


*PCI Data Security Standard:
The Risk Mitigation Challenges of the
“12 Commandments”*

Craig Norris
Regional Engagement Manager
Accudata Systems, Inc.

October 2007



Table of Contents

PCI Data Security Standard: The Risk Mitigation Challenges of the “12 Commandments”	3
Abstract	3
Where are Organizations Failing?	3
The Slaughterhouse 5: Why are these Problem Areas?	4
Protecting Stored Data	4
Regularly Test Security Systems and Processes	5
About the Author	9
About Accudata Systems, Inc.	9
Footnotes	9

PCI Data Security Standard: The Risk Mitigation Challenges of the “12 Commandments”

By Craig Norris, Regional Engagement Manger, Accudata Systems, Inc.

Abstract

It is well known for many organizations dealing with credit card services that the major credit card companies have collectively mandated that all members, merchants, and service providers storing, processing, or transmitting cardholder data must adhere to the Payment Card Industry’s (PCI) “12 Commandments” or risk possible fines and even the termination of credit card processing privileges. In addition, by September 30, 2007, all level 2 organizations handling cardholder data will have to be compliant with these standards. Unfortunately, the path to becoming PCI compliant can be very demanding due to the amount of money, time, and effort required. This article will review a few of the more challenging PCI requirements and provide some tips that you can use to help your organization achieve compliance.

There is no question that the constant publicity surrounding data breaches of consumer credit card and financial information is making many merchants weak in the knees and it is negatively affecting their profits. For instance, in a study released by Javelin Strategy & Research, 78% of consumers say they would stop shopping at a store that had experienced a data compromise. In addition, the Federal Trade Commission reported that there were 670,000 consumer cases of fraud and identity theft in 2006 (\$1.2 billion in losses) and credit card fraud was the most common form of identity theft making up 25% of the complaints. Because of this, many online shoppers do not want to disclose their credit card information and are refusing to make online purchases. These statistics alone make implementing the PCI Data Security Standard (DSS) program a must for organizations. The PCI DSS program can also help educate the industry about the importance of security while disciplining organizations that damage the whole industry with careless security efforts that can lead to the loss of cardholder information.

PCI Cases – Fact not Fiction:

- Jan. 17, 2007 – TJX Companies Inc. disclosed that they had experienced an unauthorized intrusion into the electronic credit/debit card processing system. Potential breaches are reaching over 45,700,000 credit/debit card account numbers and over 455,000 merchandise return records.
- Jan. 12, 2007 – MoneyGram announced that one of their company servers was illegally accessed earlier this year. The server held information on about 79,000 bill payment customers, including names, addresses, phone numbers, and in some cases, bank account numbers.
- Feb. 9, 2006 – An estimated 200,000 debit card accounts were disclosed by retail merchants, such as OfficeMax and others. These accounts were related to bank and credit union acquirers nationwide such as CitiBank and Wells Fargo.

Privacy Rights Clearinghouse

Where are Organizations Failing?

So where are many organizations struggling with PCI today? All of the requirements seem to be fairly well defined unlike the Sarbanes-Oxley Act, which does not provide any specific direction on how to secure information assets and has been open to varying interpretation by companies and audit firms. Nevertheless, organizations still find it difficult to become PCI compliant. In an

interesting study conducted by VeriSign, Inc., they found that organizations were most likely to be noncompliant with PCI Requirement 3 and that 79 % of the failed assessments did not meet the requirement to protect stored data. According to VeriSign, the top five PCI assessment failings were:

REQUIREMENT 3	Protect stored data	79%
REQUIREMENT 11	Regularly test security systems and processes	74%
REQUIREMENT 8	Assign a unique ID to each person with computer access	71%
REQUIREMENT 10	Track and monitor all access to network resources and cardholder data	71%
REQUIREMENT 1	Install and maintain a firewall configuration to protect data	66%

Top 5 PCI Assessment Failings

The Slaughterhouse 5: Why are these Problem Areas?

Regardless of the fact that PCI DSS is definitely comprehensive, the list of requirements allows for 12 potential points of failure. Not passing one requirement will cause an organization to not become compliant at all. Additionally, even with the PCI standard providing specific requirements, they can allow for different interpretations based on the organization. Let's review the aforementioned PCI requirement failures, analyze why these might cause trouble for some organizations, and discuss what measures can be taken to resolve the dilemma.

