PCI and Why it is Important

Michael Mozingo

ICTN 6865 Fundamental Network Security 601

East Carolina University

Dr. Phil Lunsford

November 29, 2016

PCI and Why it is Important

Millions of credit and debit card transactions are completed daily. Credit and debit card usage is steadily increasing, and with it, so is the treat of fraud. With the increase of payment card fraud, it is important for the merchants who accept these types of payments to have a common standard in place to provide security in keeping card holder information safe. This is where the Payment Card Industry, Payment Card Industry Security Standards Council (PCI SSC) and the Payment Card Industry Data Security Standards (PCI DSS) come into play.

What Is PCI?

The Payment Card Industry was created and designed as an effort among the major credit card companies to develop security standards that would help protect their customer's data (Clapper & Richmond, 2016). PCI is governed by the PCI SSC which sets standards called the PCI DSS. Webopedia defines PCI SSC as "the governing organization and open forum responsible for the development, management, education, and awareness of PCI Security Standards, including the Data Security Standard (PCI SSC, 2016). Webopedia also defines PCI DSS as "a standard that all organizations, including online retailers, must follow when storing, processing and transmitting their customer's credit card data" (PCI SSC, 2016).

History of PCI

The PCI DSS did not form overnight, instead, it took the efforts of major credit card companies many years in order for it to be fully established. Prior to the formation of the PCI DSS, major credit card companies such as, Visa and MasterCard attempted to develop their own standards in an effort to improve the security of their client's information through credit and debit card transactions (Virtue, 2012). For example, in June of 2001, Visa launched the

Cardholder Information Security Program (CISP) that went through several revisions and updates up until March 2004 (Virtue, 2012). Instead of having multiple standards created by each company, at one point, MasterCard and Visa decided to join together to validate and protect cardholder data (Virtue, 2012). Such attempts by credit card companies were great in that they were attempting to help secure customer information, however, they lacked fundamental elements that created a true standard for merchants. According to Virtue (2012), there were multiple issue with this arrangement including inconsistency and lack of collaboration, so in order to remedy this issue, all the major companies came together to create PCI DSS 1.0.

PCI DSS Version 1.0 was released on December 15, 2004 and became the first time that the five major credit card companies had collaborated to create a unified standard for merchants to follow and adhere to (Staff, 2014). According to Staff (2014), two years later, in September of 2006, version 1.1 of the PCI DSS was released, which included the need for firewalls as a security measure. Along with the release of version 1.1, the credit card companies came together to create the PCI SSC (PCI SECURITY, 2016). As with many early entries, PCI DSS was not a smooth transition. Many of the merchants that were following the standard complained that there were "a lack of consistency in audits and assessment processes by qualified service accessors" (Staff, 2014). Another issue that merchants were having was the fact that many were failing to comply and felt that the PCI SSC needed to lower the bar which led to PCI SSC creating an easier standard method in 2007 that allowed merchants to achieve PCI compliance much easier (Staff, 2014). The current version of PCI DSS, version 3.2, was released on April 29, 2016 (Thomas, 2016).

The Need for PCI

Fraud is a major problem in America with payment-card fraud being one of the biggest. America leads the world in payment-card fraud (Skimming off, 2014). Prior to the formation of the Payment Card Industry and the PCI SSC/DSS, there were no set standard that all the major credit card companies abided by. Without a proper formation of a set of rules and standards, it was difficult to ensure customer information was safe and secure. Not only is the need to keep customer information safe critical, it is also important to educate and help merchants and financial institutes properly implement these standards and ensure they are followed. Without the proper understanding of the guidelines set forth by the PCI SSC and DSS, they can become meaningless and potentially cause issues that otherwise would not have occurred. The official PCI SSC website states that they serve those who deal with payment cards which include merchants, financial institutes, point-of-sales vendors, and hardware and software developers (PCI SECURITY, 2016). Their website also states their two main priorities, which are: "helping merchants and financial institutions understand and implement standards for security policies, technologies and ongoing processes that protect their payment systems from breaches and theft of cardholder data" and "helping vendors understand and implement standards for creating secure payment solutions" (PCI SECURITY, 2016).

