**DOI: https://doi.org/10.53555/nnbma.v2i2.104** **Publication URL: http://nnpub.org/index.php/BMA/article/view/104**

# THE ROAD TO DATA SECURITY IN THE DIGITAL WORLD: THE PAST DATA THEFT CASES

**Kay K. Kim[1]***

*[1]*Department of Business Administration Fitchburg State University, Fitchburg, MA USA*

*Email: kkim@fitchburgstate.edu*

***Corresponding Author: -***

*Email: kkim@fitchburgstate.edu*

## Abstract: -

*Credit card data theft has been a critical issue in the United States for more than a decade. Many well-known and successful companies, including TJX and Sony, have been the victim of credit card data theft. Most recently, Target and Neiman Marcus, two extremely successful US retailers, have had thousands of customers' credit card information compromised. This paper details four of the most highly publicized cases of credit card data theft to affect the United States. Additionally, this paper outlines ethical and legal implications to prevent this data theft from continuing to occur in the future.*

**Keywords: -** *Credit card data theft, Hacking, Malware, Cyber-security, Firewall, Chip-and-Pin technology*

## I. INTRODUCTION

Credit card data theft has been a major issue plaguing retailers nationally for several years. The frequency with which data theft occurs at retailers is largely due to the ease with which data can be stolen. In most cases, data is stolen while the thieves are nowhere near the physical location of the retailer, making the attack largely anonymous. Often retailers remain unaware of an intrusion on their system for several days, and by the time an issue is detected, the damage has already been done (Editorial Board, 2014).

Throughout the past several years, experts in data theft have proven it very easy to infiltrate a company's point of sale system through the use of stolen credentials or by hacking company firewalls to install malicious software (malware) on a system. This malware begins to act immediately, stealing credit card names and numbers with every swipe of a card on a pin pad. Over the past ten years, several nationally and internationally recognized companies have fallen prey to credit card data theft. As can be seen in past data theft cases, an increase in digital/information technology (IT) security, in addition to an establishment of more clearly defined and strengthened regulations are essential for protecting the basic rights of IT users worldwide.

## II. Cases Of Data Theft

### A. TJX Companies

In March 2007, TJX Companies, the parent company of Marshall's, Home Goods, and TJ Maxx, created headlines when it announced that tens of millions of credit cards were exposed to a data breach during the Christmas shopping season of 2006. The quantity of cards affected has not been made public to this present day. While a Security and Exchange Commission (SEC) filing from 2007 lists the number of affected cards at more than 45 million (Greenemeier, 2007), additional data later revealed that as many as 94 million credit cards were exposed (Armerding, 2012).

The account of what happened is still debated today. One story suggests that a group of hackers took advantage of TJX's weak data encryption system to steal the credit card data during wireless transfers between two Marshall's stores in Miami, Florida. Another story claims that the TJX network was infiltrated through in-store kiosks that were used to electronically apply for a job with TJX. According to experts, this theory of data theft is conceivable because of a lack of firewalls to protect the TJX system (Armerding, 2012).

While the true method of data theft that was used is unclear, a timeline of the theft is available within an SEC filing made by TJX companies in 2007. According to the filing, the TJX IT systems were initially infiltrated in July 2005. Intrusions continued periodically throughout 2005 and then again from May 2006 to January 2007. No customer data was actually stolen until December 18, 2006. By December 21, 2006, TJX had "strong reason to believe that their computer systems had been intruded upon and that an intruder remained on their computer systems," according to the SEC filing (2007). In an effort to continue the criminal investigation, the United States Secret Service instructed TJX not to go public with the intrusion. In 2010, Albert Gonzalez, a computer hacker credited with several data breaches, was sentenced to forty years in prison for masterminding the TJX data theft (Armerding, 2012).

### B. Sony Playstation Network

In April 2011, Sony's Playstation Network, the online environment that exists for Sony Playstation video game users worldwide, was victim to the biggest gaming community data breach of all time. 12 million credit card numbers and an astonishing 77 million user accounts were affected by the data breach. Not only were credit cards stolen, but personal information such as names, addresses, phone numbers, e-mails, and purchase histories were exposed (Armerding, 2012).

While the perpetrators of this attack remain at large, the timeline of events is clear. On April 26, 2011, Sony confirmed that its Playstation Network was infiltrated between April 17 and April 19, 2011. Sony responded by completely shutting down its online service for a period of six days. Upon reentering the Playstation Network online, users were mandated to install a new security patch and change the password to their accounts. Only then could users be allowed back onto the network (Knafo, 2011).

