Interested in learning more about security?

SANS Institute InfoSec Reading Room

Data Breach Preparation

The Home Depot Data Breach is the second largest data breach on record. It has or will affect up to 56 million debit or credit cards. A trusted vendor account, coupled with the use of a previously unknown variant of malware that allowed the establishment of a foothold, was the entry point into the Home Depot network. Once inside the perimeter, privilege escalation provided an avenue to obtain the desired information. Home Depot did, however, learn some lessons from Target. Home Depot certainly communicated better than ...

LA-UR-15-21852
Approved for public release; distribution is unlimited.

Title: Data Breach Preparation

Author(s): Belangia, David Warren

Intended for: Partial fulfillment of Master Program

Issued: 2015-03-13

Data Breach Preparation

GIAC (GLEG) Gold Certification

Author: David Belangia, dwbelangia@hotmail.com
Advisor: Richard Carbone
Accepted: January 15, 2015

Abstract

The Home Depot Data Breach is the second largest data breach on record. It has or will affect up to 56 million debit or credit cards. A trusted vendor account, coupled with the use of a previously unknown variant of malware that allowed the establishment of a foothold, was the entry point into the Home Depot network. Once inside the perimeter, privilege escalation provided an avenue to obtain the desired information. Home Depot did, however, learn some lessons from Target. Home Depot certainly communicated better than Target, procured insurance, and instituted as secure an environment as possible. There are specific measures an institution should undertake to prepare for a data breach, and everyone can learn from this breach. Publicly available information about the Home Depot Data Breach provides insight into the attack, an old malware variant with a new twist. While the malware was modified as to be unrecognizable with tools, it probably should have been detected. There are also concerns with Home Depot's insurance and the insurance provider's apparent lack of fully reimbursing Home Depot for their losses. The effect on shareholders and Home Depot's stock price was short lived. This story is still evolving but provides interesting lessons learned concerning how an organization should prepare for it inevitable breach.

1. Introduction

Home Depot experienced the second largest data breach on record. ("Home Depot data breach affected 56M debit, credit cards", 2014) It started in April 2014, but Home Depot did not become aware of the problem until September 2 when law enforcement and some banks contacted them about signs of the compromise. (Kessler, 2014) By this time, the damage was done with 56 million debit and credit cards compromised with an additional 53 million email addresses being stolen. (Home Depot, 2014)

It appears the attack vector was a vendor username/password entry point coupled with the addition of a previously unknown piece of malware. Once the malware was activated, privilege escalation was used to enable the attackers to penetrate the Point-of-Sale information. ("Home Depot reports findings in Payment data breach investigation", 2014)

Home Depot does have data breach insurance for $100 million, but the important question to ask is: do the exclusions substantially alter the payback and is this enough insurance? "Chief Financial Officer Carol Tomé told analysts that the breach-related expenses incurred during the (third) quarter came to about $43 million, while projected known gross breach costs are $27 million for the fourth quarter." (Kell, 2014) According to the Credit Union National Association, the breach will costs (its) members close to $60 million to reissue cards and resolve fraudulent charges. (Holan, 2014) When the different costs are combined, Home Depot could be looking at costs up to $70-$100 million.

Data breach insurance is complicated, and insurance agencies, as well as subscribers, are determining the included requirements; forensic investigation, notification of parties, fulfillment of legal and compliance obligations, possible litigation, working with law enforcement, public relations, credit monitoring fees, crisis management – the list goes on. In addition there are different kinds of risk based on industry (health care versus retail). A primary factor in the coverage of payment will be the security maturity of Home Depot. Did Home Depot exercise prudent security or is there room for a stance of negligence by the insurance agency? (Amerding, 2014)

It is widely understood that technology-related insurance claims receive added scrutiny, especially in today's data breach environment. Attorney Golf from Anderson

Kill advises, “It’s hard to say how each claim is going to be handled because it really does depend upon what insurance policies the policyholder has in place, the circumstances of the loss, and lots of other factors.” (Ha, 2014)

Data Breach Protection Insurance is a risk mitigation strategy to protect a policyholder from costs associated when (if) a breach occurs. These policies typically cover notification obligations, liability claims, investigation costs, and potential fines and penalties. (CardFellow, 2014) While insurance may reduce the pain associated with the cost of the breach, it does not help the institution’s reputation or resolve consumer concerns. When a breach occurs, serious discussions should occur to ensure the message sent to consumers in this difficult time reflect the appropriate level of communication and is clearly articulated. Enlisting a Public Relations firm to support this message might be appropriate and help to ensure consistency of the message.

If an institution decides on pursuing data breach insurance, then the institution must understand their security posture, the potential for loss, and the offerings of coverage by the insurance company. However, this exercise is not for the faint of heart. Time and expertise must be brought to bear on the problem to ensure that when, not if insurance is needed, it provides the anticipated relief.

The Home Depot Data Breach will provide additional insights into the insurance industry, cyber posture, and many lessons learned for other organizations. By continuing to follow the story and applying lessons learned to a company’s unique requirements, the lessons from the Home Depot Breach will provide the opportunity for a more robust and secure implementation of controls. Remember, data breach protection insurance can ease the pain with financial issues, but lost customer confidence is altogether another matter.

