**Case Study – Target**

Ty McPhail

10/13/2024

**Introduction**

In 2013, Target faced a major security breach that demonstrated the critical gap between being prepared and being truly vigilant. The company had invested heavily in advanced cyberattack prevention measures and believed that its infrastructure was sufficient to ward off threats. They implemented multiple systems designed to detect, manage, and eliminate potential risks, positioning themselves as a leader in cybersecurity among retailers. However, despite having these sophisticated tools in place, Target failed to act on early warning signs. Their security software issued alerts, signaling potential risks that should have prompted immediate investigation, but these warnings were dismissed under the assumption that the threats were minimal or insignificant. According to the recent statistics, there are multiple attacks on POS systems every minute in retail outlets, restaurants, and hospitality industries (Rajah, Saravana Kumar, 2023). Adding to the problem, the company chose to deactivate an essential feature of their prevention software, one that could have automatically eradicated malicious software, due to a lack of confidence in its effectiveness. This hesitation allowed malware to persist undetected in their point-of-sale (POS) systems, leading to the theft of millions of customers’ credit card details, which were subsequently stored on remote servers by the attackers. To prevent future breaches on such a massive scale, Target must adopt a more proactive and comprehensive security approach while ensuring that all potential threats are immediately and thoroughly addressed.

**Analysis**  
Target’s mission is “To help all families discover the joy of everyday life.” This mission shows the company’s focus on delivering affordability, quality, and convenience to its customers (Target’s Purpose and History, 2024). By offering a wide variety of products, Target aims to create a unique and enjoyable shopping experience that anyone can enjoy affordably. The mission reflects Target’s commitment to balancing value with quality, establishing itself as a retailer that offers stylish and high-quality products at competitive prices.

Target employs a broad differentiation strategy. Unlike Walmart, who focus primarily on cost leadership, Target distinguishes itself through its “affordable chic” image. Target's competitive advantage lies in providing trendy, high-quality items at accessible prices. The emphasis on exclusive brands and partnerships with well-known designers further differentiates Target in a crowded retail market and gives them a leg up on other large retailers.

The threat of new entrants for Target is relatively low due to the significant capital and scale required to compete in the retail space. New competitors would need to invest heavily in logistics, supply chains, and brand development. The rise of e-commerce has slightly lowered barriers to entry, as online retailers don’t require the same physical infrastructure. Online retailers often have lower costs than physical stores, allowing them to offer competitive pricing and leaving brick-and-mortar retailers feeling more pressure to match these prices (Collins, Ava, 2024). Target works with many suppliers, which helps it to maintain leverage. While some suppliers hold more power due to exclusive partnerships, Target’s size allows it to negotiate favorable terms. Customers have high bargaining power in the retail industry due to the availability of alternatives. To combat this, Target focuses on creating customer loyalty through a differentiated shopping experience, competitive pricing, and exclusive products. Target faces a moderate threat of substitutes, particularly from online retailers like Amazon, and low-cost competitors such as Walmart, but Target’s focus on offering a combination of convenience, style, and quality keeps it relevant in the marketplace. Target operates in a highly competitive industry. Target’s strategy to compete centers around its unique product offerings, brand image, and customer experience, which help it stand out.

Target’s organizational structure is divided into sections based on product categories, regions, and functions. This setup helps the company stay flexible and respond quickly to different market demands and what customers want. Each division has independence, which allows them to make decisions, develop products, and handle marketing efficiently. This structure lets Target manage its large-scale operations while still staying focused on its core mission.

**Stakeholders**

Customers are one of the most important stakeholder groups for Target. Their trust and loyalty are essential to the company's success. Customers expect Target to provide safe, reliable products, a positive shopping experience, and to protect their personal and financial information. The 2013 data breach significantly impacted customers, leading to a loss of trust in the brand.

Target’s employees are essential to day-to-day operations and delivering excellent customer service. This group includes everyone from in-store staff to corporate employees in various departments like IT, marketing, and logistics. Employees expect a safe work environment, job security, fair pay, and opportunities for advancement.

Target’s investors and shareholders have a strong interest in the company’s financial performance. They are focused on profitability, stock performance, and long-term growth. When security breaches or other significant issues arise, these stakeholders are concerned about the impact on the company's reputation and bottom line.

