BCIS 5740

Information Security Management Assignment 5 The Case Study of Target Corporation - Data Breach

Bagam, Phani Priya

**Target Corporation – Data breach**

# Introduction:

Target Corporation is the second largest retailer in the United States of America. It has stores in all 50 states of the USA.75% of the population in the USA lives within 10 miles of a Target store. Target Corporation is a component of the S&P 500 index. Target was established in the year 1962 in Minneapolis. Target began to expand its store nationwide in 1980 as a part of the Dayton – Hudson Corporation. Later on, introduced new store formats under the Target brand in the 1990s. The Company was renamed Target Corporation in 2000. Target has nearly Target manpower is 450,000 as per the latest Annual report 2021. Target Corporation’s tagline is “Expect more. Pay less”. Gregg Steinhafel was the CEO of Target Corporation in 2013 and worked at Target for nearly 35 years.

# Data Breach in Target Corporation:

In 2013, Target Corporation the biggest retailer in the United States experienced a data breach. Target was informed about the data breach by law enforcement agencies. Target Corporation had announced that nearly 40 million credit and debit card details were stolen along with the personal data (names, telephone numbers, email addresses, home addresses) of 70 million customers. The breach occurred during pre-Christmas and Black Friday sales weeks. These are the busiest days of sales in the USA.

Target Corporation immediately eradicated all the software used by the hackers and announced a breach of data and theft of data. Target has alerted its customers by sending emails regarding the data breach. Target Corporation assured its customers that the software responsible for the data breach was identified and removed from the systems and networks of the Target Corporation, and the customers can shop at Target Corporation confidently. Target Corporation started the investigation by hiring experts to know the reasons and vulnerabilities that contributed to the data breach.

The data breach negatively impacted Target Corporation and severely damaged its reputation. Customer trust and confidence are important for any business. The data of 110 million customers were stolen in this data breach (40 million Debit/Credit Card details, 70 million personal records). Customer trust and confidence were lost due to the theft of records. Being a big retailer, investing huge amounts in securing their information assets Target Corporation was criticized for not protecting customer’s information from theft. Customers who shopped became victims and faced inconveniences. Target’s customer services also failed to respond to customers in time. The breach impacted Target Corporation Financials. Sales numbers fell by 10% in January 2014 as compared to the previous year (shopping by households in January 2014 was 33% this was down from 43% for the same month the preceding year). In the fourth quarter of 2013, earnings fell by 46% and sales were also down by 5%. As per Wall Street Journal, Target’s profit fell to $520 in the quarter ended February million from $961 million in the previous year. The Company’s revenue decreased by 1% from 2012 to 2013. The net income decreased 34.3% in the same period. The decrease in net income was attributable to costs of investigation and other costs of a security breach. The stock prices experienced a 10% loss. Target’s CEO, president, and chair of the Board who worked for 35 years in the company held himself liable for the data breach left his position. Target Corporation replaced its CIO and created a new CISO position. Institutional Shareholder Services had recommended investors remove the Board of Directors. The firm said the Board failed to protect the company from a breach of data. Target was also criticized for the delay in investigating the breach and notifying the agencies and customers. Various Agencies like the US Securities and Exchange Commission, FBI, Secret services, US Trade Federal Commission, and State attorney General opened inquiries on Target Corporation after the data breach. Members of Congress also expressed concern over the breach affecting customer’s private information. The data breach cost nearly 300 million dollars to Target Corporation. Out of which approximately 18.5 million dollars were paid to settle the investigations of 47 state governments. $39.4 million was paid to banks and credit unions for the loss and costs incurred due to the breach. Approximately, 90 million dollars was paid to Mastercard and Visa in 2015 and 10 million dollars was paid in a class action lawsuit to affected customers. In addition to the said payments, Target Corporation also incurred costs for legal fees, credit monitoring reports, and others. Target Corporation has reported the total cost of damage of $292 million in its 2016 annual financial report. Target faced more than 140 lawsuits for the data breach.

