Is the PCI Data Security Standard Enough?

By: Christina M. Freeman

ICTN 6870

Advanced Network Security

Abstract:
This paper will present the researched facts on Payment Card Industry Data Security Standard or PCI DSS as developed by the PCI Council. It will provide the history of the standard, present a foundation of the standards requirements while providing an analysis of the challenges organizations must face to be compliant. It will explore why organization should comply and how compliance has helped protect customer payment card data, contrasted with the additional rules merchants must follow. Discussion surrounding industry best practice for ensuring compliance. Finally, in light of the recent security data breaches, is the PCI standard enough to prevent data breaches and keep information secure? How have the requirements laid out in the standard helped protect the customer?

What is PCI DSS?
The Payment Card Industry Data Security Standard or PCI DSS was originally developed in December 2004. Version 1.0 was the first unified security standard which was supported by all five major credit card companies. (The history of PCI DSS) Updated on a three-year cycle, the standard is designed to "encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally". PCI DSS provides the baseline for all technical and operational requirements which are designed to protect cardholder data. It applies to all entities involved in payment card processing – including merchants, processors, acquirers, issuers, and service providers. In addition it applies to all other entities that store, process or transmit cardholder data. (Payment Card Industry Data Security Standard, 2013)

The primary goal of PCI DSS is to reduce transaction risks and raise awareness of key facets of data security. (Xia) PCI DSS requires the implementation of specific controls, testing and audit logging that when implemented and maintained reduces the risk of security breaches. In addition, if your organization is PCI compliant and security is compromised, there is the potential of relief from fines.

The data security standard categorizes organizations based on transaction volume. Level 1 organizations, process the greatest number of transactions (between 2.5 million‑6 million transactions), while a level 4 organization has the lowest number of transactions (under 20,000 eCommerce transactions and up to 999,999 other transactions). While the requirements for compliance remain the same, a level 2-4 organization may validate their compliance via a self-assessment questionnaire or if they desire they may engage a third party Qualified Security Assessor Company (QSAC). A level 1 organization must validate compliance by a Qualified Security Assessor through a QSAC. (Payment Card Industry Data Security Standard, 2009)

The Requirements
The current version of PCI DSS, version 3.0, includes a minimum set of requirements for protecting cardholder data, and may be enhanced by additional controls and practices to further mitigate risks. In addition, federal, regional or local laws and requirements may require specific

protection of the data that go beyond PCI requirements. (Payment Card Industry Data Security Standard, 2013)

The most recent version, published in November 2013, contains 12 separate requirements within 6 categories. Table 1 provides an overview of the 12 PCI DSS requirements.

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Table 1: High level overview of PCI requirements separated into categories.

Source: Payment Card Industry Data Security Standard, 2013

1. Build and Maintain a Secure Network

In order to protect cardholder data, organizations must install and maintain secure firewall configurations. Firewalls are a key element to protecting any computer network. In order to meet the standard provided by the Payment Card Industry, organizations must ensure firewalls are set to examine all network traffic and block all transmissions that do not meet the specified security criteria as required by the standard. They must ensure that all systems are protected from unauthorized access and untrusted networks. Sometimes, a path that may seem insignificant can provide an unprotected pathway from an untrusted network into an otherwise secure network.

Additionally, organizations must be aware and ensure they do not use any vendor supplied defaults for any system passwords as well as the defaults for security parameters. Individuals looking to cause harm and steal data, whether internal or external to an organization, will often use the vendor default passwords and settings, which can compromise systems. These passwords and settings are well known by hacker communities and can be easily determined through public means. (Payment Card Industry Data Security Standard, 2013)

2. Protect Cardholder Data

In order to be compliant, organizations are required to use protection methods such as encryption, truncation, masking and hashing in order to protect stored cardholder data. If security controls are circumvented and an individual is able to gain access to sensitive data, as long as the organization had the appropriate protection in place, the compromised data is unreadable and useless. Other protections can be used to mitigate risks, such as not storing cardholder data unless absolutely necessary, truncating credit card numbers if possible and not sending sensitive data via email or by any other unsecure means.

In addition, organizations must ensure any sensitive information and cardholder data is encrypted during transmission across open, public networks. Public networks are an easy target for malicious individuals looking to steal information. Organizations must pay close attention to wireless networks as malicious individuals will target misconfigured wireless networks. Vulnerabilities in legacy encryption protocols and legacy authentication protocols are a common target as well. However, encrypting all cardholder data will mitigate this risk and malicious individuals will be unable to exploit these vulnerabilities in order to obtain PCI data. (Payment Card Industry Data Security Standard, 2013)

3. Maintain a Vulnerability Management Program

Organizations must have anti-virus software or programs in place and it must be updated regularly. Malware can easily enter a network via legitimate business-approved activities. For example, employee e-mail, limited use of the Internet, or personal devices, such as laptop computers, tablets or other storage devices. Without anti-virus programs to detect, quarantine and remove any potential malware, malware can exploit system vulnerabilities.

