GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Case Study: The Home Depot Data Breach

GIAC (GSEC) Gold Certification

Author: Brett Hawkins, hawkbluedevil@gmail.com
Advisor: Christopher Walker
Accepted: January 2015

Abstract

The theft of payment card information has become a common issue in today's society. Even after the lessons learned from the Target data breach, Home Depot's Point of Sale systems were compromised by similar exploitation methods. The use of stolen third-party vendor credentials and RAM scraping malware were instrumental in the success of both data breaches. Home Depot has taken multiple steps to recover from its data breach, one of them being to enable the use of EMV Chip-and-PIN payment cards. Is the use of EMV payment cards necessary? If P2P (Point-to-Point) encryption is used, the only method available to steal payment card data is the installation of a payment card skimmer. RAM scraping malware grabbed the payment card data in the Home Depot breach, not payment card skimmers. However, the malware would have never been installed on the systems if the attackers did not possess third-party vendor credentials and if the payment network was segregated properly from the rest of the Home Depot network. The implementation of P2P encryption and proper network segregation would have prevented the Home Depot data breach.

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

1. Introduction

On September 8th, 2014, Home Depot released a statement indicating that its payment card systems were breached. They explained that the investigation started on September 2nd and they were still trying to discover the actual scope and impact of the breach. Home Depot explained that they would be offering free credit services to affected customers who used their payment card as early as April of 2014 and apologized for the data breach. They also indicated that their Incident Response Team was following its Incident Response plan to contain and eradicate the damage and was working with security firms for the investigation ("The Home Depot, Inc. - News Release," 2014). This is one of many retail breaches that have occurred and will continue to occur, until retailers become proactive in safeguarding their environments.

1.1 Making money with stolen credit cards

Payment card information is sold by cyber-criminals frequently. In more recent retail breaches, they have been able to steal payment card information from millions of customers and sell it online in what is known as the "Darknet." Once the cyber-criminal has stolen the payment card information, there is a process that takes place in order to put the information on sale on the Darknet and for the cyber-criminals to make money.

The first step in the process is selling the payment card information to brokers. The brokers buy the payment card information in bulk and sell the information to "carders" on carder websites (Westin, 2013).

The definition from "How 'carders' trade your stolen personal info" says, "Carders are the people who buy, sell, and trade online the credit card data stolen from phishing sites or from large data breaches at retail stores" (Vamosi, 2008). An example of a carder website is Rescator shown in **Figure 1** below (Lawrence, 2014). As you can see, the site has full search capabilities based on the type of card you are searching for.

Brett Hawkins, hawkbluedevil@gmail.com

© 2015 The SANS Institute Author retains full rights.

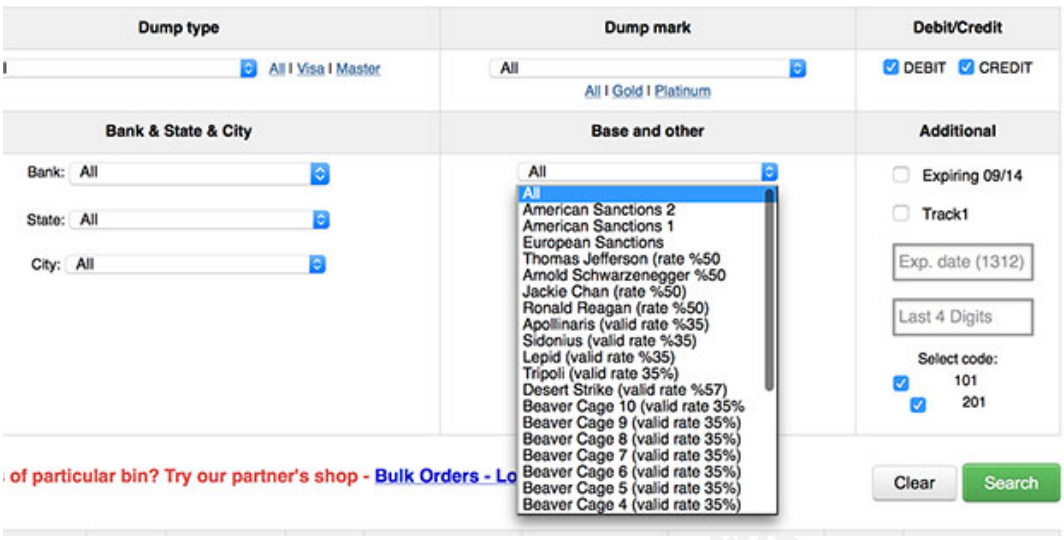


Figure 1 (Lawrence, 2014)

