Target (2013) – Breach Summary Case File

Background

Target Corporation, one of the largest retail chains in the United States, experienced a major data breach during the 2013 holiday shopping season. The breach resulted in the theft of tens of millions of customers' credit and debit card information, as well as additional personal data. This incident remains one of the most well-known retail security breaches in history and has had a lasting impact on how consumer data is handled.

Narrative of the Incident

The breach was initiated through a third-party HVAC (heating, ventilation, and air conditioning) contractor that had remote access to Target's network for billing and monitoring services. Cybercriminals used stolen credentials from this vendor to gain a foothold in Target's systems.

Once inside, the attackers installed malware on Target's point-of-sale (POS) systems. The malware was designed to capture payment card data directly from memory during transactions. The attackers used this method to harvest the magnetic stripe information of approximately **40 million credit and debit card accounts**.

Additionally, it was later discovered that personal information (such as names, mailing addresses, phone numbers, and email addresses) of another **70 million customers** had also been accessed.

The attack reportedly began in mid-November 2013 and went undetected until mid-December. Target was alerted to suspicious activity by its security monitoring tools and external partners but failed to act on the alerts in a timely manner.

Consequences and Impacts

- **Massive data exposure**: Sensitive financial data and personal information for over 100 million customers was compromised.
- **Financial cost**: Target faced over **$200 million** in costs, including legal fees, credit monitoring for affected customers, and upgrades to their cybersecurity infrastructure.
- **Reputational damage**: The breach severely damaged consumer trust and resulted in public backlash.
- **Leadership changes**: The CEO and CIO resigned in the months following the incident.

- **Industry impact**: The breach accelerated adoption of EMV chip technology in the U.S. and led to greater scrutiny of third-party vendor security practices.

Reflection Questions

As you review this case, consider:

- How did the attackers gain access to Target's systems?
- What were the key weaknesses in Target’s network and response processes?
- What role did vendor relationships play in the breach?
- What types of data were exposed, and how might this affect consumers?
- What lessons can be drawn about internal monitoring and third-party risk management?
- Which aspects of the CIA Triad were most affected?

Use this narrative as the basis for your Lab 2 CIA Triad analysis. You are encouraged to cite specific parts of this case file as evidence in your report. You should also go beyond this narrative and seek additional information about this case from reliable external sources, as it is a well-documented cybersecurity attack.

The Target breach illustrates how even indirect access to a corporate network can lead to catastrophic consequences when proper segmentation, monitoring, and response procedures are not in place. It underscores the importance of holistic risk management, not just technical controls.