# Tjx it security breach essay

Business, Industries

Part I: Description In January of 2007 the parent company of TJMaxx and Marshalls known as TJX reported an IT security breach. The intrusion involved the portion of its network that handles credit card, debit card, check, and merchandise return functions. Facts slowly began to emerge that roughly 94 million customers’ credit card numbers were stolen from TJMaxx and Marshalls throughout 2006.

It was believed that hackers sat in the parking lots and infiltrated TJX using their wireless network. Most retailers use wireless networks to transmit data throughout the stores main computers and for credit card approval. The wireless data is in the air and leaks out beyond the store’s walls. TJX used an encryption code that was developed just as retailers began going wireless. Wired Equivalent Privacy or WEP is a wireless encryption code developed in 1999 that retailers began to implement. Within a couple of years hackers broke the encryption code and rendered WEP obsolete.

Many retailers never changed to updated encryption codes such as WPA or WPA2. TJX never upgraded and once hackers got access, they were able to sniff out transmissions and see where they were going and view information logged into a central server. Of the seven Basel II detailed loss event types, this event would be considered a level 3 category external fraud. Part II: Risk Factors The risk factors that contributed to this event are: Using obsolete encryption technology, prolonged detailed customer/credit information storage, and wireless IT system/signals that link directly to customer database.

These factors would be classified within the technology and information elements in Alter’s work system framework. Using the WEP data encryption technology affects the probability of a risk event. WEP has already been decoded and deemed obsolete. TJX wasn’t specifically targeted, but became an opportunity. Hackers drove around retailers’ parking lots searching for WEP wireless signals.

It was targeted because it was weak. Keeping detailed credit card transaction information for prolonged amounts of time will increase the impact. The database continues to build with millions of records and all the information becomes vulnerable. Once the WEP system was bypassed, the hackers now had access to all the records stored. In the case TJX stored unnecessary driver license information with credit card numbers, it’s estimated that 94 million customer records were stolen. Allowing the wireless network to link directly to the customer database affects both probability and impact. If security is breached through the wireless network, it increases the probability of getting through to the customer database.

It increases the impact by adding to the loss of data. If it wasn’t accessible, only data being actively transmitted through the wireless network would be accessible. Part III: Risk Assessment Given the facts of this security breach, TJX had to of believed that the probability was medium and impact of such a risk event was very low. Internal documents that were uncovered show that they were aware of the risks of using WEP encryption. The 60 minutes story speaks about a TJX vice president who sent his bosses this email: “ We are still vulnerable with WEP as our security key. It must be a risk we are willing to take for the sake of saving money. ” According the website www.

dbdataloss. rg, the known direct costs of settling their lawsuits was approximately 64 million. TJX took minimal steps to mitigate the threat of this security breach, you would have to assume they thought there was a low probability and it would have very little impact. This was the largest high tech credit card theft in history.

The monetary costs and loss of customer confidence is very significant and hard to estimate. TJX now knows just how large an impact a security breach can have on them. Due to this lesson learned, their IT security is reviewed and tested frequently. I believe that they would have had to change risk assessment impact to high and probability to high after this event. However, having the proper controls in place will mitigate the probability and impact. The cost to implement is insignificant compared to the potential loss. This risk event was a wake-up call to many retailers, not just TJX.

Part IV: Controls The control that failed to mitigate the risk event was using WEP encryption technology. It was sufficient when it was developed, but approximately 2 years later the code was cracked. TJX knew and failed to address the obsolete technology. As a retailer that accepts credit cards, it was later proved that TJX was not compliant with PCI Security standards. PCI stands for payment card industry and credit card companies have developed this list of security measures to help protect against theft. TJX collected too much personal information, kept it too long and relied on weak security encryption.

At the time of the breach, few retailers had converted to WPA and didn’t want t to spend the money to implement new security measures. As a preventative control TJX should have implement WPA encryption technology. As a detective control, TJX should actively monitor and test their WLAN security. As a corrective control, TJX should actively implement the following PCI standards: Requirement 1: Install and maintain a firewall configuration to protect cardholder data Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters Requirement 3: Protect stored cardholder data Requirement 4: Encrypt transmission of cardholder data across open, public networks Requirement 5: Use and regularly update anti-virus softwareRequirement 6: Develop and maintain secure systems and applications Requirement 7: Restrict access to cardholder data by business need-to-know Requirement 8: Assign a unique ID to each person with computer access Requirement 9: Restrict physical access to cardholder data Requirement 10: Track and monitor all access to network resources and cardholder data Requirement 11: Regularly test security systems and processes Requirement 12: Maintain a policy that addresses information security If TJX continuously monitored its WLAN network and would have implemented new encryption technology (WPA), this security breach could have been prevented. Recently TJX has updated to WPA encryption, has implemented PCI Standards, and will use a cryptographic hash as a unique customer identifier. All retailers can use the lessons of the TJX scenario to convince budget decision-makers that the cost of securing data is far lower than the cost of responding to a data breach. Sources http://attrition.

org/dataloss/2007/01/tjx01. html [archive] http://www. boston. com/business/ticker/2007/01/tjx_intruders_s.

html http://www. informationweek. com/news/mobility/showArticle. jhtml? articleID= 199500385 [archive] ttp://www. theregister. co. uk/2008/09/15/tjx_hacker_guilty_plea/ [archive] http://www.

newser. com/story/6218/arrest-marks-tjx-hack-case-breakthrough. html/ [archive] http://www.

computerworld. com/action/article. do? command= viewArticleBasic&articleId= 9043944 [archive] http://www. msnbc.

msn. com/id/21454847/ [archive] http://www. privcom. gc. ca/cf-dc/2007/TJX_rep_070925_e. asp [archive] http://www.

cbsnews. com/video/watch/? id= 3538299n [archive] http://www. wired. com/threatlevel/2009/08/tjx-hacker-charged-with-heartland/ [archive]