Once the carder has bought a payment card on the carder website, they will buy a pre-paid credit card using that stolen payment card information. The pre-paid credit card is used to buy gift cards at stores like Amazon or Best Buy. The gift cards are then used to buy items at those stores, typically electronics, which are then resold on sites like EBay, Craigslist, or similar sites.

After the cyber-criminal purchases the items to be resold, they need the items shipped to a location that cannot be traced back to them. The items are shipped to a "re-shipper." These re-shippers receive the items to be sold and ship them to the person who bought the items posted by the cyber-criminal. This process is difficult to track. By the time a breach is detected and the stolen payment card has been blocked, the cyber-criminal has already bought the items to be resold with the gift card (Westin, 2013). This is a well-known process and is used frequently because it has been proven to make a profit for cyber-criminals.

1.2 Hasn't this happened before?

Ever since the Target data breach was disclosed by Brian Krebs on December 18, 2013, occurrences of similar retail data breaches have been on the rise. Until the Home Depot data breach, the Target breach was the largest retail breach in U.S. history (Bloomberg, 2014). In the Target data breach, 40 million payment cards were stolen

© 2015 The SANS Institute Author retains full rights.

(Krebs, 2014). The Home Depot data breach topped that by having 56 million payment cards stolen (Krebs, 2014). Some of the most notable retail data breaches that occurred after the Target breach are shown in **Figure 2** below.



Figure 2 – Timeline of large retail data breaches after the Target breach

These companies should have used the Target data breach as a learning opportunity and applied the knowledge to their own payment card systems. The impact these data breaches had on each of the companies was significant. After the Target data breach, it posted profits that quarter which were 46 percent below expected profits (Gertz, 2014). That is a large impact. I remember the day of the Target breach, looking at the Target stock price take a significant hit. I saw the same thing when the Home Depot breach happened. Large retail breaches like the ones shown above in **Figure 2** have a large impact and they will only continue to happen, unless the proper countermeasures are in place.

© 2015 The SANS Institute Author retains full rights.

1.3 Better ways to take card payments, because that's what customers want

The standard payment card in the U.S. has always used the magnetic stripe. These magnetic stripes are also called "magstripes". On that magstripe there are three tracks that contain different data, although track 3 is hardly ever used. Some of the data included on the magstripe is name of credit card owner, credit card type (Visa, MasterCard, etc.), expiration date, and credit card number. The problem with these magstripes is they are extremely easy for the criminals to read data from. The traditional magstripe credit card has been under a lot of scrutiny since the large-scale retail data breaches have started to occur more often. There are alternative methods to accepting payment cards. There is even a method to accepting traditional magstripe cards that will protect card data from being exposed.

1.3.1 Chip-and-Pin Cards

A new type of credit card is starting to become more familiar in the Unites States, called a chip-and-PIN card. The chip-and-PIN cards contain an embedded security chip and a traditional magstripe. This embedded security chip ensures that the card cannot be duplicated, as it masks the payment data uniquely each transaction (CreditCardForum, 2014). The problem with this alternative is that they cost significantly more to make than traditional payment cards and most merchants do not have systems that are capable of accepting the new chip-and-PIN cards. However, in October of 2015 if you have not changed your systems to support chip-and-PIN cards, the liability of the data breach now falls on the merchant, rather than the banks (Picchi, 2014).

1.3.2 Mobile Payments

Another alternative method to taking payment cards is by using mobile payment methods, like Apple Pay and Google Wallet. With each of these you have a "virtual wallet" in your smart device. This smart device could be a phone, tablet, or even a watch. With both of these mobile payment systems, they never pass your credit card number to the merchant. The problem is Apple Pay and Google Wallet are only accepted at a handful of places. Until more merchants adopt mobile payments, this method of payment will not see any traction gained (Lee, 2014).

