

Target 2013 Security Breach

Student Name: Zack Fok

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Instructor Name: Diwakar Yalpi

Date: 4/21/2026

In terms of a large-scale cyber incident, there is probably no other single security breach in retail history that is as significant as the Target data breach of 2013 from a consumer perspective; the breach exposed the personal and financial information of more than 40 million customers. The breach was accomplished by using access to an HVAC contractor to target systems that were poorly secured due in part to the lack of segregation in network security. While the breach involved some technical vulnerabilities, it also involved several human and organizational vulnerabilities; therefore, it is a perfect situation on which to examine cyber security from a social sciences perspective. From a psychology perspective, the Target breach reflects how cognitive biases and human errors contribute to cyber security failures. Employees and vendors alike frequently incorrectly assess risk before they are committing a security failure or unintentionally fail to follow security policies and procedures to save time or because they do not understand the risk involved. Social engineering methods, such as phishing exploits trust and authority, two traits that are part of human behavior. From a sociology perspective, the Target breach also demonstrates systemic organizational concerns, including insufficient communications, inadequate accountability, and lack of a security culture. Target received multiple alarms from its security programs prior to the breach occurring, but failed to respond in a timely manner, which indicates a disconnect between the technical staff and the decision makers. Additionally, the reliance on third party vendors demonstrates how cyber-ecosystems create shared vulnerabilities due to the interconnectedness of all organizations in a digital marketplace. From an anthropology perspective, the Target breach provides insight into social attitudes regarding cyber security. To create successful and effective outcomes in an organization, the required solutions should combine both technical and social methods. Examples of technical improvement within an organization would be network segmentation, multi-factor authentication, and continuous monitoring systems. Socially, investment into training programmed focused on human behavior for example, recognizing phishing attempts and understanding perceived risk of cyber attacks is needed. Building a strong cybersecurity culture requires active participation from leadership making “Cybersecurity a priority” by ensuring clear lines of communication and accountability audits and compliance with these requirements. Unfortunately, some obstacles are present to

organizations when implementing these changes within their organizations. Examples of obstacles include resistance to change, lack of funding and lack of knowledge of what is required. To effectively overcome these obstacles it is essential for organizations to have buy-in from their leaders, to demonstrate the financial consequences of experiencing a breach and to integrate Cybersecurity in every day business practices and not as a separate, stand-alone function. This case demonstrates the requirement of combining Cybersecurity with social sciences. Technical solutions alone are not enough to stop Cybersecurity attacks because there needs to be a method of also changing human behavior, and modifying the organization's culture. A thorough understanding of an individual's psychological tendencies, social structures and cultural values will allow for the creation of a strong, effective and comprehensive Cybersecurity strategy. A combination of approaches will reduce vulnerabilities within an organization and will promote long-term resilience towards Cybersecurity attacks.

Citations:

Steinberg, S., Stepan, K., Rattray, G., & Healey, J. (2021). *Target cyber attack: a Columbia University case Study*. Columbia University. <https://www.sipa.columbia.edu/sites/default/files/2022-11/Target%20Final.pdf>

A "Kill Chain" Analysis of the 2013 Target Data Breach. (2014).
<https://www.commerce.senate.gov/wp-content/uploads/media/doc/2014%200325%20Target%20Kill%20Chain%20Analysis.pdf>