PCI/DSS – Payment Card Industry/ Data Security Standard – Are the controls relevant?

Category: Security Risk Management Plans, Policies, Standards, Practices

Lokesh Pidawekar

Foundation of Information Assurance – IA 5010

December 1, 2013

Contents

Introduction

Information Security is practice of balancing risk and countermeasures. PCIDSS is one of the de facto standards to implement data security controls for management of cardholder data to reduce credit card fraud. The scope of PCIDSS is not limited to merchants, processors, acquirers, issues, and service providers but also it covers all those entities that are involved in storage, processing and transmitting cardholder data. PCI DSS provides technical as well as operational controls to protect cardholder data. It is essential to understand whether all these controls are relevant to security. While implementing a standard, it should address basic security requirements of an organization. Similarly, PCIDSS must also address the fundamental information security requirements with more focus towards credit card data. (PCI Security Standards Council)

History

There were individual standards available from Visa, Master card, American Express, Discover Financial Services and JCB International designed to ensure an additional level of protection of consumer financial details at the merchants themselves, typically by policy restrictions on the storage, processing, and transmission of cardholder data. It was required to bring all the best practices under one hood; hence an open global forum PCI Security Standards Council was formed in 2006. The council is responsible for the development, management, education and awareness of PCI security standard including PCI Security Standards, including the Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) requirements.

Requirements

PCIDSS describes 12 requirements and these requirements are organized into 6 logically related groups called as “control objectives” as shown in Table 1 below.

S No	Requirement	Control Objectives
1	Build and maintain a secure network	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
2	Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
3	Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or program 6. Develop and maintain secure systems and applications
4	Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer accessed 9. Restrict physical access to cardholder data
5	Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
6	Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Source: Data from PCI Data Security Standard – High Level Overview - PCIDSS V 2.0, table 1.

QSA

Qualified Security Assessor (QSA) companies are organizations that have been qualified by the Council to have their employees assess compliance to the PCI DSS standard. Qualified Security Assessors are employees of these organizations who have been certified by the Council to validate an entity's adherence to the PCI DSS. (PCI Security Standards)

Requirements at glance

Compliance requirements include several key features: a secure network, protection of cardholder data, vulnerability mitigation, access control measures, monitoring and penetration testing, and finally, adherence to a strict and well-defined security policy.

Build and Maintain a Secure Network and Systems

1. Install and maintain a firewall configuration to protect cardholder data**:**

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

It is not enough to just install a firewall, proper tuning of the firewall is more important. The requirement does not state clearly on configuration of firewall. Just installing and configuring a basic firewall is not enough, even if it meets the PCI requirements, the most important part is to implement it correctly.

2. Do not use vendor-supplied defaults for system passwords and other security parameters:

Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

Time and time again, network engineers configure routers with username/password combinations like cisco:cisco. The same can be said for practically anything that comes supplied with defaults, be it passwords or configurations. There exist plenty of black-hat scanners that search for fresh installations of Wordpress, phpMyAdmin, and various other easy-access web applications and software for that brief period just after installation when default passwords have not yet been changed. Just this momentary exposure can wreak havoc on an administrator's setup, or even the whole network.

This requirement should include any defaults, including configuration, such as ports and version replies. There exists no reason to leave SSH port 22 open to the world unless you are running a shell server, in which case that shell server should never be even the slightest bit connected to cardholder data to begin with. There also exists no reason to leave the full version reply in the Apache web server reply headers. In fact, wherever possible, the most minimal information should be supplied, or none at all if it is not critically necessary. The less entry points made available to any attacker, the more secure systems will be. (Robert Abela, November 2013)

Protect Cardholder Data

3. Protect stored cardholder data:

Protection methods such as encryption, truncation, masking, and hashing are critical components of protecting cardholder data. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should also be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not stor-

ing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.