2. Home Depot Breach

2.1. Details

Home Depot describes their security posture from the following excerpt based on their Privacy Statement:

> "When you place orders on our websites, all of your order information, including your credit card number and delivery address, is transmitted through the Internet using Secure Sockets Layer (SSL) technology. SSL technology causes your browser to encrypt your order information before transmitting it to our secure server. SSL technology, an industry standard, is designed to prevent someone other than operators of our websites from capturing and viewing your personal information.
>
> While we use industry standard means to protect our websites and your information, the Internet is not 100% secure. The measures we use are appropriate for the type of information we collect. We cannot promise that your use of our websites or mobile applications will be completely safe. We encourage you to use caution when using the Internet. Online access to your personal information is protected with a password you select. We strongly recommend that you do not share your password." (Home Depot, 2014)

On September 2, Home Depot became aware of a large data breach that started April 2014. The organized attack pilfered some 56 million debit and credit cards.

It appears the criminals used a third-party vendor's username and password to get inside the perimeter. The adversary used malware to enable elevated privileges allowing the navigation of portions of the Home Depot network.

In addition to the card information, the attack exfiltrated 53 million email addresses. ("Home Depot Reports Findings in Payment Data Breach Investigation", 2014) This is consistent with the Target compromise where 70 million email addresses were stolen. Kerner postulates that the privilege escalation flaw allowed the real damage to occur. Attackers against Windows-based computers use the Pass-the-HASH technique. Home Depot has stated that the malware was previously unknown. (Kerner, 2014)

"A source close to the investigation told the author that an analysis revealed at least some store Home Depot's registers had been infected with a new variant of "**BlackPOS**" (a.k.a. "Kaptoxa"), a malware strain designed to siphon data from cards that are swiped on the infected point-of-sale system running Microsoft Windows." (Krebs, 2014) According to experts, this card-stealing code has been widely sold on underground hacking forums. It is believed the code was modified. (Banjo, 2014)

In contrast, Information Week's Dark Reading postulated that the malware was not of the BlackPOS family of malware. The article provided characteristics that

appeared different; the subsystems were written with a console option, supported several command line arguments, used XOR encryption, included the victim's IP address, and other differences. A single change or even multiple changes could reflect a change in the code base; however, this article provides further analysis that points to completely new malware. (Peters, 2014)

On his security blog, Krebs identified that on September 14 banks were seeing evidence of the Home Depot stores breach on cybercrime underground repositories - **rescator[dot]cc**. Krebs also identified that the perpetrators appeared to be the same group of Russian and Ukrainian hackers that compromised Target, Sally Beauty, P.F. Chang's, and others. (Kreb, 2014)

As part of their proposed solution, Home Depot is deploying EuroPay MasterCard Visa and chip-and-pin security at all of its U.S and Canadian stores. (Plummer, 2014) By using the chip-and-in security, it is more difficult to copy the card for general use by the adversary.

The PCI Security Standards Council provides standards and supporting materials to enhance payment card data security. PCI DSS compliance is a multi-layered approach to implement minimum data management standards to obtain compliance. Compliance certainly does not fully protect an organization from a data breach, but it provides a good start. A card vendor requires different levels of rigor based on the dollar value of transactions. There are 12 Key Requirements for protecting Cardholder Data (PCI DSS Compliance):

1. Implement the Firewall
2. Remove or at least change vendor provided passwords
3. Protect data stored
4. Encrypt in transit
5. Use and update anti-virus software
6. Patch (software and firmware)
7. Limit access to data
8. Mandate unique IDs
9. Maintain physical access on all cardholder data

10. Maintain control of access points
11. Test security quarterly (pen testing)
12. Ensure security within the culture to include policy and actions

2.2. Timeline

On September 4, the Los Angeles Times reported a possible data breach at Home Depot. Paula Drake, Home Depot spokeswoman advised, "The home improvement chain is working with law enforcement, banking partners, security firms (Symantec Corp and Fishnet Security), and the U.S. Secret Service to investigate "unusual activity" but has not confirmed whether a breach has occurred. Home Depot has had their security teams working to understand the compromise discovered Tuesday morning." The article identified Brian Krebs as saying the compromise might affect nearly all Home Depot stores and based on the activity of several underground hacker sites it may have started as early as April. (Li, 2014)

Home Depot stated on September 8 that its investigation started September 2, after they received reports from their banking partners and law enforcement that criminals had hacked their payment data systems. (Kessler, 2014)

Reuters reported on September 9 that Home Depot confirmed Monday, September 8, that their payment security systems had been breached and warned that the breach might be as large or larger than Target's breach the year before. It was advised the breach could affect customers across both the United States and Canada. Chairman and Chief Executive Officer Frank Blake stated, "It is important to emphasize that no customers will be responsible for fraudulent charges to their accounts." (Bose, 2014)

On September 18, the Wall Street Journal reported on their web site that Home Depot estimated the breach magnitude at 56 million debt and credit cards. Between April and September, Home Depot advised that 56 million cards might have been compromised making this the second largest breach for a retailer on record. ("Home Depot data breach affected 56M debit, credit cards", 2014)

