Brew Haven Café – Cybersecurity Risk Assessment Report

1. Business Overview

Brew Haven Café, located in Delhi – Connaught Place, is a medium-sized café with 12 employees. The café uses one POS billing system, two laptops for admin and accounting work, six staff mobile phones, three tablets for order-taking, and four CCTV cameras connected to the network. A cybersecurity assessment was conducted to identify vulnerabilities, assess risks in current technology usage, and recommend improvements to strengthen the café's protection against cyber threats.

2. Key Findings

- A single Wi-Fi network is shared by customers, staff devices, CCTV, and POS system → **high cyber-risk exposure**

- No Multi-Factor Authentication (MFA) on business email, POS login, accounting software, or banking credentials

- Data backups are manual, inconsistent, and have never been tested for recovery

- POS and accounting software updates are not regularly performed (last update ~7 months ago)

- Staff use shared logins for POS system and admin laptop → no individual accountability for changes or misuse

3. Strengths Identified

- Router default admin password was changed after installation

- Antivirus is installed and active on both laptops

- CCTV footage is monitored and reviewed weekly by the manager

4. Top 3 Cyber Risks

Risk	Reason It Is Critical
Shared accounts & weak passwords	No accountability and higher chance of unauthorized access or misuse
Single Wi-Fi for POS, CCTV & Customer use	Attackers on guest Wi-Fi can compromise key business systems

Risk	Reason It Is Critical
Backups not tested	Recovery may fail in case of ransomware or data loss incident

5. Recommended Next Steps

- Enable **Multi-Factor Authentication (MFA)** on business email, POS, accounting and banking accounts

- Create **separate Wi-Fi networks** for Guest, Staff, and POS/CCTV systems

- Set **automatic daily backups** and test data restoration monthly for reliability

- Update POS, accounting software, and all devices regularly; turn on **auto-updates** where possible

- Conduct **basic cybersecurity awareness training** for employees on phishing, safe passwords, and device usage

- Implement **unique login IDs for staff** on POS and laptops to track actions and improve accountability