Due to Target Corporation’s data breach, Banks faced a lot of pressure. Many customers reported fraudulent transactions during the days of Pre-Christmas shopping. Banks could not cancel the debit/credit cards as it causes inconvenience to customers during that time. Banks put a daily limit of withdrawal/purchases on their customers to prevent unauthorized usage by hackers. After that, they had to issue new cards to the customers. After observing enormous calls of fraudulent transactions banks reported to the U.S Department of Justice, which informed Target Corporation, about a possible breach of their network. Target Corporation was issued a notice to conduct further investigation on the data breach. Target Corporation could not have detected the fraud without the banker’s complaint about fraudulent transactions. Bankers claimed the costs from Target Corporation for reissuing the cards to their customers. The ultimate sufferers were the customers who shopped at Target Corporation. Though banks canceled and re-issued credit/debit cards the customers faced inconvenience and incurred fines and penalties for payments that they missed due to the cancellation of credit cards. The major problem faced by any organization in such data breaches is the loss of customer loyalty and the trust of people. Target corporation nearly lost 10 % of its loyal customers immediately after the theft of information. Due to heavy losses, Target Corporation laid off about 400 employees and could not recruit new personnel during the 2014-15 financial year. The incident has also impacted employee morale.

## Data breach – what happened?

As per the forensic investigators, the hackers accessed the Point-of-sale network of Target Corporation and successfully installed malware in all the terminals. Through the installed malicious software, the hackers captured the data when the customers swiped their debit or credit cards for payment. The hackers exploited the vulnerabilities in Target’s security systems, and they had stolen the details of customers.

## Data breach - How Did intrusion happen?

The attackers used the credentials of the Fazio Mechanical Services contractor, who has access to Target’s network for billing and submission of contracts. The hackers were able to obtain the credentials of an employee working in Fazio Mechanical Services. The hackers sent a phishing email to Fazio Mechanical Services and the employee responded to the email without knowledge of the consequences. This gave hackers a chance to enter Target’s network and reach the payment system network and point of sale systems. Experts believed that the hackers used Citadel malware to steal login credentials from the system. Fazio Mechanical Services claimed that it complied with security practices to safeguard its information assets. In reality, Fazio Services used a free version of Antimalware software which could not provide real-time protection.

Various experts also analyzed the breach in Target Corporation and some of them opined that the attackers might have exploited the vulnerabilities in the web application with SQL injection, and XSS to gain access and attack internal systems. As per the iSGHT Partners Reports the code-named Trojan, and POSRAM were used for infecting Target’s Point-of-sale systems. The Ram-Scrapping feature of POS malware copies Debit/Credit information from the memory of the POS devices when the card is swiped. The malware used in the breach was BlackPOS. Being the biggest retailer, Target had invested a large amount of money in security systems and IT infrastructure. In September 2013, Target Corporation was certified for meeting PCIDSS standards. Payment Card Industry Data Security Standard is an international standard that sets controls created to ensure that all the companies that accept, store or transmit credit card details maintain a secure environment. According to Bloomberg article, a malware detection tool FireEye was present in Target’s systems and sent an alarm about the intrusion of hacker’s malware but was unnoticed.

## What was the purpose of the intrusion?

The reason for hacking Target Corporation was Identity theft which is to steal the personal information of the customers. The hackers had successfully stolen the credit/debit card details of customers and sold them on the black market to those who make fake debit/credit cards. According to investigators, these credit and debit cards can be used to buy gift cards from major retailers and converted into cash.

## Who was affected by the data breach? – Personal relevance.

My brother was a regular customer of Target Corporation. In early 2014, he identified a fraudulent transaction. He got a message from a credit card company about the purchase of an item worth $500. He immediately informed the credit card company and blocked his card for stopping further usage of the credit card. He notified the fraudulent transaction to the company immediately and disputed for a refund of money. The credit card company issued a new credit card within one week and refunded the money from the fraudulent transaction.

