|  |  |
| --- | --- |
| **Course** | Operating System Security |
| **Capstone Project** | Capstone Project Report |

|  |  |
| --- | --- |
| **Name of the Group Members** | **Student IDs** |
| Maisha Khatoon (Team Leader) | 100899259 |
| Bhudev Nevaniya | 100848467 |
| Pujan Bhusal | 100890113 |
| Shreeraj Shah | 100848468 |

# Threaded Project Report- Case Study#4- Target Data Breach

## Introduction

The American multinational retailer Target was the victim of one of the most significant data breaches impacting customers to ever be disclosed anywhere in the history of the globe. The breach included credit card information belonging to Target customers. The security compromise happened in 2013. The data breach affected millions of customers, and it led to the loss of their personal and financial information by criminals who gained access to the system via the breach. These crooks stole information from the customers' credit and debit cards. Because of the security flaw, these crooks were able to enter the system and do their damage. The objective of this report is to investigate the series of events that led up to the breach, the impact that it had on the company and the customers of the company, the vulnerabilities in the operating system that contributed to the attack, and the preventative measures that could be taken to ensure that incidents of a similar nature do not occur in the future.

## What happened?

Hackers were able to get the personal and financial information of more than 40 million Target customers on November 27, 2013, after gaining access to the retailer's networks and acquiring authorization to use them. On the day that the data breach took place, Target made the finding that there had been one. By using credentials that they had obtained from a third-party source, the hackers were able to effectively break into the system and take control of it. Target's heating, ventilation, and air conditioning (HVAC) systems, which were once handled in-house, were previously taken care of by a specialized business that was granted the contract to handle such systems.

The hackers were able to access the credit and debit card information of customers making transactions inside Target by putting malware on the store's point-of-sale (POS) system, which provided them access to the information customers input while using their cards to make purchases. This allowed the hackers to access the credit and debit card information of customers making transactions inside of Target. The information that was obtained includes things like names, addresses, phone numbers, and email addresses, in addition to data pertaining to credit and debit cards. The information that was obtained includes these pieces of information. These bits of data were gathered along with the rest of the information that was gathered.

Even though the attack had been going on for that amount of time, Target did not reveal the data breach until the 15th of December despite the fact that it had been going on for that amount of time. The assault went on for a considerable length of time despite the fact that it had been going on for that amount of time already. At that particular moment, the damage had already been done, and the number of customers who had been negatively affected by the situation had already reached millions.

## Who was affected??

As a result of the security breach that took place at Target, the personal information of about 40 million of its customers became available to the general public. These consumers made purchases at Target locations in 2013 between the 27th of November and the 15th of December, and their shopping trips fell within the aforementioned time frame. The information that was obtained includes things like names, addresses, phone numbers, and email addresses, in addition to data pertaining to credit and debit cards. The information that was obtained includes these pieces of information. These bits of data were gathered along with the rest of the information that was gathered.

Customers have claimed that their personal information has been used unlawfully and that their credit and debit cards have been exposed to unauthorized transactions as a direct consequence of the data breach, which had an impact worldwide owing to the magnitude of the event. Customers have also alleged that the data breach caused their credit and debit cards to be exposed to unauthorized transactions. Customers have also stated that unauthorized transactions have been made using their credit cards and debit cards. Target was compelled to pay millions of dollars in fines and compensation to customers whose personal information had been taken as a consequence of the breach, which resulted in the loss of confidence among customers in the company and caused the customers' trust to be weakened. The breach occurred because of a security flaw in the company's computer system. Not only did this have a significant impact on Target's brand, but it also had an impact on the company's financial results.

## What portion of the operation system vulnerability contribute to the attack?

The data breach at Target was caused by a confluence of operational and technical problems, none of which were corrected by the firm despite the fact that they were aware of the vulnerabilities and could have averted the leak if they had taken preventative measures. It was one of the major challenges in the operation of the firm because it was unable to adequately protect the systems of the business from unauthorized access by other parties, such as third-party suppliers. This was one of the most serious problems in the operation of the company. This was one of the most significant flaws in the way the corporation did business. The fact that the cybercriminals were successful in obtaining credentials from the vendor allowed them to get access to the servers that are utilized by Target and install malware on the point-of-sale system that is used by the retailer.

