Coalfire
IT Audit and Compliance

Whitepaper: The Costs of Failing a PCI-DSS Audit

Dan Fritsche, CISSP, QSA (P2PE), PA-QSA

Bhavana Sasne, QSA

March 4, 2015

Prepared for:

HyTrust
Cloud Under Control

Overview

In the last few years, security breaches have occurred in various shapes and forms and have shaken up many organizations, especially those in the retail industry. Breaches at Target, JPMC, Home Depot, NY Presbyterian Hospital and most recently, Anthem, have significantly impacted these organizations' financial performance and brand reputation. This paper will explore the financial consequences of these types of security breaches — including brand damage, loss of revenue, downtime, privacy penalties, forensics investigations, and cyber Insurance coverage. It will also highlight the steps that organizations can take to address cybersecurity risks.

In the wake of these breaches, many questions still linger: Were the compromised companies really compliant in the first place? How seriously did they take security and compliance issues? Who is ultimately responsible for the breach? The company itself? The organizations involved in securing the company? The standards bodies responsible for compliance? The criminals who enacted the crime?

Approaches for auditing and assessment vary from one governance, risk, and compliance (GRC) company to the next. Simply checking the box for each regulatory requirement is not sufficient. An approach to meet the challenges that go beyond compliance and address an appropriate security posture should be adopted by organizations.

This paper will help the reader understand the potential costs of failing an audit or getting breached even after having passed a Payment Card Industry Data Security Standard (PCI DSS) assessment and how HyTrust CloudControl™ can assist in avoiding failures in associated control areas under the PCI DSS 3.0. This paper strictly presents an opinion; no analysis or testing was performed.

About HyTrust CloudControl™

HyTrust CloudControl offers a robust solution for administrator controls and configuration controls on VMware vSphere and vCenter Infrastructure, providing complete functionality to meet specific PCI DSS 3.0 requirements. The solution supports 28 of the controls from the PCI DSS requirements including the access controls for hypervisors. For more information about how HyTrust can help address PCI controls, download a solution brief.

Target Audience

This assessment white paper has two target audiences:

1. The first target audience includes risk and compliance individuals in a merchant or service provider organization who require better justification to fund efforts related to Payment Card Industry (PCI) Compliance;
2. A second target audience includes Security and Risk professionals as well as Infrastructure and Operations stakeholders who want to better understand their role in breach prevention.

Breach Examples

Recent high profile cyber-attacks have raised awareness of how damaging a breach can be to affected organizations. While identifying the cost can be challenging, various analysis has been performed to better understand the impact of a breach. Following is an outline of recent breaches and the subsequent impact to each organization.

- Target
    - Date: December 2013
    - Impact: 110 million customers had their credit and debit card numbers and customer sensitive information stolen. As of February 2015, Target reported nearly $162 million of expenses related to the breach, including $444 million in insurance payments. Security analysts estimate that the overall breach costs could reach $500 million.

- Home Depot
    - Date: September 2014
    - Impact: Nearly 56 million customers were impacted, and per SEC filings from third quarter 2014, this breach cost the company almost $43 million. Home Depot describes it “recorded $43 million of pretax expenses related to the data breach, partially offset by a $15 million receivable for costs the company believes are reimbursable and probable of recovery under its insurance coverage, for pretax net expenses of $28 million." According to the SEC filing, the expenses included “cost to investigate the data breach, provide credit monitoring services to its customers, increasing call center staffing and paying legal and professional services”. The investigation is still in progress and the total estimated cost is yet to be determined. [1]

