# Target's 2013 Security Breach

Zyron Sumulong

Old Dominion University

CYSE 300: Introduction to Cybersecurity

Dr. Joseph Kovacic

May 21, 2023

In November of 2013, the Target Corporation's network was breached, resulting in stolen personal and financial data of millions of customers. Cybercriminals gained unauthorized access to Target's network through Fazio Mechanical Services, a third-party Heating, Ventilation, and Air Conditioning (HVAC) contractor. The contracting firm had network access to Target's system for maintenance and monitoring, but no proactive cybersecurity safeguards were in place. Manworren et al. (2016) states that Target's main cybersecurity vulnerability was its failure to segment its network to ensure that third-party vendors did not have access to their point-of-sale systems. As a result, the cybercriminals were able to gain access to the connection between Fazio Mechanical Services and Target, by compromising a contractor's credentials. This allowed them to access Target's point-of-sale systems and steal customers' personal information. The cybercriminals then installed point-of-sale malware known as BlackPOS. The malware is a form of memory scrapper that takes a chunk of a system's memory and looks for credit card numbers (Shu et al., 2017). This exploited Target's vulnerabilities, allowing the cybercriminals to steal credit and debit card information from customers that shopped at Target. The security breach emphasized the need for efficient cybersecurity measures to mitigate any repercussions or potential threats.

Target's cybersecurity breach had a detrimental effect on the corporation by damaging its reputation and losing its customer's trust. 40 million credit card numbers and 70 million personal records were stolen. Unfortunately, the stolen financial and personal information was sold on the black market. Customers and banks have filed more than 90 lawsuits against Target for negligence and compensatory damages (Manworren et al., 2016). The company faced financial losses, including a decline in sales and dealing with legal settlements and fines. In 2015, Target

agreed to provide $10,000 in relief to customers and a $20.25 million settlement with banks and credit unions regarding the security breach.

Six months before the cybersecurity breach, Target seemed to be prepared for the attack. The company had installed a $1.6 million malware detection tool. This malware detection tool was designed to send automated warnings when it detected malware. Target was warned about the occurring cyberattack, but Target failed to respond to these warnings(Manworren et al., 2016). Various cybersecurity measures could have been implemented to mitigate the consequences of the security breach. Implementing network segmentation, regarding their point-of-sale systems, would have created a barrier for attackers, making it more difficult for them to access their systems. Increasing cybersecurity awareness training throughout the company would have ensured employees would be capable of identifying and reporting suspicious cyber activity. It is significant for any company to implement effective cybersecurity measures to identify, monitor, detect, and mitigate any potential cyber threats within their systems.

The Target security breach of 2013 emphasized the need for efficient cybersecurity measures to defend against any potential threats. It exposed vulnerabilities in network segmentation, network security, and monitoring systems. The security breach affected a massive number of customers resulting in, damaging Target's reputation, leading to a decline in sales and a loss of customers trust. This incident led many companies to reevaluate their cybersecurity measures and implement stronger safeguards to protect against similar attacks. After the incident, Target spent 100 million dollars on enhancing Target's security measures, by upgrading point-of-sale machines, upgrading network segmentation, and enhancing monitoring and threat detection systems (Shu et al., 2017).

The need for effective cybersecurity measures will continue to grow as technology continuously develops. Cybercriminals will find new ways to conduct their malicious activities. Organizations must prioritize their cybersecurity within their systems, to defend and protect against any potential cyber threat.

## References

Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons*, *59*(3), 257–266. https://doi.org/10.1016/j.bushor.2016.01.002

Shu, X., Tian, K., Ciambrone, A., & Yao, D. (2017). Breaking the Target: An Analysis of Target Data Breach and Lessons Learned. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.1701.04940