ControlCase LLC

Payment Card Industry (PCI) Data Security Standard (DSS) Version 2.0: *Analysis of Changes, Implications and Next Steps*

By Parin Lapasia (QSA, CISA, CISSP) and Hugh Kominars (QSA, CISA, CISM), ControlCase LLC

The Payment Card Industry (PCI) Security Standards Council has recently released Version 2.0 of the PCI Data Security Standard. The new standard becomes effective on 1 January 2011. The existing standard, PCI DSS Version 1.2.1 remains in effect until 31 December 2011. In the interim, organizations now have the option to be certified using PCI DSS 1.2.1 or PCI DSS 2.0 throughout the year 2011. After 31 December 2011, however, all certifications will use PCI DSS Version 2.0.

SUMMARY OF CHANGES

Based on our analysis, the new standard has been issued to accomplish the following:

- Provide greater clarity on a number of complex requirements
- Recognize of the need for organizations to identify and address evolving risks and threats to their environment
- Reduce redundant or overlapping sub-requirements.

New to PCI DSS Version 2.0 is the elaboration of the relationship between it and the Payment Application (PA) DSS, along with clarifications of the scope of each.

Within PCI DSS Version 2.0, there are a number of important changes to sub-requirements that must be evaluated and considered by each organization and during certification activities:

- Requirement 2.2.1 clarifies the requirement for a single function per server, and states that the requirement applies to virtual servers by limiting each virtual server to a single function.
- Requirement 3.2 addresses the requirements and provisions for retaining sensitive authorization data by issuers and companies that support issuing services.
- Requirement 3.4 clarifies the security controls required when storing both truncated and hashed primary account numbers (PAN).

- Requirement 3.6 elaborates on additional industry standard encryption key management procedures (specifically those from NIST are referenced).
- Requirement 3.6.4 introduces some flexibility for periodic key changes based on industry standard practices.
- Requirement 3.6.6 provides clarification of requirements in the case that manual cryptographic key management operations are used.
- Requirement 6.2 introduces the use of risk ranking and prioritization of detected security vulnerabilities based on the Common Vulnerability Scoring System (CVSS) score.
- Requirement 6.5 supports the development of applications based on industry standard practices including but not limited to Open Web Application Security Project (OWASP) Top 10 vulnerabilities, SANS Top 25 vulnerabilities, and CERT Secure Coding.
- Requirement 8.3 clarifies the definition of two-factor authentication.
- Requirement 10.4.2 clarifies the requirements for protecting the Network Time Protocol (NTP) configuration and logging and monitoring.
- Requirement 11.2.1 and 11.2.2 clarifies that “high” vulnerabilities must be remediated to obtain a “clean” report.
- Requirement 12.1.2 requires the use of industry standard methodologies for conducting risk assessments, which include but are not limited to those from ISO 27005, OCTAVE, and NIST SP 800-30.

Although a significant portion of PCI DSS Version 2.0 has not changed from Version 1.2.1, the new version has been drafted to provide clarity on the effective implementation of preventive controls, in light of contemporary technologies and the constantly changing threat landscape.

IMPLICATIONS

Aside from providing additional information, clarification, and assistance with interpreting the existing requirements and testing procedures, PCI DSS Version 2.0 continues to reinforce and support key principles that have been proven time after time to reduce the unauthorized exposure, disclosure, and use of cardholder data. The implications of the new version include the following:

- Continued emphasis on identifying, understanding, and obtaining validation for third parties that handle cardholder information. This would be evidenced by reviewing the third parties’ respective PCI DSS reports or having the QSA assess specific third-party controls during the annual assessments.
- Demonstration of third-party compliance. Merchants and service providers must demonstrate that they manage and monitor PCI DSS compliance of all associated third-party service providers with access to cardholder information.

- ❑ Reinforcement of the scanning requirement. Four passing quarterly scans must have been recorded and retained for subsequent certifications, after the certification has been obtained.
- ❑ Continued rigor to verify firewall and router security. However, designated direct outbound communications from the cardholder environment is permitted, where specifically authorized by management for legitimate business purposes.

There are several subtle but notable enhancements within PCI DSS Version 2.0 that warrant further attention by organizations seeking to attain, maintain, and demonstrate compliance and security of their cardholder information environment.

