**Target**

Troy Smith

10/08/2023

**History of Target**

Target is large retailer based in the USA and has climbed to be the second largest retailer in the country. The store is trusted by millions of customers to keep their private information safe and protected when they check out, the same for every other retailer out there, big or small. In late 2013, a data breach jeopardized Targets status as a safe place to shop for consumers all over the country. Even though the threat of a cyber-attack is a possibility, Target was known as a leader in cybersecurity in the retail industry. They invested a large amount of money into their IT infrastructure and the security that they had to go along with it, investing in many layers that would protect it from cyber-attacks in attempt the dispute any attempt to steal information from it. They were also compliant with the standards put in place by the Payment Card Industry Data Security Standard (PCI DSS).

**Data Breach**

In December of 2013 Target was contacted by the U.S Department of Justice and was notified that a large number of credit and debit cards that have had fraudulent charges on them have been linked back to the company. A couple of days later Target made an announcement to the public informing them of the breach. Due to this breach personal information and card information such as names, mailing addresses, phone numbers, email addresses, card pins, card numbers, and expiration dates have all been leaked. This breach effected nearly 10% of all of debit and credit cards in the nation.

The breach was a premeditated cyber-attack by a group of hackers that targeted Target. To pull off the security breach the group of hackers installed malware onto Targets point-of-sale network, which is linked to the cash registers used by customers to purchase their items. The malware they installed was able to copy the data that was put into the infected point-of-sale machines and would send the information gained backed to the hackers, giving them access to all the information associated with the cards used.

**Key Issues**

When shopping at a store, the threat that a customer’s information will be leaked due to them making a purchase is the last thing on their mind. The thought that their information should be protected is a no-brainer and something that anyone should have to worry about on a typical day. Having a breach of information can cause distrust between the customers and company, some customers may no longer want to shop at target after the breach.

Another issue was the scope of the issue. This was not a small breach of information, its information over 70 million customers, making it one of the largest breaches in the history of the USA. To add on to this, it made consumers everywhere realize that if a large company like Target could become a victim to a cyber-attack like this, that it could also happen to any other company as well.

**Alternatives**

Once Target was informed of the breach by the U.S Department of Justice they immediately hired a cyber forensics team to investigate the issue. This team is how the installed malware was initially found. The team then combed through and deleted all of the malware that was installed in the system. Along with helping fix the initial breach, this team helped to strengthen Targets IT infrastructure even more to help prevent more breaches and cyber-attacks from happening in the future. Afterall, Targets image could not withstand another breach like the previous one as it would destroy whatever trust was left with the consumers who shop at Target.

Another thing Target did to help remedy the security breach was to announce it to the public. Announcing it to the public is not something that they needed to do, but Target felt the need to inform its customers of the breach, which ultimately helped build up the trust that was broken between Target and its customers.

After the breach Target also accelerated a project to implement a chip and pin payment system into all of their stores, effectively adding an extra layer of security when customers would pay with their cards. The acceleration of this project cost the company an extra $100 million but the cost was necessary to improve their security and improve the security of the customers private and card information.

Target also made some significant changes to its position. After the breach happened Target announced the resignation of its Chief Information Officer (CIO) and months later the Chief Executive Officer (CEO) was let go. In addition to getting a new CIO and CEO, Target also created two new positions to help ensure this would not happen again. These positions being called Executive Vice-President and Chief Information Security Officer and Executive Vice-President and Chief Compliance Officer.

**Best Alternative**

The best alternative or solution Target took to help fix this situation was to hire a 3rd party team of cyber investigators to help them. With their help Target was able to identify the malware that was installed in their systems and get rid of them in a timely manner. Not only get rid of them but also help defend against future attacks on the company. This decision potentially saved the company as a whole and helped strengthen their integrity after the cyber-attack.

**Data Analysis**

As expected, this data breach had some major consequences for the company. In just the fourth quarter of 2013, the same months as when the data breach occurred, Target profits fell by 46% and total revenue dropped by 5.3%.

In response to the breach, Target had to spend over $60 million to help clean up their infrastructure of any malware that was downloaded, updating their systems, and creating new positions to ensure that it does not happen in the future.

Due to the number of customers that were affected by the data breach, Target was facing over 140 lawsuits. While that may seem small compared to the amount of people affected by the breach, each lawsuit was seeking millions of dollars in damages.

The current evaluation of the total cost of the breach has it exceedingly over $500 million, with the potential to even approach the $1 billion mark. This is enough to make significant changes in any company no matter how big they are, even the second largest retailer in the USA.

**Conclusion**

Target was the target of a cyber-attack that leaked the information of millions of customers. This breach is estimated to have lost the company over $500 million and might have even climbed to near a billion dollars. While this event is horrific, it serves as a warning to all retailers and companies about the dangers of a cyber-attack. Many companies worked to strengthen their IT infrastructure to ensure that a data breach like this does not happen to their company. In the end customers can shop with more confidence in their information being safe and no longer worry as much about their information being leaked while shopping.

**Works Cited**

Line DUBÉ. (n.d). *Autopsy of a Data Breach: The Target Case*. Harvard Business Publishing.

Peterson, C. (n.d.). *Target security breach case analysis*. prezi.com.