© 2015 The SANS Institute Author retains full rights.

1.3.3 Point-to-Point Encryption

There is a way you can take traditional magstripe credit cards, while still protecting card data. This method is called point-to-point (P2P) encryption. P2P encryption encrypts card data at the point of swipe, all the way to the bank for approval/denial of the transaction. With P2P encryption, payment card data is never exposed and is encrypted before it reaches memory. The only risk that still remains with P2P encryption is if someone were to install a credit card skimmer on the actual pin-pad. However, proper security awareness training for staff and having proper controls in place, will prevent skimmers from being installed. The creations of these alternative methods were outcomes of the most common method used in the large-scale retail breaches.

1.4 The latest way to steal credit cards

There are several methods to stealing credit cards. From hacking an online database of a website that stores credit card information, to physically stealing somebody's credit card out of their purse. No matter which method is used, the goal is always the same; steal payment card information for personal gain. A known method of stealing payment card information arose in the discovery of the Target data breach, although this method did not get much attention before Target. This method continued to be discovered in thousands of other breaches, both large and small. The method used "memory scraping malware".

1.4.1 Memory Scraping Malware

Memory scraping malware has been the key component in stealing payment card information in the large retail data breaches of 2014. This malware is able to read the contents of RAM on a POS terminal when the payment card data is present in clear text. The malware uses regular expressions to grab the payment card information. Once that data is captured, it is sent to servers owned by the attacker, or the attacker's associates (Huq, 2013). This malware has been effective, as evidence of the recent retail data breaches has shown. It continues to be effective on POS systems that are not properly locked down.

© 2015 The SANS Institute Author retains full rights.

2. The Home Depot Data Breach

Home Depot was one of the many victims to a retail data breach in 2014. The unfortunate thing is the way the attacker's infiltrated the POS networks and how the attackers were able to steal the payment card data, were the same methods used in the Target data breach. The attackers were able to gain access to one of Home Depot's vendor environments by using a third-party vendor's logon credentials. Then they exploited a zero-day vulnerability in Windows, which allowed them to pivot from the vendor-specific environment to the Home Depot corporate environment.

Once they were in the Home Depot network, they were able install memory scraping malware on over 7,500 self-checkout POS terminals (Smith, 2014). This malware was able to grab 56 million credit and debit cards. The malware was also able to capture 53 million email addresses (Winter, 2014). The stolen payment cards were used to put up for sale and bought by carders. The stolen email addresses were helpful in putting together large phishing campaigns.

2.1 Prevention & Detection

There were several countermeasures Home Depot could have had in place to prevent the breach from happening and to have been able to detect the breach sooner, minimizing the impact. Home Depot didn't have secure configuration of the software or hardware on the POS terminals. There was no proof of regularly scheduled vulnerability scanning of the POS environment. They didn't have proper network segregation between the Home Depot corporate network and the POS network. The last two controls that were lacking were proper monitoring capabilities and the management of third-party vendor identities and access.

2.1.1 What would have worked?

The secure configuration of software and hardware is vital to securing any environment, especially an environment dealing with sensitive data. Home Depot did have Symantec Endpoint Protection installed in their environment. Symantec Endpoint Protection (SEP) is an antivirus solution. The problem is that they did not have an important feature turned on in the product called "Network Threat Protection" (Elgin, Riley, & Lawrence, 2014). This module acts as a host intrusion prevention system

© 2015 The SANS Institute Author retains full rights.

(HIPS). Having configured POS devices with this feature activated at my own organization, I can attest to the success of this feature when doing vulnerability assessments on these systems.

Another secure configuration missing was the use of Point-to-Point (P2P) encryption. This allows payment card data to be encrypted at the point of swipe and allows the data to be encrypted in memory. To be able to use this technology, it requires hardware that is capable of using the technology. In Home Depot's case, an upgrade to the operating system of the POS devices was also needed.