- ❑ On a quarterly basis, organizations will be required to demonstrate that they have implemented automated or manual processes to remove stored cardholder information that exceeds retention timeframes outlined in the organization's data retention policy or schedule. This will require companies to implement an efficient mechanism or process to identify and locate all instances of cardholder information.
- ❑ On an annual basis, organizations must provide evidence that they have implemented a formal/documented risk assessment process that identifies threats, vulnerabilities and controls within their technical and operational environments. Where applicable, this must cover relevant third-party processes and operations, as they related to processing, transmitting, and storing sensitive cardholder information.

The rigor needed to manage and demonstrate ongoing compliance with PCI DSS has not changed with the release of Version 2.0. Organizations seeking to become or maintain compliance with PCI DSS must continually strive to streamline and reduce the overall cost and effort associated with their compliance programs so as not to impair their business operation. The table below provides a consolidated inventory of key milestones/activities and frequency required by PCI DSS Version 2.0:

Milestones and Activities	Frequency
Log reviews for servers and network devices	Daily, if not automated
File integrity monitoring reviews	Weekly, if not automated
Anti-virus scan reports	Weekly, if not automated
Patch management (using MBSA)	Monthly
Cardholder data search on desktops, file servers and databases; implementation of data retention and disposal	Quarterly
Internal vulnerability assessment servers and network devices	Quarterly
External ASV scanning on all public IP addresses	Quarterly

User account privilege reviews and removal of users not logged in last 90 days	Quarterly
Wireless walk-through using wireless analyzer	Quarterly
Firewall and router security rule set reviews	Half-Yearly
Annual encryption key rotation	Annually
Physical security review of offsite media backup locations, if applicable	Annually
Media Inventories of medias stored onsite and offsite locations	Annually
Internal penetration testing (network)	Annually
External penetration testing (network)	Annually
Application penetration testing, if applicable	Annually
Risk assessment for the environment in scope	Annually
Policies and procedures review	Annually
Information security awareness training	Annually
Incident response training	Annually
Incident response testing	Annually
Sign-off from employees that they have read and understood the information security policies and procedures	Annually

NEXT STEPS

The changes associated with PCI DSS 2.0 reinforce the need for controls, monitoring, and ongoing assurance. Organizations should begin planning for the transition to Version 2.0 requirements during the earlier part of 2011 by assessing the differences between the new requirements and their current compliance processes and tools and cardholder data environment. After identifying those differences, organizations should plan to remediate gaps during the summer of 2011 so that they can demonstrate compliance by the 1 January 2012 deadline. To make these dates, organizations should begin coordinating with their QSAs so that certification, if required, can be scheduled when remediation has been achieved. We expect that QSAs will be in high demand during the last quarter of 2011, so early planning is warranted.

ABOUT CONTROLCASE

ControlCase is a global provider of Governance, Risk and Compliance (GRC) software, professional services, managed compliance and security services and IT GRC Software as a

Service (SaaS) solutions. Headquartered in the United States, with locations in North America, Europe, Asia and the Middle East, ControlCase provides compliance related solutions and services for companies and government agencies that require a consistent and repeatable means of complying with multiple regulations.

ControlCase is also a Qualified Security Assessor (QSA) as certified by PCI Security Standards Council and an Approved Scanning Vendor (ASV).

ControlCase is rated as 'Promising' by Gartner in the IT Governance, Risk and Compliance Management Market Scope for 2010 and an innovator of Cloud-based compliance software and services. Clients currently use the ControlCase GRC Version 5.0 to manage:

- ❑ Concurrent compliance initiative management
- ❑ Enterprise-level cardholder data discovery
- ❑ IT and data asset security vulnerability identification and management
- ❑ Risk assessments, and third party and merchant risk management
- ❑ Policy and training compliance management
- ❑ Incident identification and reporting.

ControlCase provides the following Managed Compliance Services to over 200 clients in 24 countries: quarterly ASV scanning, network penetration testing, application penetration testing, firewall and router security reviews, data discovery, log monitoring and reviews, IT policy and procedure development, and security awareness training.

For more information please visit www.controlcase.com.

ControlCase LLC
Hugh Kominars, Vice President of Markets and Partnerships
hkominars@controlcase.com
+1.703.483.6383