Everything seemed good till he was charged a penalty for missed payments during the process of issuing a new credit card. He experienced a lot of inconveniences as he needed to update his credit card information for all the billing accounts like utility bills, internet service payments, cell phone services, gym membership, and others. He was charged penalties one after another for missed payments and was unable to update new credit card information for making all the auto payments due during the month. Though the credit card company refunded the wrong transaction, he incurred nearly $150 as late charges for missed payments. It was an embarrassing moment for him. He was getting calls all the time about the declining transactions. If he had missed payments for another month, it would have negatively impacted his credit score. The data breach similarly impacted a lot of customers. This type of data breach makes the customer hesitate to shop. My brother had stopped shopping at Target and other online purchases using credit cards immediately after the incident. He was forced to use cash and cheques for most of the transactions to avoid payment through credit and debit cards.

## Personal Opinion about the breach:

The data breach in organizations impacted many customers. Like most customers, I may also be the victim of a data breach. The data breach may affect everybody as we use debit/credit cards for purchases and share our information with various organizations for obtaining various services. Organizations usually store the data of their customers. Data theft involves identity theft. The personal data stolen may be utilized for illegal activities. Then the problem will be severe as we need to prove our identity and report the theft of personal identity. Financial transactions may be disputed if they are fraudulent but misuse of personal information for illegal activities by hackers is worrisome and makes us liable till proven innocent.

In the case of identity theft, the issue needs to be reported to the concerned authorities and needed further investigations which are time taking and involve financial costs and stress. However, data breaches have become part of everyday business.

# Characteristics/aspects of information security that were affected by the breach:

Confidentiality, integrity, and availability of data (CIA) guide policies for information security within an organization. Confidentiality limits the right of entry to information means it ensures only users with rights, and privileges have access to data. Integrity provides a guarantee that transmitted data can be trusted and availability makes data available to the relevant people. The Target breach was the loss of confidentiality as credit card information of customers was stolen by hackers. However, if we observe the cause it was an attack on the integrity that is a compromise of the database configuration and security layer component. Malware and viruses are integrity attacks, that compromise the integrity of the system.

## Information security protection measures:

One of the security control measures that could have prevented the breach was employee security training. This control would have combated the attack. Target Corporation would have brought awareness to employees about the consequences of sharing too much information with outsiders. Failure to respond to FireEye alerts by employees shows the lack of training and expertise among employees. Target Corporation would have used the services of outside professionals to access its vulnerabilities. The experts were aware of the software that could be used to collect the credit card information but none of the employees were aware of this.

Another Security control measure that would have been in place was the Malware defense. These controls would have eliminated the risks that arise with company-vendor interactions. Control access is another security control measure that would have been useful in preventing the attacker’s entry and subsequent exploration into Target’s network.

Segregation of network: There should not have been a route between a network for an outside contractor and the payment data of the organization. Target Corporation would have determined the level of access the third-party vendors should have and limited the access to the network.

Account monitoring and control would have taken care of the vulnerabilities accompanied by faulty domain controllers. Secured configuration for Hardware and software on Mobile devices, Laptops, Workstations, and servers would have prevented intrusion and exploitation of systems.

# Contribution to the breach - Communities of Interest:

A community of interest is a group of people who share a common goal to achieve organizational objectives. The three communities of interest of a business are Organizational Management, Information security Management and Professionals, and Information Technology Management and professionals. The job of information security Managers and professionals is to protect an organization’s information system and stored information from attack. The focus of Information Technology management and professionals is system operations and the cost of creation of systems, making technology used in the organization user-friendly that is they are more concerned about ease of operations. General Management consists of production management, human resources management and accounting, and other legal departments. This group is concerned about the goals of the organization. Target created a new CISO post after the data breach till then CIO was responsible for both information technology and information security aspects. The management had only concentrated on the expansion of their business.

