Case Study: The Target Case

Patrick Nguyen

University of Louisville

CIS-410-50-4252: MGMT OF INFO SYSTEMS

Professor Reindhart

February 23rd, 2025

Executive Summary

On December 13, 2013, Target experienced a significant data breach, leading to fraudulent debit/credit card transactions. This is one of two breaches that caused significant disruptions for the Target Corporation. Cybercriminals accessed critical systems through Target vendors, resulting in over 70 million compromised customers. The breach highlighted significant issues in Target's infrastructure, and it is important to mitigate the issue. To prevent future incidents, Target should adopt a system of standards to regularly audit vendor systems.

Introduction

On December 13, 2013, Target's management was notified of fraudulent debit and credit card transactions linked to the Target corporation. The U.S. Department of Justice shared this information, prompting an investigation into Target's systems. Target, as a result, hired forensic investigators, confirming their worst fears of a breach. This raises the question: How did Target respond to this breach? This case study examines Target's business issues, industry/competitive landscape, and key stakeholder groups. It also explores the impact of alternatives on stakeholders and determines the most effective solution.

Background on The Business Issue: The Target Data Breach

Breach #1:

Target's first breach occurred on December 13th, 2013. Representatives from the Department of Justice informed Target's management of fraudulent debit and credit card transactions linked to Target (Dubé, pg 1.). Target took the initiative to investigate the breach and hired forensic investigators. Upon investigation, it was discovered that cybercriminals hacked into U.S. Target's systems and stole data from 40 million debit and credit cards since November 27, 2013. As a result of growing pressure, Target announced the data breach, leading to an inundated call center and website (Dubé pg.1).

Importantly, this outlines some business concerns. The timing of this breach occurred during the pre-Christmas season including Black Friday. These are some of the year's busiest days, especially for companies like Target. That being said, Target's image suffered. The company was criticized for its failure to act on initial alerts, delayed publicity of the breach, and failed to give its customer service departments proper methods of response to customers. As a result, Target scored negatively in consumer protection in late December 2013. This view led to a 46% decline in profits and a 5.3% drop in revenue (Dubé, pg 5). To put it in numbers, Target's profits declined from $961 million to $520 million compared to the same period in the previous year. Although numbers were down significantly, Dubé did think it was important to address Target's expansion into Canada as a contributor.

Breach #2 and Relations to Breach #1:

The second breach outlined in Dubé's article occurred on January 10th, 2014 (Dubé, pg. 1). Not far off from the December attack. It reported that, in addition to stolen card information, hackers also breached personal identifiable information of over 70 million additional customers. Information breached includes names, mailing addresses, and phone numbers. According to CBC News, this troubled regulators and privacy watchdogs. Consumers trust companies to protect their personal information when shopping and these breaches divide Target and its consumers.

February 1st, 2014, Target reported that it had spent $61 million in response to the data breaches. However, this would soon be set off by over $100 million in cyber insurance, reimbursements to banks for cards, fines for non-compliance with PCI-DSS, costs of credit monitoring for consumers, years worth of legal battles, and costs of communication and customer management activities (Dubé, pg. 5). It is obvious that Target is in a bind. Reporters

estimate that this breach will exceed $500 million and has the potential to reach the $ 1 billion mark.

Many business issues have been presented including the data breach itself and financial loss. However, it is difficult to predict the long-term financial impacts involving the breach. Target faced over 140 lawsuits, each seeking millions back in damages (Dubé, pg. 5). One mentioned issue involves trust between the consumer and the company. One class-action suit accuses Target of violating several laws as a result of negligence. Their handling of customer data and waiting to publicly disclose the breach is a concern to consumers. It is believed that waiting too long increases the vulnerability of consumer data. Understandably, Target should have been more proactive about disclosing the issue. Furthermore, Target's negligence towards cyber alerts is unfavorable from a consumer standpoint.

A month after Target's damage report, the court divided the lawsuits into three groups: financial institutions, consumers, and shareholders (Dubé, pg. 5). The separation of stakeholders allows the court to address specific issues regarding the data breach. Financial institutions account for 29 of the suits and believe that Target should reimburse costs arising from the breach. Some of these costs include reimbursements for card issuance, customer relations, refunds for fraudulent transactions, and more.

Industry and Competitive Analysis

Mission:

As stated, Target is a well-known corporation in the United States and a favorite among communities worldwide. According to Target, its mission is to help families discover the joy of everyday life. This brings purpose to the organization, driving business decisions and ensuring

positive experiences for customers. Target's business model is one foundation built to serve current and future guests, team members, vendors, and much more. Target is committed to that regardless of how the environment evolves around them. It guides their purpose, and team culture of caring, growing, and winning.