PCI Compliant

Merchants that accept credit and debit cards do not have to be PCI compliant, however, those that are show that they have gone through the process and have better capability of keeping their customer's information secure. Becoming PCI complaint is not a simple nor easy task as there are multiple factors and considerations that much be taken into account before they can be labeled complaint.

For a business or company to become and remain PCI DSS compliant, they must follow the 12 major requirements that have been are split into six different principles created and maintained by the PCI DSS. Figure 1 shows the breakdown of the six principles and their corresponding requirements. These requirements were created so that businesses would have a clear understanding of what the credit card companies require in regards to keeping their customer information confidential and secure.

Build and Maintain a Secure Network	Requirement 1
	Requirement 2
Protect Cardholder Data	Requirement 3
	Requirement 4
Maintain a Vulnerability Management Policy	Requirement 5
	Requirement 6
Implement Strong Access Control Measures	Requirement 7
	Requirement 8
	Requirement 9
Regularly Monitor Test Networks	Requirement 10
	Requirement 11
Maintain an Information Security Policy	Requirement 12

Table 1: PCI Requirements and Principle's

PCI DSS has 12 major requirements. These are: "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. 3) Protect stored cardholder data. 4) Encrypt transmission of cardholder data across open, public networks. 5) Use and regularly update anti-virus software or programs. 6) Develop and maintain secure systems and applications. 7) Restrict access to cardholder data by business need-to-know. 8) Assign a unique ID to each person with computer access. 9) Restrict physical access to cardholder data. 10) Track and monitor all access to network resources and cardholder data. 11) Regularly test security systems and processes. 12) Maintain a policy that addresses information security" (Harran & Mckelvey, 2013, p. 120). Knowing these 12 requirements is just the beginning in becoming and maintaining compliant. Not only do merchants have to know the requirement, they have to be able to comply with them.

In order to comply with the first requirement, an implementation of a firewall is not enough. The implementation of a firewall is an important first step in securing the network as it helps protect it from malicious activities such as unauthorized access, viruses, and malware. The reason why simple implementing a firewall is not good enough is because firewalls have to be configured for both inward and outward traffic while also being configured within wireless networks (Basic Requirements, 2016). Another requirement of the company's firewall is that they should also be implemented on every internet connection within the network while also being placed between demilitarized zone (DMZ) and the internal network (Basic Requirements, 2016).

Not using vendor-supplied default passwords is extremely important in eliminating hackers and other cyber criminals from being able to have access to the system. In order to comply with this requirement, merchants must change the default password for these systems

and replace them with a strong password. Systems that are not being used must have their passwords changed along with disabling the account so hackers cannot access those systems. (Basic Requirements, 2016). Establishing strong passwords and disabling old and unused accounts will greatly assist in prevent a data breach.

Cardholder data storage should be kept to an absolute minimum. Any information that is stored should be encrypted and a policy should be put into place that outlines the type of information that is to be stored and for how long it should be stored before being destroyed (Basic Requirements, 2016). The more cardholder data that is stored, the harder it becomes to handle it all and ensure that information is not attained by unauthorized users. Not only should cardholder data be kept to a minimum, whenever cardholder data is being transmitted across open and public networks, it must be encrypted. In order to verify this is being done correctly, merchants must use only trust keys and certificates, only use protocols that support secure versions/configurations, and use appropriate encryption strength (Basic Requirements, 2016). Transferring information through open and public networks is never a good idea as it is easier for hackers to get their hands on the information being transmitted. Any information that contains sensitive customer information, especially those that include cardholder data, must be encrypted at all times.

