Achieving Compliance with the PCI Data Security Standard

June 2006

By Alex Woda, MBA, CISA, QDSP, QPASP

This article describes the history of the Payment Card Industry (PCI) data security standards (DSS), what is involved in an assessment and how to reduce the risks in a credit card processing environment. A high level overview of the standards is provided along with some insight into acceptable techniques for reducing the scope of the review, implementing compensating controls, and methods to consider in achieving a PCI DSS compliant network and systems.

What is the PCI Data Security Standard?

The Payment Card Industry data security standard (PCI DSS) was introduced in 2001 by VISA USA. The main objective of the standard was to reduce large scale credit card compromises in e-commerce web sites, acquiring organizations and merchants. The DSS is divided into 6 main sections, 12 subject areas and, contains a list of detailed security standards for network devices, servers, databases and user management. (See Table 1) There are also standards for information security management procedures and information security policies. It is a mandatory compliance standard for all Acquiring organizations, e-commerce sites, retailers and any organization that collects, processes or stores credit card information.

During the same time period, MasterCard introduced a program called Site Data Protection (SDP) which is an external vulnerability scanning requirement. The SDP established the standards for "patching" systems, implementing network firewalls and securing databases for systems which face the Internet. The SDP requires that all Internet facing systems (IP addresses visible on the Internet) be scanned on a periodic basis (usually quarterly) and be free from severe vulnerabilities to be compliant.

In 2004, VISA collaborated with MasterCard to jointly consolidate the PCI data security standards with the MasterCard Site Data Protection (SDP) security scanning requirements into one comprehensive program. Visa went one step further and developed a set of detailed questions and compliance requirements (similar to the ISO 17799 categories) and created two assessment programs:
1. A detailed assessment program (202 detailed standards)
2. A self assessment program. (Approximately 78 standards)

In the USA the program is called the PCI Cardholder Information Security Program (CISP) and in Canada it is called PCI Account Information Security (AIS). These are annual assessment programs, not a one-time review. The security assessment also requires quarterly vulnerability security scans to be completed. Only approved and tested security scanning vendors and qualified data security companies are allowed to conduct the assessments and scanning tests. The list of qualified scanning vendors can be found on the MasterCard web site and the list of qualified data security assessors on the Visa sites for each region. Ie Visa USA and Visa Canada. See https://sdp.mastercardintl.com and www.visa.com

The security standards and scanning requirements are updated each year and new standards are added by the Card Associations based on both security compromises that have recently occurred in the industry as well as the adoption and implementation of new technologies. The security requirements in the standard are a collection of security best practices and specific security techniques that have apparently been put in place as a result of actual security compromises e.g wireless network security hack, web server compromise, stealing credit card numbers from databases and other methods of breaking into systems and networks.

What happens if a merchant is not in compliance?

Failure to comply with the standards and implement appropriate security controls may result in fines and/or other penalties being assessed on the merchant or service provider. In the event of a credit card data compromise, the card associations may levy a fine on the Acquirer, as much as $500,000 and $25 per compromised card. The Acquirer has the option of passing the fine down to the merchant or service provider. If the merchant or service provider has passed the PCI DSS and scanning requirements and also passes a forensic review, conducted by the card association after the compromise has been discovered, the merchant or service provider may not be subjected to the maximum stiff penalties and may be considered to be in Safe Harbor. Companies that make the effort to achieve compliance are seen as cooperative and exhibiting a level of due care.

Companies which do not have a plan to achieve compliance or create misleading compliance reports are not seen in a favorable light and may be subject to more severe penalties. A recent incident involving a large-scale card compromise in the Card Systems International environment demonstrates the power that can be exerted by the Card Associations. Card Systems International was forced to shut down its processing service for credit cards and has had its assets sold at a fraction of their worth.

Who must comply with PCI DSS?

Any organization that collects, processes, stores or transmits credit card information is required to be in compliance with the PCI DSS. This includes: Merchants – bricks and mortar, service companies and e-commerce sites; Acquirers – banks or third party organizations that process credit card information and are linked to the Card Association network such as Visa Net; and Service Providers – which may host numerous e-commerce sites, process financial transactions through an ATM or collect and process credit card data on behalf of Visa or MasterCard members. These companies are also referred to as payment gateways.

Companies which issue credit cards, and authorize transactions, such as banks and large retailers, are not acquiring credit card transactions and therefore currently are not required to demonstrate compliance with the PCI DSS.

What is the status of Industry compliance?

Recent industry surveys indicate that fewer than 20% of all large merchants and service providers have achieved full compliance with the PCI DSS. Those merchants and service providers that are not able to fully comply with the standards must document detailed action plans to remediate the weaknesses and become compliant. Since some of the standards are difficult to achieve, ie. All credit card numbers must be encrypted or truncated if they are stored or some measure of compensating controls must be implemented to reduce the risk in the interim. The compensating controls may include the implementation of firewalls and detailed logging of access to the credit card processing systems and databases in lieu of implementing a full scale database encryption solution. Compensating control selection and implementation needs to be evaluated by a Qualified Assessor.

How is the compliance program managed?

The card associations have given the responsibility of managing the PCI DSS compliance program to the Acquirers and Acquiring banks. It is the Acquirer’s responsibility to contact the merchants, payment gateways and service providers to inform them of their compliance requirements and dates required to be in compliance. Merchants and service providers must select a qualified and approved Assessor, complete the assessment and remediate weaknesses and gaps noted in the review. The Acquirer may ask for detailed action plans for remediation.

Compliance Requirements are defined by Transaction Volume

Transaction volumes define the level of assessment required for the merchant or service providers. The transaction volumes are monitored by the Acquirers. Merchants which use a centralized processing switch to consolidate all transactions will be classified based on the total volume of transactions. Usually, this type of merchant will require an on site PCI DSS assessment. Merchants that have individual outlets linked to the Acquirers and do not consolidate transactions will be classified as a collection of merchants. Each merchant will then have to complete a self assessment questionnaire and be required to complete the security scans. This arrangement is not as cost effective as the consolidated approach since the costs of providing training to store managers, coordinating external scans, correcting security weaknesses and reporting to acquirers, may increase the cost of compliance by at least a factor of ten.

There are three main categories based on transaction volumes that define what a merchant or service provider needs to do to meet the compliance requirements:

1. Large merchants and service providers that process more than 6 Million cards annually, are required to conduct an onsite assessment using a qualified independent security assessor that is approved by Visa. Depending on the complexity of the networks, systems and electronic commerce services, the assessment may range from one week to six weeks of work.

2. Bricks and mortar merchants that process less than 6 million and more than 1 million transactions annually are required to complete a self assessment questionnaire and submit it to the Acquiring organization. E-commerce sites that process less than 1 Million and more than 20,000 transactions annually also need to go through the same process.

3. Merchants with fewer than 1 Million transactions also need to complete the self assessment questionnaire.

All merchants, service providers and e-commerce sites are also required to have quarterly vulnerability scans completed according to the MasterCard SDP standard. These scans must be completed by a Qualified Scanning Vendor and the merchant must pass the scanning tests.

These are only general guidelines, for a more detailed description of compliance requirements contact your Acquirer or visit the regional Visa web sites.

Self Assessment Questionnaire

In order to ease the roll out of the PCI DSS, a self assessment questionnaire was created for merchants and service providers that have lower transaction volumes.   The self assessment questionnaire is modeled after the detailed PCI assessment program but does not have as detailed requirements. E.g. the self assessment program asks if a firewall is in place. The detailed assessment program has a list of firewall rules that must be in place.

Merchants and service providers with lower volume transactions are required to complete the self assessment questionnaire and submit it to the Acquirer annually.   In Canada, Visa requests that the self assessment questionnaire be reviewed by a Qualified Independent Security Assessor before being submitted. At a minimum, the questionnaire should be completed by a person or party independent of operations, and should be reviewed and approved by a member of Senior Management. Careful attention should be given to completing the self assessment accurately and completely. Failure to accurately complete the self assessment questionnaire may result in fines or the removal of Safe Harbor protection.

External Scanning Requirements

All merchants and service providers are also required to complete quarterly external vulnerability scans from a qualified scanning vendor. In some cases, the technical scanning services offered by select scanning vendors have been priced as a commodity in the industry. These services attract merchants and service providers that are searching for the lowest price per IP address to be scanned.

It is important to note that the responsibility for ensuring that the scanning of web sites, servers and firewall devices are completed properly and completely lies with management and not the scanning vendor. Management must also ensure that action is taken on noted weaknesses and that they are corrected properly. This requires careful analysis of the results of the scans and a risk assessment to be completed.

It has been noted that approximately 10% to 20% of external scans are not done correctly and reports are not accurate. Some examples noted are false positive vulnerabilities, incomplete scans, intrusion prevention systems blocking scans and errors in the scanning software. It is highly recommended to have the scanning reports analyzed by a security expert.

Scope of the PCI Assessment and Scan

Any system or network component, including application systems, that are connected to or that process, collect, transmit or store credit card information are in scope in the compliance requirement. This could mean every single PC, network device and server in your environment.

Managing the scope of the compliance assessment is a complex task. Most retail organizations have grown IT operations organically, expanding networks and systems as required and controlled in house. This is also typical of companies that have e-commerce sites – growth has been accomplished through acquisition or scaling existing architecture to handle more capacity and provide better response times. In a large number of merchant sites and service providers which have undergone an assessment, it has been noted that the payment card processing environment is just another application on the corporate network. In some cases, databases with credit card information are linked with back office systems and business intelligence tools on the same network. Similarly, it has also been noted that web servers that collect credit card data reside on the same network as general web servers and are accessible to a majority of employees. With this type of architecture, all systems, network components, employees and databases are in scope of the PCI DSS review and external scanning needs to be done for every IP address visible on the Internet.

Beware of quick fix technology solutions

The number of technology products that are supposed to help you become compliant for SarBox, PCI, HIPAA, etc. is astounding. A number of professional services firms are also offering pre-assessment services to assist clients in becoming compliant and are promoting technology solutions to achieve compliance. While most of these solutions will support the compliance program, they may not be the most cost effective way to secure card holder data, demonstrate compliance or reduce the risk.

10 Things to do to achieve compliance

Listed below are ten suggestions an organization can do to reduce the risk and the complexity of the PCI assessment.

1. Conduct an IT Risk Assessment

By conducting a high level IT risk assessment your organization should be able to identify where card data is stored, how it is accessed and identify the general security controls in place. The risk assessment should be mapped to the PCI data security standards to gauge how well compliance is being met and what are the gaps.

2. Reduce the Scope

Isolate, compartmentalize and secure. One of the best security practices which can be implemented to reduce the scope of the compliance review and increase the level of security is to isolate networks and systems that process or store credit card information from other systems. Think of creating a model of water-tight compartments on a battleship. Key assets and resources are always locked away in areas that have many layers of security controls and are isolated in specially designed water-tight compartments. This means that critical systems are put into security zones where all access goes through choke-points and layers of control. This can be done with firewalls, virtual network segments with access control and a detailed monitoring system which records all access by systems and users.

3. Understand the control environment

In the 1990's, Carnegie Melon University introduced and promoted the term Capability Maturity Model and used it as a guide to measure how well an IT department was delivering quality in software development. A number of other industries have adopted the concept of measuring the effectiveness and quality of processes and controls by using a maturity model. E.g COBit has such a model for controls. The general attributes that are used to measure the effectiveness of controls, including security processes can be defined by the 5 Levels:

Level 0: Control is not documented
Level 1: Control is documented
Level 2: Control is consistently applied (implemented)
Level 3: Control is working (tested)
Level 4: Control is monitored (process improvement)

This maturity scale provides a measurement and comparison of how effective the controls are in an organization. When conducting an assessment of the control environment of an organization that processes credit cards, at a minimum acceptable level, the control must be documented and implemented. Testing the control is also recommended to ensure it is working properly. When evaluating the key controls in the PCI assessment ensure the control is documented.

4. Buy Compliant Systems

All vendors that create and implement cash register systems, application program interfaces for e-commerce sites, transaction switches and payment application software need to have their software reviewed and certified by a Qualified Payment Application Security Company. Merchants should only buy compliant systems or upgrade their existing systems to compliant systems. A compliant system does not store credit card numbers or the magnetic stripe data in the clear. Either the data is masked, truncated or encrypted.

5. Do not store credit card numbers or Track 2 data

It is a hard habit to break. Credit card numbers in databases can be used for settlement, trace requests, charge backs and business intelligence. It is useful data to a merchant that wants to make processes easier to manage and gain a little insight into the purchasing patterns of customers. Not any more. It is forbidden to store the primary account number or any of the other elements known as Track 2 on the magnetic stripe or any ‘card not present’ data. (Card validation codes)

After the card transaction is authorized and the payment is processed, mask or truncate the card number, delete track 2 data and ensure that the data is not stored in any of the transaction repositories or stages of processing. That means electronic logs, journals and switching systems.

6. Update policies and standards

All company policies relating to information security need to fit with the PCI requirements. All third party contracts also need to include clauses that third parties will comply with PCI standards and in the case of a security breech, there is right to audit and conduct forensic analysis. Many organizations do not have detailed information security policies and do not see the value in having policies. An information security policy is similar to a contract. It is an agreement between the owners of the system and service with the users and customers that all activity and interaction with systems and data is approved, authorized and follows standard processes. Good security policies can actually improve business practices since Users and owners will have a much better understanding of security practices and rules for protecting data integrity, confidentiality and availability.

7. Implement Detailed System Logging

Any system component which processes credit cards or controls network access to key systems needs to have logs enabled. The logs should be managed through standard time stamps and stored in a secure location that is difficult to tamper with. Logs should be reviewed and assessed for effectiveness to ensure that they capture adequate information to determine what has been done, by whom and when. In the event of a security or data breach, this information is crucial when trying to determine what happened, how much was compromised and by whom.

8. Implement Network Perimeter Controls

Firewalls are not enough. Today's current networks need to have strong perimeter controls that can deal with complex threats. Malicious code, viruses, worms, spyware and zero day exploits have raised the bar on protection requirements. One vendor cannot manage all threats. Multiple devices and layers of control are required to detect and prevent network attacks. At a minimum, an organization needs to have implemented an intrusion detection system, virus control and network segmentation to be in compliance with the PCI DSS. This also includes protection for mobile devices.

9. Harden Servers

All servers that store and process credit card data or reside on the Internet must be configured securely and have documented configuration standards. This means that all unnecessary services are disabled, user access is strictly controlled and logged, access permissions are enabled on key files and all critical files and programs are carefully monitored for unauthorized changes. A vulnerability management program which includes implementing system patches in a timely manner also needs to be in place.

10. Control Vendor and Remote Access

It is easy to circumvent all security controls if the back door is wide open. Dial in access to databases and cash register systems is usually enabled for support purposes. This type of access bypasses network firewalls and access control and the access may not be logged. It is highly recommended to implement strong access control, detailed logging and two factor authentication for remote access to critical systems.

Summary

The PCI DSS is a step in the right direction to curb the rising number of incidents of mass credit card compromises and fraud. While the standards are not necessarily aligned specifically to the processing environment of a retailer, they provide an excellent base for an E-commerce site or service provider. Bricks and mortar merchants should use the services of an Assessor to properly scope the review, assess the risks and document the control environment. The PCI DSS is a very difficult standard to achieve and to be in full compliance. Realize that the standard is not an end state, but rather a process to be implemented. The standards should be a guide that encourages organizations to assess new technologies and business methods for the strength of security in systems and processes before they are implemented.

Table 1 - PCI Security Sections and Standards – Overview

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect data

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

Protect Card Holder Data

Requirement 3: Protect stored data

Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

Requirement 7: Restrict access to data by business need-to-know

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

Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

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

Requirement 11: Regularly test security systems and processes

Maintain a Policy that Addresses Information Security

Requirement 12: Maintain a policy that addresses information security

About the Author:

Alex Woda is the General Manager of Dyntek Canada Inc. an information security solution provider and Qualified Data Security Assessor and Security scanner for Visa and MasterCard. Mr. Woda is a Certified Information Systems Auditor (CISA) and has worked extensively in the financial services industry. Mr. Woda has an MBA, and undergraduate degrees in Computer Science and Music. Mr. Woda has taught numerous courses and is an adjunct professor at the Schulich School of Business. He is also a Qualified Data Security Professional (QDSP) and a Qualified Payment Application Security Professional (QPASP). He can be reached at Alex.Woda@Dyntek.com.