Stakeholder Groups

1. **Customers:** Direct victims of identity theft in the Target Data Breach case. Many of these customers likely experienced emotional distress along with inconvenience, and financial losses. The breach occurred during the pre-Christmas shopping season and included Black Friday. About 40 million victims were discovered during the December breach which increased to 70 million when PII was leaked in the next.
2. **Financial Institutions:** Banks incurred substantial costs as a result of this breach. This resulted from the issuance of new cards to victims of the Target Data Breach. The number of cards affected was more than what banks could handle. Strict limits were placed on customers until new cards were issued. However, this does not address the financial and logistical challenges faced by these institutions.
3. **Target Executives/Board Members:** The result of this breach has affected Target executives and shareholders. On March 5th, 2014, Target announced that their Chief Information Officer resigned from their position. This person held that position since 2008. Interestingly, Target announced the new Executive Vice-President and Chief Information Security Officer, and Executive Vice-President and Chief Compliance Officer (Dubé, pg. 6). Target's goal is to centralize all security management activities that had been dispersed in different groups beforehand. Additionally, Target's CEO was let go

in May 2014. The board of directors was convinced that Mr. Steinhafel was not the right person to protect the firm's assets. This took a major toll on Target's leadership.

Porter's Five Forces:

Porter's Five Forces is one method for understanding the competitive forces in an industry. It serves as a framework including the topics below:

1. **Threat of New Entrants**

Target is one of the leading retail stores in the world. According to MBA Skool Team, the threat of new entrants is a weak force to Target. Companies entering this industry would need to achieve economies of scale to compete. Furthermore, new entrants would need to have the knowledge base and similar business practices to compete. Target has the tools to gain a competitive edge in the market that new entrants do not have. Furthermore, industry investment costs are huge and barriers to entry are high. That being said, new entrants would have to acquire all licenses and follow the legal requirements before entering this industry. This includes but is not limited to business licenses, registering your business, insurance, and even compliance with cybersecurity standards (PCI-DSS). Even in compliance with security standards, new entrants should understand there is always a risk to information security. Target did work to strengthen its infrastructure, but that doesn't mean it would not happen again.

2. **Bargaining Power of Buyers**

Target consumers are thought to fall in the "esteem" category of Maslow's Hierarchy of Needs (Abdurakhmonov, pg. 3). This is defined as looking for superiority, self-respect, status, and prestige, according to Abdurakhmonov. Target needs to maintain and offer good quality products at a reasonable price. Target will need to study changing preferences and spending patterns to keep up with consumers. That being said, Target's bargaining power for consumers is

high. The number of substitutes is on the higher spectrum, meaning customers can easily switch to a different retailer. Most companies supply the same or similar products, making it easy for them to switch. Overall, price sensitivity is a key factor in maintaining buyers along with ensuring the security of trust with their data.

3. **Bargaining Power of Suppliers**

According to Akbar Abdurakhmonov, Target's Cost of Goods Sold was 71% of total sales in 2019. That being said, he uses this as a great indicator of the dependability of Target on the products delivered to suppliers. Despite the dependability, he describes it as a weak force. To begin, it is argued that the number of suppliers in the industry is large, meaning that suppliers have less control over prices. Another point made involves the variety of products for sale. Target has a diverse set of suppliers, and Akbar found that no single supplier is responsible for over 5% of the company's total sales. This is favorable for Target.

The information is useful in strengthening Target's Bargaining power of suppliers. However, their Vendor was an attack vector in this data breach. This ultimately weakens the bargaining power of suppliers. It shows that Target will need to do more research into who they are taking in as vendors. Fazio Mechanical served as Target's HVAC Firm vendor. They had remote access to Target's network for electronic billing, contract submission, and project management. Cybercriminals obtained their login credentials through phishing emails. As stated, Target will need to be more mindful of their vendor's security practices.

4. **Threat of Substitutes**

The threat of substitutes with Target can be seen as moderate to high. Products sold by Target are easily substitutable. Competitors like Walmart, Amazon, and other brick-and-mortar stores make it easy for consumers to find similar products, especially Amazon. Target is also

known for e-commerce. In regards to cybersecurity, Target has made improvements to its systems. Before the breach, Target was working on adopting Chip-and-Pin technology, which enhances security and reassures customers that their financial information is better protected. However, the Target breach makes other competitors more attractive to consumers, which is understandable.

5. **Industry Rivalry**

The retail industry is an ever-growing industry that attracts investments from national and international investors (MBA SKOOL). It can be an intense sector for sure. Target competes with retail stores such as Walmart, Amazon, and Costco, all of which have strong brand recognition. To maintain a competitive edge, companies invest in variety and issue competitive discounts to consumers. Various promotional campaigns, new technology, and improved e-commerce platforms are also used for a competitive edge. However, Target's past data breach does pose some issues with industry rivalry. The financial costs associated will make it difficult for Target to invest in promotional advertisements. Furthermore, the breach has created a sense of distrust among consumers. This in and of itself will make customers shop at rivals within the industry.

Target's Attempted Solutions

Target's initial reaction to this breach was not great for public appearance. There is sufficient evidence that Target ignored signs regarding the breach. Target is generally known as being well-protected from this common attack and is even considered to be one of the retail leaders in cybersecurity. Defense in Depth includes segmentation, firewalls, malware detection software, intrusion detection software, and plans for data loss. Even internal/external audits perform regular tests on all of Target's security measures (Dubé, pg. 3). Furthermore, Target was certified as being compliant with PCI-DSS, which establishes the minimum levels of security for

merchants. However, one hiccup in Target's vendor made it easy for threat actors to exploit Target's systems. Target was well prepared for this, but it's clear they need to review which vendors have access to what.

