Daniel Schnoll
Professor Miner, Professor Grill
ITWS 4130 Managing IT Resources
Due November 26, 2018

Case #4 - Cyber Breach at Target

Data breaches are becoming an increasingly common occurrence for major corporations. Target is no exception, and they were the… target… of a data breach in September 2013. Their data breach began with a phishing email campaign targeting one of their HVAC suppliers. The hackers gained control of the user's computer, stole passwords, and managed to use the stolen credentials to access Target's network. Industry experts say "there should never be a route between a network for an outside contractor and the network for payment data", and for good reason. Information systems have flaws, and it is incredibly difficult (and expensive) to maintain the QA necessary to test for every potential exploit. Knowing this, Target should not have given all of its vendors access to this system. Target should have employed tools and programs to be used internally, and at no point should any third party contractor be able to view sensitive data if it is not absolutely necessary.

However, the breach did not stop with a poorly vetted vendor's security infrastructure. This was simply the hacker's ticket inside. Once they had access to Target's global network, they installed malware on the POS systems in the stores themselves. This malware scraped credit card data as it was passed from the POS system to the payment processing providers. The way Target's network was set up allowed the hackers to update the malware remotely as security teams managed to patch the virus, therefore allowing them to continually evade being shut down for good.

Furthermore, Target routinely ignored security breach warnings from FireEye, the company in which they contracted cyber security monitoring. They received two initial warnings, once when the breach was first detected around Black Friday, and a second warning when the FireEye team began detecting unusual activity on December 2. In addition, two months prior to the attacks, "Target's security team highlighted vulnerabilities in Target's POS system and asked to review Target's payment network", further highlighting Target's carelessness in handling cyber security [1]. In summary, Target had a number of cybersecurity oversights that could have been mitigated if the company had taken more preventative measures. They did not properly vet their third party vendors, and should have made sure they took their own company's system security seriously. It was because of their carelessness with exposure of data to third party contractors, and improper network segmenting, that the hackers were able to get into their network in the first place. Then, there were the security flaws in their POS systems, which allowed the hackers to scrape data from sale terminals as transactions were made. Finally, the Target security team ignored warnings from their contracted security team, which could have put an end to the breach sooner.

Target is therefore entirely to blame for this data breach. Not only was their infrastructure poorly equipped to properly mitigate the breach, but human error and overall incompetence allowed the breach to persist until the DOJ intervened, ultimately informing them of the

seriousness of the attack. Target's executive board issued letters to shareholders saying they took their oversights seriously. The company also did previously acknowledge one of their major risks was cyber security, and recognized "failure to detect and appropriately respond to data breaches could expose them to both public and private litigation" [1]. As such, they should have known to delegate more resources to assessing and managing their cybersecurity risk. Target was well aware of the risks at hand. Breaches cannot be entirely mitigated, only managed. One of the important takeaways is Target's board was quick to respond, so after the breach was discovered, they did handle it properly. However, Target should have taken more preventative measures to ensure the integrity of their security systems.

Sources:

[1] Cyber Breach at Target (Harvard Business Pack)