Protecting Stored Data

From the very instant that a merchant receives a customer's credit card information, all of the credit card data must be encrypted! In a National Federation of Independent Business/Visa survey that was presented at Visa's March 2007 conference, small business owners said that they believe they are doing a good job of securing customer data, despite the fact that this is frequently not true. Among the respondents that said they retained their customer's data, more than 25% keep customer records in unsecured files and 36% of those accepted credit card numbers at their stores. One of the biggest problems with this requirement is that merchants must accurately know where credit card data flows from its inception, where it traverses the network and resides, and what its "state" is along the way. As an example, you should identify and examine all desktops, laptops, servers, and databases that handle any type of cardholder information. This includes all of the database files and SQL tables that contain credit card numbers and all of the applications that create or access credit card numbers. No matter what type of system touches the credit card information, it must be protected by encryption.

Tip

Start identifying all of the systems that touch cardholder data because these systems will be included in the scope of your eventual PCI DSS compliance validation. It is also key that you understand the compartmentalization of the cardholder systems and how they are using firewalls and network filter controls since this may dictate if nearby systems are

also within the scope of your PCI DSS compliance validation. You may be surprised to find out that the total number of systems retaining cardholder data (including data warehouses, development servers, middleware and backup systems) is quite large. Document the flow of credit card data throughout your organization and business functions (e.g., the marketing department may need customer data but does not need the associated credit card information). Understand where data goes from the point of acquisition (even from customers or 3rd parties) to the point where the data is disposed of or leaves your network. You should also be sure that you identify all of the computers and networks that connect to your organization's infrastructure and applications. These can include network connections from business units, vendors, partners and the systems of remote employees. All credit card data in motion should be encrypted using methods such as SSH, VPN, or SSL/TLS for encryption.

If you are not confident of your IT department's ability to accurately identify sensitive information, there are very good Data Loss Prevention tools that can assist in this effort. These tools are designed to sift through all of your information across the enterprise and accurately report on which systems house this type of information, where it is on the system, and who has access to the information. Once you have identified the information, review your access controls to enforce "need to know." Also see if it is possible to minimize how many and which systems have this sensitive information.

Regularly Test Security Systems and Processes

Many organizations perform little or no testing on the adequacy of the security controls governing their network and Internet facing web site applications on a regular basis. Failure to periodically run internal and external network scans to identify weaknesses can prove costly by leaving back doors open to hackers and malicious code. Organizations may be protected at a given moment, but new vulnerabilities appear daily which is why networks should be consistently patched and hardened. According to the National Vulnerability Database provided by the Department of Homeland Security's National Cyber Security Division, on average 19 new vulnerabilities are posted to the Internet every day.

One good example of the need for the regular testing of systems and processes is the recent incident with TJX. The TJX breach was due to an insecure wireless network. The Wall Street Journal reported that investigators believe that the hacker was able to use a laptop and a telescope-shaped antenna to penetrate the WLAN network due to the older security technology that was being used. The \$17.4-billion retailer's wireless network had less security than many people have on their home networks. For 18 months TJX had no knowledge they had been compromised, and this allowed the hackers to download at least 45.7 million credit- and debit-card numbers.

Tip

When it comes to scanning your information systems for vulnerabilities, make certain to use tools and techniques that expose vulnerabilities in devices on wired or wireless networks. There are an enormous number of security risks linked to wireless protocols, weak encryption methods, and the lack of security awareness that exists at the user level. Cracking methods have become much more advanced with open source tools that can be found on the web at no charge.

A substantial number of successful attacks are carried out against systems that were not patched with the latest security updates. In addition to a systematic patching process, the greatest protection against network and application security threats is the consistent use of vulnerability scanners that can see all of the applications and devices on your network,

identify vulnerabilities, and supply remediation information. Nevertheless, scanning your network for vulnerabilities will not reveal everything and may only uncover issues that might have previously occurred instead of what a real, attack-like penetration testing provides. In order to be aware of its readiness, it is imperative (and required by PCI) that you perform an annual penetration test on your information systems to measure how well they can endure an attack. This type of test actually exploits vulnerabilities to better quantify the true risk of any particular finding. According to a report found in The Retail Data Security 2005 Benchmark Study, only 51% of retailers perform network penetration testing. A frightening 14% of the survey respondents indicated that they had suffered a customer data security breach. Vulnerability scanning provides a look into known weaknesses but does not address the elements of a successful intrusion. Your testing should include a deeper dive that will bring to light the real threats to your organization's assets.