Recommended Solution

Target itself seemed suited to take on a common attack like this, so it seems that security across vendors needs to be enhanced. As a result, Target should work to ensure vendors are following proper security protocols while accessing the Target network. Here are a few solutions:

1. Strengthening Vendor Management and Security Protocols

The first approach for Target involves placing stricter security requirements on third-party vendors. Target would implement security frameworks by enforcing compliance with industry standards along with security clauses in their vendor contracts. Importantly, standards require or address security awareness. This was one critical factor in Target being breached in the first place. The overall goal is to ensure vendors are meeting baseline standards before retrieving access to critical infrastructure.

Customers: This approach ensures that vendors are following a higher security standard, which, overall, improves the security of the supply chain. Customer data would be more secure, decreasing the risk of exposing sensitive data. It could pose some issues for customers in the sense of delays in service and product availability, as a result.

Financial Institutions: Financial institutions benefit greatly from reduced risk of exposure. This solution improves vendor security practices and can lead to stronger protection of financial data. Interestingly, it is something for financial institutions to learn from too. Target's requirement to vendors may require financial institutions to take on additional measures also.

Target Executives/Board Members: Leadership in Target took a huge hit as a result of this breach. This demonstrates that executives are taking the appropriate actions to enhance security and mitigate security issues. Overall, it has the potential to diminish reputational damage and financial loss.

2. **Conducting Risk Assessments on Vendors with Regular Audits and Training**

In addition to Target's security audits, they would implement a system of regular audits and training for their vendors. These would occur at set times of the year and would assess the internal and external environments of vendors.

Customers: This solution has similar benefits to alternative 1. However, customers gain confidence knowing that Target's vendors have a great security posture. Again, this would more than likely cause disruptions with vendors.

Financial Institutions: Like alternative 1, financial institutions would be reassured that Target's vendors are maintaining a great security posture, decreasing the likelihood of a data breach.

Target Executives/Board Members: This option offers top leadership the ability to report vendor-related risks. This is a pro to alternative 1 as reports are continuous. It is implied that the vendor should be following baseline standards anyway.

3. **Segment and Isolate Vendor Connections**

Target could enhance network security by segmenting and isolating vendor connections if compromised. This ensures that malware does not spread to other critical infrastructure on Target's network. That being said, this involves strict access control and monitoring to ensure vendors access what they need for their system. Alerts were initially sent out, but Target chose to ignore them.

Customers: Alternative 3 heightens protection, creating better security for customers. Segmentation ensures minimal spread of malware. It is important that this may cause disruptions in vendor services.

Financial Institutions: Overall, this reduces the risk for financial services. It works to contain and reduce the chance of attacks on financial data, protecting Target, and financial institutions.

Target Executives/Board Members: Top leadership can expect to see a strong containment strategy with alternative 3. It offers a clear strategy and limits damage, ensuring protected operations. However, it would require a significant financial contribution from Target. The breach has already allocated millions to lawsuits and fines, making this a questionable alternative.

Choosing a Solution

Based on the information given, solution 2 is best. Conducting audits should be a normal procedure in any company, especially in the cybersecurity sector. While Target conducts regular audits and security testing of its systems, its external partners must do the same. Having a great security posture is important, especially if you handle confidential data daily. The incident in Fazio Mechanical was something easily preventable. Something as simple as teaching a class. This incident violated all sides of the CIA Triad. Confidentiality of customer data was exposed, systems were modified, and information was made available to dangerous actors. Solution 1 is great but it is baseline. It encompasses standards and training, but it lacks monitoring of systems for Target. Alternative 2 encompasses monitoring but it's implied to contain the given standards. Alternative 3 is a great choice, but could be expensive for Target. This company has suffered many financial losses and it would be tough to implement.

Conclusion

In conclusion, the Target data breach serves as a reminder that even well-established companies are at risk. Target's significant investments in its cybersecurity infrastructure proved well from its point of view. However, their lack of security in vendor management led to financial and reputational damage. Moving forward, Target can implement better solutions for ensuring the confidentiality, integrity, and availability of consumers, financial services, and its systems.

Works Cited

Akbar Abdurakhmonov. “Five Forces Analysis of Target Corporation.” *ResearchGate*, 21 Apr. 2019, www.researchgate.net/publication/333245579_Five_Forces_Analysis_of_Target_Corporation.

CBC. “Target Data Hack Affected 70 Million People.” *CBC*, 10 Jan. 2014, www.cbc.ca/news/business/target-data-hack-affected-70-million-people-1.2491431. Accessed 24 Feb. 2025.

Dubé, Line. *Autopsy of a Data Breach: The Target Case*. Vol. 14, no. 1, 1 Mar. 2016, pp. 1–8. *HEC Montreal Centre for Case Studies*.

Team, MBA Skool. “Target Porter Five Forces Analysis.” *MBA Skool*, 23 Apr. 2022, www.mbaskool.com/five-forces-analysis/companies/18381-target.html.