Risk Assessment Report – Valiente Coffee Shop

Company: Valiente Coffee Shop

Date: September 30, 2025

Prepared by: [Your Name]

# 1. Introduction

This report provides a risk assessment for Valiente Coffee Shop. It identifies key assets, potential threats, vulnerabilities, and recommendations to improve the overall cybersecurity posture of the business.

# 2. Company Overview

Valiente Coffee Shop is a small local café with two locations and approximately 10 employees. The shop uses point-of-sale (POS) systems for payment processing, provides guest Wi-Fi, manages employee accounts and devices, and operates a website for online orders.

# 3. Identified Assets

- Point of Sale (POS) terminals  
- Customer payment data  
- Employee laptops & accounts  
- Wi-Fi network (guest & employee)  
- Company website (online ordering system)

# 4. Risks & Vulnerabilities

|  |  |  |  |
| --- | --- | --- | --- |
| Asset | Threat | Vulnerability | Risk Level |
| POS System | Credit card theft | Outdated or unpatched software | High |
| Customer Wi-Fi | Unauthorized access / malware | Weak password / no network segmentation | Medium |
| Employee Email | Phishing attacks | No multi-factor authentication (MFA) | High |
| Website | DDoS or data breach | No Web Application Firewall (WAF) | Medium |
| Laptops | Ransomware infection | No antivirus / irregular updates | High |

# 5. Recommendations

- Regular updates & patch management for POS and laptops  
- Enable multi-factor authentication (MFA) for employee email  
- Separate guest Wi-Fi from employee network with strong WPA3 encryption  
- Install and maintain antivirus protection on all laptops  
- Deploy a Web Application Firewall (WAF) to protect the website  
- Provide regular cybersecurity awareness training for employees  
- Schedule regular backups of critical systems and customer data

# 6. Conclusion

This assessment identifies the areas where Valiente Coffee Shop is most vulnerable. By implementing the recommended security controls, the coffee shop can significantly reduce its exposure to cyber threats while maintaining customer trust and business continuity.