Cyberattacks on tjx: vulnerabilities and potential fixes research paper

Business, Company

In the case of the TJX. com, the portion of the company that was compromised was the credit card numbers and information for all of the customers that hold a credit card for any of the stores under the TJX umbrella (eSecurity Planet Staff, 2010). The sad truth of the matter is that nearly any company has the potential to be victim to a cyber attack, and nearly all company's systems have the potential to be vulnerable to this attack, given the level of skill and ingenuity that many hackers have. However, the TJX corporation failed to disclose some pertinent information to cardholders when they realized that the attack was happening-- in particular, it was not until 2007 when the data breach was announced. By the time the breach was announced, the system had been vulnerable for two years (eSecurity Planet Staff, 2010).

There are specific controls that are used to regulate the credit card industry, especially because the credit card industry controls and obtains so much identifying personal and financial information about so many people. The credit card industry is, in theory, under close supervision by a number of overarching supervisory bodies; there are very strict controls in place because of the amount of personal information that can be gleaned from credit cards and credit card-holder accounts. According to Vijayan (2007): " According to the documents, TJX knew before the breach that its wireless networks were insufficiently protected, but took no steps to mitigate the situation. The company also knew that storing Track 2 data was a violation of PCI policies, but it continued to do so anyway In addition, the forensic analyst who conducted the investigation, said he had never seen such a ' void of monitoring and capturing via logs activity' in a Level 1 merchant like he saw

at TJX, the court filings noted.” Essentially, there were two things wrong with the way that TJX was conducting business: first, the company was paying insufficient attention to its in-house security policies, including transferring sensitive customer information over unsecured networks. Secondly, the company was obtaining and storing information that they legally had no business storing-- information that the government refers to as “ Track 2 data” (Vijayan, 2007).

In the wake of the scandal, TJX found it necessary to fix a variety of different holes in their security policy. Most notably, the Federal Trade Commission noted that to continue forward, TJX had to implement a number of changes to their security policy (eSecurity Planet Staff, 2010). As a result of the security breach, TJX is now subject to increased FTC oversight, but also has had to designate an employee or employees to oversee the cyber-security policy of the company. They must also utilize further firewall systems and encryption systems to conform to current federal standards.

It was an attempt to cut corners on security which caused TJX to have problems with their network security in the first place. While upgrading security systems can be costly, implementing policy changes is hardly more expensive than the $250 million dollars that the security breach cost the company. There are very few trade-offs that are worth mentioning-- further checks and balances in the PCI control department may slow down processing speeds, but not significantly.

Regardless of the culpability of the company, the information for nearly 48 million credit and debit cards was obtained by the group that was responsible for the cyberattack (eSecurity Planet Staff, 2010). Initially, the

TJX companies suggested that the multi-million dollar spending spree that the attackers went on at Walmart cost the company approximately $25 million, but it turned out that the damage to the company was much further-reaching. In the end, the company ended up being responsible for nearly $250 million dollars worth of damages, both in legal fees and otherwise.

The leader behind the TJX attacks was a man named Albert Gonzalez, although he led a number of other individuals in the quest to break into company computer systems. As a threat actor, he primarily acted upon the financial world; his purposes seemed to be primarily driven by financial gain, not ideological destruction or cyberterrorist activity (Higgins, 2010). For the TJX attack, Gonzalez was given twenty years in prison, a sentence that is largely unprecedented in American legal jurisprudence (Higgins, 2010). Gonzalez is, by far, the most visible figure in the TJX hacking case. He had previously been convicted for hacking into websites and computer systems and obtaining financial information; indeed, some sources suggest that Gonzalez was cooperating with federal investigators on a different case while masterminding the TJX attack (Jones, 2010). Gonzalez has been diagnosed with Asperger’s Syndrome, which is a form of autism. Although he is incredibly intelligent, Gonzalez’s Asperger’s Syndrome makes it difficult for him to empathize with his victims (Jones, 2010). This does not mean that Gonzalez did not understand that stealing the credit card information for 48 million cards was wrong-- it just meant that he could not understand the magnitude of the heist in the same way that an average person does (Jones, 2010).

For the TJX attack, in addition to Gonzalez, Stephen Watt, Damon Toey,

Humza Zaman, and Christopher Scott were all charged in relation to the crime (Jones, 2010). Each member of the team offered a different skillset, and together, they wrote a variety of different types of code that could extract information from unsecured wireless networks, like the ones being used by TJX. One of the primary technical problems was that TJX was sending unencrypted data over a poorly-secured wireless network; once the hackers obtained access to the system, they could freely monitor the system remotely for long periods of time without any kind of detection by the cybersecurity system that was in place in the TJX companies.

In the wake of these cyber attacks, the TJX companies have had to change the way they deal with cyber security. They have spent more than $130 million to upgrade their security systems, and they have been hit with heavy fines from both the government and regulatory agencies because of their complicity in the attacks and their blase actions with so much personal information.

References

eSecurity Planet Staff (2010). Zaman Jailed for TJX Cyber Attack. Cyber Security Planet, [online] March 15. Retrieved from: http://www. esecurityplanet. com/headlines/article. php/3870541/Zaman-Jailed-for-TJX-Cyber-Attack. htm [Accessed: 3 Oct 2013].

Higgins, K. (2010). TJX, Heartland Hacker Hit With A Second 20-Year Prison Sentence. Dark Reading, [online] March 26. Retrieved from: http://www. darkreading. com/attacks-breaches/tjx-heartland-hacker-hit-with-a-second-2/224200531 [Accessed: 3 Oct 2013].

Jones, J. (2010, 22 March). TJX Hackers Faces Record-Setting 25-Year

Cybercrime Sentence. Microsoft Security Blog, [web log] Retrieved from: http://blogs. technet. com/b/security/archive/2010/03/22/tjx-hackers-faces-record-setting-25-year-cybercrime-sentence. aspx [Accessed: 3 Oct 2013].

Tjx. com (2013). About Us. [online] Retrieved from: http://www. tjx. com/about. asp [Accessed: 3 Oct 2013].

Vijayan, J. (2007). TJX violated nine of 12 PCI controls at time of breach, court filings say. ComputerWorld, October 26.