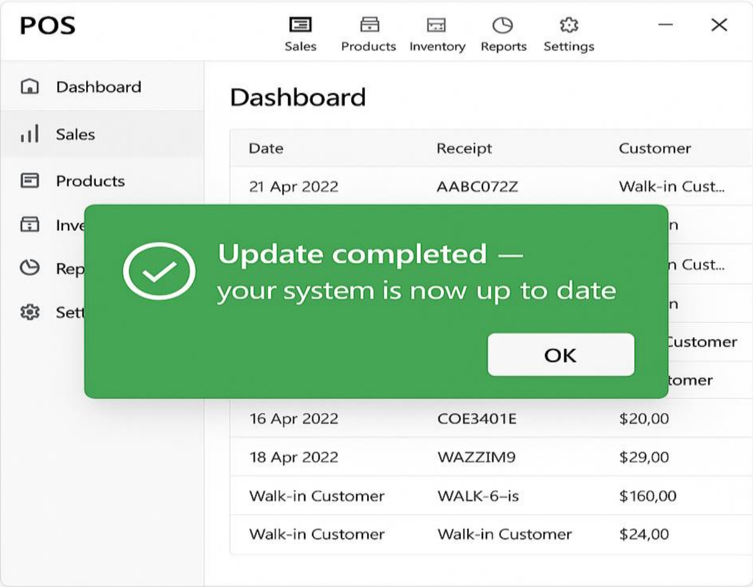
Each action was assigned a target timeline to ensure timely completion.

8.2 Implementation Evidence

To validate the application of the treatment plan, evidence was collected in the form of screenshots. These screenshots show the actions that were implemented as part of the cybersecurity improvement process.

The following implementation evidence was recorded:

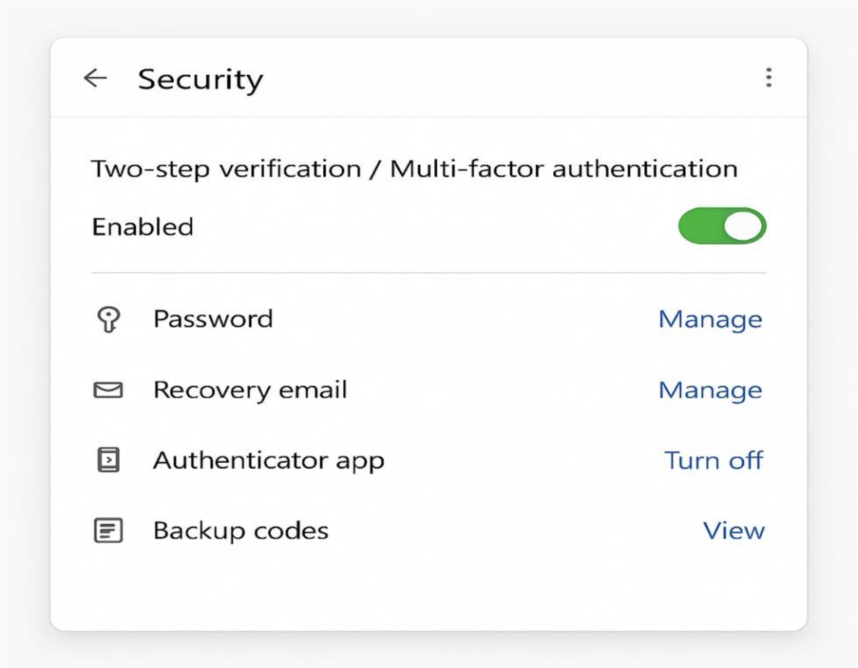
- **Wi-Fi network separation successfully completed**
- **POS system updated to the latest version**
- **Multi-Factor Authentication (MFA) enabled**



Dashboard

Update completed —
your system is now up to date

Date	Receipt	Customer
21 Apr 2022	AABC072Z	Walk-in Cust...
		n
		n Cust...
		n
		Customer
		tomer
16 Apr 2022	COE3401E	$20,00
18 Apr 2022	WAZZIM9	$29,00
Walk-in Customer	WALK-6–is	$160,00
Walk-in Customer	Walk-in Customer	$24,00



