06 - 09 - 2020

The Case of TJX Companies, Inc. 2005 - 2006 Cyber Attack

Mohammed Sadiq Abuwala
Student ID - 45921407
Email - sadiqabuwala.mohammed@students.macquarie.edu.au

TABLE OF CONTENTS

Introduction

TJX Companies Inc is a leading off-price department store corporation, headquartered in Framingham, Massachusetts. In late 2006, the company discovered that it had been a victim of a massive cyber attack which involved theft of millions of vital customer records. At the time of the incident, it was reported to be one of the largest data breaches to date. This case study analyzes the threat actors, attack, causes and impact of the incident. We also discuss how the company responded to the attack and what they could have done differently. Finally, strategic recommendations are made on how such attacks could be prevented in the future.

Chronology of Incident

18/12/2006	TJX discovers security breach.
19/12/2006	TJX hires external auditors to monitor and evaluate the breach. (TJX Companies Inc, 2007)
3/01/2007	TJX informs law enforcement and credit card companies. (TJX Companies Inc, 2007)
17/01/2007	TJX makes a public announcement about the security breach.
13/03/2007	Federal Trade Commission (FTC) launches an investigation.
25/04/2007	Credit card companies file lawsuits against TJX to recover damages amounting to millions of dollars incurred for replacing customer's credit and debit cards.
04/05/2007	Up to 21 U.S. and Canadian lawsuits have been registered and seek damages from the company.
12/07/2007	U.S. Secret Service Agency arrests four members of the ring. The ring leader, Albert Gonzales was eventually arrested in 2008.

24/09/2007	TJX starts making settlement agreements in regards to lawsuits from customers, banks, and credit card companies. notifying all customers whose private information might
29/02/2008	TJX starts notifying all customers whose private information might have been compromised due to the attack. The notification also mentions compensation being offered by the company. (TJX Companies Inc, 2007)

The Attack

On multiple occasions, somewhere during the middle of the year 2005, hackers sitting outside a Marshalls store in St Pauls, Minnesota were able to point an antenna towards the store. This allowed them to capture wireless transactions which were taking place inside the store while they were being sent through the company's wireless network. Upon listening to the captured wireless transactions for two days, they were able to crack the store's WEP security code.

Once inside the store's wireless network, they were further able to take advantage of the lapse in physical security at the store by entering the store and loading custom software onto the payment kiosks via USB terminals. Hackers are said to have planted unauthorised software on TJX's computer network, to enable them to steal at least 100 files containing data on millions of accounts from systems in Framingham, Massachusetts and Watford in the UK (TJX hack the biggest in history, 2020).

Using the information they had gained from the attack, the hackers gained access to the TJX headquarters' corporate networks. This second attack took place almost a year later from the first attack between May and December 2006. Once inside the network, they were able to access the company's centralized corporate database. The hackers would eventually get away with approximately 45.7 million separate payment cards from transactions dating back to the beginning of January 2003 (Xu, Grant, Nguyen and Dai, 2008).

Threat Actors

The hackers were a group of 10 individuals who were based all over the world. They were led by Albert Gonzalez who was based in the U.S. He would eventually be arrested for charges relating to other hacks and then also convicted for his part in the

TJX cyber attack. Gonzalez, who once dubbed his criminal enterprise "Operation Get Rich or Die Tryin'," had argued in court filings that his only motive was technical curiosity and an obsession with conquering computer networks. But chat logs the government obtained showed Gonzalez confiding in one of his accomplices that his goal was to earn $15 million from his schemes, buy a yacht and then retire (Zetter, 2010).

Discovery & Response

I. Detection & Investigation

On December 18, 2006, the company learned of suspicious software on their computer systems (TJX Companies Inc, 2007). An investigation was called immediately and two leading computer security firms, General Dynamics Corporation and International Business Machines Corporation were hired to assist in the investigation. They determined that there was strong evidence that their corporate network had suffered a hack and that the hackers were still maintaining access to the network. Thereby, the company immediately started designing and implementing a plan to monitor the ongoing intrusion and also to protect the data stored on the network.

On December 22, 2006, the company notified law enforcement officials of the recent attack that they had suffered.

II. Compromised Information

Further investigation revealed that information related to payment card, check and unreceipted merchandise return transactions for customers of several stores belonging to the corporation were stolen. Affected customers spanned multiple countries - UK, Canada and Puerto Rico.

Personal Identification Numbers (PIN) were not stolen as part of the customer information. Eventually, the company would report that approximately 45.7 million credit or debit cards had been compromised. TJX said three quarters of the stolen cards were expired or had a magnetic stripe masked (TJX hacked to the max: 45 million cards, 2020). Even so, it is believed that drivers' license, military and state identification numbers, together with related names and addresses" provided from returned merchandise without receipts at US and Canadian chains may have been stolen . The company identified about 455,000 such individuals (TJX Companies Inc, 2007).

III. Public Disclosure

The company notified law enforcement agencies immediately (4 days) after the incident. The agencies recommended that the company not disclose the intrusion to the public as the intrusion and the investigation was still on-going. Public disclosure would apparently hinder their investigation.

Finally, on 17 January, 2007, the company announced to the public about the data breach for the first time. Sherry Lang, the public relations executive, announced to the press and public about the cyber attack that had occurred. While she disclosed that the company had suffered a cyber attack and had customer information stolen, they were still not truly aware of the extent of the customer information stolen. The public was left in confusion as to the true count of customer information or specifically what data was stolen.

After a week, as all affected parties started demanding more answers, the company released a pre recorded video message to the public. Furthermore, the vice chairman of the company tried to downplay the incident by stating that the attack they had faced was similar to other retail companies in the sector.