This requirement is essential, but often gets ignored or mostly overlooked once the first requirement is completed. For example: With PCI compliance, it is required that CVV numbers not be stored whatsoever, and that cardholder data such as the card number, ZIP code, and cardholder name all be stored in an encrypted format. All too often, neither of these two requirements is completed. (Robert Abela, November 2013)

4. Encrypt transmission of cardholder data across open, public networks:

Sensitive information must be encrypted during transmission over networks so that they are not easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

One side that sometimes gets overlooked is the communication from servers to payment processor, and all steps in between. Most payment processors as accept only secured communication methods. However, if there is a middle step in the process - such as a shopping cart mirror server hosted in a different data center which transmits, by non-encrypted communication, the cardholder data to central database server before making it to the payment processor. If this in-between traffic happens over public networks and then it must also be strongly encrypted, just like communication between servers and clients. (Robert Abela, November 2013)

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software:

Malicious software, commonly referred to as "malware"—including viruses, worms, and Trojans enters the network during many business approved activities including employee e-mail and use

of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats. Additional anti-malware solutions may be considered as a supplement to the anti-virus software; however, such additional solutions do not replace the need for anti-virus software to be in place.

6. Develop and maintain secure systems and applications:

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor provided security patches, which must be installed by the entities that manage the systems. All systems must have all appropriate software patches to protect against the exploitation and compromise of cardholder data by malicious individuals and malicious software.

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need-to-know:

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. "Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.

In any and every possible area, Least Privilege should be applied and strictly enforced to minimalize the damage.

8. Assign a unique ID to each person with computer access:

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for their actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users and processes. The effectiveness of a password is largely determined by the design and implementa-

tion of the authentication system—particularly, how frequently password attempts can be made by an attacker, and the security methods to protect user passwords at the point of entry, during transmission, and while in storage.

Also, as mentioned in the prior requirement, #7, this requirement does not exclusively apply to actual personnel, but services as well. Along with the principle of Least Privilege, services should possess unique access exclusive to each service unless the sharing of access is absolutely necessary (which should be avoided via protected communication pathways wherever possible). If a user can cause damage by sharing his or her credentials, so too can a service exploited by a hacker when its access is shared among other services.

9. Restrict physical access to cardholder data:

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, "onsite personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A "visitor" refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. "Media" refers to all paper and electronic media containing cardholder data.

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data:

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

11. Regularly test security systems and processes:

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

This requirement proves to create a rather tricky problem: A vulnerability scan is only as effective as the list of vulnerabilities it knows to scan for. Indeed, it is impossible to truly account for all unknowns, so the best a vulnerability scan can do is check for the conceivable known methods of intrusion. This is not just limited to checking firewalls, ensuring anti-virus scanners are up-to-date, or verifying traffic is encrypted.

Maintain an Information Security Policy

12. Maintain a policy that addresses information security:

A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, "personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are "resident" on the entity's site or otherwise have access to the cardholder data environment.

Relevance of Controls

There are more than 280 controls specified in PCI standard and the requirements seem to be technically prescriptive; still we find out that some of the requirements are too vague to implement.

Lack of Awareness

Lack of education and awareness about payment security and, poor implementation of the PCI standard leads to many of the security breaches happening today. It does not matter how good technological security controls are applied, people will always remain the weakest link. The PCI-DSS standard doesn't provide any criteria to measure the awareness of people against security threats such as social engineering or spear phishing. PCIDSS mainly focuses on prescribing technical controls such as firewall, intrusion detection and prevention, patching, passwords with exception of Requirement 12 which is, "Maintain a policy that addresses security for all personnel". If we look at some of the recent breaches at RSA, Epsilon etc., we will notice that it is important to understand human behavior and security. In addition to existence of security awareness program, PCI should also include methodology to evaluate its effectiveness. There should be conscious effort to include human factor in drafting the standard. (David Barton, May 2012)

Lack of control over third party tools

As of now there is no control to maintain which controls are maintained by entity and which controls are managed by service providers. With emergence of cloud it's important to have controls with respect to third party providers because security is a shared responsibility. Service providers should not get away from this and must acknowledge responsibility for maintaining required PCI DSS controls.