Three communities of interest are responsible for the information security of the organization as it impacts the business. Information security management personnel should take care of all intrusion detection and prevention systems to protect the integrity of the systems and bring awareness about security measures among employees. Information technology personnel should take care of all hardware and software-related issues for the smooth running of business activities. The ultimate responsibility of information technology and security vests with general management which is responsible for overall business activities. The Management should oversee information technology and security-related issues After the data breach, the CEO was ultimately made responsible and had to leave the position.

The Management which is responsible for the overall organizational activities should clearly define the roles of information security management and information technology management and arrange for security checks and audits from outside agencies for assessing the vulnerabilities which can be exploited by hackers. By not following the above aspects the company failed to prevent the breach.

## organization's business and security needs:

In my opinion, sometimes an organization’s business needs and security needs collide. Business needs always win over security needs. The management is always concerned about revenues and profits. The goal of every business is earning a profit, organizations cannot survive without profits. Companies always try to protect their information. Sometimes, the demand for quick access to data leads to compromises with security. Having proper security controls, if the data is not accessible quickly according to business needs, the business cannot function. Like any other business function, information security is also driven by the analysis of cost, and benefit. The management has to take decisions and balance costs, benefits, and risks for making the information accessible to authorized users.

# Role of the Security Policies in avoiding the data breach:

EISP, Enterprise Information Security Policy, is a high-level information security policy also known as an organizational security policy. It is a top management level document, written by CIO, that details the company’s philosophy on security. EISP defines the purpose, scope, and applicability of the security program. It defines the structure of the organization and identifies the people responsible for information security. This policy would have prevented breach as it clearly defines the roles and responsibilities for the protection of information assets and disciplinary actions for failure to protect.

ISSP, Issue Specific Policy, addresses the specific areas of technology. It addresses issues like the usage of email and the use of the internet. ISSP clearly states the authorization for access to information and usage of the resource. This policy could have prevented breach as it clearly limits the access of the resource and defines the necessary care to be taken for accessing and using resources.

SysSP, System Specific Security Policy, functions as standards or procedures used for configuring or maintaining systems. SysSPs include Access Controls Mechanisms. Access controls define who may use the resource and how. Proper access controls if placed would have prevented the breach at the target corporation. It would have limited full access of vendors to a network of Target Corporation.

# Incident Response

The target corporation failed to detect and prevent a breach. It would have used intrusion detection and prevention systems to the prevention of breaches. The Target Corporation could have reacted immediately and alerted the customers about the breach. The company responded after the breach and took all the measures to remove malware from the network and the information assets.

## Information Security Plan:

The Information Security plan is planning for achieving information security objectives. The policy places an important role in the information security plan. System Specific Security policy is suitable for Target Corporation. The important aspect of planning is to protect confidentiality, integrity, and availability of the information. The first step in the plan is to prioritize the information and its assets. Evaluation of security risks and vulnerabilities. Identifying the preventive measures. Risk analysis, assessment, and management. Determining the standards, disaster recovery, and incident response plans and management (whom to inform when an incident is reported). The Framework includes the above-mentioned activities and clearly defines the roles and responsibilities of the employees for the protection of information assets and information.

System-specific policies like access controls for access to information systems, services, and assets will be clearly defined to prevent unauthorized access. Users will be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords. A clear policy for the usage of storage devices will be implemented.

## Potential consequences of the Data breach

The data breach negatively affected Target Corporation. The potential consequences are as follows:

Recovery Costs

Legal Expenses

Other financial losses such as – Revenue loss

Dip in the share prices

Recovery costs: Target Corporation took various steps to recover from the data breach and minimize future risk. The company hired experts for investigating the breach. Target Corporation offered one year of free credit monitoring for its customers. The company set up a call center and assistance services for addressing and helping customers regarding breach-related issues.

The point-of-sale systems were equipped with chip and PIN-enabled technology. The overall cost of the arrangements was more than $250 million.

Legal Expenses: Target has incurred Legal expenses in addition to recovery costs. The company faced 140 lawsuits throughout the country. Target has settled $18.5 million pertains to 47 states. Apart from the legal expenses settled the company hired professional law firms for handling the lawsuits and incurred additional costs.