Firewalls can help in protecting viruses and malware, however, more must be done in order to fully comply with PCI DSS. Malware and viruses can cause major damage as they can be used by criminals to steal sensitive customer information and bring networks completely down. To comply with requirement 5, merchants must ensure all anti-virus software are kept current, perform periodic scans, and generate audit logs that are retained per PCI DSS requirement (Basic Requirements, 2016).

According to Basic Requirements (2016), in order to properly comply with developing and maintaining secure systems and applications, merchants should "identify and documents a list of all the software assets that are used for developing application as well as develop a system that monitors each item for possible vulnerabilities on a regular basis". As the merchant grows and new technology is introduced, it was natural that they may develop their own application to better suit their needs, however, they must be able to ensure they systems stay secure. When creating new applications, the developers can use the PCI DSS as a guide, therefore, increasing the likelihood that it complies with the standards (Bonner, O'Raw, & Curran, 2011)

Restricting access to cardholder data by business need-to-know is extremely critical. Only those that need to know the information should be allowed access to it, otherwise, the information could easily get into the wrong hands and be used for nefarious purposes. To better comply with this requirement, it is important for merchants to clearly define roles that have access needs and the extent of these roles (Basic Requirements, 2016).

Assigning each individual with computer access a unique ID helps in potentially tracing those that are responsible for data leaks. Not only can it help in tracing back to the person who committed the leak, it can also prevent people from doing it in the first place as it holds them accountable for anything that happens under their ID.

According to Basic Requirement (2016), if physical access to devices is not restricted, it can make it easier for those with malicious intent to get their hands on the data. Once they have access to the data, they can use it for a number a things along with making a physical copy it so that it can be taken with them. In order to comply with this requirements, access to data centers, server rooms, and other facilities that hold confidential data should have a strong physical security presence (Basic Requirements, 2016). Many companies utilize security cameras,

security guards, and badge readers to limit access to only those that have a business need-to-know.

Having a track record of all access to network resources and cardholder data is a must. If there is a breach and customer information so happens to be compromised, it is important to have a track of the activities that happened on the network. Having the record will make it much easier for the company and for law enforcement to track down those responsible.

One way merchants can verify they are being complaint with the PCI DSS is to regularly test their security systems and processes. Regularly testing the security system will confirm the required level of network protection, along with ensuring that no vulnerabilities are left out during routine operations and information security procedures (Basic Requirements, 2016). Merchants can establish a time table as to when they would like to test their systems. It may be tedious at first, however, the more times it is done, the better their overall security will become.

Basic Requirements (2016), states "a well-developed, comprehensive information security policy serves as a basis for PCI compliance of an organization". The policy should be made available for every employee in the organization and clearly states what the company is trying to achieve. In order to ensure it is effect, the policy should be regularly updated and communicated within the comply (Basic Requirements, 2016).

Merchant Levels

When it comes to PCI, there are four different merchant levels that companies fall into. Merchant level 1 is any merchant that processes more than 6,000,000 transactions per year, has had a data breach that consequently resulted in account data being stolen, and any merchant that's has been identified by any card association as Level 1 (Rouse, 2015). Level 2 merchants are any that process between 1,000,000 and 6,000,000 transactions (Rouse, 2015). Level 3

merchants process between 20,000 and 1,000,000 while Level 4 process less than 20,000 transactions annually (Rouse, 2015).

These merchant levels also have different criteria associated with them. Level 1 merchants are required to have someone onsite who handles audits, however, the other levels only need to fill out the self-assessment questionnaire and must sign up for a quarterly scan (Braintree, 2008). According to Braintree (2008), these scans are to check for any vulnerability on IP address that are outward-facing and can cost $150-$2500 per IP address yearly.

