Michelle Green

CIS-410-50-4238

Professor Reinhardt

October 08, 2023

Case 2 – Autopsy of a Data Breach: The Target Case

Synopsis

On December 13,2013, Target management received a notification from a U.S. Department of Justice representative that there were a “large number of fraudulent debit and credit card transaction” (Dube, *Autopsy of a Data Breach: The Target Case*) linked back to purchases made at Target. After hiring a team to investigate the data breach, it was discovered that Targets systems had been hacked, and data had been stolen since November 27. “On December 19, 2013, Target announced the breach and theft of customer data” (Dube, *Autopsy of a Data Breach: The Target Case*). The Target data breach created difficulty for consumers banks and credit card companies because of the amount of cards effected. When banks normally deal with data breaches similar to Targets, companies are able to cancel cards and send out new ones. While banks were coming up with solutions, Target was trying to handle their public relations and ensure customers “that they could continue to confidently shop in its stores” (Dube, *Autopsy of a Data Breach: The Target Case*). They also stated that no customer would be held liable for the transaction and that they were investigating the source of the breach.

The U.S. Justice Department, Secret Service, and the private firm Target hired confirmed that the attack was set into motion by cybercriminals. By targeting the PoS network and installing malware on the terminals the perpetrators could “capture all the data stored on credit and debit card that are swiped at the infected terminal” (Dube, *Autopsy of a Data Breach: The Target Case*). This is extremely difficult for intrusion detection software to detect.

While Target is usually on top of their cybersecurity measurements, this attacked a vulnerability in their infrastructure. Target had recently invested in an anti-malware system called FireEye that uses a team of experts to monitor the results of the system 24/7 and should then alert the Target security team of any suspicious activity. Target had been receiving alerts since November 30th, but the alerts were analyzed and were not seen as a threat. The attack could have been prevented if the software that destroys “malicious and unauthorized software had not been deactivated because Targets experts didn’t trust it” (Dube, *Autopsy of a Data Breach: The Target Case*). Then at the end of November more suspicious activities were detected but ignored.

The breach caused an increase in public distrust. Their “failure to act on the initial alerts, delay in making the breach public, and the inability of its customer service department to respond to customers” (Dube, *Autopsy of a Data Breach: The Target Case*) the consumer perception skewed negative. Target saw a decline in profit and revenue for the quarter and the year. The breach itself may have cost up to $1 billion dollars. It also altered the chain of command in Target, two new positions were created: Executive Vice-President and CIO and Executive Vice-President and CCO. They also replaced the CEO in May of 2014 and some board members. The breach also impacted multiple projects within Target, such as the “implementation of chip-and-PIN” (Dube, *Autopsy of a Data Breach: The Target Case*) payment.

Comparison

In our course text Adventures of an IT Leader in Part Three: The Hero’s Ordeal (Ch 10 -12) our lead character faces a similar situation. As the new CIO of IVK Barton faces his first crisis. While he is a few hours away from speaking to “Wall Street analysts” (Austin, *Adventures of an IT Leader*) he gets a call from one of the managers under him. He is stating that there has been a customer service outage and a possible security breach in the form of emails. The possible cause of this can all be traced back to the IT and previous CIO new security initiative being shut down by the previous Loan Operations manager (the present-day CIO). After numerous calls with CEO and legal Barton is able to finish his meeting and face the situation when he got back to the office. A meeting is held between the new CEO and the managers of different departments as they hammer out all the possible solutions. When Barton recommends that online operations be shut down and their customers be notified the other managers agree, but the CEO explodes demanding that the problem be solved without shutting down operations and notifying the public because he is only here to fix things not make thing worse. Two of the managers vocally retaliate against his plan of action, they are fired. (Austin, *Adventures of an IT Leader*)

I see a lot of similarities between both IVK and Targets situations. The one that sticks out to me the most is the possibility that the security issues could have been prevented. If Target’s experts were to take a closer look at the alerts, they were getting, and if they kept the software that destroys malicious software, they could have prevented and destroyed the malware that attacked their systems. It is also possible that IVK could have prevented their IT issues especially if it was a security breach if the system was updated when it was first brought up. The main difference is how the data breach was discovered. Target had an internal entity reach out to them about the fraudulent transactions while IVK’s issue was discovered internally. The last similarity I see is the change of staff. In the beginning of Adventures of an IT Leader we are introduced to IVK in the midst of a staff change, a new CEO is brought in to turn around the company and Barton moves into the CIO position. While Target, in order to change after the data breach, they added two new position and changed CEO and board members. The main difference Is that Targets board members deliberately searched for external hires to turn around, while IVK CEO was external hire known for turning around companies and the CIO was promoted internally.

Works Cited

Dube, Line *Autopsy of a Data Breach: The Target Case* Harvard Business Publishing, 2016.

Austin, Robert D. *Adventures of an IT Leader*. Harvard Business Review Press, 2016.