**Cybersecurity Enhancement Implementation Report for TAP**

**Introduction:** This report provides an overview of the key security measures implemented to enhance cybersecurity within our organization. By implementing robust security controls and conducting vulnerability assessments, we aim to safeguard sensitive data, mitigate security risks, and fortify our overall cybersecurity posture.

**Implemented Security Measures:**

1. **Blocking File Types:**
   * **Objective:** Prevent the transmission of potentially harmful file types via email.
   * **Rationale:** To reduce the risk of malware infections and data breaches resulting from malicious attachments.
   * **Outcome:** Implemented a mail flow rule to block specified file types in external emails, enhancing email security.
2. **Disclaimer Banner for External Emails:**
   * **Objective:** Increase user awareness of potential security risks associated with external emails.
   * **Rationale:** To provide visual cues to users regarding the origin of external emails and potential security threats.
   * **Outcome:** Successfully implemented a disclaimer banner for external emails, enhancing user awareness of security risks.
3. **Spoof Intelligence: Block the Domains:**
   * **Objective:** Mitigate the risk of email spoofing and phishing attacks by blocking malicious domains.
   * **Rationale:** To protect against phishing attacks and email spoofing, which can lead to data breaches and financial losses.
   * **Outcome:** Strengthened email security by proactively blocking potentially harmful domains.
4. **Vulnerability Testing through Nessus for the Website:**
   * **Objective:** Identify and address security vulnerabilities in the organization's website.
   * **Rationale:** To reduce the risk of cyberattacks and data breaches by identifying and remedying vulnerabilities.
   * **Outcome:** Conducted comprehensive vulnerability testing on the website, identified and mitigated security risks, and improved overall website security posture.

**Conclusion:** The implementation of these security measures demonstrates our commitment to enhancing cybersecurity within the organization. By proactively addressing potential vulnerabilities and implementing robust security controls, we aim to safeguard sensitive data, mitigate security risks, and ensure the integrity of our digital assets. Continued monitoring and assessment of security measures will be essential to maintaining effective cybersecurity defenses in the ever-evolving threat landscape.