In addition to anti-virus programs, organizations need to ensure they are developing and maintaining secure systems and applications. Malicious individuals will manipulate security vulnerabilities in order to gain access to a network. Software vendors provide security patches which will fix many system vulnerabilities. In order to be compliant, organizations are required to have the most recently released, appropriate software patches applied to all critical systems so as to protect against exploitation and compromise of cardholder data. (Payment Card Industry Data Security Standard, 2013)

4. Implement Strong Access Control Measures

PCI compliance requires organizations to implement strong access control measures by 1) restricting access to cardholder data by business need to know, 2) identifying and authenticating access to system components, and 3) restricting physical access to cardholder data.

First, critical data should only be accessed by authorized personnel, when they have a need to know, based on job responsibilities. Processes need to be in place to enforce this policy. Next, assigning a unique ID for each individual who has access to critical systems promotes

accountability and allows for all actions to be traced to authorized individuals or processes. Enabling strong access controls surrounding password requirements will strengthen the authentication system. Finally, allowing physical access to data or systems that contain cardholder data can allow individuals to access devices or data and to remove systems or hardcopies, and must be restricted. (Payment Card Industry Data Security Standard, 2013)

5. Regularly Monitor and Test Networks

Compliance requires organizations to track and monitor all access to network resources and cardholder data by implementing logging mechanisms. In a situation where data compromise is occurring or has occurred, if an organization has the ability to track user activities, the event can be detected and the impact can be minimized. Without activity logs, preventing, detecting and determining the cause of a compromise, is extremely difficult.

As new vulnerabilities are continuously being introduced, organizations must stay current and must regularly test security systems, processes, and custom software to ensure security controls continue to reflect an ever-changing environment. (Payment Card Industry Data Security Standard, 2013)

6. Maintain an Information Security Policy

Finally, organizations must maintain an information security policy that addresses information security for the entire organization and contains roles, responsibilities and expectations for personnel. Every employee in an organization is responsible for protecting sensitive data and this responsibility should be addressed in an information security policy and communicated throughout the organization. (Payment Card Industry Data Security Standard, 2013)

According to Verizon's 2014 PCI Compliance Report only 11.1% of companies were in compliance with all 12 requirements in 2013. While 71.1% were mostly compliant. These numbers are up drastically from the previous year, but improvement, specifically for organizations that are fully compliant, needs to be made. (Verizon 2014 PCI Compliance Report)

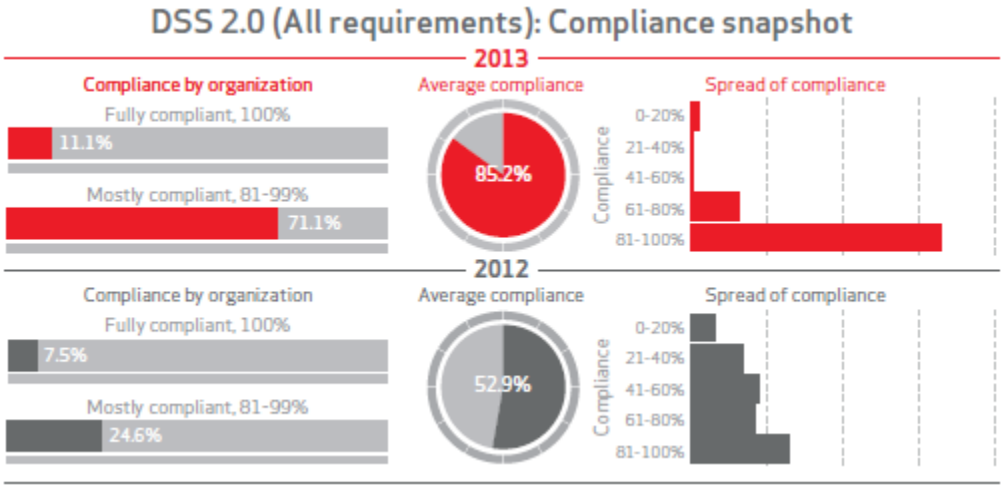

Figure 1: Snapshot for all requirements: Dataset 2012 and 2013

Source: Verizon 2014 PCI Compliance Report

The Challenges

Compliance to the PCI DSS can be a major challenge and many organizations have difficulty achieving full compliance. First, attaining and maintaining compliance with PCI DSS is expensive and very time-consuming. Feedback from organizations state that it is a challenge to tackle the scope of systems needing to comply with the standard. Often credit card data is stored and used in many applications within an organization and can even be beyond the IT perimeter. All systems that handle card data are in scope, as well as any system that receives data from or provides data to that system. Second, just because your organization may be in compliance, it does not guarantee that you are safe from security breaches. There are always new vulnerabilities being exploited and it is a challenge to keep up. An organization will never be able to be completely secure. Lastly, as new technologies emerge, it is constantly adding new risks. Mobile devices, e-commerce, cloud computing and big data broaden the PCI scope and bring additional challenges with them. (PCI Compliance and Scope Reduction)