Tech Times stated that on November 25 Home Depot was still striving to fix the issues and now has fallen prey to another attack; Home Depot has been hit with 44 civil

lawsuits. Shortly after the attack, multiple state attorneys general launched multistate probes into the compromise and subsequent actions. These suits represent customers, payment card institutions, issuing banks, shareholders and other parties. During the November 2 filing with the Security and Exchange Commission, Home Depot warned it was being swamped with investigations and lawsuits. (Plummer, 2014)

Home Depot has started allowing the use of PayPal at their stores. The customer must take some initial actions to enable the account, but once that is accomplished, the customer only requires a telephone number and their pin. "PayPal is a paragon of the rising alternative payment technologies. It is an established company, but it's also clearly an innovator." (Koppenheffer, 2014) This innovative approach allows the protections provided by PayPal (to the customer and the retailer) as well as the protections inherit in the credit card usage.

2.3. Communications

Communicating to the public and law enforcement once a data breach has occurred must be measured and appropriate. Continually notifying consumers regarding a data breach with incomplete or incorrect information is not desirable. On the other hand, the institution does not want to be perceived as uncaring. This is a delicate balancing act.

The company and affected parties want the customer to know when their information has been compromised. The customer can take appropriate action, but partial or incorrect information provides an environment where the customer and the press might perceive the institution is holding information back. The customer might believe that the breached company does not understand the breach fully and thus is incompetent. Institutions that suffer a breach are at risk of the second breach: **Customer Trust**. (Bit9, 2014) Institutions must consider their risk, customer relationships, security posture and incident response in a unique fashion that is appropriate and measured for their environment.

Reuters started criticizing Home Depot on September 8 remarking that almost a week had passed and that Home Depot had not yet confirmed or denied the reports. Reuters further articulated that Home Depot was working with authorities to investigate the matter. Target made initial disclosures on the breach scope but had to generate a

series of updates that angered and confused customers. This minimalist communications strategy might be from the lessons learned on Target. Home Depot CEO Frank Blake advised, “On the one hand, you can wait to communicate anything until you have the facts at hand, or you can communicate the facts as you know them. We chose the latter path.” (Young, 2014)

Congress passed the Privacy Act of 1974 to establish an approach to dealing with the collection, maintenance, use, and dissemination of Personally Identifiable Information (PII). The Department of Justice provides an overview of the Privacy Act of 1974 in its 2012 Edition stating, “the Act has four basic policy objectives:

1. To restrict disclosure of personally identifiable records maintained by agencies,
2. To grant individuals increased rights of access to agency records maintained on themselves,
3. To grant individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete, and
4. To establish a code of "fair information practices" which requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records.” (Overview of the Privacy Act of 1974, 2014)

Responding to this legislation and the additional burden of state legislation makes for a confusing and potentially expensive environment for those organizations that do not plan. Home Depot obviously collected a lot of PII during the execution of their primary business. However, the requirements for collecting, protecting and maintaining this information are fundamental to the business.

During a crisis, organizations have the opportunity to win or lose support from their customers. In an article for the Huffington Post, Cummings states, “Instead of building trust with customers, Home Depot chose to communicate very little with the public, distributing only a very few carefully worded press releases. Considering that trust in big business is near all-time lows, Home Depot’s head-in-the-sand crisis management approach is more costly than it might appear.” (Cummings, 2014)

Home Depot provided a payment card announcement on its web site that provided information on how the breach was discovered, how long had it been going on, what they were doing about it, what was stolen, and how to protect the customers. In addition, Home Depot provided a Frequently Asked Questions on how to enroll in identity protection services and how to prevent identify theft. ("The Home Depot Reports Findings in Payment Data Breach Investigation", 2014)

2.4. Home Depot and Consumer Responses

While some folks may argue that Home Depot's response was slow, and that they made various errors, the impact on Home Depot's stock price was not much worse than the other major building supplies store, Lowes. Lowes was guilty by association. Home Depot discovered the breach, as many organizations do, by notification from external parties. The breach had been going on for several months. This seems to be a normal occurrence in today's data breach prone environment.

Based on Home Depot's ability to recreate the events leading up to the breach, it appears they were collecting logs at a sophisticated level. The ability to recreate events from logs where the incursion occurred months before indicates a solid approach to log maintenance.

The particular variant of malware was reported as using XOR encryption, so it is understandable that IDS/IPS systems or Antivirus signatures did not detect the malicious code. (Peters, 2014) Research also found no fatal flaws with Home Depot's defenses. With the attention Home Depot is receiving from this breach, if the organization were grossly negligent, then there would be plenty of research available.

Once the consumer has the awareness that a compromise has occurred, it is too late. If the consumer has not taken proactive steps to protect their PII, such as credit monitoring, reduction of credit cards, monitoring statements, and not using a debit card at a retailer, then the damage could be extensive. Banks typically will notice fraudulent transactions after consumers start complaining. (Schleicher, 2014) With a traditional credit card, the consumer is safe from losses with respect to fraudulent charges. With a debit card, the consumer could have his accounts impacted until the fraudulent use is

resolved. That aside, monitoring one's credit might help in avoiding or at least noticing indications of identity theft.