Future of PCI

PCI has come a long way since its creation in 2004. An increase of mobile usage over the last 12 years has increased paperless transactions and increased challenges and hurdles for compliance with the PCI DSS (Kitten, 2013). Jeremy King, PCI Security Standards Council European director, stated the biggest challenge for the council going forward is the increase in technology (Kitten, 2013). King also stated the council has seen an enormous increase in mobile commerce rollouts, however, the card security has been an afterthought and that they must continue to work with experts in order to produce security solutions (Kitten, 2013). With the release of PCI DSS 3.2, PCI SSC has taken into account the increase in security threats. To help eliminate breaches in the future, the new version includes using two-factor authentication and penetration test (The future, 2016).

Conclusion

The Payment Card Industry along with the Security Standards Council and the Data Security Standards has proven to be an important part of keeping credit card and debit card transactions much more secure then before it was created. With new versions being released that includes improvements and new and/or revised standards, it will continue to be a major factor in

the foreseeable future. The standards that are currently being utilized took many years to develop and much collaboration from the major credit card companies to materialize, however, the payoff has been worth it. Businesses now have a clear understanding of what it takes to become PCI compliant and the associated cost and factors that go along with compliance. As technology changes, so will the need for PCI to adapt to adapt to the changes. PCI will need to continue to grow and be able to keep up with the times in order to maintain its goals in keeping cardholder data secure.

References

*Harran, M., & Mckelvey, N. (2013). PCI compliance - no excuses, please. *International Journal of Information and Network Security, 2*(2), 118. doi:http://dx.doi.org.jproxy.lib.ecu.edu/10.11591/ijins.v2i2.1940

Virtue, T. M. (ed) (2012) Front Matter, in Payment Card Industry Data Security Standard Handbook, John Wiley & Sons, Inc., Hoboken, NJ, USA. doi: 10.1002/9781119197218.fmatter

Staff, 3DSI. (2014, January 23). The History of PCI Compliance. Retrieved October 11, 2016, from http://www.3dsi.com/blog/history-of-pci-compliance

Thomas, T. (2016, May 03). An In-Depth Look at the PCI 3.2 SAQs. Retrieved September 25, 2016, from https://www.pcicomplianceguide.org/an-in-depth-look-at-the-pci-3-2-saqs/

*Clapper, D., & Richmond, W. (2016). SMALL BUSINESS COMPLIANCE WITH PCI DSS.*Journal of Management Information and Decision Sciences*, *19*(1), 54-67. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/1804900242?accountid=10639

Skimming off the top. (2014, January 15). Retrieved September 29, 2016, from http://www.economist.com/news/finance-and-economics/21596547-why-america-has-such-high-rate-payment-card-fraud-skimming-top

Protecting the payments ecosystem. (2016). Retrieved September 29, 2016, from https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/site-data-protection-PCI.html

PCI SECURITY. (2016). Retrieved November 01, 2016, from https://www.pcisecuritystandards.org/pci_security/

Rouse, M. (2015, June). PCI DSS merchant levels. Retrieved November 05, 2016, from http://searchsecurity.techtarget.com/definition/PCI-DSS-merchant-levels

Braintree. (2008, June 24). What does it cost to become PCI Compliant? Retrieved October 18, 2016, from https://www.braintreepayments.com/blog/what-does-it-cost-to-become-pci-compliant/

PCI SSC. 2016 in *Webopedia.com.* Retrieved November 2nd, 2016, from http://www.webopedia.com/TERM/P/PCI_SSC.html

Kitten, T. (2013, March 16). The Future of PCI. Retrieved September 17, 2016, from http://www.bankinfosecurity.com/interviews/pcijeremy-king-i-1926

Basic Requirements of PCI DSS (2016). Retrieved November 02, 2016, from http://pcidsscompliance.net/

*Bonner, E., O'Raw, J., & Curran, K. (2011). Implementing the payment card industry (PCI) data security standard (DSS). *Telkomnika, 9*(2), 365-376. Retrieved from http://search.proquest.com.jproxy.lib.ecu.edu/docview/899198241?accountid=10639

The future of PCI. (2016, July 25). Retrieved November 15, 2016, from http://www.sfgnetwork.com/blog/payment-processing/the-future-of-pci/