Impact

The company's second quarter earnings were released after the cyber attack was disclosed to the public. Compared to previous years, second-quarter earnings for 2007 lowered the company's profits by $118 million; as a direct result from costs related to the data breach (Xu, Grant, Nguyen and Dai, 2008). In the end, the company eventually paid US$9.7 million to 41 states in a settlement. Apart from being investigated by local authorities, the company was also investigated by Canadian law enforcement agencies who released a scathing review stating how the company had ignored both federal statutes and PCI DSS.

Additionally, many customers who had their information compromised in the cyber attack reported fraudulent activities in their payment statements. Therefore, banks had to bear the cost of replacing these credit/debit cards for the affected customers. The case led banks to reissue cards to customers as a precaution against further fraud beyond cases detected as far away as Sweden and Hong Kong, according to the Massachusetts Bankers Association, which was tracking fraud reports linked to Framingham, Mass.-based TJX, parent company of stores across North America and the United Kingdom (The Sydney Morning Herald, 2007).

Response Analysis

I. What worked well

Although the intrusion was detected very late (17 months after it began), the company immediately hired external companies specialising in IT security to investigate the incident. Furthermore, the company also notified law enforcement officials of the cyber attack in a timely manner.

II. What didn't work well

TJX was using an outdated security policy for its wireless networks within its stores. At the time of the attack, the company was employing WEP security for its wireless networks while the industry standards stated that a much stronger WPA security should be employed. A new version of PCI DSS was released in 2006 and suggested the WPA encryption protocol. The company did not follow through with this regulation which in effect made it non compliant with PCI DSS.

At some point, the hackers were able to physically gain access to the in store kiosks. This allowed them to load software into the terminals. As these terminals were directly connected to the TJX network, the attackers now were also able to gain access to the TJX network. This showed negligence or unawareness by store employees on the need for maintaining physical security of terminals at the store in addition to its store products.

TJX reported that they decided against immediate public disclosure due to recommendations made by law enforcement agencies. Yet, this vital information related to the incident was somehow leaked and reported in a Wall Street Journal report first. This did not portray a positive outlook of the company and brewed mistrust amongst the public. When the company finally made a public disclosure one month after the discovery of intrusion, the announcement did not provide an action plan or compensation to customers.

TJX did not have a plan in place for regular security audits or logs of the processes being conducted on their network. Due to this, they were unable to detect the intrusion for up to 18 months since it first took place.

Recommendations

The company needs to focus more strongly towards IT security. As the company owns a large number of retail stores, it must be PCI DSS compliant and hence upgrade to WPA security for their wireless networks. Payment kiosks should be located in the range of security cameras so that constant vigilance can be maintained. Training should be conducted throughout the company to increase awareness about the importance of maintaining IT security. A company of such scale should go through regular quarterly audits so that intrusions are detected early. Furthermore, a system should be put into place which rewards employees for reporting bugs.

TJX should disclose such cyber attacks to the public early. Customers affected should be contacted timely and directly. Visible and honest communication creates the impression that the company is proactively involved in solving the current crisis.

TJX did not have any risk mitigation or response plan at the time of the incident. Constant vigilance of your systems, your procedures and your people working on those systems is the price of computer security today. If you are not willing to pay that price, you may just find yourself in the daily headlines (Lundquist, 2007). The company should have a risk matrix model which evaluates potential risks in different categories facing the company and steps that can be taken to mitigate these risks. Communication channels and response teams should be put in place to manage these risks.

Conclusion

The analysis of this cyberattack depicts how some large organizations are still not prioritizing IT security. Despite concerns raised by the IT department on the need for upgrades to their wireless security policy, TJX opted for cost savings rather than increased spending. Due to this incident, the company faced penalties and further scrutiny from government regulators, lawsuits from credit card companies and affected customers, loss of confidence; among other concerns. Eventually, TJX suffered losses far higher than the expenses they would have incurred if they had maintained a robust IT security policy. This shows that TJX must adhere to current world standards in relation to their IT security policy. Furthermore, they should realize the need for continuously maintaining and upgrading their security policies to maintain a positive security posture.

(1984 words)

References

TJX Companies Inc, 2007. *FORM 10-K*. [online] Available at: <https://usatoday30.usatoday.com/money/industries/retail/2007-03-29-tjxfiling.pdf> [Accessed 6 September 2020].

ComputerWeekly.com. 2020. *TJX Hack The Biggest In History*. [online] Available at: <https://www.computerweekly.com/news/2240080607/TJX-hack-the-biggest-in-history> [Accessed 6 September 2020].

Xu, W., Grant, G., Nguyen, H. and Dai, X., 2008. Security Breach: The Case of TJX Companies, Inc. *Communications of the Association for Information Systems*, 23(31), p.584.

Zetter, K., 2010. *TJX Hacker Gets 20 Years In Prison*. [online] WIRED. Available at: <https://www.wired.com/2010/03/tjx-sentencing/> [Accessed 6 September 2020].

Computer Fraud & Security, 2020. TJX hacked to the max: 45 million cards. (4), pp.2-3.

The Sydney Morning Herald, 2007. Data Theft Believed to Be Biggest Hack. [online] Available at: <https://www.smh.com.au/national/data-theft-believed-to-be-biggest-hack-20070330-gdpsoi.html> [Accessed 6 September 2020].

Lundquist, E., 2007. *Protecting Data Requires Constant Vigilance*. [online] eWEEK. Available at: <https://www.eweek.com/security/protecting-data-requires-constant-vigilance> [Accessed 6 September 2020].