Application Security

PCIDSS prescribes effective network controls in term of segregation of network, implementation of firewall, end to end encryption but it does not specify application security controls more rigorously. In present situation, application level threats are evolving daily. OWASP (Open Web Application Security Project) provides a list of top 10 every 4 years. The standard should include new controls for checking new vulnerabilities and align with common vulnerabilities listed by OWASP, SANS etc.

In another scenario, if someone installs a new POS device or application incorrectly, even if it's compliant with the Payment Application Data Security Standard, it will still be non-compliant.

And as infrastructure goes out of compliance, so does control over cardholder data. (PCIDSS V 3.0 Change Highlights)

There are few controls which are technically prescriptive but the implementation seems vague. Consider an example of Web application firewall; this requirement was not available in earlier editions. PCIDSS V2.0 included a requirement for installing a web-application firewall in front of public-facing web application but it does not specify details. The vendors just included layered signatures on top of packet filtering firewall and marketed it as application firewall. Also, the standard does not specify how data can be collected and processed out of the web application firewall. There is no mention of log review or how the firewall is effective in blocking the illegitimate traffic. So, like other controls SSC must pay attention in describing the requirement of control and there should be defined means to check the effectiveness of control.

Code Review V/S Web Application Firewall

Public-facing web applications are primary targets for attackers, and poorly coded web applications provide an easy path for attackers to gain access to sensitive data and systems. The requirement for reviewing applications or installing web-application firewalls is intended to reduce the number of compromises on public-facing web applications due to poor coding or application management practices. The standard requires either of these. As best practice, program code should be made as clean and secure as possible and Web Application Firewall (WAF) should be implemented so that if vulnerability is present in code, WAF can take care of that. Also, WAF can be configured to block the attack for latest vulnerabilities till the code is fixed. These are complementary technologies and work best in tandem but PCI sets them to compete.

Malware control

Although Requirement 5 deals with deployment of antivirus programs, there is a need to align this in systems which are not commonly affected by malware such as Mainframes and unix based operating systems. Since Banks and other financial firms still use Mainframes and other legacy system for processing transaction, Requirement 5 should increase the scope to other devices as well. (PCIDSS V 3.0 Change Highlights)

Virtualization compliance

Virtualization is driving factor in Cloud computing. When it comes to virtualization controls, PCI DSS V2.0 does not provide specific requirement but a vague statement. It treats both physical and virtual components as system components where system components are defined as any network component, server, or application that is included in or connected to the cardholder data environment. Virtualization components are virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors. As industry is moving into cloud, it is important to define controls specific to cloud. Taking this into consideration PCI SSC has released a cloud computing guideline in February 2013. (PCIDSS V 2.0)

Mobile security

Mobile is one of the emerging markets for e – commerce. With emergence of mobile wallet and payment applications, it is important to address compliance of this unique platform. The PCI DSS standard does not cover specific security requirements for mobile payments. There are no controls for protecting mobile payment solutions and integrating mobile devices in organization. The Council released a best practices guide for mobile security more than a year ago, but it would be more beneficial to release additional guidance pertaining to mobile data security

Default passwords and default configuration

PCI DSS strongly recommends changing vendor provided default configuration and passwords of devices. This requirement is difficult to implement in virtualization environment because a

virtual machine can easily be duplicated and configured with vendor supplied default settings. It is a challenging process to implement same checking control for virtual systems as that of physical systems, because it might require scanning within the virtual infrastructure or may the machine can be provisioned for very short instance. (PCIDSS V 3.0 Change Highlights)

Does compliance mean security?

Most of the time people mistake compliance with security. Compliance to any standard does not guarantee security otherwise what are the reasons of data breached in PCI compliant companies. An organization must perform risk management according to the risk appetite, just getting certification or accreditation cannot guarantee security. Moreover security should be a continuous process and should not be restricted to any one framework. For PCIDSS, most of the requirements are assessed only at the time of audit but there is no way to monitor the compliance on continuous basis. Unfortunately, compliance level of requirement can be true at that point of time but turns non-compliant next day; so an organization seems to be compliant on paper, but non-compliant on the next day.

There are multiple instances where organizations reported breaches when it was certified as PCI compliant.