Both the consumer and the institution must prepare for the inevitable breach. A white paper from Bit9, *Breach Preparation: Plan for the Inevitability of Compromise*, suggests that institutions prepare a Breach Preparation Plan. The white paper identified seven important area of concern:

1. Ensure the board is notified as soon as the breach is discovered.
2. Ensure solutions are put in place and maintained.
3. Determine a communications approach for both customers and the public.
4. Determine requirements for external help (consultants and who).
5. Ensure the board agrees with and understands this plan.
6. Determine communications requirements for a graded approach including a complete company network outage.
7. Determine team membership for the response team. (Bit9, 2014)

3. Data Breach Lawsuits

3.1. Costs

On September 25, the National Law Journal reported that Home Depot was the victim of malicious software that enabled potential harm to its customers through its checkout terminals. Bronstad advised that Home Depot had incurred $62 million in expenses, including legal costs. (Bronstad, 2014)

According to the Credit Union National Association, "the breach will cost its members close to $60 million to reissue cards and cover potential fraudulent charges." (Holan, 2014)

Home Depot has not determined the full costs of the breach as identified in their earnings report dated Tuesday, November 18. **"**The Company's fiscal 2014 diluted earnings-per-share guidance does not include an accrual for other probable losses related

to the breach. Other than the breach-related costs contained in the Company's updated fiscal 2014 diluted earnings-per-share guidance, the Company is not able to estimate the costs, or a range of costs, related to the breach. Costs related to the breach would include liabilities to payment card networks for reimbursements of credit card fraud and card reissuance costs; liabilities related to the Company's private label credit card fraud and card reissuance; liabilities from current and future civil litigation, governmental investigations and enforcement proceedings. Then there are the future expenses for legal, investigative and consulting fees, incremental expenses and capital investments for remediation activities. Those costs may have a material adverse effect on the Company's financial results in the fourth quarter of fiscal 2014 and/or future periods." (Home Depot, 2014)

There are many federal and state laws that try to protect an individual's privacy; and as data breaches continue, these laws are interpreted in different ways. The digital age has altered the concept of data ownership and handling. Of note are the Fourth Amendment of the Constitution, the Health Insurance Portability and Accountability Act, the Stored Communications Act, and many state generated laws such as California Senate Bill 1386. As these data breaches continue to occur, organizations are struggling with the requirement to produce electronically stored information to opposing counsel. This is problematic since eDiscovery is pertinent under the relevancy standard contained in the Federal Rules of Civil Procedure (FRCP).

The FRCP advocates the following measures: Data Assessment (identify the data), Privacy Policies (vendors as well), Apply Technology, and maintain Audit Trails and Chain-of-Custody Logs. These proactive measures can help limit exposure to risk. (Bartholomew, 2012)

3.2. Legal Impacts

With continued data breaches, the breached company can expect multiple lawsuits from the states where their various operations exist. It is prudent for these companies to understand the differences in requirements where their operations exist and plan for the recovery process. There are many examples where companies have tried to satisfy the more stringent requirements in one state and only perform what is necessary in other

states. This is a disastrous plan, as the District Attorneys from the other states will feel it is their duty to bring the company to court. It is a safer approach to apply the most stringent requirements uniformly. The first security breach law is California Senate Bill 1386. This bill provides specific requirements for California residents. In Information LawGroup's report, *10 Years After SB 1386, California Attorney General Issues First Ever Report and Recommendations on Data Breaches,* the report provides a reminder that California has a statue that requires businesses to use reasonable and appropriate security procedures and practices to protect personal information. (Information LawGroup, 2013)

The consumer has to deal with the hassle of card cancellation, credit monitoring, realigning automatic bill pays, and delays in the ability to use the credit card until the new card arrives. It might affect the consumer when they try to use the card and it is rejected. This can be problematic unless the consumer has alternate means of settling the account, not to mention the embarrassment.

The continued requirement to watch one's credit is paramount to those few who have their identities compromised. Other information associated with the breach include things like email, physical addresses, social network names, and any other usernames and passwords. Hackers and data thieves have gotten more intelligent about using associated data for their benefit. (Sedlack, 2014) Normally, the consumer is not liable for any charges, but if the compromised item is a debit card, then funds in the bank can be frozen until the disputes are resolved.

3.3. Additional Impacts

The U.S. Government has passed laws to provide a federal data privacy framework. This started with the Privacy Act of 1974, 5 U.S.C. 552a. This act provides requirements and some criteria for collecting Personally Identifiable Information. This was the beginning of legislation to mandate protection while allowing commerce. It provides five principles: 1) privacy is directly affected by use; 2) increasing use is essential; 3) opportunities are endangered by misuse; 4) the right of privacy is fundamental, and 5) Congress must act to ensure these principles are enforced.

