**10/22/2023**

**(IS 401/501-01 MERGED) (FA23) CYBERSECURITY PRINCIPLES**

**Case Study: Target (2013)**

**Pod 6**

**Amogh Patel**



**Table of Contents**

[I. Introduction](#_kgtr0uk8ag6k)

[II. Overview of the Target 2013 data breach](#_z98tau765t86)

[III. Lessons Learned](#_9n5moymm8tko)

[IV. Opinion](#_w1qze3ezgala)

[V. Conclusion](#_w8kki1drmcn8)

[VI. References](#_dw3sxxrdjtfc)

# I. Introduction

In 2013, Target, a major U.S. retailer, suffered a significant data breach that exposed the compromise of 40 to 70 million customer records, including sensitive credit card information, resulting in financial losses exceeding $200 million. This breach had far-reaching consequences, severely damaging Target's reputation and leading to the departure of its CEO and CIO. The root causes of the breach were multifaceted, including insufficient network segmentation, weak security controls, and an inadequate response process. Target's adherence to minimum security standards, like the Payment Card Industry Data Security Standards (PCI DSS), proved insufficient in the face of evolving cyber threats. The breach underscored the importance of swift responses to security alerts, as it lasted for nearly three weeks.

In the aftermath of the breach, Target made significant investments in cybersecurity operations, established a Cyber Fusion Center, and adopted chip and PIN credit cards to enhance security. High-level executive changes reflected the seriousness with which Target addressed the incident, setting an example for other organizations facing similar crises. The lessons learned from the Target breach are universally applicable and crucial for all stakeholders navigating the complexities of cybersecurity.

# II. Overview of the Target 2013 data breach

The Target 2013 data breach was a significant cybersecurity incident that occurred between November 27th and December 15th, 2013. During this breach, cybercriminals managed to access Target's network, resulting in the loss of customer information, including credit card numbers. The breach impacted between 40 to 70 million customer records, making it one of the largest data breaches at the time. The breach had far-reaching consequences for Target, with estimated costs exceeding $200 million, damage to the brand's reputation, and a decrease in short-term revenues. Furthermore, both the CEO and CIO of Target lost their jobs due to the breach.

One significant weakness that contributed to this breach was the issue of network segmentation. In this case, a heating, ventilation, and air-conditioning (HVAC) subcontractor had permission to remotely access Target's network for monitoring in-store HVAC systems. The breach occurred when the cybercriminals stole the supplier's permission credentials. Analysts believe that the hackers used a botnet to scrape these credentials, and they subsequently used them to access Target's network. The critical problem was that once the hackers gained access to the network, they could move laterally within it, eventually reaching a segment of the network containing Point of Sale (POS) payment systems.

Network segmentation is a crucial security measure designed to isolate sensitive systems from less critical areas of the network. It aims to prevent unauthorized access to critical assets and limit the lateral movement of cybercriminals within a network. In the case of the Target breach, the failure to effectively segment the network allowed the hackers to move from a less critical system (the HVAC system) to the highly sensitive POS systems, where they could compromise customer credit card data.

This breach underscores the importance of implementing and maintaining strong network segmentation, ensuring that different segments have limited access to one another. It also emphasizes the need for organizations to regularly review and update their security controls and risk assessments to adapt to evolving threats. Inadequate network segmentation, combined with other factors, allowed the breach to escalate, resulting in significant financial and reputational damage for Target.

# III. Lessons Learned

1. **Defense in Depth and Overreliance on Third-Party Controls:** The breach highlighted the importance of having multiple layers of security controls (defense in depth). Over Reliance on third-party contractors' controls can be risky. In this case, the HVAC contractor's credentials were compromised, and Target's security relied on them to protect their network.

2. **Siloed Approach to Security:** The breach underscores the need for a holistic, enterprise-wide approach to security. Isolating security controls and budgets in silos can lead to a fragmented and ineffective security posture. Organizations should consider the cumulative impact of various security risks.

3. **Timely Updates and Adaptation:** Security controls and processes need to be regularly updated and adapted to evolving threats. Relying solely on established standards, like PCI DSS, may not be sufficient to address emerging threats. It's essential to stay current with security best practices and emerging risks.

4. **Incident Response and Alarm Handling:** A crucial lesson is the importance of having an effective incident response plan. When security alarms were raised, there was a failure to trigger an adequate incident response in a timely manner. Swift response is critical to mitigating damage in a security breach.

5. **Proactive Detection and Monitoring:** Investing in proactive detection and monitoring systems can help identify and respond to security incidents in a timely manner. In Target's case, a newly installed FireEye malware detection system did raise alerts, but these alerts were not acted upon promptly.

9. **Investment in Cybersecurity:** Target's investment in improving its cybersecurity operations and creating a Cyber Fusion Center shows that organizations should allocate resources and invest in advanced security measures to prevent future breaches.

10. **Accountability and Leadership Changes:** The breach resulted in accountability at the highest levels, with the CEO and CIO losing their jobs. This demonstrates the importance of leadership accountability and swift action in response to security incidents.

12. **Preparedness for Inevitable Breaches:** Organizations should operate on the assumption that a breach is not a matter of "if" but "when." Having disaster recovery and business continuity plans in place is critical for recovery and resilience.

# IV. Opinion

The Target data breach in 2013 serves as a reminder of the significant and far-reaching consequences of cybersecurity failures. It highlights the interconnectedness of our digital world and the need for organizations to continually evolve their security measures to stay ahead of evolving threats. The breach underscores the importance of not only having robust security controls in place but also fostering a culture of security awareness at all levels of an organization. The fact that the breach took place over an extended period before detection emphasizes the need for proactive monitoring, timely incident response, and continuous improvement in security postures. Furthermore, it's evident that data breaches can have severe financial and reputational impacts, as Target's experience demonstrates. The case study offers valuable lessons for businesses of all sizes, emphasizing the need to invest in cybersecurity, engage in continuous risk assessment, and establish incident response plans to minimize the damage in case of a breach.

# V. Conclusion

The Target breach serves as a cautionary tale for organizations to take cybersecurity seriously, implement a proactive and layered security strategy, respond swiftly to alarms, and continuously adapt to evolving threats. The breach also underscores the importance of transparency, accountability, and learning from past mistakes to improve security and maintain customer trust.

# VI. References

1. Meeuwisse, R. (2017). Cybersecurity for Beginners 2nd Edition: Case Study -bTarget 2013.

2. Kerbs, B. (2015, September 21). Kerbs on Security. Inside Target Corp., Days After 2013 Breach.

3. Kassner, M. (2015, February 2). ZDNET. Anatomy of the Target data breach: Missed opportunities and lessons learned.

4. Plachkinova, M., & Maurer, C. (2018). Security Breach at Target. Journal of Information Systems Education, 29(1).

5. ChatGPT - For outline and grammar check.