"*N.J.-based Heartland last Jan. 20, 2009 disclosed that intruders had broken into its systems and stolen data on what was later revealed to be a staggering 130 million credit and debit cards. That number easily eclipsed the94 million cards that were compromised in the massive breach disclosed by TJX Companies Inc. in 2007.However, it wasn't just the scope of the Heartland breach that made it remarkable, but also the company's insistence that it was certified as fully compliant with the requirements of the Payment Card Industry Data Security Standard (PCI DSS) when it was compromised.***"** (Jaikumar, Jan 2010)

Compliance just addresses the requirements specified in document whereas security addresses the overall risk of an organization. New products like DLP solutions, cloud are not in purview so

management will not care for putting these controls, too much money will be spent on old stuff. We are doing risk assessment and den putting controls purchasing solutions. We are just purchasing age old solutions

Compensating Controls

One of the problems with PCIDSS is, compensating controls are deceptive. Compensating controls is a work around for those controls which cannot be fulfilled due to legitimate reason. The QSA is responsible to validate the compensating control. So compensating controls can make it possible to bypass certain requirements by providing additional controls in certain circumstance however lack of unification and stringent constraints imposed by SSC in selection and use of these controls may act as barrier.

Consequences of being non-compliant

Penalties and dispute

The PCI SSC has no registration entity to handle any sort of listing or inspection of compliant members, nor does it explicitly restrict merchants from participation for non-compliance (unless a merchant finds itself the victim of compromise and, thus, under the watchful eye, and punishment, of the PCI DSS). Because of this, merchants are almost exclusively responsible for not only their own ability to adhere to PCI standards, but their own inspection and certification of compliance as well.

PCI SSC does not validate or enforce any organization's compliance with its PCI Security Standards, nor does it impose penalties for non-compliance. These areas are governed by the payment brands and their partners. When a breach occurs, the card companies collect their fines from the third-party banks that process the card transactions, instead of the merchants, who have more in-

centive to fight the fines. A third-party bank then simply collects the money from the customer's account or sues them for uncollected balances, using the indemnification clauses in their contracts to justify it. The card companies collect their fines with no hassle and merchants, in the meantime, are left fighting to dispute the fines and get their money back from the card companies. (Kim Zetter, March 2013)

There are fines levies by banks and credit card providers on account of non-compliance. In addition penalties for non-compliance, organizations can be made to pay fine if there is a situation of credit card data theft or breach. Even if the company was PCI compliant, data breach cost around $50-$90 fine per cardholder data compromised and suspension of credit card acceptance by a merchant's credit card account provider. This is a PCI contract dispute. This particular dispute arises, in part, because the payment processors deduct their 'fines' from the revenue they collect for the merchant. The merchant has to sue the payment processor to get his money back rather than the processor having to sue the merchant to collect the fine. There is a presumption in favor of the payment processor built into the system. (Ericka, March 2013)

The Genesco case

The merchant, Genesco, Inc., experienced a year-long data breach in which hackers stole customers' payment card account data as Genesco transmitted it, unencrypted, to the acquiring banks, Wells Fargo Bank and Fifth Third Financial Corporation, for payment authorization. Upon identifying the breach and a corresponding increase in payment card fraud, Visa imposed more than $13 million in contract-based liability assessments on Wells Fargo and Fifth Third. The banks then recovered the money from Genesco. Genesco contended that Visa had no basis to impose liability assessments based on alleged violations of the PCI DSS, as the Standard—according to Genesco—does not require encryption of data being transmitted to acquiring banks. Genesco also asserted about not finding crude forensic evidence that hackers were able to steal payment card information stored within Genesco's computer system, where encryption is required. Genesco further contended that Visa calculated the assessments based on each cardholder account that Genesco processed during the year-long the data breach. (Ericka, March 2013)

Genesco filed a lawsuit to challenge Visa's practices for enforcing a major non-compliance penalty. It's the first known case to challenge card companies over the self-regulated PCI security standards. According to Torsten George, vice president of worldwide marketing, products, and support for Agiliance, one of the best outcomes of the Genesco case would be if it would spur the creation of an independent governing body that would assess PCI compliance and the penalties associated with it. Though the PCI Data Security Standards Council does a lot to maintain the integrity of the standard itself and the certification of Qualified Security Assessors, the brands and processors are left to decide the fate of non-compliant organizations in their own way. (Ericka, March 2013)

Penalties as method of compliance

There is one more aspect of penalties; most of the small companies are ready to pay fines instead of investing in security. It is approximately an average $10 to $100 per month per non-compliance merchant. While the penalty model was created to bring more merchants under the radar, but since the cost of compliance is more than penalties, this creates negative incentive for processors to push them for compliance.

