The TJ Maxx Credit Card Incident

2007. TJ Maxx, the largest off-price clothing retailer in the United States still suffers from the biggest credit-card theft in history. The company lost at least 45 million credit and debit card numbers resulting in a huge amount of fraudulent transactions due to weak security systems in at least one store. In addition, the customers lost believe in TJX- which led to a huge cut of sales.

About TJ Maxx (TJX)

TJX operates 800 stores in the US and produces a net income of $690,420,000 (2006). Until the end of year 2006, they were growing day by day, leading their market sector. A part of their success derived from the use of modern technology within their stores. However, this rapid economic improvement turned upside down on January 17, 2007 when TJX announced that their systems were compromised and credit-card data was stolen. As a result, their stock-exchange price decreased by nearly 10 percent within several days.

… TJX produces a net income of $690,420,00 and leads its market sector

The site of crime

One of their stores, located near St. Paul (Minn.), became famous for the hugest loss of credit card information ever. In July 2005, hackers began to access the local computer system of this Marshals store to get access to the whole TJX network.

The Marshal store used wireless price-checking devices to avoid a large amount of wires within the store. The submitted data is received by a server that requires the employees to log in. In the early phase of the theft, the hackers streamed data to a laptop using antennas to catch the radio within peak hours. Even though their identity is unknown, people believe that they used to be Romanian hackers due to their way of compromising the system. It is also questionable how many hackers were involved in this case: Investigations show that they left messages on the system to prevent redundant work.

The technical background

They used common technique to intercept the data from these devices. Nowadays, there are two important standards dealing with wireless encryption: the Wired Equivalent Privacy (WEP) Standard, a standard that was developed in 2000 and Wi-Fi Protected Access (WPA), developed in 2003. While a lot of WEP networks were hacked with easy accessible software within minutes, the wireless industry created the better WPA standard. Besides having a better encryption rate and a reliable authentication system, it provides higher payload integrity. In order to achieve this higher security, it is required to use appropriate devices and software. Unfortunately, TJX did not upgrade their systems to the WPA standard. Furthermore, the store near St. Paul missed to install and configure the whole security software as they were supposed to do. As a consequence, the hackers got easy access to the local system and managed to create their own user accounts with full administrator rights. In order to synchronize the store data with the whole company, every local store manager had access to the central database of Marshal in Framingham (Mass.), containing business and customer related data such as credit card numbers and contact information. During business hours, the hackers intercepted all the data that was processed within the store including unencrypted information during the credit card approval process. In addition, they managed to create procedures within the database to backup the existing credit-card numbers using the decryption tool for the TJX software.

… TJX used WEP for their mobile devices, a standard that has been hacked several times prior to this accident

After having access to these files, they continued collecting the data via internet due to privacy reasons: With a huge number of compromised computers all over the world, they were able to retrieve any kind of file with the confidence of being undetected. Having unlimited remote access to the TJX system, even more hackers were able to process the data.

The consequences

All in all, the hackers managed to get at least 45.7 million credit and debit card numbers- a new record in history. Unofficial sources say that they might have captured about 200 million. In addition, they grabbed thousands of Social Security Numbers and driver's license numbers. While getting more numbers day by day, the hackers then sold packages of credit card numbers on private internet pages all over the world. These sites served smaller crime gangs. During this time nobody, including TJX or any customer, knew about who had access to their credit card information. In the following months, several small purchases were recorded throughout the US, but only one gang has been arrested: They bought several WALMART gift cards worth $1 million dollar and used to spend them for electronics and jewelry. One WALMART employee became suspicious because of the large number of small transactions within a small time frame and called the police. This case led to further investigations at TJX that disclosed the credit card theft: On December 18, an auditor found uncommon data and processes within the TJX system. This led to the press release in January, in which the company had to publish the theft. Meanwhile a lot of customers received suspicious bills with transactions they had never made. Due to mostly small amounts, the huge credit card companies were not able to see whether the card is compromised or their client is just spending a lot of money in small transactions. Furthermore, TJX deleted its own records of the stolen data during regular processes. Thus, a lot of credit card numbers are still in circulation without any knowledge of their owner.

... Hackers managed to get at least 45.7 million credit and debit card numbers […], they might have captured about 200 million.

Payment Card Industry data security standard

The credit card industry defined specific rules for the behavior with credit cards. For every step in processing a credit card purchase, there are some specifications that every company hast to fulfill. Actually, TJX violated some important parts of these specifications: Firewalls and Anti-Virus software

was not installed properly, data was unencrypted during the approval process and they missed to track access to the network resources. These violations lead to the question: who has to pay for this accident?

Financial responsibilities

The financial damage coming along with this case was immense: Despite the amount lost due to unauthorized credit card payments, the banks had to cover the expenses for replacing all compromised cards. Even though TJX pointed out that three quarters of the stolen credit cards were useless (because of expiration or missing security codes), it is rumored that the whole replacement process will cost about $300 million. The banks have to bear the costs of this incident while TJX only has to cover a small amount. TJX however, has to face other costs: business analysts estimate $1 billion to rehabilitate from this accident, including expenses to renew their security system and increasing their reputation within publicity. De facto, TJX only spent $5 million for new security systems while a renewal might cost $100 million. In order to ensure the customers of a secured system, they set up customer hotlines where every compromised card holder can get important information. To get customers back into their stores, TJX has to spend a lot of money in gift cards for victims of this incident.

… Business analysts estimate $1 billion to rehabilitate

While the banks are not willing to pay for security gaps in their clients systems, they put pressure on the legislation: New bills force full financial responsibility for companies whose security systems are breached.

Conclusion

To put everything in a nutshell, one can say that the investment into state-of-the-art technology ensures a much higher security level. These investments may seem very expensive without having any security problems, but as the TJX incident shows, the expenses after huge problems could ruin the whole

company. Due to new bills and regulations, companies will have to pay for the damage they caused while the huge banks are trying to pay as little as possible. It is of highest importance to check and update security systems regularly in order to prevent being an easy target for the growing cybercrime community. The TJX case "will probably serve as a case study for computer security and business students for years to come. This one could be considered a worst-case scenario."

References

1. How Credit-Card Data Went Out Wireless Door, Wall Street Journal, May 4, 2007, by Joseph Pereira
2. Payment Card Industry data security standard
3. T.J. Maxx hack exposes consumer data, CNET News.com, January 18, 2007, by Joris Evers
4. MSN Money
5. Breach of data at TJX is called the biggest ever, The Boston Globe, March 29, 2007, by Jenn Abelson
6. T.J. Maxx data theft worse than first reported, MSNBC, March 29, 2007, by Mark Jewell