Name: Justin Cotman
School of cybersecurity, Old Dominion University
CYSE 201S: Cybersecurity and Social Sciences
Instructor name: Diwakar Yalpi
Date: 5/6/26

Introduction

Over 40 million customers' financial and personal information was compromised in the Target data breach in 2013. Through a third-party HVAC vendor with lax security access, attackers gained access to the network. Because access controls were unable to halt them, they traveled between internal systems. Employees failed to act quickly enough when suspicious activity was identified by security tools. This example demonstrates how human choices impact cybersecurity lapses.

Analysis

To comprehend this breach, you must look at human behavior. Due to alert fatigue and inadequate risk assessment, workers disregarded or postponed responding to security alarms. According to Verizon, over 70% of security breaches occur due to human mistake. Teams' inability to communicate and follow security policies was another organizational issue that raised risk. Attackers have increased opportunities as a result of budget decisions that decreased expenditure in vendor supervision, monitoring, and training.

Social science viewpoints show why the attack was successful. Stress and information overload can cause employees to pay less attention during security situations. I know when i'm stressed I tend to get off track or can't stay focused

Solutions

Technical controls should be combined with human-centered actions. Configure automated threat detection to lessen the need for human assessment. Enforce stringent permissions and restrict vendor access to just systems that are necessary. Employees should regularly practice responding to alarms and phishing. Monitor reaction times and hold teams responsible for alarms that are missed.

Stronger accountability and leadership procedures are also necessary for companies. Security reports should be reviewed by managers, who should also react fast to high-risk alarms. Cybersecurity teams, executives, and outside vendors must communicate clearly with one another. Policy compliance and cybersecurity duties should be included of employee performance appraisals. These activities raise awareness and strengthen workplace security practices.

Reflection

This example demonstrates the need for both technology and social science expertise in cybersecurity. Because authorities neglected to impose more stringent controls and personnel disregarded warnings, technical defenses were unsuccessful. How weariness and stress impair focus during security events is explained by psychology. Sociology demonstrates how weaknesses in security procedures are caused by poor corporate culture and inadequate communication. Studying how people act, speak, and react under duress might help you improve cybersecurity.

References

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, 2(2), 121–135.
Verizon. (2023). *Data Breach Investigations Report*. Verizon Enterprise.