Case Analysis
Autopsy of a Target Breach: The Target Case

Mason Tatafu
CIS 410
02/23/2025

Introduction

Target is a big store that people shop at all over the country. It sells all kinds of things like clothes, electronics, and food. Lots of people use credit and debit cards to pay, so Target has to keep their payment info safe. But in 2013, Target got hacked. Hackers stole credit and debit card details from over 40 million customers. They also got names, emails, and phone numbers from 70 million more people.

The hack wasn't super fancy, it happened because of a simple mistake. Hackers got into Target's system through a weak spot in another company that worked with them. Once inside, they put virus software on the checkout machines, which let them steal customer info while people paid. Target's security systems noticed something was wrong, but nobody stopped it in time. Because of that, things got way worse than they should have. This caused big problems for customers, banks, and Target itself. This case looks at how it happened, what went wrong, and how it could have been prevented.

Current Situation Analysis

Target's biggest mistake was not keeping customer data safe. Hackers got into the system by using login details stolen from a company that worked on Target's air conditioning. Once inside, they put virus software on the checkout machines, which stole credit and debit card info when people paid. The attack went on for weeks before anyone noticed.

Even though Target had security systems, they didn't work well because the company was too slow to react. The security software noticed something was wrong early on, but Target didn't do anything right away. If they had acted faster, the damage could have been much smaller. Instead, millions of people had their information stolen, leading to lawsuits, lost money, and customers losing trust in Target.

Industry and Competitive Analysis

As a major retailer, Target operates in a highly competitive landscape alongside Walmart and Amazon. Customers expect seamless shopping experiences, both in-store and online, with a strong emphasis on security. A failure to protect customer information can drive shoppers toward competitors that are perceived as safer.

Competitive Landscape

The retail business is tough, and a security mistake can hurt a company. Online shopping has made things even harder, so keeping customer info safe is super important. If people think a store isn't safe, they can just shop somewhere else. Also, companies that work with outside vendors need to make sure those vendors have good security, because a weak spot in one system can mess up everything. More people are using digital payments like Apple Pay and Google Pay instead of regular credit cards, so stores have to make sure their payment systems are extra secure.

Internal Security Challenges

Target had the tools to stop the hack but did nothing. The system sent warnings but nobody fixed the problem. This showed how bad Target was at handling cyber threats. Because they ignored it, a small issue turned into a big disaster.

Who Was Affected

Customers

People who shopped at Target got hit the hardest. Hackers stole their credit and debit card details, which meant they could take their money. Also, names, phone numbers, and emails got leaked, making it easier for scammers to trick them. Lots of customers had to cancel their cards, keep checking their bank accounts, and stress out about their private info being out there.

Banks & Credit Card Companies

Banks and credit card companies had a big headache. They had to send out tons of new credit cards and give people back their stolen money. This cost them a lot. Because of this mess, banks had to get better at spotting fraud and keeping customers safe from scams.

Target Employees

This was bad news for Target's workers, especially the ones in IT and security. The company ignored warning signs before the hack, so when everything went wrong, people blamed the security team. Some got fired, some had to fix the problem, and customer service workers had to deal with thousands of angry shoppers. Even big bosses at Target had to quit because of how badly the company handled the whole thing.

Investors

People who owned Target stock saw their investment drop in value. Lawsuits, refunds, and fines cost Target a lot of money. Investors got worried that customers wouldn't trust the store anymore, which could mean fewer sales. All this made them nervous about Target's future.

Government & Regulators

After the breach, government agencies started looking into what went wrong. They wanted companies like Target to do a better job of protecting customer data. Because of this, new rules were made to force businesses to take cybersecurity more seriously so this kind of thing wouldn't happen again.

Third-Party Vendors

One of Target's outside vendors, an HVAC company (they do heating and cooling), got hacked first. The hackers used their login info to break into Target's system. This made people realize that even outside companies can be a weak spot in security. After this, businesses had to be way more careful about who had access to their networks.

Exploring Different Solutions

Stricter Vendor Security (Best Option)

The attack stemmed from weak security in a third-party vendor's system. Target could have prevented this by enforcing stricter security policies, including multi-factor authentication, limited network access for vendors, and routine security audits. Had these precautions been in place, the hackers may never have gained access.

Faster Intrusion Detection and Response

Security tools detected the attack early, yet Target failed to act. A rapid response system that immediately isolates threats and alerts key personnel could have contained the breach before

customer data was stolen. Implementing an automated security framework would ensure that future threats are addressed the moment they arise.

Employee Cybersecurity Training

Another failure in this case was the neglect of security alerts. Employees may not have fully grasped the severity of the warning signs, delaying intervention. Regular cybersecurity training would equip employees with the knowledge to recognize threats and respond swiftly. While training alone would not have stopped the attack, it could have played a role in minimizing its impact.

Recommended Course of Action

Target's failure to respond to security alerts was its most critical mistake. To prevent similar incidents, the company must strengthen its cybersecurity approach. Vendor security needs to be a top priority since the breach originated from weak external access controls. Stricter authentication measures, limited vendor access, and regular security audits should be mandatory.

Additionally, Target must ensure that all security alerts are addressed immediately. Any detected threat must prompt immediate action rather than being ignored. Cybersecurity should be a core focus at every level of the company, not just an IT concern. Having security systems in place is only effective if they are properly managed and acted upon.

Conclusion

The Target data breach was entirely preventable. Hackers exploited weak security in a third-party system, deployed malware on payment terminals, and stole millions of customer records. Despite having security tools that flagged the intrusion, Target failed to act in time, allowing the situation to worsen.

This case demonstrates why companies must take cybersecurity seriously. Security tools alone are not enough—they must be used effectively. Vendor security must be tightly controlled, security alerts must be addressed without delay, and employees must be well-trained in cybersecurity awareness. Had Target taken these steps, the breach might not have occurred. Businesses that handle sensitive customer information must make security their top priority to avoid severe consequences.