**Environmental Scan: Brown & Haley**

**Site Supervisor Description:**

* **Name:** Dan Fabian
* **Contact Information:** [dfabian@brown-haley.com](https://www.google.com/url?sa=E&q=mailto%3Adfabian%40brown-haley.com)
* **Role:** Office Manager
* **Length of Time with Organization:** 15 years
* **Contact Method:** Met through a work agency a couple of years ago.
* **Relevant Information:** Dan oversees the day-to-day operations of the office, including IT infrastructure and cybersecurity practices. He is responsible for implementing new technologies and processes, making him a key stakeholder for this project. He has expressed concerns about the company's current cybersecurity posture and is actively seeking ways to improve it.

**Introduction to Brown & Haley and Current Situation**

Brown & Haley is a well-established chocolate candy factory located in Tacoma, Washington. Known for its Almond Roca and other confections, the company has a significant presence in the region and distributes its products nationally and internationally. While Brown & Haley has embraced technology for manufacturing and sales, its cybersecurity practices have not kept pace with the evolving threat landscape. This presents a significant risk to the company's operations, intellectual property, and reputation.

**Problem/Improvement Area**

Brown & Haley needs a comprehensive penetration test conducted to assess the security of its IT infrastructure, both in the factory and office environments. This assessment will identify vulnerabilities and weaknesses that could be exploited by malicious actors, providing a roadmap for implementing necessary security improvements.

**SWOT Analysis**

* **Strengths:**
  + Established brand recognition and market share.
  + Strong local presence and community ties.
  + Experienced workforce in manufacturing and sales.
  + Existing IT infrastructure, albeit with security gaps.
  + Management's willingness to invest in security improvements.
* **Weaknesses:**
  + Outdated cybersecurity practices and infrastructure.
  + Lack of dedicated cybersecurity personnel.
  + Limited employee training on cybersecurity awareness.
  + Potential vulnerabilities in both physical and digital security.
  + No documented incident response plan.
* **Opportunities:**
  + Implementing robust cybersecurity measures to protect sensitive data and intellectual property.
  + Enhancing brand reputation and customer trust by demonstrating a commitment to security.
  + Leveraging technology to improve efficiency and productivity in a secure environment.
  + Meeting increasing industry regulations and compliance requirements.
  + Attracting and retaining talent by fostering a secure and technologically advanced workplace.
* **Threats:**
  + Increasingly sophisticated cyberattacks targeting manufacturing and food industries.
  + Data breaches and ransomware attacks leading to financial losses and reputational damage.
  + Industrial espionage and theft of intellectual property.
  + Disruption of operations due to cybersecurity incidents.
  + Regulatory penalties for non-compliance with security standards.

**Process of Developing a Project Charter**

Developing a project charter is a crucial first step in any project, as it formally authorizes the project and provides the project manager with the authority to allocate resources. It serves as a foundational document, outlining the project's purpose, scope, and key stakeholders, and guiding the project team throughout its lifecycle.

1. **Identify the Need:** This usually starts with a business case or a problem statement, outlining the reason for initiating the project.
2. **Define High-Level Scope and Objectives:** What are the project's goals? What are the key deliverables? What's included and excluded?
3. **Identify Key Stakeholders:** Who are the individuals or groups impacted by or who can influence the project?
4. **Assign a Project Manager:** This individual will be responsible for leading and managing the project.
5. **Develop the Project Charter:** This document formally authorizes the project and outlines key information.
6. **Review and Approve the Charter:** Key stakeholders review and approve the charter, signifying their agreement and commitment.

**Research on Charter Elements**

* **Clear Project Objectives:** Instead of vague statements, use SMART (Specific, Measurable, Achievable, Relevant, Time-bound) objectives. For example, instead of "Improve cybersecurity," a SMART objective would be "Reduce the number of critical vulnerabilities identified in a penetration test by 50% within six months." This aligns with research emphasizing the importance of clear goals for project success (Locke & Latham, 2002).
* **Well-Defined Scope:** Clearly delineate what is included and, importantly, what is *excluded* from the project scope. This prevents scope creep and ensures the project team focuses on the agreed-upon deliverables. For example, a penetration test charter might explicitly exclude physical security assessments. This is supported by research showing that clearly defined scope reduces project failure rates (PMI, 2021).
* **Stakeholder Analysis:** Go beyond just listing stakeholders. Analyze their influence and interest levels using a power/interest grid. This helps prioritize communication and engagement strategies. Research by Mitchell, Agle, and Wood (Mitchell et. al., 1997) highlights the importance of stakeholder salience in project management.
* **Risk Assessment:** Include a preliminary risk assessment in the charter, identifying potential risks and outlining mitigation strategies. This proactive approach helps avoid surprises and delays later in the project. This aligns with research on risk management best practices (Kaplan et. al., 2024).
* **Communication Plan:** Outline how communication will be managed throughout the project. Specify communication frequency, methods, and responsible parties. Research by Pinto and Slevin (Pinto et. al., 1988) emphasizes the crucial role of effective communication in project success.
* **Defined Success Criteria:** Clearly define what constitutes project success. These criteria should be measurable and tied to the project objectives. For example, "Successful completion of the penetration test and delivery of a comprehensive vulnerability report within the allocated budget and timeframe."
* **Explicit Authorization:** The charter must include a clear statement of authorization from the project sponsor, granting the project manager the authority to proceed and allocate resources.
* **Version Control:** Implement version control for the charter to track changes and ensure everyone is working with the most up-to-date document.

By incorporating these research-backed recommendations, project charters become more effective tools for guiding projects towards successful completion. They provide clarity, alignment, and a solid foundation for decision-making throughout the project lifecycle.

**Intersection between SWOT Analysis and Project Charter**

The SWOT analysis directly informs the project charter by providing a clear understanding of the context in which the penetration testing project will take place. The identified weaknesses (e.g., outdated cybersecurity practices) become the drivers for the project objectives. The opportunities highlighted in the SWOT analysis contribute to the project's business case, justifying the investment in security improvements. Threats underscore the urgency and importance of the project. Finally, the strengths can be leveraged to support project execution. For example, management's willingness to invest in security improvements facilitates securing necessary budget and resources within the project charter.

**Conclusions based on SWOT Analysis**

The SWOT analysis reveals a clear need for improved cybersecurity measures at Brown & Haley. The penetration testing project is crucial to identify and address vulnerabilities before they are exploited by malicious actors. By investing in this project, Brown & Haley can mitigate the identified threats, capitalize on the opportunities, and strengthen its overall security posture. This will not only protect the company's assets but also enhance its reputation and ensure its long-term sustainability. This project will allow me to utilize my cybersecurity knowledge and skills to make a significant contribution to the organization and gain valuable real-world experience. My role will be to plan, execute, and document the penetration test, working closely with Dan Fabian to ensure the project aligns with the company's needs and objectives.

**References**

Kaplan, R. S., & Mikes, A. (2024). *Managing risks: A new framework*. Harvard Business Review. https://hbr.org/2012/06/managing-risks-a-new-framework

Locke, E. A., & Latham, G. P. (2002). *Building a practically useful theory of goal setting and task motivation*. American Psychologist, *57*(9), 705.

Mitchell, R. K., Agle, B. R., & Wood, D. J. (1997). Toward a theory of stakeholder identification and salience: Defining the principle of who and what really counts. *Academy of management review*, *22*(4), 853-886.

Pinto, J. K., & Slevin, D. P. (1988). Project success: Definitions and measurement techniques. *Project Management Journal*, *19*(1), 67-72.

Project Management Institute (PMI). (2021). *A guide to the project management body of knowledge (PMBOK guide)* (7th ed.).