In 2009, the Ponemon Institute conducted a study of multinational organizations. The results of the study paint the following picture of the challenges at hand:

- Cost of PCI is, on average, 1/3 of the overall security budget.
- 79% have had a data breach.
- 55% of companies focus only on protecting the credit card data but not other sensitive information.

- There is uncertainty as to what personnel are the most accountable for PCI DSS compliance.
- Smaller companies are less compliant than larger companies. (Xia)

Why Comply?

Global credit card fraud losses were greater than 11 billion dollars in 2012. The FBI is issuing warnings to retailers to "be wary of 'card-targeting malware' thought to already be responsible for the breaching of over 100 million people's card data." (Verizon 2014 PCI Compliance Report)

Organizations that accept credit cards are faced with multiple penalties for non-compliance. Starting with hefty fines and going as far as losing the right to accept credit cards, there is an enormous business risk when an organization does not comply with PCI DSS. While implementing PCI requirements is not a guarantee that an organization is safe from security breaches, the security controls required in order to be PCI compliant provide a fairly secure technology environment. (Kidd)

PCI DSS compliance can bring many benefits to all businesses. When your organization complies with the standard, it sends a message to your customers that your systems are secure and your business can be trusted with their sensitive information. The reputation your organization develops with card companies is strong as well. Additionally, PCI compliance requires strong security standards that help with compliance with other federal regulations, such as the Health Insurance Portability and Accountability Act and Sarbanes-Oxley Act. (Why Comply with PCI Security Standards?)

If an organization chooses not to comply, therefore not implementing the security controls required by PCI and they face a security breach, the substantial fines, negative publicity and the consequences of that breach can destroy the organization. (Kidd)

Non-compliance can result in numerous consequences that will affect an organization far into the future. Consequences include:

- Damaged reputation from customers, merchants and financial institutions
- Loss of business
- Lower share price for publically traded company
- Lawsuits
- Insurance claims
- Cancelled accounts
- Merchant fines
- Government fines

(Why Comply with PCI Security Standards?)

Best Practices

In order to ensure security controls remain implemented in an organization's IT environment, corporate strategy should guarantee the requirements set forth by PCI DSS are integrated with the overall security strategy and the business-as-usual processes and procedures. The PCI DSS suggests multiple best practices to ensure the standard is properly implemented into an organization. It includes:

1. Monitoring of security controls to ensure they are operating effectively and as intended.
    a. Includes firewalls, intrusion-detection systems, intrusion-prevention systems, anti-virus, access controls.
2. Ensuring all failures in security controls are detected and responded to in a timely manner, by:
    a. Restoring the security control,
    b. Identifying the cause of failure,
    c. Identifying and addressing any security issues that arose during the failure of the security control,
    d. Implementing mitigating controls to prevent the cause of the failure recurring, and
    e. Resuming monitoring of the security control, maybe with enhanced monitoring for a period of time, to verify the control is operating effectively.
3. Review changes to the environment, by:
    a. Determining the potential impact to PCI DSS scope,
    b. Identifying PCI DSS requirements applicable to systems and networks affected by the changes, and
    c. Update PCI DSS scope and implement security controls as appropriate.
4. Changes to organizational structure such as a company merger or acquisition should result in reviewing the impact to PCI DSS scope and requirements.
5. Periodic reviews and communications should be performed to confirm that PCI DSS requirements continue to be in place and personnel are following secure processes.
6. Review hardware and software technologies at least annually to confirm that they continue to be supported by the vendor and can meet the organization's security requirements, including PCI DSS.

(Payment Card Industry Data Security Standard, 2013)

Does it work?

Most experts would say that compliance with PCI compliance does not equate to security. However, the '2011 PCI DSS Compliance Trends Study' found that 64% of the companies that comply with the standards reported no data breaches involving credit card information in the previous two years. Only 38% of non-compliant companies could claim the same. (PCI DSS appears to reduce breaches) However, it is reported that organizations spent over 130 billion dollars on cybersecurity in 2011, and yet, data breaches continue to rise. (Mark)

Is it enough?