Target relies on a vast network of suppliers to stock its shelves with the products customer’s demand. Suppliers are stakeholders because their business depends on a successful partnership with Target.

The communities where Target operates stores are also important stakeholders. They benefit from jobs, economic activity, and community support. In return, these communities expect the company to be socially responsible, ethical, and actively engaged in local development  
  
**Alternatives**

To boost its security and improve overall operations, Target could several courses of action. The first solution would be investing in advanced cybersecurity technologies. Using solutions like AI-driven threat detection systems and stronger encryption methods could help Target prevent future attacks. These tools would help Target spot potential threats right away, keeping customer data safer. By being proactive about cybersecurity, Target can not only prevent future breaches but also build customer trust with better data protection.

Another solution would be to create a comprehensive cybersecurity training program for all employees. This program could teach staff the best practices for staying safe online, like recognizing phishing emails and responding to security alerts. They would also be better equipped to notice suspicious interactions with their POS systems. When employees know what to look for and how to react, it creates a culture of security where everyone plays a part in protecting sensitive information. This alternative would be similar to examples given in *Adventures of an IT Leader* and would effectively put more necks in the noose and distribute responsibility across the staff, ensuring that everyone be vigilant regarding security.

The third solution would involve conducting regular security audits and assessments. By bringing in third-party experts to review their systems and processes, Target could identify any weak spots and areas that need improvement. This ongoing evaluation ensures that their security measures stay effective and that their response to potential threats remains strong. It also shows customers that Target is serious about transparency and security.

**Proposed Solutions**

Investing in AI-driven security solutions is a strategic move for Target that offers advantages over traditional methods. A key benefit is real-time threat detection; AI can analyze vast amounts of data swiftly, identifying patterns that may signal a cyber threat. This capability allows Target to respond to potential breaches as they occur, preventing significant damage before it escalates. AI systems can also learn and adapt over time, improving their effectiveness at recognizing new attacks in the ever-evolving cybersecurity landscape. By automating many processes, AI also reduces the likelihood of human error, freeing up Target’s IT team to focus on more hands-on tasks. While the initial investment in AI technology may be higher than basic employee training or audits, the long-term cost savings can be substantial. Preventing data breaches can help Target avoid costly legal fees, fines, and reputational damage associated with security incidents, like the 2013 breach. Prioritizing AI-driven security not only protects customer data but also enhances trust in the brand, demonstrating Target's commitment to safeguarding personal information. The other two options have significant limitations. Improved employee training may not be effective against sophisticated phishing attacks as it heavily relies on human behavior and diligence. Strengthening network security measures can be resource-intensive and may still leave vulnerabilities, especially against advanced cyber threats that can bypass traditional protocols. Adopting AI technology positions Target as a leader in cybersecurity, prepared for future challenges and maintaining customer loyalty.

**Conclusion**

Target data breach illustrates that even well-prepared organizations can fall victim to cyberattacks if they do not remain vigilant. The breach could have been largely avoided if Target had responded to the initial alerts from its security systems and maintained trust in the tools designed to protect its operations. Moving forward, it is essential for Target to recognize that effective cybersecurity solutions require ongoing diligence and proactive measures. This means not only investing in advanced technologies like AI but also fostering a culture of awareness and responsiveness among employees.

**References**

Collins, Ava. “The Rise of E-Commerce and It’s Impact on Brick-and-Mortar Stores.” *Association For Entrepreneurship USA*, afeusa.org/articles/the-rise-of-e-commerce-and-its-impact-on-brick-and-mortar-stores/#:~:text=Price%20competition:%20Online%20retailers%20often%20have%20lower%20costs%20than%20physical. Accessed 6 Oct. 2024.

Rajiah, Saravana Kumar. “The Security Vulnerabilities of POS Systems and How to Address Them.” *Encora*, Encora, 12 Jan. 2023, www.encora.com/insights/the-security-vulnerabilities-of-pos#:~:text=According%20to%20the%20recent%20statistics,%20there%20are%20multiple%20attacks%20on.

“Target’s Purpose and History.” *Target. Expect More. Pay Less.*, corporate.target.com/about/purpose-history#:~:text=To%20help%20all%20families%20discover%20the%20joy%20of%20everyday%20life. Accessed 6 Oct. 2024.