James Everett Tourtellotte IV

ITN 267

Case Study 2 - The Target Attack

6/4/2023

A Summary of the Target Attack:

The Target Corporation, a major U.S. retailer, suffered a massive data breach during the 2013 holiday season. It was a wake-up call to businesses about the necessity for Cybersecurity in the consumer sector of big businesses. Sometime in mid-December 2013, the company disclosed that hackers had gained unauthorized access to its systems, compromising the financial data of approximately 40 million customers who had shopped at its stores between Late November and December 15, 2013. The information stolen included credit card and debit card numbers, card expiration dates, CVV codes, and more Personal Financial data. When looking into the large breadth/scale of this hack it was revealed that the attackers had also stolen additional data, including email and mailing addresses, from as many as 70 million customers - strikingly these were not all of the initial 40 million victims. The breach was believed to have been executed through malware installed on the point-of-sale (POS) systems in Target's retail stores.

How was this accomplished? When you research this attack, we find out that the hackers gained access to Target's network initially by infiltrating a third-party HVAC vendor that had a business connection to Target. Using the vendor's credentials, they were able to move laterally through the network, eventually reaching POS systems. This type of compromisation was crucial to the breach as it allowed for the attack surface to increase exponentially. The consequences for target were rather high. The company spent over $200 million on breach-related expenses, including card replacement costs, legal fees, investigations, and improvements to its cybersecurity infrastructure. The company's profits plunged in the wake of the incident due to loss of customer trust. If you take a look at the report on their sales for the following year, you can see that it decreased by around 46% in the fourth quarter of 2013 compared to the same period in the previous year.

What Laws or Regulations might have been broken?

When one analyzes the Target breach, you come to the conclusion of gross mishandling of the incident. More than a few laws were violated, one of which noted by barley.com is the Pennsylvania “Breach of Personal Information Notification Act”. This is a state-level law that outlines the guidelines businesses need to adhere to when protecting data of customers, and notifying them of incidents that occur. The action, or inaction, of target is what put the nail in the coffin in regards to breaking the law. Their inability to swiftly notify their customers put their business at risk as they were in violation of multiple laws at the state or national level. Another example could be the FTC Act which prohibits unfair and deceptive practices. In the context of data security this could imply the lack of adequate decision making when the malware was first discovered.

From a Consumer’s Perspective:

Realistically speaking, I would not feel too bad at all. The way this was handled was as expected in regards to how I view corporate america. I do not see many redeeming qualities of small, or large, businesses in the consumer realm - especially in the process of becoming a cyber security expert. What we see time and time again is gross negligence and corner-cutting by multi-million dollar organizations, in any field. Whether it is Logistics, to the supply chain, we consistently see a pattern of profit prioritization. If I am speaking in a tone that is not completely Jaded - I would be pretty mad seeing this. It is clearly outlined in this situation that the people at the top of the food chain were doing their best to prevent a PR Disaster, instead of doing what is right - and cleaning the systems of any sort of malware leftover. Finally, if I am speaking comically - there is a chance I would not care at all if my personal information was stolen. That occurred right after the recession was clearing up, the majority of Americans were doing terribly financially. What were those Cyber criminals going to take from them? The last fifty dollars of available credit they had?

How should Target customers be reassured that this won’t happen again?

There is a large issue within American Corporate Culture that involves diverting to PR as opposed to fixing the issue. For example the article states a message via target’s CEO outlining the issue and their take on the incident. We can see the PR move as follows: “Target was certified as meeting the standard for the payment card industry

(PCI) in September 2013. Nonetheless, we suffered a data breach. As a result, we are conducting an end-to-end review of our people, processes and technology to understand our opportunities to improve data security and are committed to learning from this experience.”. This is a nothing-burger of a response in regards to the situation at hand. As we have discussed previously the Target Breach had adequate solutions to prevent or detect this from occurring, however they failed to act within a reasonable amount of time. This issue of PR handling is a plague within American society. This plague is exacerbated by the notion that it affects aspects of our lives that are highly significant. For example, our credit card data. Target needs to make a move from investing in PR Firms, to investing in adequate Cyber Security Solutions for their Business.

In my own opinion, Target customers could feel reassured if there was said implementation paired with superiority over even the CEO and Shareholders of Target. Why would this be an adequate means of appeasing their customers? How about we take the window of attack into consideration. The malware was first identified on or around November 30th. Right before the holiday season. The lack of administrative action leads me to believe that the PR Disaster of malware infecting their systems might have hurt their profit margins - because it was right before Christmas. The gross negligence that occurred sounds like there was a divergence or disagreement between Target Higher-Ups and the individual(s) running the SOC in Minneapolis. Whether the concern was the downtime, greed, or something else - the Cybersecurity Professional should have superiority upon decision making in regards to the realm of his or her expertise. The customers of Target would feel reassured if they knew that there was someone who would prioritize their Cyber Security over a company’s bottom dollar.

Citations:

https://www.forbes.com/sites/maggiemcgrath/2014/02/26/target-profit-falls-46-on-credit-card-breach-and-says-the-hits-could-keep-on-coming/?sh=199a0c287326

https://www.barley.com/the-target-data-breach-what-can-you-and-your-business-learn/#:~:text=These%20laws%20include%20a%20web,the%20Health%20Insurance%20Portability%20Act

https://www.infoworld.com/article/2609942/target-contractor-says-it-was-victim-of-cyber-attack.html

https://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data