Security

Two-step verification / Multi-factor authentication

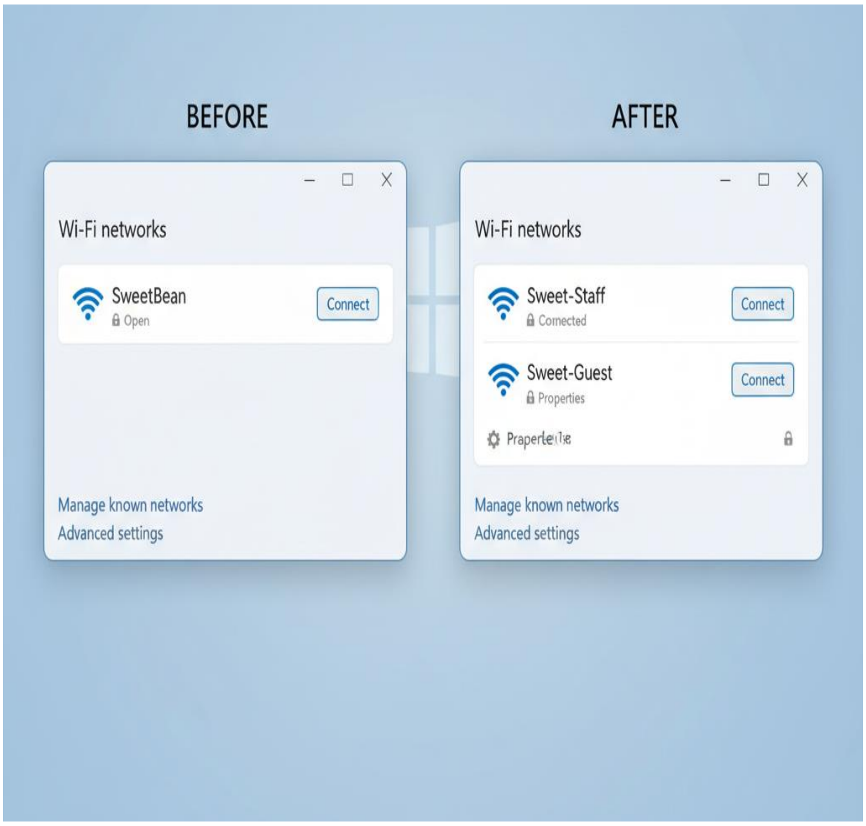
Enabled

Password — Manage

Recovery email — Manage

Authenticator app — Turn off

Backup codes — View



BEFORE

Wi-Fi networks

SweetBean — Open — Connect

Manage known networks

Advanced settings

AFTER

Wi-Fi networks

Sweet-Staff — Cornected — Connect

Sweet-Guest — Properties — Connect

Praperleute

Manage known networks

Advanced settings

8.3 Summary of Improvements

After completing the initial phase of risk treatment:

- Critical risks such as Wi-Fi security and lack of MFA were addressed
- Security of key systems such as POS and user accounts improved
- Business awareness toward cybersecurity increased

9. CONCLUSION

This project presented a simple and practical Cybersecurity Risk Assessment Framework designed for small retail and service businesses with limited technical knowledge and budget. The framework helps business owners identify cyber risks, evaluate their severity, and take necessary actions to improve security using easy-to-follow steps.

Through a simulated case study of "Sweet Bean Café," several cybersecurity gaps were identified, including weak Wi-Fi security, lack of Multi-Factor Authentication (MFA), shared user accounts, outdated software, and poor backup practices. A structured Risk Register and Risk Treatment Plan were developed to address these issues based on priority and impact. Initial implementation evidence shows that the business has started taking steps to improve its cybersecurity posture.

Overall, the framework successfully demonstrates that even small businesses can enhance their cybersecurity with simple, low-cost measures. It provides a starting point for adopting better security practices and building cyber awareness among staff members.

- **FUTURE ENHANCEMENT**

Although the framework is simple and effective for small businesses, it can be further enhanced in the future. Possible improvements include:

- Adding automated tools for risk assessment and reporting
- Expanding the framework for medium-sized businesses and other sectors
- Introducing more technical controls such as intrusion detection and monitoring
- Developing a mobile or web-based version of the framework for easy use
- Conducting real-world assessments on multiple small businesses to improve accuracy

These enhancements can make the framework more scalable, efficient, and suitable for a broader range of organizations.