The E-Government Act of 2002 mandated federal services and programs take advantage of online capabilities. It also provided encouragement for citizens to access the information and participate. It instituted the concept of transparency. Consumers have the right to know what information is being collected, how that information is being used, and the ability to modify the information if it is incorrect. (Overview of the Privacy Act of 1974, 2014)

The Office of Management and Budget (OMB), which reports directly to the President, is required under the Privacy Act to prescribe guidelines and regulations for Agency use in implementing the Act. This includes the development and implementation of the Federal Information policies and standards. (Kropf, 2007)

Bloomberg BNA, using information from Privacy and Security Law Report stated that a group of attorneys general opened an investigation into the data breach. It was advised that these investigations are an attempt to understand the compromise and how the retailer is working with affected customers. Connecticut Attorney General George Jepson will be leading the multi-state investigation. (Kessler, 2014)

The U. S. Judicial Panel on Multidistrict Litigation (JPML) advised that the multiple ligations need to be centralized. According to The Top Class Actions web site designed to connect consumers to settlements, lawsuits and attorneys, the parties are not in agreement on where to centralize the cases. The panel advised Georgia is the most likely candidate location for the effort based on Home Depot being headquartered in Georgia and with the majority of lawsuits originating in Georgia. (Devis, 2014) On December 18, Heidi Turner reported that "11 lawsuits were consolidated in Atlanta federal court in the Northern District of Georgia." (Turner, 2014)

Both Home Depot and Lowe's released earnings identifying that Lowe's stock benefit over Home Depot was temporary. The stock value for both companies was lower based on the news of the breach. The damage from events similar to this breach has proven that the public attention is temporary if a breach is handled well. Stocks historically return to normal once the damage has been reflected in the quarterly reports. There is reason to believe that the cost for Home Depot might be double, based on credit union costs and lawsuits. (Blankenhorn, 2014)

David Belangia, dwbelangia@hotmail.com

3.4. Insurance

Proactively procuring data breach insurance will help minimize the financial impact of the breach. Data breach insurance is a risk mitigation strategy. It depends on the institution understanding their environment, data, and controls to ensure that exceptions or conditions within the insurance policy do not invalidate the data breach claims. The institution must understand what the policy covers, what might invalidate a claim, and it must ensure its security posture is maintained to prevent the exclusion of future claims. Data breach insurance is new and institutions must ensure the appropriate sub-organizations within the company are involved in negotiating the policy and conditions with an understanding that the institution must maintain a security posture that prevents possible exclusion of claims.

To prepare, the institution must provide as secure an environment as possible. This preparation will support minimizing (hopefully preventing) the breach and the extent of the breach. SANS Institute provides a SANS Top Twenty Critical Controls that provides a good starting point on important controls and the priority and importance of select controls. The PCI Data Security Standard and other standards provide checklists, processes, and recommended auditing approaches. Implementing critical controls and processes raises the bar for a data breach occurrence but are no guarantee that a breach will not occur.

Proactively understanding where the institution's critical data resides within the environment is essential. Once the institution understands where its data resides, what is collected, why it is collected and how it is used, then the application of additional controls specifically for that data improves the institution's position in relation to controlling and monitoring access, and identifying issues.

Data breach insurance supports protecting the policyholder from costs associated when (if) a breach occurs. These policies typically cover notification obligations, liability claims, investigation, and potential fines and penalties. (CardFellow, 2014) Data breach insurance helps cover the cost of the breach but does little for the reputation of the business. NetDiligence has provided an annual study (*Cyber Liability & Data Breach Insurance Claims*, 2013) for the last three years. The annual report provides several key

findings appropriate for the Home Depot breach. Firstly, PII is the most frequently exposed information for an incident (28.7%). The average number of records lost during 2013 was 2.3 million per incident. The average cost per record was $6,790. The average cost of Crisis Services was $737,473 with a legal defense averaging $574,984. The average cost for a legal settlement was $258,099. (Greisiger, 2013) Again, these numbers are expected to rise substantially based on the magnitude of recent events.

It is important to note that a company may incur expenses that are outside the coverage of their policy; for example, those losses related to the loss of current or future customers as well as a negative impact on the brand image.

Cyber Data-Risk Managers provides some example rates for insurance (Table 1: Estimated Costs of Insurance). These rates vary by industry and risk. Their company advises potential customers to work with their experienced cyber insurance brokers to determine the coverage that is correct for a given institution. (Cyber Data-Risk Managers, 2014)

Table 1: Estimated Costs of Insurance (Cyber Data-Risk Managers, 2014)

Industry	Revenue	Limit	Premium
Healthcare	$25 million	$1 million	$12,900
Financial	$100 million	$1 million	$37,000
Retail	$50 million	$1 million	$26,000

Another consideration with insurance is to ensure that the company is not excluded based on negligent computer security. Christine Marciano reported in CSO that a common exclusion is based on negligent computer security. Compliance with standards and other similar compliance efforts are essential to allow recovery under a data breach insurance policy. (Amerding, 2014)

"A lot of companies are purchasing specialized cyber insurance policies so those have to be examined," said Joshua Gold, a New York-based attorney and shareholder at law firm Anderson Kill. Covered costs could include forensic, accounting and credit

monitoring, crisis management and notification, and call center expenses to respond to consumer inquiries. (Ha, 2014) As a consumer, one is advised to check other potential policy coverages for damages. There is the potential that coverage for some of the losses might be covered under more traditional non-cyber insurance policies.

