**Project Progress Report and Reflection 1 (PPRR1) Target Data Breach**

**Project Definition and Objective**

The 2013 Target data breach stands as one of the most significant security incidents in the history of U.S. retail, affecting approximately 98 million customers by compromising credit card details and personally identifiable information (PII). The breach occurred due to vulnerabilities in Target’s network, exploited through a third-party vendor, Fazio Mechanical. Attackers used phishing to access Target’s system and installed malware on the point-of-sale (POS) systems, resulting in the exfiltration of vast amounts of customer data. This project will focus on the cybersecurity vulnerabilities that enabled this breach, the challenges Target faced in preventing the breach, and how improved security practices could have mitigated or prevented the incident.

The objective of this project is to analyze the technical aspects of the breach and propose a cybersecurity plan that addresses the vulnerabilities exposed by the attack. The plan will focus on third-party risk management, network segmentation, advanced malware detection, and incident response strategies. By examining the flaws in Target's infrastructure and security processes, the project aims to create a comprehensive cybersecurity approach that not only highlights lessons learned but also provides actionable solutions to prevent similar breaches in the future.

**Approach**

To solve the problem of security vulnerabilities that led to the Target data breach, the approach will involve a multi-faceted cybersecurity plan. The plan will address specific technical and procedural gaps within Target’s infrastructure, such as poor third-party vendor security, lack of real-time malware detection, and ineffective incident response protocols. The plan will include:

* **Vendor Risk Management:** Ensuring third-party vendors comply with stringent cybersecurity practices, including the use of stronger malware protection.
* **Network Segmentation:** Isolating critical systems, such as POS networks, from other parts of the business infrastructure to limit access in case of compromise.
* **Enhanced Malware Detection and Prevention:** Deploying robust, real-time malware detection systems that can handle custom malware, like the BlackPOS variant used in the breach.
* **Incident Response Plan:** Developing a more effective security monitoring and response framework to ensure immediate action when alerts are triggered, avoiding negligence, as seen in Target's handling of alerts from FireEye.

This approach aims to not only rectify past mistakes but also create a resilient system that can withstand future cybersecurity threats.

**Summary and Next Steps**

The project seeks to thoroughly analyze the factors that contributed to the Target data breach and design a comprehensive cybersecurity plan addressing those issues. The next steps will involve further research into advanced malware protection, vendor risk management strategies, and reviewing successful incident response models used in other industries. Additional research will also include reviewing industry standards like PCI-DSS (Payment Card Industry Data Security Standard) and integrating them into the proposed solutions.

**Next steps:**

* Investigate existing frameworks and tools for vendor risk management.
* Review advanced incident response models.
* Explore modern malware detection and prevention systems for retail POS networks.

**Bibliography:**

* Krebs, B. (2014). *Inside Target Corp., Days After 2013 Breach*. Retrieved from <https://krebsonsecurity.com>
* Smith, B. (2015). *The Target Data Breach and Lessons Learned*. Forbes.
* Yao, D., & Wang, Z. (2014). *Target Data Breach Case Study*.