**Executive Summary**

Brown & Haley, a renowned confectionery company based in Tacoma, Washington, faces increasing cybersecurity threats common to the manufacturing and food industries. While the company has a robust IT infrastructure supporting its operations, its cybersecurity practices have not kept pace with the evolving threat landscape. Recognizing this vulnerability, Office Manager Dan Fabian initiated this project to proactively assess and enhance the company's security posture. This project aligns with Brown & Haley's strategic objectives of protecting its intellectual property, maintaining business continuity, and safeguarding its brand reputation (Corvell, 2024).

The primary objective of this project is to identify and assess vulnerabilities in Brown & Haley's IT infrastructure to reduce the risk of cyberattacks and data breaches. Specific objectives include:

* Identify and document all critical vulnerabilities in the company's network, systems, and applications.
* Assess the potential impact of these vulnerabilities on business operations.
* Provide actionable recommendations for remediation to improve the company's security posture.
* Enhance employee cybersecurity awareness and training.
* Comply with industry regulations and best practices for cybersecurity.

**Project Scope**

This project will encompass a comprehensive penetration test of Brown & Haley's IT infrastructure, including both the factory and office environments. The scope includes:

* **Network Penetration Testing:** Assessing the security of the company's network perimeter, including firewalls, routers, and other network devices.
* **Web Application Penetration Testing:** Evaluating the security of the company's website and other web applications.
* **Wireless Network Penetration Testing:** Analyzing the security of the company's wireless networks.
* **Social Engineering Testing:** Simulating social engineering attacks to assess employee susceptibility to phishing and other social engineering tactics.

The scope explicitly *excludes* physical security assessments, penetration testing of third-party systems not directly managed by Brown & Haley, and any activities that could disrupt critical business operations.

**Milestones and Deliverables**

|  |  |  |
| --- | --- | --- |
| Milestone | Deliverable | Date |
| Project Initiation | Project Charter Approved | 2024-01-15 |
| Planning and Scoping | Penetration Test Plan Document | 2024-01-29 |
| Vulnerability Scanning | Vulnerability Scan Report | 2024-02-12 |
| Penetration Testing | Penetration Test Report | 2024-02-26 |
| Remediation Recommendations | Remediation Plan Document | 2024-03-11 |
| Project Closure | Final Project Report and Presentation | 2024-03-25 |

**Risks and Communication Plan**

**Potential Risks:**

* **Service Disruption:** Mitigated by conducting testing during off-peak hours and having rollback plans.
* **Undiscovered Vulnerabilities:** Mitigated by using multiple testing tools and techniques, and retesting after remediation.
* **False Positives:** Mitigated by thorough validation of findings.

**Communication Plan:**

* **Weekly Status Reports:** Provide Dan Fabian with weekly updates on project progress, identified vulnerabilities, and remediation recommendations.
* **Final Report and Presentation:** Present a comprehensive final report and presentation to Dan Fabian and other key stakeholders, outlining the project findings and recommendations.
* **Ad-hoc Communication:** Maintain open communication channels with Dan Fabian and the IT team to address any questions or concerns throughout the project.

Communication with stakeholders, including Dan Fabian, IT staff, and executive management, will be maintained throughout the project lifecycle through regular meetings, email updates, and a final presentation of findings and recommendations. This proactive approach aligns with best practices for risk communication (Hooker & Leask, 2020).

This penetration testing project will significantly enhance Brown & Haley's cybersecurity posture, protect its valuable assets, and strengthen its reputation as a secure and reliable business partner.

**References**

Hooker, C., & Leask, J. (2020). *Risk Communication Should be Explicit About Values. A Perspective on Early Communication During COVID-19*. *Journal of bioethical inquiry*, *17*(4), 581–589. <https://doi.org/10.1007/s11673-020-10057-0>

Covell, J. (2024). Brown & Haley. In *International Directory of Company Histories*. <https://www.encyclopedia.com/books/politics-and-business-magazines/brown-haley>