In *Don't Waste Your Money on Cyber Breach Insurance*, Dark Reading suggests insurance is not a substitute for solid data security. "These insurance policies can't eliminate risk, they can only help you control and minimize it", says Rich Santalesa, senior counsel for Infolaw Group. (Dark Reading, 2014) Key risks to obtaining a policy to fit an institution's requirements is the fact that the insurance vehicle is fairly new and is completely different than anything existing today.

According to sources, Home Depot carries a $100 million insurance policy for breach-related expenses. "Chief Financial Officer Carol Tomé told analysts that the breach-related expenses incurred during the quarter came to about $43 million, while projected known gross breach costs were about $27 million for the fourth quarter. (Kell, 2014) The insurance policy reportedly has a $7.5 million deductible. (Murphy, 2014)

Home Depot believes that $27 million of the $62 million cost to provide credit monitoring, increased call center staffing, and legal/professional fees will be paid by the insurance. Wesley McGrew, expert on retail breaches, expects that Home Depot will bear the costs related to fraud and payment card replacement. Mr. McGrew postulates that banks typically have retailers cover that cost if the company has security shortfalls. (Finkle, 2014)

Home Depot is estimating the costs at around $62 million to cover the investigation, credit monitoring service, call center staffing, and other required steps. It is expected that the insurance will cover $27 million. As the story continues to develop, information will become clear on why the insurance payoff was so low. The retailer's profit rose by 4.4% and was below their target of 4.8% for the full year, is expected to be impacted by the data breach, and associated activities. (Trefis Team, 2014)

Buying the correct amount of insurance for a company depends on its financials, industry, operations, and risk exposure. (Marciano, 2014) According to Christine

Marciano of Cyber Data Risk Managers LLC, the maximum amount for any one company is $300M. In the 2013 Ponemon Study *Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age*, it surveyed Risk Managers and asked them to predict their company's financial exposure due to security exploits and data breaches for the next 24 month period. The average estimate was $163M. (Ponemon Institute, 2013) Having insurance should allow the affected company to concentrate on remediation, communication, and coordination of other non-financial agendas. The insurance provider will require the ensured company to institute solid cyber protections or the insurance policy might not pay as expected.

4. Conclusion

Protection of privacy is becoming more and more of an issue in today's data breach environment. The National Institute of Standards and Technology provides guidance not only defining PII, but also on how to implement controls to protect the information. The SANS Critical Security Controls provides a prioritized list of controls and offers suggestions on measurement and implementation.

Forty-six states, the District of Columbia, Puerto Rico, and the Virgin Islands have laws requiring notification of breaches when PII is involved. (Stevens, 2012) moreover, legal and regulatory requirements for protection of PII are very complex. This complexity is due in part to the differing state laws.

Surviving a large data breach is possible. The institution must take proactive measures to ensure that when the breach occurs, the company is prepared. The breach is inevitable for most organizations regardless of the institution's security posture. An adversary needs only one or two vulnerabilities and the company is at risk. Hoping for the best is not a plan.

While an institution is not suffering from this type of event, it would be wise to understand how the event could occur and develop plans. Understanding what information the company collects, how valuable that data is, how the company protects

that information, applies best practices, discusses and procures insurance, if appropriate, and develop a Breach Preparation Plan that includes communications (who, what, when, and where). Additionally, the company must understand the federal, state, and other government laws it might be subject to when dealing with a breach. Where the data resides, whom the information is about, and even where the compromise occurs could be major factors.

The odds are high, that a data breach will occur in most organizations so by preparing while there is time for the company to influence the outcome is very prudent. Take action and do not become the next victim.

The Home Depot Data Breach undoubtedly will provide many lessons learned for institutions. Readers should continue to follow the story and apply those lessons learned. Remember data breach insurance can ease the pain of financial issues, but lost customer confidence is another matter altogether.

David Belangia, dwbelangia@hotmail.com

5. References

Amerding, T. (2014, October). Cyber Insurance: Worth it, but beware of the exclusions. *CSO.* Retrieved from http://www.csoonline.com/article/2835274/cyber-attacks-espionage/cyber-insurance-worth-it-but-beware-of-the-exclusions.html.

Banjo, S. (2014, September). Home Depot Confirms Data Breach. *Wall Street Journal*. Retrieved from http://www.wsj.com/articles/home-depot-confirms-data-breach-1410209720.

Bartholomew, A. (2012, April). U.S. Data Privacy Laws Challenge the E-Discovery Process. Retrieved from http://www.exterro.com/blog/u-s-data-privacy-laws-challenge-the-e-discovery-process/.

Bit9. (2014). Breach Preparation: Plan for the Inevitability of Compromise. *Bit9.* Retrieved from https://www.bit9.com/resources/ebooks/eguide-breach-preparation/.

Blankenhorn, D. (2014, November). Lowe's Stock Benefit From Home Depot Breach Is Temporary. *Seeking Alpha.* Retrieved from http://seekingalpha.com/article/2694905-lowes-stock-benefit-from-home-depot-breach-is-temporary.

Bose, N. (2014, September). Home Depot confirms security breach following Target data theft. *Reuters.* Retrieved from http://www.reuters.com/assets/print?aid=USKBN0H327E20140909.

Bronstad, A. (2014, September). Lawsuits Piling Up in Home Depot Security Breach. *The National Law Journal.* Retrieved from http://www.nationallawjournal.com/id=1202671405651/Lawsuits-Piling-Up-in-Home-Depot-Data-Security-Breach.

