Are Companies Really Protecting Consumer Information

Carl Brackett

East Carolina University

Abstract

Technology has changed through the years and has affected the way items are purchased, whether it is online or at conventional stores. Cash or check is not the only means of paying for a purchase as people have started taking advantage of debit or credit cards since they are suppose to be safer than carrying cash. The real question that comes to mind, are people really safer using a debit or credit card?

People are under the impression that their information associated to these cards are safe and secure when making a transaction, but the fact is unclear to most individuals that the information is vulnerable when these companies do not take appropriate security measures to keep this information secure. Over the last several years, there have been many incidents where this data has been obtained from security breaches like Target, Wal-Mart, TJ Max, Home Depot, or online websites like Apple or eBay.

Investigating these types of security compromises will provide knowledge and specific examples of security breaches that were not properly prepared for when an attack occurred on their data, which the consumer trusted with the company when they slid their card at the company's register. These breach examples will provide some insight on how security management can prepare for future attacks and lessons learned from previous experiences. Conclusions will be based on information provided by these specific examples of security compromises.

Keywords: security, breach, compromises, companies, data

Introduction

Through the years, people have changed the way they purchase items from a store. Technology has played a major role in this endeavor since new payment methods have been developed other than using cash. Since the development of the Internet, places are able to easily accept credit and debit cards. The question is the data associated with these cards being protected correctly by companies?

Consumers like the fact they do not need to carry cash on their person when they have one of these plastic cards with them. What the consumer does not realize is the amount of information that is stored on the card itself. The information that is embedded into the tracks of the card, particularly track 1 and 2, contain the consumer's name, expiration date and primary account number ("Magnetic stripe card," n.d.). This information alone is enough for anyone to use the consumer's card to make a transaction, especially if it is an online purchase.

This research is going to explore several incidents that have occurred in the last several years. It will show examples of how companies have dealt with these situations that occurred and what may have been done differently to prevent them from occurring. Companies assume they are secure for electronic transactions when they get their certifications, but do not realize that being certified does not mean their data is secured. Securing consumer information is an ongoing process that should be updated regularly to make sure the company is in compliance with emerging technology trends.

Conclusions will be based off of findings from this research to evaluate how companies can secure consumer information and provide a safe environment for their consumers to make transactions onsite or web based.

Literature Review

Technology changes on a daily basis and has no exceptions when it comes to securing it or the data that interacts with it. Companies earn certifications and think they are in compliance with security standards, but in reality they are setting themselves up for a future cyber attack. Companies that store or transmit card data need to at least implement Payment Card Industry Data Security Standard (PCI DSS), but it is not a requirement by federal law ("Payment Card Industry Data Security Standard," n.d.). This standard exists to help with credit card fraud to make sure a company has some security features in place to protect consumer data ("Payment Card Industry Data Security Standard," n.d.).

Most companies use a card reader to take the information from a consumer's credit or debit card. These card readers make a record of the sensitive information the card contains to make the transaction. The responsibility fails on the company to safe guard this information and delete it accordingly to their security policy guidelines. If the company is not securing this information correctly they are not in compliance with PCI DSS standards.

The United States is the only country left using the old card swipe system; this is why half of the world's credit card fraud happens in the United States ("October 2015: The End of the Swipe-and-Sign Credit Card," 2014). This system is being phased out and replaced with a newer system that uses a microchip embedded in the credit or debit card instead of using the magnetic strip on the card ("October 2015: The End of the Swipe-and-Sign Credit Card," 2014). The credit or debit card will be inserted into the card reader through a slot to read the embedded microchip instead of being swiped to

have the information read off of the card ("October 2015: The End of the Swipe-and-Sign Credit Card," 2014). Company security breaches will be more difficult for a hacker to get consumer information with this new technology in place ("October 2015: The End of the Swipe-and-Sign Credit Card," 2014).

Every company needs a good security plan in place that is updated on a regular basis or a potential threat could occur. A good example would be the Home Depot breach that occurred back in September 2014 ("Notice to Our Customers," 2014). This breach occurred due to a third party vendor's username and password being used to get on the corporate network ("Home Depot hackers stole 53 million emails, too," 2014). The problem occurred once the hackers had access to the network, they were able to send out malware that effected some card readers attached to Home Depot's payment system ("Home Depot hackers stole 53 million emails, too," 2014). Even though Home Depot has patched the vulnerability to their system, the damage has already been done. If proper procedures were in place and had been followed, this attack may have never happened.

Even though Home Depot had a security team, a breach in their network still occurred. This leaves questions to what security measures did they have in place for third party vendor access. These are the type of questions that need to be answered and documented in their corporate security plan. The company has to take responsibility in making sure that vendors they associate with have the same type of security standards they implement themselves. It may be impossible to stop every type of attack that may occur but documentation will show that the company is trying to protect the company's assets and consumers data.