Revenue loss: Target’s profit dropped by 46% during the final quarter of 2013. In January (2014) shopping by households was down by 10% compared to the previous year. In the fourth quarter of 2013 sales were also down by 5%. Net income decreased by 34% due to recovery costs.

Effect on Share price: The data breach has impacted the share price the company stock prices experienced a 10% loss.

## Potential action plans to address the consequences of breach:

Cyber security Measure: If there were additional security measures the breach could not have occurred. Network segregation and encryption techniques could have prevented the data breach.

Training to Employees: Though the company invested in the malware detection tool FireEye, the employees could not detect the warnings of the tool. Proper training and expertise could have detected the intrusion and would have prevented the attack.

Third-party Access to Network: Proper access controls would have prevented the intrusion which occurred through third-party vendors. Limited access of the network of the Target corporation to vendors would have prevented the data breach.

Cyber Security Insurance Coverage: Cyber insurance covers business liability for the data breach. It includes customer information, credit card numbers, account numbers, and health records. The recovery costs can be claimed from the insurance company in case of a data breach. The victim companies can transfer their risk to insurance companies.

A proper Contingency plan and incident response can also help recover from the data breach and cyber security coverage also help the organization to transfer part of its risk.

Contingency Plan: A contingency plan is a plan made for unexpected adverse events. As technology helps businesses Planning for unexpected adverse events involves three communities of interest. In Contingency planning, three communities of interest position their organizational units to prepare for detection, reaction, and recovery from the events that cause threats to the security of information assets. Contingency planning has four components namely – Business impact analysis, Incidence Response Plan, Disaster Recovery Plan, and Business continuity plan. The contingency plan includes the following (NIST contingency planning and implementation approach)

Contingency Planning Policy Statement: This is necessary to guide the three communities of interest to understand the security information system requirements and needs. The policy is to be clearly defined by CISO in consultation with CIO and should be approved by the management. The System Specified Security Policy is useful in the case of Target Corporation. The data breach occurred because of poor access controls and poor encryption of software, Networks were not segregated properly, and due to overlooking of several warnings.

Business Impact Analysis (BIA): Identifies and prioritizes important assets/systems of the organization’s business functions. Business requirements in terms of confidentiality, integrity, and availability are determined. The security is to be looked at from a business risk perspective in this initiation stage.

Preventive Controls: Proactive measures that prevent disruptions to system availability. In this case, access controls, firewalls, and network segregation.

Contingency strategies: Recovery strategies that ensure complete and fast recovery of systems after a disruption.

Incident response: This is a critical part of contingency planning. Target’s initial response to the breach increased the severity of the loss. Target received reports from FireEye about malware, but the company failed to recognize and act until the Federal Government was involved. An effective cyber incident response plan could have prevented the breach.

The incident response outlines who is part of the cyber incident response team (Board members, IT leaders, professionals, IT security personnel, legal, and HR experts). What are the roles of the cyber incident response team during an attack. The organization’s key function and how the operations will continue throughout an attack. When and how stakeholders should be informed about an attack. What federal and state and local regulations the organization should follow when responding to an attack.

Testing and training exercises: Testing and training identify planning gaps.

Plan maintenance: The plan should be updated regularly to remain current with the organizational changes.

Review and Auditing: This ensures that the plan is examined periodically to check its consistency with the current business technology practices. Periodic audits ensure alignment with relevant controls, standards, and controls.

# What I Learned

## About myself: I am glad that I have chosen Information Security Management as one of my electives. Before pursuing this course subject, I have limited knowledge about Information Security and was unaware of most of the security issues that were faced by Organizations and individuals.

## Password Protection: I have learned about protecting passwords relating to debit, credit cards and e-mail, social media accounts that I use in my daily life and how to create a secured password and the precautions to be taken while creating the passwords.