Home Depot had another software configuration that was not secure on the POS devices, the operating system. An operating system is the most important software on a device. The operating system running on the POS devices was Windows XP Embedded SP3 (Mick, 2014). Windows XP machines are highly vulnerable to attacks, so the fact that Home Depot's POS registers were still running this operating system, is just asking to get compromised. They should have upgraded to a more current Windows operating system for their POS devices. Some examples of more current Windows POS operating systems are Windows Embedded POSReady 2009, Windows Embedded POSReady 7, and Windows Embedded 8 Industry (Wikipedia, 2014, p. xx). I have successfully upgraded POS devices in my own organization to more current embedded operating systems. The newer operating systems are compatible with P2P encryption, antivirus, and many other applications that are vital to locking down your POS systems.

In all of the sources I have looked at regarding the Home Depot breach, none have mentioned Home Depot having a vulnerability management program in place. If Home Depot had a vulnerability management program, performing monthly vulnerability scans of the POS environment; they could have used the results of those scans to show leadership the significance of the gaps in that environment and possibly started to mitigate the risk of that environment before the breach occurred.

Network segregation is another big gap in this breach. I will touch on this in more detail later, but Home Depot should have had the POS environment in its own restricted virtualized local area network (VLAN) and restricted access between the POS environment and the Home Depot corporate environment.

© 2015 The SANS Institute Author retains full rights.

Another question arises from this breach. How did the attackers steal third party vendor credentials from Home Depot? Home Depot was not properly managing its third party vendor credentials and should have allowed minimal access to that vendor account. I will touch on this in more detail later.

Prevention is ideal, but detection is a must. Even if Home Depot couldn't have prevented the attack, they still should have had monitoring capabilities, so that it did not take 5 months to detect an intrusion (Elgin, Riley, & Lawrence, 2014). Having the capability to forward any network or host activity in the POS environment to a SIEM, would have been beneficial to Home Depot and could have allowed them to detect the breach sooner, minimizing the impact.

2.1.2 What is working?

The fact I have actual experience locking down POS environments during my professional career and have been successful in securing those environments, I can tell you first-hand what is working. A defense-in-depth approach needs to be implemented.

First, upgrading your POS devices to a current, supported operating system is a must. If you are not running a current, supported operating system, all other system hardening you do is a waste. Second, ensure you have up-to-date antivirus software with HIPS capability. If an attacker penetrates your POS network, this will add another layer of defense in preventing the compromise of your POS devices. Third, you need to have automatic updates activated on the POS devices. It is vital that you follow patch management best practices and keep the POS devices on the most current patches. This is required for PCI compliance. Fourth, you need to enable P2P encryption on the POS devices. This requires a pin-pad that supports this technology.

The fifth thing that you will need to implement is the disabling of all unnecessary ports and services on the POS devices. There is no reason the POS devices need to have services such as NetBIOS running. Another important system hardening configuration is to disable the use of USB ports on the POS devices. You can do this physically by installing USB port blockers, or through software that blocks the use of USB ports. In most cases, you will need to leave just 1 USB port active for the connectivity from the POS register to the pin-pad device. If somebody were able to circumvent your physical or software-based USB protection, you need a way to notify your security team of such an

© 2015 The SANS Institute Author retains full rights.

act. Software can be installed on your POS registers that alerts you if a USB device has been inserted into the POS register. You also need to make sure that proper password and account policies are set on the POS devices. Now that all the host-based protections are in place, let's talk about the networking-based countermeasures that need implemented.

First, you need to segregate the POS network from your corporate network. You can do this by making the POS network its own private VLAN. Second, once you have segregated the POS network, you need to apply rules on the networking device responsible for the VLAN, so that you can restrict access between your corporate network and POS network. Third, you need to have all outbound Internet access coming from your POS network restricted at your corporate firewall. Firewall rules should be in place to only allow connections for the vital functions, such as credit card processing and Windows Updates. Having all of these preventive countermeasures in place is great, but you also need to be able to detect potentially malicious activity.

You should have a SIEM in place that is able to retrieve Windows event logs, Domain Controller logs, anti-virus logs, DNS logs, firewall logs, and other networking device logs. This will give visibility into the real-time activity in your POS environment and will allow you to create alarms within your SIEM to alert your security team of any malicious activity.

2.1.3 What will work in the future?

I would like to think that the current methods of prevention and detection of POS environments will work in the future. The reality is that the bad guys find new ways to exploit vulnerabilities every day and technology advances at a significant rate. Credit cards may not even exist in the future. There might be a significant vulnerability found in the chip-and-PIN cards down the road, which causes us to question how to take payments, just as the traditional magstripe card is causing questioning now.