Another flaw in the firm's defence against potential threats was that its systems were not adequately segregated from one another and monitored in the way that would have been most effective. This was an area of vulnerability for the organization. Because the firm's network was not adequately segregated, the hackers were able to move laterally across the system and access vital data. This allowed them to compromise the organization. Because of this, they were able to put the firm in jeopardy. As a direct consequence of this, they were in a position to effectively undermine the organization. It was probable that this would take occur due to the fact that there was not sufficient segmentation in place to prevent it from taking place. Because the company was unable to recognize the presence of malware on its POS system, the hackers were able to continue stealing data for a period of weeks before they discovered what had happened.

Hackers were able to quickly get credentials and gain access to Target's systems because the firm maintained a loose policy concerning passwords, which made it simpler for them to do so. This made it easier for hackers to break into the company's networks. The computer network of the firm was accessible to hackers as a result of this vulnerability. Because of this, the hackers were able to get access to the system with relative ease. Because the company utilized default passwords and did not implement two-factor authentication, hackers were able to readily access important information and get login credentials. This was made possible because the company did not implement two-factor authentication. This was a possibility since the organization in issue did not use a system that required authentication through a combination of more than one factor.

## What can be done to prevent the attack?

The chance of similar attacks being carried out in the future will decrease as a direct result of Target and maybe other businesses taking a variety of actions to enhance their security posture. This will have the effect of reducing the possibility that similar attacks will be carried out in the future. The following are some instances of each of these:

Businesses should impose stringent limits on the use of passwords by their employees in order to protect the credentials of their staff members from being stolen. These laws should require employees to use passwords that are not only tough but also unique to them. In addition to this, it is essential to demand the use of not one but two different authentication procedures.

It is vital for companies to separate their networks into discrete parts in order to restrict lateral movement to the greatest extent that is realistically possible and to set up monitoring systems in order to detect and respond to security breaches. In addition, businesses have to compartmentalize their computer systems in order to make it simpler for them to carry out their own internal monitoring, which is another need.

Companies need to do exhaustive background checks on their third-party suppliers and maintain close tabs on how well they are performing in order to guarantee that their third-party suppliers are following the most up-to-date security best practices and are not putting the company at risk. In addition, companies need to ensure that their third-party suppliers are not putting the company in danger. This will ensure that the security of the organization is not jeopardized in any manner, which is of the utmost importance.

Conducting regular security audits and tests: Businesses should make it a standard practice to conduct routine security audits and penetration testing in order to identify possible security vulnerabilities and ensure that they are taking the required actions to remedy such issues. Companies should also make it a standard practice to conduct routine security audits and tests in order to identify potential security flaws. It is important to perform this in order to identify any potential flaws in the system's security and to verify that the required actions are being taken in order to address these problems. In addition to this, businesses should make it a standard operating procedure to make certain that they are addressing these concerns by taking the appropriate safety measures on a consistent basis.

Continuous education in matters of safety and security is something that every employer is obligated to provide to their staff on a consistent basis. It is essential that this training be delivered in a regular and reliable manner.

In conclusion, the 2013 Target data breach was a catastrophic event that negatively impacted the company's brand and financial line, affecting millions of consumers. The company's inability to adequately protect the access of its third-party vendor to its systems, its lack of system segmentation and monitoring, and its lax password policy all contributed to the breach. Companies may protect themselves against future attacks by instituting security best practices such strict password restrictions, system segmentation and monitoring, careful screening and monitoring of third-party suppliers, routine security audits and testing, and staff education. Taking these measures can help businesses safeguard their customers' personal and financial data and lower the likelihood of a data breach occurring.

# References:

1) <https://redriver.com/security/target-data-breach#:~:text=What%20Happened%20During%20the%20Target,was%20one%20of%20the%20largest>.

2) <https://slate.com/technology/2022/04/breached-excerpt-hartzog-solove-target.html>

3) <https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/>

4) <https://www.idstrong.com/sentinel/that-one-time-target-lost-everything/>

5) <https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013->

[data-breach-affected-consumers/102063932/](https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-)

6) <https://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013->

[breach/](https://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-)

7) <https://www.lifelock.com/learn/data-breaches/target-data-breachvictims-could-get-up-to-10000>