Experts believe the attack on the Playstation Network should serve as a warning to anyone who shares personal information or makes online purchases. As the Huffington Post states, "Sony is far from the only company vulnerable to data theft, and without improvements to web security, we can expect hacks like this to happen again" (Knafo, 2011). Michael Sutton, the head of Research and Development at Zscaler, a company that specializes in securing information stored online, indicated that "Sony was just the latest in an increasingly long list of corporations" targeted by "very motivated, very focused, and likely well-funded hackers. They [the hackers] will find a way in, unless you have the absolute best security controls. In most of these cases, we are finding that these security controls were not the best they could have been" (Knafo, 2011).

### C. Neiman Marcus

On January 11, 2014, Neiman Marcus, a popular luxury department store chain in the United States, announced it was "the victim of a criminal cyber-security intrusion" during the 2013 holiday shopping season (Wallace, 2014). The company has not disclosed the quantity of credit cards that were affected by the data breach, but an apology was issued to all customers for the chain's failure to protect their customers' information. Karen Katz, Neiman Marcus' chief executive, expressed, "We deeply regret and are very sorry that some of our customers' payment cards were used fraudulently after making purchases at our stores. We want you always to feel confident shopping at Neiman Marcus, and your trust in us is our absolute priority." Katz revealed that only cards used in-store were affected in the breach. Online shoppers were not affected (Tsukayama, 2014).

Neiman Marcus first discovered a potential breach of data in mid-December 2013, at which time the company hired a forensic investigator to research the issue. On January 1, 2014, the investigation revealed evidence of a definite breach of credit card data. Nine days afterward, Neiman Marcus addressed the public with information on the breach, sharing the fact that an unknown number of credit cards were affected and that shoppers should check their bank statements for any possible fraudulent charges. While no information on the specific technique used in breaching Neiman Marcus' systems was provided, many believe the attack to have been linked to an even more significant data breach that occurred at the same time period at another popular US retailer (Tsukayama, 2014).

### D. Target

In the same month that Neiman Marcus had its systems breached to an unknown extent, one of the largest retailers in the United States, Target, suffered the same fate. On January 10, 2014, Target revealed that a data breach occurred during the 2013 holiday shopping season that impacted up to 110 million customers. The breach, which is one of the most noteworthy in history due to the stature of the victimized company, consisted of 40 million customers' credit and debit card information being stolen and another 70 million customers' personal information, including names, addresses, phone numbers, and e-mail addresses being exposed (Wallace, 2014).

Brian Krebs, an expert in cyber-security, revealed that the Target data breach originated from the stolen credentials of a Heating Ventilation and Air Conditioning (HVAC) vendor in Mechanicsburg, Pennsylvania. The vendor had been hired to work on numerous Target stores and was given near unlimited access to Target's systems. Through the HVAC vendor, hackers initially infiltrated Target's systems on November 15, 2013, uploading malware on a handful of registers at Target between November 15th and Thanksgiving 2013 to serve as a test. After the test was a success, it only took the hackers two days to upload the malware in the majority of Target stores (Morran, 2014).

The data breach at Target occurred despite firewalls, malware detection software, and data-loss prevention tools already actively being in place at the retailer. In a statement made to the Senate Judiciary Committee, Target's Chief Financial Officer, John Mulligan, stated that retailers are facing "increasingly sophisticated threats" that outmatch current data security methods. Mulligan additionally revealed that Target had not known of the attack on their systems until the Justice Department notified the company of what was happening on December 12, 2013, nearly one month after the initial hacking occurrence (Pagliery, 2014).

## III.Ethical Implications Arising From Digital/It Systems

The digital age has opened doors to the global economy, making it easier, quicker, and more efficient for technology users to carry out their business, whether it is purchasing, marketing, or selling goods. While the ease and time efficiency associated with utilizing IT systems are remarkable benefits, these benefits have brought about dangerous consequences for users both across the nation and around the world. The exploitation of personal data and the resulting compromise of user privacy are one of the greatest problems and concerns that stem from the development of information technology and the growth of the digital age. IT systems, such as the internet, have brought with it an explosion of accessible data, including personal data (McAdams, Neslund, & Zucker, 2012). The data theft cases for TJX Companies, Sony Playstation Network, Neiman Marcus, and Target have demonstrated the vulnerability of the IT sources that were used at these corporations and how the confidential information of customers, which were intended to be stored and protected in secure databases, had been permeated to unintended persons and places.