## From the discussions held in the class, I have learned about how personal information is important and how it affects the person if the information has been stolen and misused. I have learned how to be careful while using email and what messages to respond to and what not (phishing in email). I have also learned about the rules one needs to follow working in organizations and how to prevent others from using the computer system assigned in the workplace and other devices. How to protect the data of the organization and the responsibility of the employee in the organization towards information assets.

About Information security:

In the modern world, information is playing a vital role in every organization. Like any other asset, information has become a valuable asset. Every organization tries to protect the information of its business. Due to the advent of the internet whole world is connected. The internet has become an interconnection of millions of networks. The vulnerability had increased, and organizations were constantly being targeted by hackers for extortion of information. The need for securing the information assets of the company has forced the management to think about information security and frame guidelines to be followed. Information security deals with the protection of information and its critical elements, including the systems and hardware that use, store, and transmit the information. I have learned about what information security is and its importance to organizations and individuals. Through the course, Information Security Management, I have learned How three communities of interest are responsible for safeguarding information and their roles and responsibilities towards information security. I have learned the threats and vulnerabilities that affect the information of the organization. I have also learned about data breaches through intrusion into organization networks and systems using various techniques of intrusion and malware. Various safeguarding measures, controls (access controls), and technologies such as firewalls, and VPNs were explained. The guidelines and framework of various policies, practices, and standards to be followed about information security are learned (ISO, NIST cybersecurity frameworks). The techniques used for stealing the information and the types of parties involved in information theft are understood. The process of Risk management and its framework roles and responsibilities of management in the implementation of risk management, incidence response, and contingency planning, policies were learned. Organizational legal and ethical responsibilities and various laws and agencies that protect information security and also the certification courses required for information security professionals also learned through this course.

About Target Corporation: Target Corporation is the second biggest retailer in the USA. By analyzing the data breach that happened to Target Corporation I have learned how organizations fail to detect and prevent vulnerabilities and how information breach causes business losses in the form of lawsuits and penalties. The incident brings out the need for disaster preparedness and recovery plans. Target Corporation successfully removed all the malware that affected their systems and point-of-sale networks and took the necessary steps for recovery from the data breach. Target Corporation spent a lot of money investigating the vulnerabilities that caused the breach and changed its information security systems and technologies. Target Corporation promptly reacted and handled the breach incident and guided its customers. Through recovery plans, Target Corporation succeeded in attracting customers back. Target Corporation understood the importance of information security by creating the CISO post.

Various articles of experts were referred to understand the technical details of the breach and the consequences of the breach in the case of Target Corporation. The information was searched on google and articles published by Wall Street Journal and Bloomberg were referred for understanding the impact of the breach on financial numbers.

Reference:

Anatomy of the Target data breach: Missed opportunities and lessons learned.

<https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/>

Target Breach Lesson: PCI Compliance Isn’t Enough

<https://www.technewsworld.com/story/Target-Breach-Lesson-PCI-Compliance-Isnt-Enough-80160.html>

Timeline of Target's Data Breach And Aftermath: How Cybertheft Snowballed For The Giant Retailer.

<https://www.ibtimes.com/timeline-targets-data-breach-aftermath-how-cybertheft-snowballed-giant-retailer-1580056>

Wallstreet journal articles

<https://www.wsj.com/articles/target-to-pay-18-5-million-to-settle-massive-2013-data-breach-1495561952>

https://www.wsj.com/articles/target-hit-by-creditcard-breach-1387406300

Yahoo Financials.

Stanwick, Peter. “A Security Breach at Target: A Different Type of BullsEye.” International Journal of Business and Social Science 5.12 (2014): 23-25. Print.

Tipton, Stephen, and Young Choi. “The Target Security Breach: A Case Study.” International Journal of Business Administration 6.2 (2014): 59-60. Print.

<https://www.techtarget.com/searchsecurity/tip/FAQ-Were-executives-held-accountable-after-the-Target-data-breach>

[Target CIO resigns as security revamped over data breach | CBC News](https://www.cbc.ca/news/business/target-cio-resigns-as-security-revamped-over-data-breach-1.2561648).