# Restaurant Cybersecurity Assessment

Internal Review Report

Prepared by: Emmanuel Amadi

Date: 2025

## 1. Executive Summary

This report provides the results of an internal cybersecurity assessment conducted for the restaurant's operational, network, and point-of-sale (POS) environments. The objective of this review was to identify practical, low-cost security improvements that reduce the risk of payment fraud, unauthorized access, operational disruption, and reputational impact. To protect the privacy of the organization and as per rules of assessment, no photos will be used display any network information.

Overall, the restaurant benefits from several strong foundations, including a wired and isolated POS infrastructure, company-delivered cybersecurity and PCI compliance training, role-based POS credentials, and corporate-supported backup and recovery capabilities.

However, the assessment also identified several medium to high-risk issues that should be addressed to improve overall security posture.

Top Risks Identified:
1. Unsecured guest Wi-Fi accessible to anyone within range.
2. Infrequent internal Wi-Fi password rotation practices.
3. Visible POS passwords and unattended POS sessions.
4. Limited camera coverage outside the manager's office.
5. IoT lighting controls potentially sharing networks with business systems.
6. Credential compromise handling lacking standardized procedures.

Implementing the prioritized recommendations in this report will strengthen defense against common threats, protect payment integrity, and enhance operational reliability.

## 2. Scope & Methodology

Scope:
The assessment focused on:
• Wi-Fi and network usage
• POS access and credential hygiene
• Employee cybersecurity awareness
• Backup and incident readiness

Out of Scope:
• Intrusive scanning or penetration testing
• Access to payment card data or financial systems
• Configuration changes to production systems

Methodology:
Assessment was performed through observation, informal staff interviews, review of POS use practices, and analysis based on industry best practices (NIST CSF, PCI considerations).

## 3. Environment Overview

The restaurant operates with a wired POS system, multiple dining rooms, and four banquet rooms utilizing internal Wi-Fi for presentations. Guest Wi-Fi is open-access. POS devices, manager workstations, and IoT lighting systems support business operations. Corporate IT provides training, backup systems, and escalation playbooks.

## 4. Findings & Risk Assessment

- F1 – Open guest Wi-Fi with no authentication (High Risk)
- F2 – Internal Wi-Fi password rotated infrequently (Medium–High Risk)
- F3 – POS passwords visible near terminals (High Risk)
- F4 – POS terminals left unlocked when staff walk away (High Risk)
- F5 – Limited camera coverage around sensitive systems (Medium Risk)
- F6 – IoT lighting possibly sharing networks with business systems (Low–Medium Risk)
- F7 – Employee credential breaches lack centralized response (Medium Risk)

## 5. Recommendations & Roadmap

- R1 – Secure guest Wi-Fi (0–30 days, High Priority)
- R2 – Establish Wi-Fi password rotation (0–30 days, High Priority)
- R3 – Remove written POS passwords (0–14 days, High Priority)
- R4 – Reinforce POS lock/logout practices (0–30 days, High Priority)
- R5 – Expand camera coverage (30–60 days, Medium Priority)
- R6 – Segment IoT systems and enable MFA (30–60 days, Medium Priority)
- R7 – Formalize credential compromise response (60–90 days, Medium Priority)

## 5.1 Recommendations & Roadmap (Integrated Table)

| Priority | Recommendation | Related Finding(s) | Description / Action Steps | Timeline | Owner |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| High | R1 – Secure the Guest Wi-Fi Network | F1 | Convert the open guest network into a password-protected network rotated every 30–90 days or a captive portal with acceptance screen. | 0–30 days | Owner / ISP / IT Support |
| High | R2 – Establish Wi-Fi Password Rotation Policy | F2 | Limit internal Wi-Fi password distribution, rotate every 6–12 months, and change whenever staff with access leave. | 0–30 days | Management |
| High | R3 – Remove Written POS Passwords Near Terminals | F3 | Remove all visible written passwords, secure admin credentials, and remind staff not to write down codes. | 0–14 days | Management |
| High | R4 – Reinforce POS Lock/ Logout Behavior | F4 | Brief staff on locking POS screens when stepping away; optionally reduce auto-timeout to 1–2 minutes. | 0–30 days | Management / Corporate |

| | | | | | |
|---|---|---|---|---|---|
| Medium | R5 – Increase Security Camera Coverage | F5 | Add or reposition cameras around POS areas, cash handling zones, and network hardware. | 30–60 days | Owner / Security Vendor |
| Medium | R6 – Verify IoT Lighting Segmentation & MFA | F6 | Ensure IoT lighting is on a separate or guest VLAN and that app accounts use strong passwords and MFA. | 30–60 days | Management / IT |
| Medium | R7 – Strengthen Identity Compromise Procedures | F7 | Log credential compromises, reset passwords, enforce MFA, and monitor for follow-up phishing attempts. | 60–90 days | Management / Corporate Security |

## 6. Conclusion

This assessment shows that the restaurant can significantly improve its cybersecurity posture with targeted, low-cost actions. Strengthening Wi-Fi controls, securing POS authentication practices, improving monitoring, and formalizing identity handling procedures will materially reduce operational and payment-related risks. Implementing the 30/60/90-day roadmap will result in a more resilient and secure environment aligned with industry expectations.

## 6.1 Emerging Threats & Industry Guidance

The hospitality industry continues to face a growing landscape of cybersecurity threats driven by high transaction volume, reliance on third-party vendors, and extensive use of Wi-Fi and POS systems. Understanding these emerging risks ensures the restaurant remains proactive rather than reactive in defending payment systems, customer data, and business operations.

1. POS Malware and Credential Harvesting

Threat actors frequently target POS environments and vendor credentials. Modern cloud POS systems reduce card storage but attackers now focus on manager credentials, remote access tools, and weak integrations.

2. Wi-Fi Attacks and Rogue Access Points

Unsecured or poorly segmented Wi-Fi networks enable man-in-the-middle attacks, rogue access points, and lateral movement attempts that can threaten business systems.

3. Social Engineering & Business Email Compromise (BEC)

Restaurants experience high rates of fake invoices, gift card scams, payroll redirection attempts, and vendor impersonation. Fast operations and high email volume increase susceptibility.

4. Exploitation of IoT Systems

IoT lighting, cameras, tablets, and automation devices can introduce attack surface if not segmented from POS and business networks.

5. Third-Party Vendor Data Exposure

Delivery platforms, loyalty tools, and scheduling vendors create shared risk. Compromises often originate from vendors rather than the restaurant itself.

Maintaining Compliance & Best Practices:

Aligning with PCI DSS and hospitality best practices is essential:

• PCI DSS Requirements: Credential security (Req. 2 & 8), wireless protection (Req. 4), malware defenses (Req. 5), physical POS security (Req. 9), and incident response (Req. 12).

• Hospitality Guidance: HTNG, AHLA, and NIST emphasize segmentation, Wi-Fi controls, MFA adoption, ongoing awareness training, and vendor risk management.

Supporting Documentation:

PCI DSS v4.0 – https://www.pcisecuritystandards.org/

NIST Cybersecurity Framework – https://www.nist.gov/cyberframework

HTNG Security Guidelines – https://htng.org/

AHLA Hospitality Cybersecurity – https://www.ahla.com/