CardFellow. (2014). Data Breach Insurance, Prevention & Cost. Retrieved from http://www.cardfellow.com/blog/data-breach-insurance-prevention-cost/.

Cummings, K. (2014, September). Home Depot's Sloppy Mistakes Tarnish Its Once Bold Brand. *The Huffington Post.* Retrieved from http://www.huffingtonpost.com/kellie-cummings/home-depots-sloppy-mistakes_b_5867068.html.

David Belangia, dwbelangia@hotmail.com

Cyber Data-Rick Managers. (2014). Retrieved from http://databreachinsurancequote.com/cyber-insurance/cyber-insurance-data-breach-insurance-premiums/.

Dark Reading. (2014, September). Don't Waste Your Money On Cyber Breach Insurance. *Information Week, Dark Reading.* Retrieved from http://www.darkreading.com/dont-waste-your-money-on-cyber-breach-insurance/d/d-id/1138422?.

Devis, C. (2014, December). Home Depot Data Breach Class Action Lawsuits Grouped in MDL. *Top Class Actions.* Retrieved from http://topclassactions.com/lawsuit-settlements/lawsuit-news/45716-home-depot-data-breach-class-action-lawsuits-grouped-mdl/.

Finkle J, Bose, N. (2014, September). Insurance Will Absorb Some Costs in Home Depot's Giant Privacy Breach. *Insurance Journal.* Retrieved from http://www.insurancejournal.com/news/national/2014/09/19/341105.htm.

Greisiger, M. (2013). *Cyber Liability & Data Breach Insurance databreach insurance Claims.* Retrieved from http://www.netdiligence.com/files/CyberClaimsStudy-2013.pdf.

Ha, Y. (2014, December). Insurance Questions, Lawsuits Arise in Wake of Target's Data Breach. *Insurance Journal.* Retrieved from http://www.insurancejournal.com/news/national/2013/12/22/315222.htm.

Holan, M. (2014, November). How much did the Home Depot data breach cost local credit unions? *Washington Business Journal's BizBeat.* Retrieved from http://www.bizjournals.com/washington/blog/2014/11/how-much-did-the-home-depot-data-breach-cost-local.html?page=all.

Home Depot. (2014, January). *Shop with Privacy and Security.* The Home Depot, Inc. Privacy and Security Statement. Retrieved from http://www.homedepot.com/c/Privacy_Security.

Home Depot (2014, September). The Home Depot Announces Third Quarter Results; Reaffirms Fiscal Year 2014 Guidance. Retrieved from http://ir.homedepot.com/phoenix.zhtml?c=63646&p=irol-newsArticle&ID=1990548.

David Belangia, dwbelangia@hotmail.com

Home Depot data breach affected 56M debit, credit cards. (2014, September). *WJLA*. Retrieved from http://www.wjla.com/articles/2014/09/home-depot-data-breach-affected-56m-debit-credit-cards-107289.html.

Home Depot Reports Findings in Payment Data Breach Investigation. (2014, September). Retrieved from https://corporate.homedepot.com/MediaCenter/Documents/Press%20Release.pdf.

Information LawGroup. (2013, July). *10 Years After SB 1386, California Attorney General Issues First Ever Report and Recommendations on Data Breaches.* Retrieved from http://www.infolawgroup.com/2013/07/articles/breach-notice/10-years-after-sb-1386-california-attorney-general-issues-first-ever-report-and-recommendations-on-data-breaches/.

Kell, J. (2014, November). Home Depot warns there'll be more costs due to its data breach. *Fortune.* Retrieved from http://fortune.com/2014/11/18/home-depot-breach-impact/.

Kerner, S. (2014, November). Home Depot Breach Expands, Privilege Escalation Flaw to Blame. *E-Week.* Retrieved from http://www.eweek.com/security/home-depot-breach-expands-privilege-escalation-flaw-to-blame.html.

Kessler, M. (2014, September). Attorneys General Launch Multistate Home Depot Breach Investigation. *Bloomberg BNA.* Retrieved from http://www.bna.com/attorneys-general-launch-n17179894898/.

Koppenheffer, M. (2014, May). Paying with PayPal at Home Depot Just Got a Lot Easier. *The Motley Fool.* Retrieved from http://www.fool.com/investing/general/2014/05/21/paying-with-paypal-at-home-depot-just-got-a-lot-ea.aspx.

Krebs, B. (2014, September). Home Depot Hit by Same Malware as Target. *Krebs on Security.* Retrieved from http://krebsonsecurity.com/2014/09/home-depot-hit-by-same-malware-as-target/.

Krebs, B. (2014, September). Banks: Credit Card Breach at Home Depot. *Krebs on Security.* Retrieved from http://krebsonsecurity.com/2014/09/banks-credit-card-breach-at-home-depot/.

David Belangia, dwbelangia@hotmail.com

Kropf, J. (2007, June). Networked and Layered: Understanding the U.S. Framework for Protecting Personally Identifiable Information. *World Data Protection Report.* BNA.