It is estimated that 56 million credit and debit card numbers were stolen from Home Depot between April and September 2014 ("Home Depot: 56M Cards Impacted, Malware Contained," 2014). Since the breach has been contained Home Depot has added enhanced encryption to their payment system at all US locations ("Home Depot: 56M Cards Impacted, Malware Contained," 2014). This new encryption method takes the card information and randomizes the data causing the information to be scrambled and useless to anyone trying to access it ("Home Depot: 56M Cards Impacted, Malware Contained," 2014).

Another example that occurred in November 2013, a year earlier, was the Target Store breach ("Target Hackers Broke in Via HVAC Company," 2014). The breach into Target was gained by using a third party vendor's username and password which allowed hackers to gain access to the network to install malware onto the point of sale systems ("Target Hackers Broke in Via HVAC Company," 2014). This allowed the hackers to record transaction details for purchases made at Target locations. Even though current PCI standards do not require point of sale systems to be on a separate network, a two-step authentication process is required for any type of remote access given to users including vendors and subcontractors ("Target Hackers Broke in Via HVAC Company," 2014).

Forty million credit and debit card numbers were stolen from Target during the security breach ("Target Breach, By the Numbers," 2014). The hackers also obtained an estimated 70 million records containing consumer information like names, addresses and email addresses during the breach ("Target Breach, By the Numbers," 2014). Target did not have any chip-enabled terminals installed at any locations for payment before the breach that could have prevented the attack from even

occurring ("Target Breach, By the Numbers," 2014). They estimated 100 million dollars to upgrade their locations with the new chip-enabled terminals ("Target Breach, By the Numbers," 2014).

Earlier in 2006, Wal-Mart stores were targeted by a hacker gaining access to the network with old employee credentials for VPN access (Zetter, 2009). Once the hackers had access to the network they started targeting the point of sale programming team (Zetter, 2009). The hackers were only detected due to a server crash that had occurred from the hackers trying to run password-cracking software (Zetter, 2009).

What is interesting in this security breach is that Wal-Mart was not compliant with PCI standards; findings from an internal security audit found that customer data was poorly protected (Zetter, 2009). To help the company get in compliance with PCI standards they had an external security audit performed, that found multiple issues like unencrypted customer data being stored on servers and easily guessed passwords that were used across different locations (Zetter, 2009).

These issues were listed in a report that security auditors gave the company ten months before the breach was identified on their network (Zetter, 2009). Wal-Mart knew they had issues to resolve to protect consumer data and may have avoided a security breach if someone would have disabled the dismissed employee's VPN access in a timely fashion. The investigations did not show any evidence of customer data being stolen during the security breach (Zetter, 2009). Issues that were revealed in the auditors report have been corrected (Zetter, 2009). In August 2006, Wal-Mart became PCI compliant and performs two PCI audits every six months (Zetter, 2009).

In 2005, TJ Max had 45.7 million credit and debit cards information stolen by a security breach (Jewell, 2007). This breach occurred when a hacker or hackers cracked the password for the wireless network at a Marshall's location, which is part of the TJ Max Group, to gain access to the main network (Brian, 2007). Since the wireless network was using WEP for its security protocol it was not hard for the hacker or hackers to crack the key (Brian, 2007).

What is interesting is that TJ Max had an auditor's report showing the vulnerability to the network already but failed to have the issues corrected before the breach occurred (Brian, 2007). Also stolen in this security breach was 455,000 consumers license information that had returned an item to the store without a receipt (Jewell, 2007). Although it is not clear who performed the security breach, data transactions from January 2003 to June 28, 2004 were accessed (Jewell, 2007). The transactions that took place November 24, 2003 to June 28, 2004 have been deleted like they should have been prior to the security breach (Jewell, 2007).

So far the examples provided have been for card transactions that have been swiped inside a company location, but online companies are also a target to a security breach when a hacker is out to steal consumer information. A good example would be the online Ashley Madison website breach that occurred in July 2015 (Yadron, 2015). It is unknown how the hacker gained access to the consumer information, but released some of the data to prove they were in possession of it (Yadron, 2015).

The company is assuming it was not an employee of the company but possibly a third party vendor (Yadron, 2015). Keeping consumer information secure on the Internet is no different than swiping a credit or debit card at the register. The data is stored on a

system somewhere in the world that needs constant attention to keep the security on it up to date. It can have the same security holes or vulnerabilities that can be seen in the point of sale systems in a company.

In 2014 another security breach where consumer information was obtained, would be when celebrity photos from different Apple iCloud accounts appeared on the Internet. The breach may have originated from the Find My Phone app on Apple iOS devices (McCormick, 2014). The hacker may have used this app to guess the username and passwords instead of the app shutting down after multiple access attempts (McCormick, 2014). Apple has not confirmed the security breach but there are claims the app does not protect the encrypted data from certain attacks (McCormick, 2014).

Even though Apple claims there was not a security breach, they are tightening security for iCloud accounts with a two-step authentication process to secure consumer accounts against security breaches (Kirk, 2014). This authentication process will require a number passcode in addition to accessing the account making it harder for a hacker to guess the password for the account (Kirk, 2014).