In 2009, Heartland Payment Systems suffered a major security incident involving the loss of customer credit card data. The concern was that Heartland did all the right things. They invested in the security and were compliant with PCI DSS and still were the victims of a data breach. Security experts were disturbed because what happened to Heartland weakens the foundation upon which PCI DSS is built. The security measures that PCI DSS requires be put into place could not prevent this attack and organizations feel they cannot justify the cost. One security expert stated "The benefits of complete PCI and the necessity of full compliance are now being widely questioned." (Ogren)

More recently, there were major data breaches at Target and Neiman Marcus, and once again the integrity of the standard comes into question. Target, which was PCI compliant at the time, exposed the credit card data of 40 million people and according to a subject matter expert, "Nothing in the PCI standard would have helped Target detect and block the intrusion before it happened." According to Neiman Marcus's CEO, the company had security measures in place that exceeded PCI requirements and the company was still breached and exposed 1.1 million payment cards.

An analyst with research firm Gartner stated these breaches "highlight weaknesses in PCI and in the security industry". She continued by stating that a major concern with the standard is "Companies are not being assessed for their readiness in dealing with new threats". The director of emerging technologies at the SANS Institute stated that "the breaches point out PCI implementation failures rather than a lack of controls in the standards itself. There's plenty in the standard that should have enabled Target and Neiman Marcus to catch the intrusions on the way in or to find and block the path the intruders took to break into the networks. Doing security right is not trivial. But the problem is not some lack of requirements in PCI DSS or other standards". (Vijayan)

Conclusion

The question remains, are the security requirements enforced by PCI DSS enough to keep an organization secure? Based on widely, public information the answer is no. Ensuring your organization is compliant with the security requirements cannot guarantee that the organization is safe from attack and data breaches. However, implementing the security controls into your organization and having a focused security strategy can certainly reduce the likelihood of a data breach, therefore the intent of what PCI DSS was trying to accomplish did not fail. If we focus on the original goal of PCI DSS, it has been a major success. PCI DSS has reduced risk, raised awareness for data security and enhanced security as a whole. Organizations are paying more attention to and spending more money on system security by being required to be PCI compliant. In addition, customer confidence over the security of personal information has increased. So, while compliance does not guarantee security, the risks have been dramatically reduced. Organizations should take the requirements set forth by this standard and build upon them. As

one subject matter expert stated “PCI should be the “floor” of security and should not be treated as a “ceiling””. (Xia)

References

The history of the PCI DSS standard: A visual timeline. (2013, November 1) *SearchSecurity*, Retrieved on January 24, 2014 from http://searchsecurity.techtarget.com/feature/The-history-of-the-PCI-DSS-standard-A-visual-timeline

Payment Card Industry Data Security Standard. (2013, November) *PCI Security Standards Council*, Retrieved on March 12, 2014 from https://www.pcisecuritystandards.org/security_standards/documents.php

*Xia, Robert Yang. (2011, June 30). Insight to Payment Card Industry Data Security Standards (PCI DSS) Retrieved on March 12, 2014 from http://uwcisa.uwaterloo.ca/Biblio2/Topic/ACC626%20Insight%20to%20PCI%20DSS%20Y%20Xia.pdf

* Payment Card Industry Data Security Standard. (2009, April). *Card Technology Today, 21(4),* 9.

PCI Compliance and Scope Reduction. (2014, February). *Voltage Security*, Retrieved on March 12, 2014 from https://www.voltage.com/wp-content/uploads/Voltage_UC_PCI-Compliance.pdf

*Verizon 2014 PCI Compliance Report. n.d. *Verizon Enterprise Solutions*.

*Kidd, Robert. (2008, November). *Computer Fraud & Security*, *2008(11),* 13-14

Why Comply with PCI Security Standards?. *PCI Security Standards Council*, Retrieved on February 24, 2014 from https://www.pcisecuritystandards.org/security_standards/why_comply.php

*PCI DSS appears to reduce breaches. (2011, May). *Computer Fraud & Security*, *2011(5),* 3, 19

Mark, Chris. (2013, January). In 2013 the only Certainties are Death, Taxes and the PCI DSS. *Transaction World*, Retrieved on February 24, 2014 from http://www.transactionworld.net/articles/2013/january/compliance.html

Ogren, Eric. (2009, February 5). Heartland breach highlights PCI limitations. *SearchSecurity*, Retrieved on January 24, 2014 from http://searchsecurity.techtarget.com/news/1346993/Heartland-breach-highlights-PCI-limitations

Vijayan, Jaikumar. (2014, January 24). After Target, Neiman Marcus breaches, does PCI compliance mean anything?. *ComputerWorld*, Retrieved on February 24, 2014 from http://www.computerworld.com/s/article/9245709/_After_Target_Neiman_Marcus_breaches_does_PCI_compliance_mean_anything_