## IV.Law And Its Application To It Systems

Fast changing technology in the digital world has made it a continuous challenge for IT systems to ensure data security. Criminal behavior, such as hacking, data aggregation, data mining, phishing, spear phishing, and cyberattacks, have made it increasingly difficult for businesses and clients to maintain faith or trust in the security of IT systems. While the weakness of IT systems and their inability to keep up to pace with rapidly evolving technology are to blame for data security breaches, the main source of this problem lies in the lack of laws governing digital/IT control. While various government groups and the United Nations have attempted to provide a means for controlling the internet and IT systems, no existing judicial or legislative body has obvious or natural jurisdiction over these electronic systems in their entirety (McAdams et al., 2012). The lack of control, ownership, and law enforcement has made this technology defenseless to security adversities.

The digital world up to the present time has been managed in a quasi-deregulated or unregulated manner with minimal government regulation. In relation, the United States has had no comprehensive privacy law addressing the internet and digital environment; instead, the privacy of users has largely been left to the self-regulation of service and content providers (McAdams et al., 2012). The creation, defining, enactment, and refining of regulations are essential for protecting the intellectual and personal data of both businesses and clients alike. Regulations over IT systems can better ensure that the information supplied electronically or stored in electronic databases are used by the intended source for solely its intended purpose and held confidentially at its intended location.

## V. Conclusion

IT systems have changed and developed throughout the past twenty years and will continue to make further advancements as the digital age progresses. With changes to any system, laws and regulations must follow not only to ensure that these systems evolve in an orderly, rational manner, but also to ensure that the basic amendment rights of all individuals impacted by these systems are not violated. In order to better guarantee that all information stored or relayed through electronic systems are guarded from data theft, it is critical for all involved parties to play their part. More pecifically, the IT sector must continue to develop the latest security technologies to safeguard the intellectual property of users, businesses utilizing IT systems must be diligent with exploring and implementing the latest and greatest information security mechanisms that have been developed to be able to protect the confidential information of their clients, the government must set forth clear regulations to lay out the rules and guidelines for proper use of IT systems and to protect the basic rights of users, and all users of IT systems must take precautionary measures and use sound judgment before remotely storing or publicly exposing any confidential information. The establishment of regulation, as well as each party's acknowledgement and active execution of their responsibilities will enable the digital environment to achieve Aristotle's profound observation that "law is order and good law is good order".

**References**

[1].Armerding, T. (2012). The 15 Worst Data Security Breaches of the 21st Century. Retrieved from http://www.csoonline.com/article/700263/the-15-worst-data-security- breaches-of-the-21st-century

[2].Editorial Board. (2014). Changes in Credit Card Security are Long Overdue. *Washington Post.* Retrieved from http://www.washingtonpost.com/opinions/changes-in-credit-card- security-are-long-overdue/2014/02/10/bef387d6-9015-11e3-b46a- 5a3d0d2130da_story.html

[3].Greenemeier, L. (2007). TJ Maxx Parent Company Data Theft is the Worst Ever. *Information Week*. Retrieved from http://www.informationweek.com/tj-maxx-parent-company- datatheftis-the-worst-ever/d/d-id/1053522?

[4].Knafo, S. (2011). Sony Playstation Network Hack is Just the Beginning of Giant Data

[5].Theft: Experts. *Huffington Post*. Retrieved from http://www.huffingtonpost.com/2011/05/06/playstation-theft-sony-hack_n_858355.html

[6].McAdams, T., Neslund, N., & Zucker, K. (2012). *Law, Business, and Society*. New York, NY: McGraw-Hill.

[7].Morran, C. (2014). Credentials Used for Target Hack Reportedly Stolen from HVAC

[8].Vendor. *The Consumerist*. Retrieved from http://consumerist.com/2014/02/05/credentials- used-for-target-hack-reportedly-stolen-from-hvac-vendor/ Pagliery, J. (2014). Target to Invest in Chip-Based Cards. *CNN Money*. Retrieved from http://money.cnn.com/2014/02/04/technology/security/target-senate/

[9].Tsukayama, H. (2014). Neiman Marcus: We Deeply Regret Data Breach. *Washington Post.* Retrieved from http://www.washingtonpost.com/business/technology/neiman-marcus-we-deeply-regret-data-breach/2014/01/16/7bd54b30-7ee8-11e3-93c1- 0e888170b723_story.html

[10]. Wallace, G. (2014). Target and Neiman Marcus Hacks: The Latest. *CNN Money*. Retrieved from http://money.cnn.com/2014/01/13/news/target-neiman-marcus-hack/