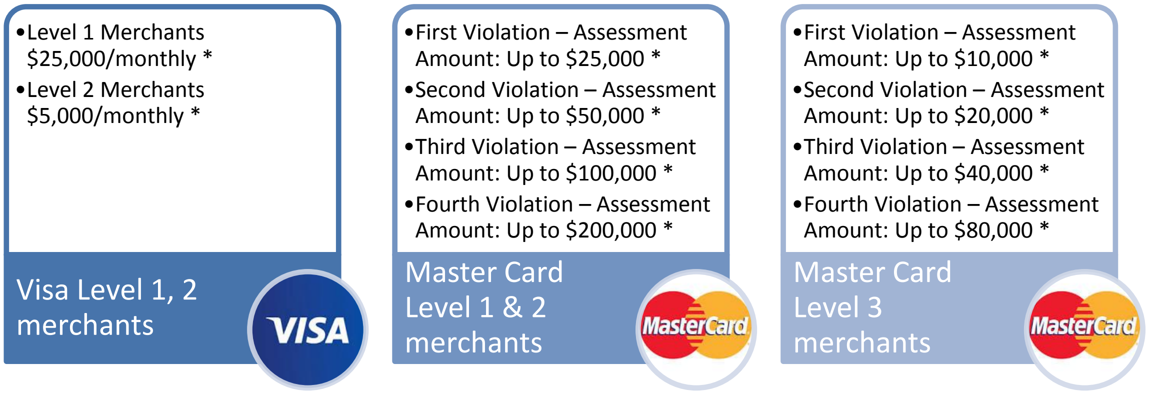
- New York-Presbyterian Hospital and Columbia University
    - Date: September 2010

[1] http://www.sec.gov/Archives/edgar/data/

- Impact: Exposure of 6,800 patient records including lab reports, medications, patient status, and vital signs. New York- Presbyterian paid the Office of Civil Rights (OCR) $3.3 million in settlement fees and Columbia University paid $1.5 million as part of their settlement.

PCI DSS Noncompliance Fines

Payment brands and their partners impose penalties on merchants or service providers for non-compliance. The charges could range from $5,000 to $100,000 per month depending on the payment brand and nature of non-compliance.Shown below are some examples of possible fine amounts that Visa or Master Card could charge the merchants for non-compliance.



- Level 1 Merchants $25,000/monthly *
- Level 2 Merchants $5,000/monthly *

Visa Level 1, 2 merchants

- First Violation – Assessment Amount: Up to $25,000 *
- Second Violation – Assessment Amount: Up to $50,000 *
- Third Violation – Assessment Amount: Up to $100,000 *
- Fourth Violation – Assessment Amount: Up to $200,000 *

Master Card Level 1 & 2 merchants

- First Violation – Assessment Amount: Up to $10,000 *
- Second Violation – Assessment Amount: Up to $20,000 *
- Third Violation – Assessment Amount: Up to $40,000 *
- Fourth Violation – Assessment Amount: Up to $80,000 *

Master Card Level 3 merchants

The Aftermath: What Does a Breach Cost?

Research done by the Ponemon Institute in 2013-2014 shows that average cost of a data breach varies widely by country. In 2014, the cost per compromised record was $201 in the USA, $158 in the UK, $127 in Japan, and $51 in India. The average total organization cost per incident in the same research performed in 2014 was $5.85 million in the USA, $3.68 million in the UK, $2.36 million in Japan and $1.37 million in India. Depending on the industry type the cost can vary as well. [2] Here are some US based costs (as of 2014):

- $417,700: Average detection and escalation costs.

[2] http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis

* Note that these are sample numbers; the fines are decided by respective payment brands or their partners and can change dramatically depending on the nature of non-compliance.

- $509,237: Average notification costs. Notification costs can include IT activities such as: consolidating lists of contacts in databases, determining applicable regulatory requirements, and engaging external experts and other expenses.
- $1.6 million: Average post breach costs. Costs include helpdesk activities, inbound communications, special investigations, remediation, legal expenses, identity protection services and regulatory interventions.
- $3.3 million: Average lost business costs. Business that was lost included abnormal turnover of customers, increased customer inquiry activities, and reputation losses.