I think we are getting a glimpse into the future with Apple Pay and Google Wallet. The magnifying glass will shift from credit card security to mobile device security. The idea of a virtual wallet seems like it could be 5-10 years from having a significant adoption rate. How will mobile device manufacturers and mobile payment software companies react to the bad guys finding vulnerabilities in their systems? Will they be able to quickly release patches that fix security vulnerabilities related to the virtual wallet? I

© 2015 The SANS Institute Author retains full rights.

think it is a large change that will heavily impact the retail landscape and will happen sooner than people think.

2.2 Preventing Home Depot, Target, and Other Retail Breaches

I previously stated many countermeasures that Home Depot should have had in place, but wanted to go into detail on 3 that I thought were the most important and could have been applied to all retailers that experienced a breach in the past year. The 3 main preventive measures that should have been in place were P2P encryption, proper network segregation, and managing third party vendor credentials appropriately.

2.2.1 Point to Point Encryption

The protection of credit card data is continuing to get more attention, since these large retail breaches have been occurring. Even after the attackers infiltrated the POS environments and installed the memory scraping malware on the POS registers, 1 countermeasure could have been in place to prevent the attackers from stealing credit cards. That countermeasure is P2P encryption.

P2P encryption provides encryption at the point of swipe when using your credit or debit card. In the use case of debit cards, it even encrypts your 4-digit PIN code you enter. All of this is done before the data reaches memory, which prevents data from being captured in memory. The device that is used for swiping the credit card is injected with a derived unique key per transaction. This is only used for the payment card encryption and is not the same key used for the PIN encryption when using a debit card. Once you swipe your card, the payment card data is encrypted inside a tamper-resistant security module with the payment card industry standard 3DES algorithm, using the derived unique key for the transaction (TSYS, 2014). That encrypted data is then sent securely to an off-site hardware security module owned by the POS solution provider, where the payment card data is decrypted (Knopp, 2013). The decrypted card data is then encrypted again using the bank's encryption key(s) and sent to the bank where the data is decrypted again. The bank then sends the approval/denial back for the payment card. **Figure 3** below shows the process.

© 2015 The SANS Institute Author retains full rights.

