T

T. J. Maxx is a subsidiary of the TJX companies' one of the largest chain departmental store in the USA retailing home fashion and apparel. The company which has annual sales revenues exceeding fifteen billion dollars experienced one of the worst ever recorded case of system breach . The company had more then forty five million of its customer's confidential data was stolen by hackers who breached the company's data base . According to the records filed by the company with the security exchange department they discovered the system breach in December 2006 . Their system was breached by hackers who got unauthorized access to their clients credit cards, debit cards and check clearing information resulting to one of the largest data breach ever recorded. Hacking or cyber security breach can be done for a variety of reasons these reasons included unauthorized extraction of data, data duplication, data exfiltration, data tampering, data deletion, data downloading, data eavesdropping, data spoofing and malicious data attack .

Cyber security threats can be complex, varied and are often evolving. Those who carryout cyber security breaches are often highly motivated . they therefore try to breach even the most secure systems (Bidgoli 2006). Cyber security can handily be fool proof but preventive measures can be introduced to a system to reduce the risks of exposure to hackers. Most of the cyber security breaches often result in loss of sensitive confidential and valuable data. Security breach can also be conducted in order to sabotage a system or uses the system in an authorized manner. In other words in cyber security breach enables hackers to violate the internal usage of a system. The company had much personal information which they kept for a longer

period. Their system had weaker encryption technology making the system vulnerable to hackers. They were therefore able to extract and download personal data belonging to over forty five million T. J. Maxx customers. The credit and debit cards data was later encoded on fake credit cards and used to purchase more that a million dollars worth of mrchandise from the Wal-Mart stores.

The breach resulted in loss of their client's personal information which included credit card information, personal social security details, driver's license details and numbers. These details were downloaded by hackers who intruded into the company's system. The security breach was made possible due to their wireless network having weaker encryption codes

Debit cards and credit cards contain a lot of information stored on the magnetic strip . This information is usually stored as unencrypted data and it is therefore visible as clear text to a computer swipe systems. Therefore when the credit card is swiped on a merchants terminal or a stores terminal in order to make a payment the data travels to a payment network from the payment terminal (Stolfo et al 2008) . This process is quite fast and can take only a few seconds however through this journey the data is most vulnerable. In the few seconds that the data travels to the network is all travels hackers with access to the system can steal the information. Hackers are able to access the system by penetrating security firewalls or unlocking the data codes that are used to secure the system. In this case the hackers were able to penetrating T. J. Maxx security firewalls and since the company was using a weaker encryption data system the hackers were able to easily

unlock the data codes and download millions of consumers' confidential data details.

The data that was stolen was used encode fake credit cards that were used to purchase merchandise at other store by impersonators. The individuals who were caught for impersonating the credit card owners admitted buying the stolen information from unidentified hackers. This implies that personal information was stolen and sold to the highest bidders. Therefore there was loss of confidentiality since most card users provide information to the card companies on the assumption that whatever personal details they provide would only be used to expedite their card transactions. The possibility of such information falling into the wrong handss as it was in this case only puts them in vulnerable positions not only in terms of monetary losses accruing from the misuse of the given information but also in security terms.

Such an argument can arise bearing in mind that these cards usually contain information that can easily give a hacker their residential addresses , place of work , occupation among other confidential details that an individual would rather have remain confidential or in the hands of trusted individuals or entities. Such a los therefore can lead to loss of confidence in the organizations that provide services and goods and in return acquire confidential information to enables such services or transactions to take place. It is on the basis that the information provided remains confidential that majority of such service are able to provide even the most intimate details of their lives. So those who learn that such information has fallen into the wrong hands feel betrayed and are unable to predict or anticipate the future acts of the thieves besides being monetarily stripped.

One of the reasons that make organizations such as T. J. Maxx attractive to hackers is that they are personal data goldmines. Any organization that transacts with consumers on other payments methods besides cash is therefore vulnerable since it is universal knowledge that if they transact through cards then the definitely have consumer data that is loaded with confidential information. It is on the basis of the information that they hold that majority of their consumers assume that those with access to such information are people of high integrity who are capable of maintain the confidentiality that they are entrusted with.

To protect data from being easily accessible or to minimize the risks the first set should to ensure that the company does not collect a lot of unnecessary personal information (Bayuk 2010). The data collected should also not be kept for long. They should also use a system that encrypts data from the card swipe point to ensure that the risks of exposing it to hackers on the journey to payment network are minimized.