Reputational Loss: Reputation is perhaps the most important asset to a company and is very difficult to protect. Losses emerging from reputation damage can be a greater risk to the company than any other and is practically incalculable. An Economist Intelligence Unit whitepaper entitled "Reputation Risk: Risk of Risks" states that companies struggle to categorize and quantify reputational risk.[3] While it may be difficult to quantify reputational risks, organizations are advised to understand and prioritize various threats to the company reputations.

Brand damage: This is one of the most difficult impacts to quantify. Brand damage could also result in loss of trust from consumers and this trust can be difficult to regain, potentially impact brand or reputation. According to CBS News, Target went from being one of the top 10 brands ranked by BrandIndex to number 21 by January of 2013. This was just months after their data breach was announced.[4] Besides declines in sales, companies then spend significant money in various campaigns to re-gain this lost brand recognition.

Compliance fines: Compliance fines vary depending on the nature of breach. The Health Insurance Portability and Accountability Act's (HIPAA) Privacy and Security Rules were enacted to define the manner in which patient information can be used and how it should be protected utilizing the appropriate safeguards. Failure to comply with HIPAA rules can result in civil and criminal penalties. Fines range between $100 per violation to a maximum of $1.5 million per violation, and could include jail time if found to be criminally liable. PCI DSS fines established by the major payment card brands levy fines ranging from $5,000 to $100,000 per month for PCI DSS compliance violations.

Privacy regulatory defense and penalties: Claims are made after a breach by various parties, particularly by consumers and banks. Legal defense expenses arise when companies are defending against those claims. According to a NetDiligence Cyber Liability and Data Breach Insurance Claims Study, the average cost for legal defense was $500,000 while the legal settlement costs averaged around $1 million per incident.

[3] http://www.eiu.com/report_dl.asp?mode=fi&fi=1552294140.PDF

[4] http://www.cbsnews.com/news/targets-brand-takes-a-massive-hit-amid-data-breach/

Forensics and Investigations: Major payment brands contractually require a forensics investigation if the breach involves unauthorized access to payment card data. Forensic investigators pre-approved by the PCI Security Council may be required to perform the investigation. Typically, third parties are engaged to ensure the quality and maintain the objectivity as internal investigations may be questioned on integrity issues. Average fees could range between $200 and $2000 per hour. The examinations and investigations performed provide details on the severity and scope of the breach. [5]

Credit or Identity Monitoring: To maintain good customer relationships and to try and retain customers, companies may provide credit and identity monitoring services to customers whose data may have been stolen. Identity restoration is a service that affected parties could request if they suffer actual identity theft. Costs for these services, which includes credit and identity monitoring and restoration of stolen identities, range between $10 and $30 per individual, per year.

Notifications as per State Laws: Forty-seven states, the District of Columbia, Guam, Puerto-Rico, and the US Virgin Islands have enacted security breach notification laws. This legislation requires private or government entities to notify individuals of security breaches where personally identifiable information has been compromised. Notification costs differ depending on the number of records or individuals affected. These costs range between $0.50 and $5 per notice. Most of the network risk insurance policies typically cover this cost; however, cost related risk management procedures and mitigation costs are not usually covered.

Cyber Insurance coverage: Cyber insurance types and premiums vary based on the size of the company and other circumstances. Companies can opt for specific coverage policies including, customer notification expenses, credit/identity theft monitoring, privacy and security liability, business interruption, cyber extortion, hacker damage costs, regulatory defense and penalty costs, forensics and investigations; and privacy attorney costs. But not all companies choose to have having cyber insurance policies. Analysis data from Ponemon Institute shows that 10% of companies held cyber insurance policies in 2013; however, that number has increased to 26% in 2014.

The one factor most likely to bring a premium down after a breach is the ability to show continuous improvement in controls and monitoring. Insurers want to make sure that their customers are not likely to suffer from the same incident or be an easy target for similar breaches.