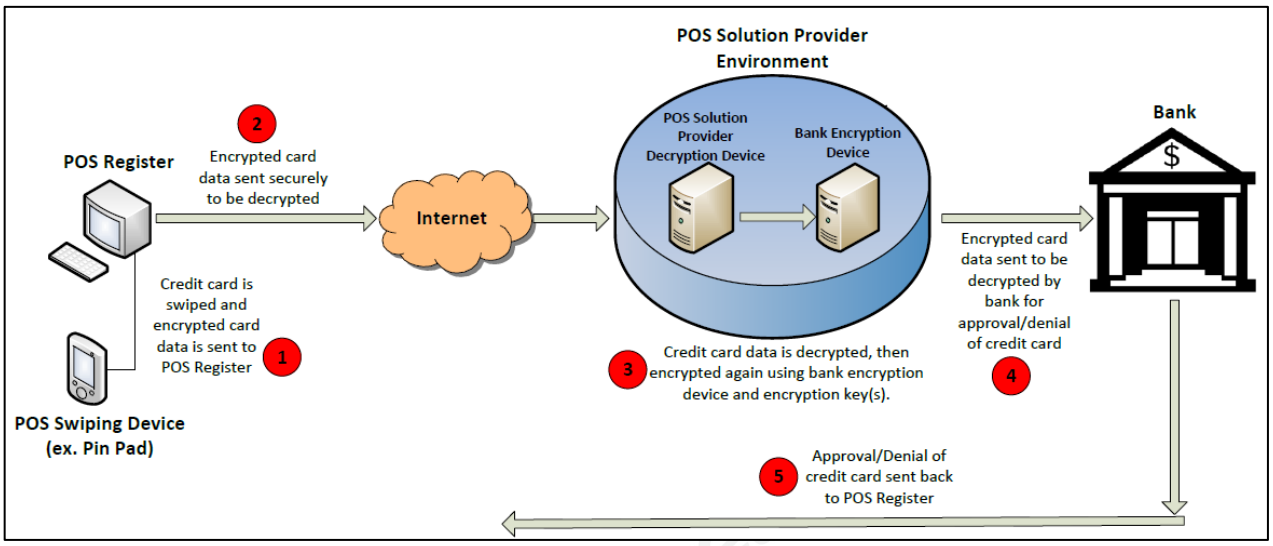


Figure 3 – P2P Encryption Data Flow

As you can see this is a robust solution. It could have prevented the attackers from stealing card data. Home Depot actually started to implement encryption before the breach occurred, as it was rolled out to a quarter of their stores. The problem was when the breach actually began was before the encryption was fully implemented (Bluefin News & Blog, 2014). This is 1 of the 3 main countermeasures that should have been in place to prevent the retail breaches.

2.2.2 Network Segregation

The protection of the perimeter is a vital component in preventing the large retail breaches that have occurred and is also critical when implementing a defense-in-depth approach. The POS network should be properly segregated from the rest of the corporate network. The use of private VLAN's comes into use with this type of countermeasure. Using a networking switch, you can place the devices on the POS network into their own VLAN. Static IP addresses should be assigned to all POS devices within the IP range you specify. Once the devices are in their own VLAN, network traffic between the corporate environment and the POS environment should be restricted using an Access Control List (ACL) on the networking switch. This setup is shown below in **Figure 4**.

© 2015 The SANS Institute Author retains full rights.

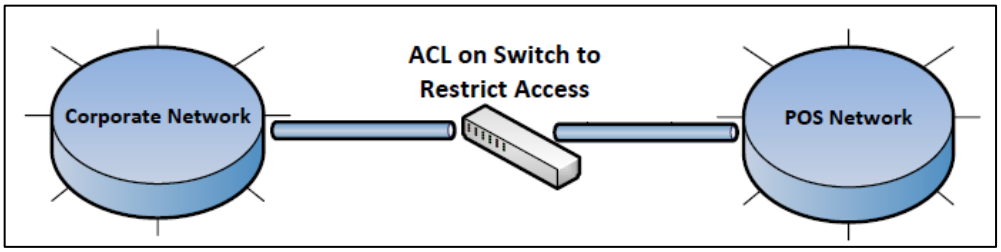


Figure 4 – Network Segregation of Corporate and POS Networks

The ACL should deny all traffic between the 2 environments, except traffic needed with necessary devices. An example of a necessary device could be your corporate anti-virus server, so that anti-virus definitions can be pushed to the POS devices.

Logging should be enabled on the networking switch and configured to forward those logs to your SIEM, so you can see accepted and denied connections between your corporate network and POS network.

Network segregation also allows you to configure firewall rules for that environment easier. You can setup special firewall rules for that VLAN, such as denying all outbound Internet access through the firewall, except for the necessary connections. An example of a necessary connection would be the hosts needed to communicate with for the credit card processing. Segregation of the network is good, but the need to restrict user access to those trusted corporate hosts is also critical.

2.2.3 Managing Third Party Vendor Credentials

Poor management of third-party vendor credentials was a common fault in the Home Depot and Target data breaches. The attackers were able to gain access to a vendor-specific environment used by the retailers and were then able to pivot to the corporate networks. This demonstrates the importance of having sufficient controls in place. The least privileged principle needs to be used. All third-party vendors should be allowed the minimal access needed to perform their tasks and should be denied access to internal resources, unless required.

An identity and access management solution should be used to manage the identities and access of all internal and external employees (third-party vendors). Each external employee should have their own account, so that there is accountability for anything performed on their behalf. Account review procedures should also be in place,

© 2015 The SANS Institute Author retains full rights.

specifically for third party vendor accounts. Auditing of these third-party vendors is critical. This will allow the detection of abnormal behavior. Having all of these controls in place for managing and monitoring the third party vendor accounts, will detect any misuse of third-party vendor credentials. This would have been vital in detecting an intrusion earlier in the Home Depot and Target breaches.