Furthermore, when it comes to testing processes, all changes that could affect ingress and egress filter rules should go through a formal process before changes are made to firewalls, routers, VPN, and WLAN devices. These changes should be reviewed carefully for proper justification, and management must be made aware of any known new security risks. Information systems environments will always have to change in order to help the business obtain its objectives; therefore, all changes must continually be reviewed and fully documented.

Assign a Unique ID to Each Person with Computer Access

A critical concern of PCI compliance is traceability and accountability of who did what and when. Even though organizations realize that the main techniques used to address this requirement are user and password management, both of these techniques are difficult to implement because you need to incorporate tools to automate these tasks or you must assign technical staff to handle them. Large networks can have heterogeneous environments with many points of entry (e.g., firewalls, VPN access) that make it difficult to track user accounts and behavior on information systems without the proper infrastructure. These same organizations may not be monitoring domain password policies correctly for all changes and this could impact compliance with this requirement.

Tip

Organizations must be able to identify and log all user and administrative access to information systems and the applications containing credit card information. Organizations must create a unique ID for every individual that will have computer access and possess a documented policy that is signed by all employees, pointing out that all ID's and credentials are to be used only by the people to whom they are specified. Organizations need to be capable of verifying who is attempting access to an asset, control what they are permitted to see or modify, and do so based on their organization role.

Management must make sure they enforce a policy for aging passwords and that aging passwords can be confirmed. As an example, if a company has a policy that states all passwords will be changed every 45 days, they must be able to demonstrate that this actually occurs. Additionally, organizations have to be able to show that there is a repeatable process in place for providing passwords for new employee hires and removing passwords when an employee no longer works for the organization.

PCI is also requiring two-factor authentication to identify users seeking to access resources remotely whether they are employees, administrators, or 3rd parties. While

authenticating users who log onto the network by account name and password only is typically the easiest and least expensive method of authentication, organizations are realizing the weaknesses of this method. Passwords can be guessed or cracked using dictionary attacks or users can be tricked into disclosing their passwords to other people. One way to stop social engineers and reduce additional risks associated with passwords is to apply two-factor authentication. If users are obligated to type in a password and provide additional information such as a PIN from a card or token, then a hacker would not be able to get into the network with a password alone. Two-factor authentication can be established by using the combination of something a user knows (password), something a user possesses (ATM card), or with something the user is (fingerprint).

Finally, it is crucial that organizations use an enterprise-wide authentication framework that will control how users can securely connect to the network based on the risks related to the work they are conducting. The ideal way to meet this compliance is by developing a repeatable process using technologies and policies that will protect user identities and data.

Track and Monitor all Access to Network Resources and Cardholder Data

Many organizations have disparate networks and must manually track each system's log files in order to comply with PCI. Individually sifting through system logs can not only be an extremely time-consuming process but also a major drain on IT especially when you need to determine the cause of a compromise. Organizations have to track and monitor all access to network resources and cardholder data including real time, daily, and active events. Besides managing these logs, most organizations don't have a good policy in relation to the various types of information being logged and they have no way of sustaining the integrity of the data being logged. To finish, when it comes to having access to credit card data, organizations should not only have audit trails in place, but they should only provide this kind of sensitive information to people who need-to-know.

Tip

Even though analyzing logs and event data analysis is directly specified in PCI, it simply is good practice for any organization to monitor events. In an average information systems environment, event data is distributed, very large, and at times hard to decipher. Utilities that analyze events are provided within most operating systems by default but they only offer basic features. Consequently, many IT personnel will not have any method of being alerted when specific critical events are logged, such as the unauthorized access of cardholder information. For the most part, the event browsing and filtering capabilities provided by these tools are restricted.

However, there are a number of impressive software- and hardware- based Security Information Management (SIM) solutions that provide comprehensive log management. SIM solutions can overcome many of the obstacles associated with the need to centralize events, automate the aggregation and correlation of event data, issue alerts, and provide extremely detailed reporting capabilities. While aggregating events, SIM solutions will not only assist with creating a baseline of normal network activity, but they will also provide built-in rules to categorize them and trigger alerts and procedures as a result. Many solutions also provide default rule sets that classify events according to PCI requirements.