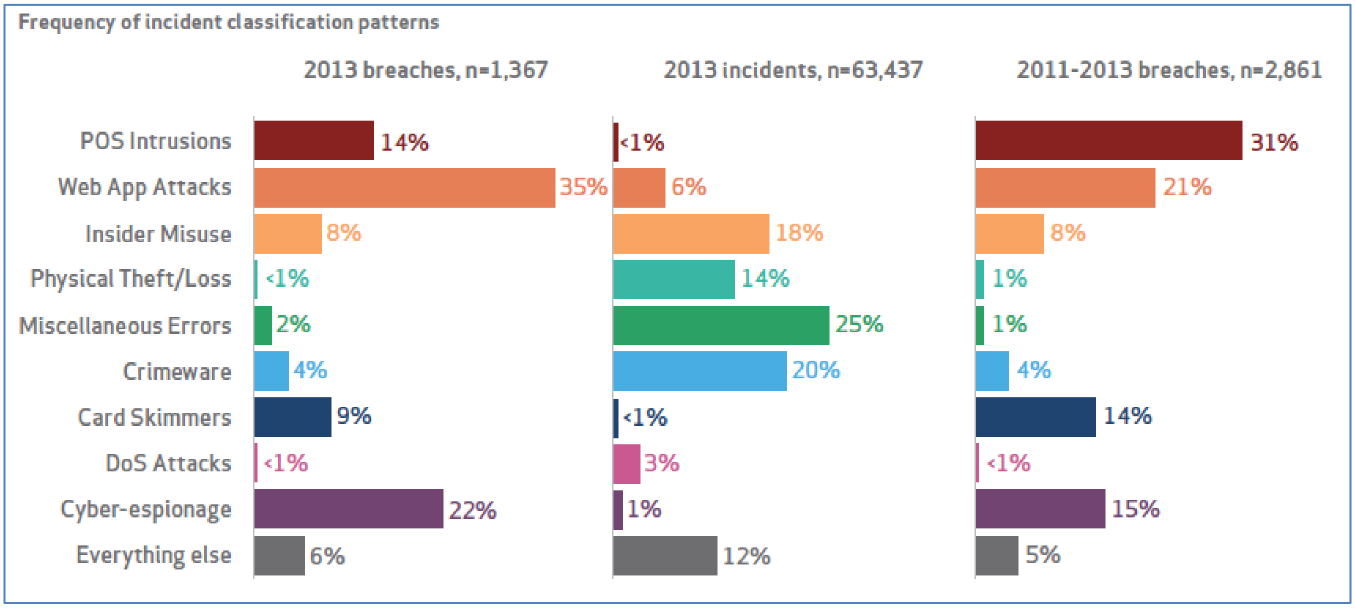
Because of all these factors, it is difficult to pin down the final cost of data breach, and it could take years to determine the total cost for any breach that has occurred in an organization.

[5] http://www.zurichna.com/internet/zna/sitecollectiondocuments/en/products/securityandprivacy/

Invest in Improving Security Posture

Considering the various costs that companies face when a breach occurs, proactive measures to improve their security posture is critical. One commonality among the recent breaches outlined earlier is that privileged user or administrator credentials were used to gain access to the organization. To prevent these kinds of attacks, organizations should consider adopting strong administrator controls, security monitoring, and active response measures, to their security portfolio.

Data breach investigations performed by Verizon in 2014 show that 90% of the breaches can be described by nine basic patterns.[6] Not all of the attacks apply to each industry, but the intent of the diagram below is to display the incident and attack patterns to highlight the controls that could have been in place to prevent those type of attacks.



