# The Unlocked Back Door: A Risk Analysis for Café Connect

Prepared for: Café Connect CEO

Prepared by: Security Analyst

Date: August 31, 2025

## Part I: Foundation - Identifying Core Components

### 1. Threat Agents

Café Connect may not be a bank, but that does not make it invisible to attackers. Three types of plausible threat agents are:

- Financially Motivated Cybercriminals: These actors target POS systems and payment data. Given Café Connect’s shared network between POS and desktops, attackers could gain access to credit card details, leading to fraud, fines, and reputational harm.

- Opportunistic Hackers: Weak Wi-Fi security is an open invitation. Attackers sitting in the café could exploit the outdated WPA2 setup to launch attacks or pivot into internal systems.

- Insider Threats: Overworked staff or disgruntled employees could misuse shared passwords or take advantage of unlocked physical access points. Insiders are often overlooked but pose a very real risk.

### 2. Vulnerability Catalog

Four critical vulnerabilities identified are:

- Weak Wi-Fi Security (Technical): Password is the store’s phone number, rarely updated, and still using WPA2 without a login portal.

- No Proper Network Segmentation (Technical): POS systems and staff computers share the same network, allowing malware to spread easily.

- Lack of Enforced Password Policy (Operational): Staff share simple passwords like CafeSummer2024!, making unauthorized access highly likely.

- Poor Physical Security (Physical): Back doors are left open during deliveries, and the back office with the main router is often unlocked.

## Part II: Analysis - Assessing the Risk

### 3. Likelihood and Impact

Two of the most dangerous threat-vulnerability pairs are:

1. Cybercriminals exploiting poor network segmentation:  
- Likelihood: High – Retail systems are frequent targets, and automated attacks are widespread.  
- Impact: Critical – A breach of cardholder data could trigger financial losses, regulatory fines, and loss of customer trust.  
- Justification: Lack of segmentation makes lateral movement almost trivial.

2. Opportunistic hackers abusing weak Wi-Fi security:  
- Likelihood: Medium-High – Public Wi-Fi is a common target.  
- Impact: High – Loyalty program and customer information could be stolen, harming reputation and enabling fraud.  
- Justification: The outdated setup is an easy entry point.

### 4. Risk Calculation

Using a simple risk matrix:

|  |  |  |
| --- | --- | --- |
| Threat-Vulnerability Pair | Risk Level | Rationale |
| Cybercriminals + Poor Network Segmentation | Critical Risk | High likelihood and critical impact. |
| Opportunistic Hackers + Weak Wi-Fi | High Risk | Medium-high likelihood with high impact. |

### 5. Data Asset Value

The most valuable data asset is the BeanStock Loyalty Program database. From a business perspective, it drives customer engagement and targeted marketing. From a regulatory standpoint, it contains personal data (names, emails, birthdates) protected by data privacy laws (e.g., GDPR, PCI-DSS relevance for linked payment details). A breach could damage both reputation and compliance status.

## Part III: Mitigation - Proposing Solutions

### 6. Mitigation Strategies

For the highest-risk issue (network segmentation):  
- Technical Control: Implement enterprise-grade firewalls and VLANs to separate POS, corporate, and guest Wi-Fi networks. This limits attacker movement.  
- Administrative Control: Establish a clear access control policy with regular reviews to ensure employees only access systems they truly need.

### 7. Cost-Benefit Consideration

Network segmentation may require investment in new firewall equipment and IT setup time. However, the benefits—protection of payment data, compliance with PCI-DSS, reduced risk of large-scale breaches, and preserved customer trust—far outweigh the costs. A single breach could cost hundreds of thousands in fines and lost sales, while segmentation costs a fraction of that. This makes it a clear and worthwhile investment.

### 8. Vendor Risk

To manage risks with third-party vendors after their past incident, Café Connect should:  
- Conduct a full vendor security assessment, including incident reports, remediation steps, and proof of compliance.  
- Update contracts to include data protection clauses, breach notification requirements, and liability terms.  
Additionally, periodic audits and diversifying vendors could further reduce risk exposure.