Configuresoft
Security. Compliance. CONTROL.

WHITE PAPER

"You sure you want to charge that? Is the PCI DSS protecting you?"

Abstract

By Chris Farrow

Director, Configuresoft Center for Policy & Compliance

The Payment Card Industry Data Security Standard, or PCI DSS, was established to create a unified security standard whose implications have grown due to new industry regulations. Security requirements were established in six major areas that cover 12 requirements.

Credit card vendors enforce the PCI DSS and penalties are harsh for merchants who fail to comply. The following white paper outlines the six major areas that many businesses may not yet be fully aware.

Introduction

Originally established as various security programs by each of the individual credit card companies and the CISP (Cardholder Information Security Program) to address growing monetary losses, the credit card industry came together to establish a unified security standard in 2004. Ratified by VISA, MasterCard, American Express, Diners Club, Discover, and JCB, the Payment Card Industry Data Security Standard (PCI DSS) now has additional implications in light of other privacy regulations such as GLBA and California's SB 1386.

Although the PCI DSS became fully effective on June 30, 2005, a large number of businesses are still not fully educated on the security requirements. Nor do many know to which businesses the requirements apply or what the penalties are for failure to comply.

To begin with, the PCI DSS is enforced by the credit card vendors. Failure to comply with the security requirements could result in stiff penalties, including possible restrictions on the merchant and permanent restriction of the merchant's participation in credit programs. A monetary fine of up to $500,000 per incident can also be leveled. While the consequences for failing to comply sound harsh, the credit industry loses well in excess of $1 billion a year to theft and fraud. These losses are eventually passed on to consumers in the form of increased fees and interest rates.

So what exactly are the security requirements that vendors and merchants can be audited on?

Six Major Areas of Focus

The PCI DSS focuses on six major areas of security requirements, covering 12 requirements that must be applied to all system components. This is defined as any network component, server, or application included in, or connected to, the cardholder data environment.

Build and Maintain a Secure Network

The two requirements in this section address proper installation and configuration of firewalls and not using vendor-supplied defaults for system passwords and other security parameters. The best practices for enterprise firewalls are covered in fairly good detail. Note, there is also a requirement for personal firewall software to be installed on any mobile system or any employee-owned computer that is used to access the organization's network (workstations and laptops are not mentioned as covered equipment in the front of the document but are included here). The second requirement covering vendor-supplied defaults is a little sparse, but there is a critical requirement regarding the development of configuration standards for all system components. These configuration standards must be based on industry standards, such as the guidelines from NIST or CIS, and address all known vulnerabilities.

Protect Cardholder Data

The third and fourth requirements fall in the second section and cover protecting stored data, then encrypting cardholder and sensitive information before transmitting them across public networks. These two requirements have good recommendations on storage of sensitive data along with solid guidance on encryption procedure, including key management. The requirements here are updated and do account for traditional hard-wired and wireless networks.

Maintain a Vulnerability Management Program

The third section focuses on the proper use and implementation of anti-virus software programs and how to develop and maintain secure systems and applications. While the section on secure development practices is a good starting point, many organizations are not taking into consideration guidelines from the Open Web Application Security Project (see www.owasp.org). We were disappointed to find that

there were no recommendations in this section for anti-spyware controls. Most of the anti-virus vendors are already providing solutions. We feel language should be added in this section to deal with privacy-violating malware.

Implement Strong Access Control Measures

The fourth section is the largest, covering policy and procedural requirements #7, #8, and #9. These three requirements focus on restricting access to data on a business need to know basis, assigning a unique computer ID to each person and restricting physical access to cardholder data. There is a fair amount of guidance here on proper identity management, as well as the physical security aspects, including storage and destruction of cardholder data and other sensitive financials.

Regularly Monitor and Maintain Networks

Requirements #10 and #11 fall into the fifth section, which begins with tracking and monitoring all access to network resources and cardholder data. For tracking and monitoring, the proper use of logging and audit trails is covered. Some technology recommendations such as Network Intrusion Detection Systems (NIDS), Host Intrusion Detection Systems (HIDS) and file integrity checking are also outlined. The 11th requirement mandates the regular testing of security systems and processes including regular vulnerability scans and penetration testing.

Maintain an Information Security Policy

The 12th and final requirement for formal policies and procedures includes an incident response plan. Considering this is an area that is often overlooked and always checked on by auditors, this requirement should have probably been the very first. Effective security plans are incredibly tough to implement without a proper foundation built on policies and procedures.

The details for each specific requirement can get somewhat involved with numerous policies, procedures, and technical requirements. Visa and MasterCard are the definitive resource for the PCI DSS. The links appear to be in flux, so we recommend that you search the Internet for PCI DSS information. The standard will offer great details. You can go online and download a copy to determine which requirements are most appropriate for your business.

Conclusion

On the surface, the credit card industry appears to be going in the right direction, and the Configuresoft Center for Policy & Compliance applauds its diligence to get vendors and merchants to step up their efforts in securing sensitive credit card information. The real challenge here will be in getting these requirements enforced. As long as the PCI DSS relies heavily on self-auditing, many vendors will continue to drag their feet. The PCI DSS needs to show it has teeth; it will probably take a large, public incident with hefty fines to motivate the vendors to comply with the standard.

About Configuresoft

Configuresoft is the recognized leader in highly scalable enterprise configuration management, security patch management, and policy compliance technology. Based in Colorado Springs, Colorado, the company's products offer large-scale computing environments the ability to collect and analyze the most detailed information available about system application settings, events, and operational trends, to a centralized point of management and control. Configuresoft serves eight of the "Global 25" corporations, as the only configuration management solution to offer both system-wide configuration controls and provide the tools to keep mission-critical systems in compliance with rapidly growing mandates, operational standards, and evolving process methodologies.