Source: Verizon 2014 Breach Investigations Report

Below are some of the causes for the various attacks displayed in diagram above:

- Brute forcing remote access connections
- Use of backdoor
- Privilege abuse
- Inadequate input validation

[6] http://www.verizonenterprise.com/DBIR/

- Use of unapproved software
- Web downloads on systems with no anti-virus software
- Unapproved or malicious use of organizational resources
- Unintentional actions
- Unauthorized network or system access

Most of the attacks occurred because the systems and networks were not configured in a secure manner, let alone in a PCI DSS compliant manner. Access controls for virtualization technologies were thought to be out of scope and were ignored as a result; however, the PCI DSS 3.0 standard requires appropriate testing in virtualized environments. Failures to meet specific requirements could result in PCI DSS assessment failure. Listed below are controls and requirements that could have been in place to prevent attacks that occurred:

- Restrictions on remote access
- Password policies
- Lockout policies
- Whitelisting for use of website from the POS Systems
- Antivirus on systems (POS systems)
- Segmentation of network
- Two-factor remote authentication set up
- Input validation for websites
- Logging of system, network or application activities
- User Account reviews
- Access restrictions

HyTrust CloudControl™

Along with the many advantages of using virtualized and cloud solutions comes the need for better security and protection. Whether it is cardholder data specific to PCI DSS or PHI data, all systems that are used to support a sensitive environment are required to comply with appropriate compliance standards.

HyTrust CloudControl has capabilities that help with secure configurations as well as satisfy various PCI DSS controls. HyTrust CloudControl can be adopted by retailers who are looking to achieve PCI compliance and by government agencies desiring to protect confidential data with a virtualized or cloud infrastructure. The virtual environment also falls under the scope of PCI DSS if it stores, processes, or transmit cardholder data. HIPAA, The Federal Risk and Authorization Management Program (FedRAMP), and other privacy regulations also require compliance efforts where HyTrust CloudControl and VMWare solutions can be utilized.

HyTrust CloudControl was designed to provide a solution for administrator and configuration controls on VMWare and VSphere infrastructure. The various PCI control areas that HyTrust CloudControl supports are listed below:

- Configuration hardening (Requirement 2: Vendor defaults)

- Separation of duties (vmnetwork/host; dev/test/prod) (Requirement 6: Secure Systems)

- Least Privilege role-based access controls (Requirement 7: Restrict Access to cardholder data)

- Authentication controls including password management and two-factor (Requirement 8: Identify and Authenticate Access)

- Reporting and auditing of administration activity (Requirement 10: Track and Monitor all access)

- Mixed mode administrative segmentation (Not prohibited by PCI DSS but supports PCI DSS 3.0 best practices and guidelines and supports multiple controls including 2-factor authentication; asset-based authorization to maintain isolation between cardholder data environment (CDE) and non-CDE components at hypervisor level; detailed logging of hypervisor administration activity; hypervisor configuration hardening)

- Sampling reduction - Centralized operational processes and controls (Auditors could reduce the sample size of audit if standardized and centralized consistent controls are present)

Utilizing HyTrust CloudControl for each of the above can help lower the cost of PCI DSS compliance by addressing the PCI controls in an efficient manner known to appropriately address and even protect beyond the minimum control requirements. Used appropriately, the solution can also to help segment the cardholder data environment which can then result in a reduced scope for an audit.

Summary and Conclusion

A few years ago, a small proportion of companies considered data breaches to be something that would impact their business. Today, only a few companies consider data breaches something they can ignore. Understanding the potential costs is critical to determine the risk any company faces should a breach occur. The costs associated with securing a company’s environment and meeting compliance standards pale in comparison to potential breach costs. This paper has outlined some of the costs and risks of data breaches so that merchants and service providers can understand the importance of protecting against these threats and take appropriate action. HyTrust’ CloudControl provides an excellent option to help ensure critical PCI DSS 3.0 controls can be met, thus reducing the risk of data breaches. The paper primarily focused on how HyTrust CloudControl could be adopted for the PCI DSS 3.0 standard; however, this solution can be also utilized for security controls within HIPAA, FedRAMP, and various other regulatory compliance standards.

Contact information:

Coalfire: www.coalfire.com
Phone: 877-224-8077
Email: info@coalfire.com
HyTrust: www.hytrust.com
Phone: 650-681-8100
Email: info@hytrust.com