3. Conclusion

The key takeaway from this paper is that the Home Depot breach could have been prevented by taking a proactive approach. Learning how Target was breached in December of 2013 should have immediately prompted Home Depot to assess their environment and address the gaps that existed before becoming compromised. Taking the preventive measures that I have outlined could have prevented the Home Depot breach and will be able to prevent other retail data breaches in the future. These types of retail breaches are becoming more common. I hope that retailers will learn lessons from previous breaches to safeguard their environment and prevent it from happening to them.

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

References

Bloomberg. (2014, May 14). *Target's Data Breach: The Largest Retail Hack in U.S. History – Bloomberg*. Retrieved from http://www.bloomberg.com/infographics/2014-05-14/target-data-breach.html

Bluefin News & Blog. (2014, September 15). *Home Depot Had Started Payment Encryption Work Before EMV Implementation - Bluefin Payment Systems : Bluefin Payment Systems*. Retrieved from https://www.bluefin.com/2014/09/15/home-depot-started-payment-encryption-work-emv-implementation/

CreditCardForum. (2014, December 2). *2014 Chip and PIN Credit Cards In The USA: Who Offers Them* [Blog post]. Retrieved from http://creditcardforum.com/blog/chip-and-pin-credit-cards-usa/

Elgin, B., Riley, M., & Lawrence, D. (2014, September 18). *Home Depot Hacked After Months of Security Warnings - Businessweek*. Retrieved from http://www.businessweek.com/articles/2014-09-18/home-depot-hacked-wide-open

Gertz, A. (2014, July 30). *The Real Cost of a Retail Data Breach | The Art of Data Protection*. Retrieved from http://data-protection.safenet-inc.com/2014/07/the-real-cost-of-a-retail-data-breach/#sthash.pw1r5hAM.dpbs

Huq, N. (2013, July 16). *A look at Point of Sale RAM scraper malware and how it works | Naked Security*. Retrieved from https://nakedsecurity.sophos.com/2013/07/16/a-look-at-point-of-sale-ram-scraper-malware-and-how-it-works/

Knopp, J. (2013). *Point-to-Point Encryption: A Merchant's Path to Cardholder Data Environment Scope Reduction | MasterCard | Security Matters*. Retrieved from http://arm.mastercard.com/securitymatters/compliance/pci-dss/point-point-encryption-merchants-path-cardholder-data-environment-scope-reduction/

Krebs, B. (2014, May 14). *The Target Breach, By the Numbers*. Retrieved from krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/

Krebs, B. (2014, September 14). *Home Depot: 56M Cards Impacted, Malware Contained*. Retrieved from krebsonsecurity.com/2014/09/home-depot-56m-cards-impacted-malware-contained/

Brett Hawkins, hawkbluedevil@gmail.com

© 2015 The SANS Institute Author retains full rights.

Lawrence, D. (2014, September 4). *The Amazon.com of Stolen Credit Cards Makes It All So Easy - Businessweek.* Retrieved from http://www.businessweek.com/articles/2014-09-04/the-amazon-dot-com-of-stolen-credit-cards-makes-it-all-so-easy

Lee, N. (2014, October 29). *Dabbling in the future of payment: A week of Apple Pay and Google Wallet*. Retrieved from http://www.engadget.com/2014/10/29/week-apple-pay-google-wallet/

Mick, J. (2014, September 8). *DailyTech - Appalling Negligence: Decade-Old Windows XPe Holes Led to Home Depot Hack*. Retrieved from http://www.dailytech.com/Appalling+Negligence+DecadeOld+Windows+XPe+Holes+Led+to+Home+Depot+Hack/article36517.htm

Picchi, A. (2014, September 5). *Why new "chip-and-pin" cards won't protect you -- yet - CBS News*. Retrieved from http://www.cbsnews.com/news/why-new-chip-and-pin-cards-wont-protect-you-yet/

Smith, M. (2014, November 10). *Home Depot IT: Get hacked, blame Windows, switch execs to MacBooks | Network World*. Retrieved from http://www.networkworld.com/article/2845620/microsoft-subnet/home-depot-it-get-hacked-blame-windows-switch-execs-to-macbooks.html

The Home Depot, Inc. - News Release. (2014, September 8). Retrieved from http://phx.corporate-ir.net/phoenix.zhtml?c=63646&p=irol-newsArticle&ID=1964976