In 2014 eBay was hacked where consumer information was stolen when employee login credentials where used to gain access to the network (Kelly, 2014). The hacker stole customer names and encrypted information like passwords, email addresses and phone numbers (Kelly, 2014). The security breach occurred in February 2014 to March 2014 but was not discovered until early May 2014 (Kelly, 2014). Financial information for the company and PayPal were not stolen with the rest of the consumer's information (Kelly, 2014).

Although eBay has not seen any kind of irregular activities with their accounts since the security breach, they asked their users to change their passwords ("eBay Urges Password Changes After Breach," 2014). They emphasized not to use the old password anywhere else as it may make them vulnerable to a security breach on another site ("eBay Urges Password Changes After Breach," 2014). The online auction site does not reveal what type of encryption they store their passwords in, but at least they are taking more precautions than most companies.

Conclusion

Companies that use technology in their business have to develop a security policy that they can keep up to date on a regular basis to provide the necessary services to its consumers. They are obligated to secure any type of information they obtain from a consumer since they are putting trust into the company by making a transaction. Technology changes only a daily basis when it comes to security, even when it involves a simple card reader that reads a magnetic strip on a credit or debit card.

The information provided by these cards can affect the consumer tremendously, since their most confidential information can be retrieved from it. Not all consumer information involves credit or debit cards especially when companies are online like eBay or Apple. These companies have to have the same security standards or maybe a little more since they can be accessed from anywhere in the world by the Internet.

From the examples that were researched in this paper, there were similarities in many of the security breaches. Companies may think they are secure but need to make sure third party vendors that they hire also follow the security guidelines put in place by the company. These companies that have a security team or policy in place need to make

sure they are enforcing it, since one of security breaches occurred because of an old VPN account that did not get disabled soon enough.

It is the company's responsibility to make sure they are taking the proper steps to look after the consumer whether they are at a store location or on an online website. If the proper precautions are taken and kept up to date regularly, security breaches may not affect the company or the consumer as frequently.

References

Brian. (2007, May 5). Details of TJX Hack Emerge – Wireless Networks the Weak Point. Retrieved from http://bhconsulting.ie/securitywatch/?p=85

eBay Urges Password Changes After Breach. (2014, May 21). Retrieved from http://krebsonsecurity.com/2014/05/eBay-urges-password-changes-after-breach/

Home Depot hackers stole 53 million emails, too. (2014, November 6). Retrieved from http://money.cnn.com/2014/11/06/technology/security/home-depot-breach-emails/

Home Depot: 56M Cards Impacted, Malware Contained. (2014, September 18). Retrieved from http://krebsonsecurity.com/2014/09/home-depot-56m-cards-impacted-malware-contained/#more-27975

Jewell, M. (2007, March 30). T.J. Maxx theft believed largest hack ever. Retrieved from http://www.nbcnews.com/id/17871485/ns/technology_and_science-security/t/tj-maxx-theft-believed-largest-hack-ever/#.VbByGLc105u

Kelly, G. (2014, May 21). eBay Suffers Massive Security Breach, All Users Must Change Their Passwords. Retrieved from http://www.forbes.com/sites/gordonkelly/2014/05/21/eBay-suffers-massive-security-breach-all-users-must-their-change-passwords/

Kirk, J. (2014, September 5). Apple CEO vows to tighten iCloud security. Retrieved from http://www.computerworld.com/article/2602965/security0/apple-ceo-vows-to-tighten-icloud-security.html

Magnetic stripe card. (n.d.). In *Wikipedia, the free encyclopedia*. Retrieved July 16, 2015, from https://en.wikipedia.org/wiki/Magnetic_stripe_card

*McCormick, J. (2014). Apple looks for iCloud loopholes after celebrity photo leak. *Silicon Valley Business Journal*. Retrieved from http://www.bizjournals.com/sanjose/news/2014/09/02/apple-looks-for-icloud-loopholes-after-celebrity.html

Notice to Our Customers. (2014). Retrieved from https://corporate.homedepot.com/MediaCenter/Documents/Important%20Customer%20Notice.pdf

*October 2015: The End of the Swipe-and-Sign Credit Card. (2014, February 6). *Wall Street Journal*. Retrieved from http://blogs.wsj.com/corporate-intelligence/2014/02/06/october-2015-the-end-of-the-swipe-and-sign-credit-card/

Payment Card Industry Data Security Standard. (n.d.). In *Wikipedia, the free encyclopedia*. Retrieved July 21, 2015, from https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

The Target Breach, By the Numbers. (2014, May 6). Retrieved from http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/

Target Hackers Broke in Via HVAC Company. (2014, February 5). Retrieved from http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

*Yadron, D. (2015). Hackers Target Users of Infidelity Website Ashley Madison. *Wall Street Journal*. Retrieved from http://www.wsj.com/articles/affair-website-ashley-madison-hacked-1437402152

Zetter, K. (2009, October 13). Big-Box Breach: The Inside Story of Wal-Mart's Hacker Attack. Retrieved from http://www.wired.com/2009/10/walmart-hack/