Lui, S. (2014, September). Possible data breach at Home Depot Highlights retailer's vulnerability. *Los Angeles Times*. Retrieved from http://www.latimes.com/business/la-fi-retail-hacking-20140904-story.html.

Marciano, C. (2014, November). How Much Cyber Insurance Coverage Should Companies Buy? *Cyber Data Risk Managers LLC.* Retrieved from http://databreachinsurancequote.com/cyber-insurance/how-much-cyber-insurance-coverage-should-companies-buy/.

Murphy, T. (2014, November). Home Depot faces dozens of lawsuits over data breach that hit debit and credit cards. *Candadian Underwriter.ca.* Retrieved from http://www.canadianunderwriter.ca/news/home-depot-faces-dozens-of-lawsuits-over-data-breach-that-hit-debit-and-credit-cards/1003368354/.

Overview of the Privacy Act of 1974. (2014, June). Department of Justice. Retrieved from http://www.justice.gov/opcl/policy-objectives.

PCI DSS Compliance. (January). About the Payment Card Industry Data Security Standard. Retrieved from http://www.gopai.com/Solutions/Merchant-Solutions/Data-Breach-Security/PCI-DSS.

Peters, S. (2014, September). Home Depot Breach May Not Be Related To BlackPOS, Target. *Information Week, Dark Reading.* Retrieved from http://www.darkreading.com/home-depot-breach-may-not-be-related-to-blackpos-target/d/d-id/1315636.

Plummer, Q. (2014, November). Home Depot Data Breach Backlash: 44 Civil Lawsuits in the Works. *Tech Times.* Retrieved from http://www.techtimes.com/articles/20956/20141125/home-depot-data-breach-backlash-44-civil-lawsuits-in-the-works.htm.

Ponemon Institute. (2013, August). Managing Cyber Security as a Business Risk: Cyber Insurance in the Digital Age. *Ponemon Institute, LLC.* Retrieved from http://assets.fiercemarkets.com/public/newsletter/fiercehealthit/experian-ponemonreport.pdf.

David Belangia, dwbelangia@hotmail.com

Sedlack, T. (2014, August). Data Breach Collateral Damage. *RIS, Retail Info Systems News.* Retrieved from http://risnews.edgl.com/retail-news/Data-Breach-Collateral-Damage94462.

Schleicher, M. (2014, October). Home Depot Data Breach Already Causing Customer Losses. *Tech insurance Small Business Center.* Retrieved from http://www.techinsurance.com/blog/cyber-risk/home-depot-daata-breach-already-casuing-customer-losses/.

Stevens, G. (2012, April). Data Security Breach Notification Laws. *CRS Report to Congress.*

Turner, H. (2014, December). More Lawsuits Filed in Home Depot Data Breach. *Lawyers and Settlements.* Retrieved from http://www.lawyersandsettlements.com/articles/data-breach/home-depot-greater-chautauqua-federal-credit-union-20325.html#.VKwuLWPVtps.

Trefis Team (2014, September). Home Depot: Could The Impact Of The Data Breach Be Significant. *Forbes.* Retrieved from http://www.forbes.com/sites/greatspeculations/2014/09/24/home-depot-could-the-impact-of-the-data-breach-be-significant/.

Young, J. (2014, September). In wake of Target, Home Depot tight with info in breach response. *Reuters.* Retrieved from http://www.reuters.com/article/2014/09/08/us-home-depot-dataprotection-disclosure-idUSKBN0H31UC20140908.

David Belangia, dwbelangia@hotmail.com

Last Updated: August 22nd, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Tampa - Clearwater 2017	Clearwater, FLUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Network Security 2017	Las Vegas, NVUS	Sep 10, 2017 - Sep 17, 2017	Live Event
SANS Dublin 2017	Dublin, IE	Sep 11, 2017 - Sep 16, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MDUS	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, DK	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, GB	Sep 25, 2017 - Sep 30, 2017	Live Event
Data Breach Summit & Training	Chicago, ILUS	Sep 25, 2017 - Oct 02, 2017	Live Event
Rocky Mountain Fall 2017	Denver, COUS	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS SEC504 at Cyber Security Week 2017	The Hague, NL	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Oslo Autumn 2017	Oslo, NO	Oct 02, 2017 - Oct 07, 2017	Live Event
SANS DFIR Prague 2017	Prague, CZ	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZUS	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, SG	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS AUD507 (GSNA) @ Canberra 2017	Canberra, AU	Oct 09, 2017 - Oct 14, 2017	Live Event
Secure DevOps Summit & Training	Denver, COUS	Oct 10, 2017 - Oct 17, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VAUS	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, JP	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS Brussels Autumn 2017	Brussels, BE	Oct 16, 2017 - Oct 21, 2017	Live Event
SANS Berlin 2017	Berlin, DE	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS San Diego 2017	San Diego, CAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, AE	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FLUS	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Amsterdam 2017	Amsterdam, NL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Milan November 2017	Milan, IT	Nov 06, 2017 - Nov 11, 2017	Live Event
Pen Test Hackfest Summit & Training 2017	Bethesda, MDUS	Nov 13, 2017 - Nov 20, 2017	Live Event
SANS Paris November 2017	Paris, FR	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, AU	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS San Francisco Fall 2017	OnlineCAUS	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced