

Understanding PCI: A white paper for executives making decisions on compliance



January 2009

Intended Audience

This document is intended for IT executives and senior managers responsible for PCI compliance. The level of technical competency of the reader is not pertinent.

Sponsored by Tevora Business Solutions

This white paper is sponsored and presented by Tevora Business Solutions, a leader in creating secure enterprises. Tevora is an international security consulting firm focused on information assurance, compliance and governance. Our consultants utilize proven methodologies that assist enterprises in securing their sensitive information with long-range strategic planning and a consistent focus on best business practices. This approach leaves management free to focus on growth, development and profits.

A typical Tevora engagement starts with a business case and gap analysis, giving all senior managers pertinent information, actionable options and expected returns. Our full-range of services deliver end-to-end security for companies in the Financial Services, Government, Education, Health Care, BioTech / Pharma, Retail and Hospitality industries.

Executive Summary

To protect client information and deter fraud, Visa, American Express, Diner's Club, Discover, JCB and MasterCard collaborated to create a new set of regulations known as the PCI (Payment Card Industry) Data Security Standard (DSS). This standard affects every company that handles, processes, stores or transmits credit card information, or related card data.

Compliance with the industry-imposed standards became mandatory as of December 31, 2007. Since credit card companies are determined to prove that consumer information is safe in their hands, they have instituted severe penalties for non-compliance with the PCI DSS, which can include fines ranging from \$5,000 to \$500,000, and perhaps even termination by the credit card issuers.

The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

Demonstrating compliance with PCI is about following industry best practices. Proof of compliance may be obtained in the form of a Recommendation of Compliance (ROC), issued by a Qualified Security Assessor (QSA) in good standing as acknowledged by PCI Security Standards Organization.

Understanding PCI: A white paper for executives making decisions on compliance

"Locking down cardholder data is an important security component that will benefit financial institutions and merchants, and is equally important to maintain consumer trust in Visa," said Michael E. Smith, senior vice president of Enterprise Risk and Compliance at Visa USA. "Nothing is more important to Visa than securing commerce."

Smith's statement was a reaction to a steady escalation in credit card fraud and identity theft cases that has had a negative impact on credit card companies, financial institutions and e-commerce companies, as well as on consumer confidence. In less than ten years, buying goods and services over the Internet has become so commonplace that billions of dollars changes hands through online credit card transactions every year.

In 2004 Visa and the other leading credit card companies – American Express, Discover Financial Services, JCB and MasterCard Worldwide – joined forces to form the PCI Security Standards Council, an independent entity dedicated to creating a new set of industry regulations that would form the PCI (Payment Card Industry) Data Security Standard (DSS). The standard officially took effect on June 30, 2005.

Those impacted by the PCI DSS standard, which includes all merchants and service providers that handle, transmit, store or process information concerning any of the major credit cards or related card data, were given more than two years to achieve compliance. The PCI specifications advised these entities to seek advice from partners who know how to design and implement practices required by the standard.

The compliance grace period ended on December 31 of 2007. While specific requirements are set independently by individual payment card brands, any company that has yet to adopt the PCI DSS standard faces fines up to \$500,000, higher processing fees and possible termination by the credit card issuers.

What is PCI?

The Payment Card Industry Data Security Standard is intended to protect credit card data, wherever it resides, ensuring that members, merchants and service providers maintain the highest information security standard. When customers offer their credit card at the point of sale, over the Internet, on the phone or through the mail, they want to do so with the confidence of knowing that their account information is safe.

The PCI DSS version 1.1 is a set of comprehensive requirements for enhancing payment account data security.

There are six primary areas covered by PCI that are divided into 12 requirements:

Build and Maintain a Secure Network

1. Install and maintain firewalls
2. Do not use vendor-supplied or default passwords

Protect Cardholder Data

3. Protect stored data
4. Encrypt transmissions of cardholder data as well as sensitive information as it travels across public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to need-to-know
8. Assign unique IDs to each person with computer access
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Monitor and track all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

PCI Compliance

Merchants and service providers must obtain compliance validation to demonstrate their adherence to the PCI Data Security Standard. Validation requirements vary based on the levels defined by the PCI DSS and Visa. They range from self-assessment questionnaires to the yearly submission of a signed Recommendation of Compliance (ROC) by a Qualified Security Assessor (QSA) in good standing as acknowledged by PCI Security Standards Organization.

Who Should Comply?

The following individuals and businesses are required to attain a signed Recommendation of Compliance (ROC):

Level 1 Merchants:

- Any merchant, regardless of acceptance channel, processing more than 6,000,000 Visa transactions per year
- Any merchant that has suffered an attack that resulted in an account data compromise
- Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system
- Any merchant identified by any other payment card brand as Level 1

Level 1 Service Providers:

- All VisaNet processors (member and nonmember) and all payment gateways

Level 2 Service Providers:

- Any service provider that is not in Level 1 and stores, processes or transmits more than 1,000,000 Visa account transactions annually

These security requirements also apply to all “system components” i.e., any network component, server, or application included in, or connected to, the cardholder data environment, including:

- Network components such as firewalls, switches, routers, wireless access points, network appliances, and other security appliances
- Servers that include, but are not limited to, web, database, authentication, DNS, mail, proxy, and NTP
- Applications include all purchased and custom applications, including internal and external (web) applications

PCI Implementation

A Level 1 PCI assessment includes a comprehensive review of how credit information is handled. The review should focus on the following areas:

- Cardholder Data-Primary Account Number, Cardholder Name, Service Code, Expiration Data, Full Magnetic Stripe, CVC2/CVV2/CID, PIN/PIN Block, as well as any data repository where more than 50,000 or more account numbers reside.
- System Components-Network components, servers or applications included or connected to cardholder data. Applications include all purchased and proprietary/custom applications, as well as internal and external Internet applications.
- Network Components-Firewalls, switches, routers, wireless access points, network appliances and other security appliances. Server types include: Web, database, authentication, mail, proxy, network time protocol (NTP) and domain name server (DNS).

Typically a 3-6 month engagement, this assessment satisfies the six primary areas of security specified by PCI. A tactical and precise implementation can be achieved through a three-step process.

1. Gap Analysis

A tactical gap analysis helps outline specific strategies for a comprehensive and cost-effective road to compliance. In addition to scope reduction, control validations will be made to assure that remediation efforts can be direct and focused.

2. Remediation

Remediation covers all necessary recommendations from writing security policies to implementing security controls. Remediation services should always be performed by a QSA in good standing, to ensure direct and efficient ROI.

3. Assessment

An onsite assessment that ensures compliance. Once the engagement is complete, the QSA issues a Recommendation of Compliance.

Conclusion

The purpose of the PCI standard is to protect credit card data by reducing fraud and theft. A Qualified Security Assessor can make certain that a client's IT infrastructure meets all conditions of compliance.

There are several sound business reasons to seek PCI compliance:

- Reduce risk of an information breach
- Preserve consumer confidence
- A safer, more resilient infrastructure

While penalties for non-compliance vary among credit card networks, companies can be barred from processing credit card transactions, higher processing fees can be applied, and in the event of a serious security breach, fines of up to \$500,000 may be imposed.

Through the assistance and expertise of a QSA, compliance with the PCI DSS can be achieved in an efficient and cost-effective manner.