TSYS. (2014). *Point-to-Point Encryption (P2PE)*. Retrieved from http://www.tsys.com/acquiring/engage/white-papers/Point-to-Point-Encryption.cfm

Vamosi, R. (2008, September 29). *How 'carders' trade your stolen personal info - CNET*. Retrieved from http://www.cnet.com/news/how-carders-trade-your-stolen-personal-info/

Westin, K. (2013, December 21). *Stolen Target Credit Cards and the Black Market: How the Digital Underground Works - The State of Security*. Retrieved from http://www.tripwire.com/state-of-security/vulnerability-management/how-stolen-target-credit-cards-are-used-on-the-black-market/

Wikipedia. (2014). Windows Embedded Industry. In *Wikipedia, the free encyclopedia*. Retrieved December 26, 2014, from http://en.wikipedia.org/wiki/Windows_Embedded_Industry

Winter, M. (2014, November 7). *Home Depot hackers used vendor log-on to steal data, e-mails*.

Brett Hawkins, hawkbluedevil@gmail.com

© 2015 The SANS Institute Author retains full rights.

Retrieved from http://www.usatoday.com/story/money/business/2014/11/06/home-depot-hackers-stolen-data/18613167/

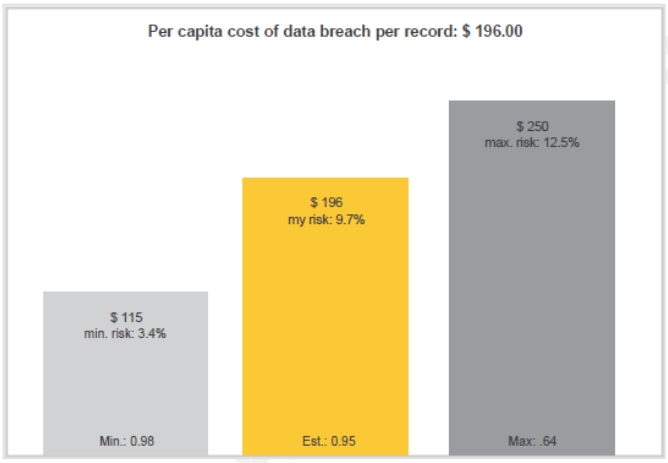
© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

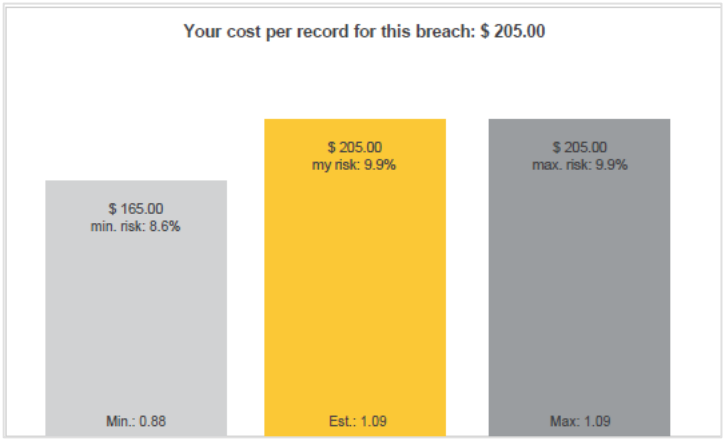
Appendix A

Data Breach Cost Calculator

Based on the results generated from the Symantec Data Breach Calculator (http://www.databreachcalculator.com), the average cost per data breach at Home Depot, according to its risk profile before it was breached, was $23,506,667. The average cost per compromised record was calculated at $196 as shown in the chart below.



Companies in the same industry with a similar risk profile to Home Depot have a 9.7% likelihood of experiencing a data breach in the next 12 months. One of the key factors affecting this calculation is the absence of a CISO at Home Depot. This increases the cost of a data breach significantly. You will see evidence of this in the chart below, which shows the cost per compromised record, if an organization similar to Home Depot were to be breached and did not have a CISO. If Home Depot would have performed a risk-based cost-benefit analysis, they would have realized the cost to implement adequate controls highlighted in this case study would have been far less than the cost of a breach.



Brett Hawkins, hawkbluedevil@gmail.com

© 2015 The SANS Institute Author retains full rights.