Install and Maintain a Firewall Configuration to Protect Cardholder Data

At first glance, people look at this requirement as simply installing a firewall on their network perimeter and think that all is well. Not quite. Many people fail to realize that this requirement states that organizations must not only have a working firewall that is configured and documented correctly for ingress and egress filtering rules, but it also requires the use of trusted zones (such as DMZ's) and the use of perimeter firewalls installed between wireless networks and the cardholder data environment. These are just a few of the many specific details within the 1st PCI requirement that tend to get ignored.

Tip

Organizations need to thoroughly review firewall configurations and the policies that control the traffic flowing into and out of a network. Many firewalls go untouched for quite some time after their initial network installation. Because business application needs and customer requirements change over time, many rules are adjusted to allow for additional ports and services to be opened for communication between trusted and untrusted segments. All changes on these devices must be approved, accurately documented, and reviewed on an ongoing basis to make sure that they are hardened and only allow secure information to flow between network segments. Documented configuration standards for these protections are mandatory along with specific documentation that justifies your network practices. Finally, do not forget that configurations have to provide security for assets that store, transmit or process cardholder data which includes the appropriate network segmentation of this information from wireless and mobile devices.

Conclusion

PCI is designed to safeguard credit card data from the time it is received until the end of its life cycle. The stakes are high for organizations that rely on heavy use of credit card processing to sell products and services, especially on the Internet. It only takes one security breach and the harm to a merchant's organization can be permanent. Understanding which requirements of the "12 Commandments" are the most challenging for other organizations can help you to avoid wasting time, money, and effort on the wrong ideas or technical solutions. Furthermore, it is important to know that PCI isn't concerned with how many employees you may have or what your annual revenue is; therefore, organizations must look at the requirements not simply as a checklist but as a practical guide to developing a risk management program. Implementing sound security policies, utilizing technologies for log and vulnerability management, properly building network segmentation and securing the perimeter through the use of firewalls can go a long way towards helping you achieve PCI compliance.

About the Author

Craig Norris, CISSP, CISA, MCSE, Security+, CAPM, TICSA, is a Regional Sales Manager at Accudata Systems, Inc. He has been involved with information technology and security for over 12 years. He can be reached at cnorris@accudatasystems.com or by calling Accudata Systems at 800-246-4908.

About Accudata Systems, Inc.

Accudata Systems is an IT consulting and integration firm with more than twenty-five years experience providing high impact IT services and integrated solutions. With focused competencies in Enterprise Platforms, Security, Infrastructure, and Assessment & Compliance. Accudata Systems provides a full array of services and solutions ranging from technology assessments to project deployment and support. As trusted advisors to our clients, we assist them in creating and supporting a computing environment that maximizes their investment in information technology. Accudata Systems is headquartered in Houston, Texas and has offices in Dallas, Austin, and San Antonio. Get more information at www.accudatasystems.com

Footnotes

ⁱ Visa. Visa USA Pledges \$20 Million in Incentives to Protect Cardholder Data: First Payment Brand to Combine Financial Incentives and Fines to Encourage Adoption of Industry Security Standards. http://usa.visa.com/about_visa/press_resources/news/press_releases/nr367.htm. San Francisco, December 12, 2006

ⁱⁱ Maintaining Trust in Payments. Visa Security Summit. March 8, 2007. http://usa.visa.com/download/personal/security/visa_securitysummit_coghlan.pdf

ⁱⁱⁱ Federal Trade Commission. FTC Releases Top 10 Consumer Fraud Complaint Categories. Identity Theft Again Leads the List. <http://www.ftc.gov/opa/2006/01/topten.shtm>. January 25, 2006.

^{iv} Privacy Rights Clearinghouse. <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

^v VeriSign. Lessons Learned: Top Reasons for PCI Audit Failure and How to Avoid Them VeriSign® Global Security Consulting Services. https://www.verisign.com/static/PCI_REASONS.pdf

^{vi} Visa 2007 Conference. Maintaining Trust in Payments: Conference Report. March 8, 2007.

^{vii} Department of Homeland Security. <http://nvd.nist.gov/nvd.cfm?startrow=1>. June 26, 2007.

^{viii} The Wall Street Journal. Breaking the Code. How Credit-Card Data Went Out Wireless Door. http://online.wsj.com/article_email/article_print/SB117824446226991797-IMyQjAxMDE3NzA4NDIwNDQ0Wj.html. May 4, 2007.

^{ix} Retail Systems Alert Group. 2nd Annual Benchmark Study 2006-2007. http://www.cisco.com/web/strategy/docs/RDS2006_Final.pdf