Conclusion

In my opinion, PCI DSS controls are subjective and complex but we still need to focus on the factors it prevents, detects and/or corrects. There are issues in implementation of controls, since most of the controls are subjective in nature. All of the PCI DSS requirements are there for a reason and provide cover for a significant number of the other requirements. The reason for many data breaches can be narrowed down to lack of fundamental security controls. PCI DSS is evolving and we can expect more clarity and definiteness in coming versions of Standard. We should use DSS to make the environment more secure by consistently and rationally measuring the strength of a control and attack. People should have informed opinion about PCI in terms of what it's doing to them and what it's doing for them. It's good for those people who were not doing security at all, now they are forced to do security.

Despite the complexity and bureaucracy it entails: PCI-DSS really, seriously, puts security into the minds of (at least some of) senior management. There are annual audits. So again, anyone working with credit cards is constantly thinking about not doing stupid stuff because you could literally go out of business if you don't comply. The main area of concern is that even though the new standards reference risks management strategies that must be met, the standard doesn't enforce companies to adopt any of those strategies. In particular, the standard doesn't address the fact that risk assessments need to be done by an industry-certified professional and are only performed on an annual basis. Also, PCI DSS 3.0 does not include any changes surrounding mobile security.

One of the largest problems with PCI compliance is the absolute lack of real, technical requirements. For example, the very first requirement is to have a firewall designed to protect cardholder data. That sounds good on paper, but nothing actually says how or to what degree this firewall must protect data.

Hence, PCI compliance is a good idea in abstract; however it should be viewed only as a starting point, given its rather minimalistic and generic approach to meeting compliance requirements.

REFERECES LIST

1. PCI Security Standards Council. *Payment Card Industry (PCI) Data Security Standard Requirement and Security Assessment Procedures*, Version 3.0. November 2013

2. PCI Security Standards Council. *Payment Card Industry (PCI) Data Security Standard and Payment Application Data Security Standard*, Version 3.0 Change Highlights. August 2013

3. PCI Security Standards Council. *About the PCI Security Standards Council*. https://www.pcisecuritystandards.org/organization_info/index.php. (accessed on October 19, 2013)

4. Approved Companies and Providers. https://www.pcisecuritystandards.org/approved_companies_ providers/index.php (accessed on October 19, 2013)

5. Jaikumar Vijayan. *Heartland Breach Shows Why Compliance Is Not Enough*. Jan 6, 2010.

http://www.pcworld.com/article/186036/heartland_data_breach.html (accessed on October 19, 2013)

6. Ericka Chickowski. *Genesco Lawsuit Could Shake PCI Compliance Regime To Its Core*.

March 21, 2013. http://www.darkreading.com/compliance/genesco-lawsuit-could-shake-pci-complian/240151339 (accessed on October 19, 2013)

7. Kim Zetter. *Retailer Sues Visa Over $13 Million 'Fine' for Being Hacked*. March 12, 2013. http://www.wired.com/threatlevel/2013/03/genesco-sues-visa/ (accessed on October 19, 2013)

8. David Barton. *What Good is PCI-DSS*. May 02, 2012.

http://www.infosecisland.com/blogview/21192-What-Good-is-PCI-DSS.html (accessed on October 19, 2013)

9. Robert Abela. *PCI Compliance - The Good, The Bad, and The Insecure - Part 2*. October 24, 2013. https://www.mavitunasecurity.com/blog/definitive-pci-dss-compliance-guide-web-application-security/ (accessed on November 17, 2013)