INFORMATION TECHNOLOGY FLASH REPORT

Understanding PCI DSS Version 3.0 – Key Changes and New Requirements

November 8, 2013

On November 7, 2013, the PCI Security Standards Council (PCI SSC) announced the release of a new version of the PCI Data Security Standard (PCI DSS) and the Payment Application Data Security Standard (PA-DSS). The PCI DSS is the widely accepted set of policies and procedures used to optimize the security of credit, debit and cash card transactions and protect cardholders from misuse of their personal information.

PCI DSS 3.0 was released this week and will become effective beginning January 1, 2014. However, during 2014, both PCI DSS 2.0 and 3.0 will be available and companies can validate to either version. On December 31, 2014, version 2.0 will sunset and only version 3.0 will be authorized for validation beginning January 1, 2015.

PCI DSS 3.0 aims to do three things:

- Provide additional guidance and clarity on how to comply with the standard;
- Introduce new requirements to bring the standard in line with emerging threats and changes in the marketplace; and
- Establish security activities as part of “business as usual” practices that are required to be carried out year-round, not just during compliance validation.

Notable changes include, but are not limited to:

- Increased requirements for managing third-party suppliers
- Increased point-of-sale terminal security
- More flexibility and education around passwords
- More robust requirements for penetration testing and validating segmentation
- Enhanced testing procedures to clarify the level of validation expected for each requirement
- Expanded software development lifecycle security requirements for PA-DSS application vendors

Although many of the modifications in the standard are clarifications and provide improved consistency in language, there are several significant changes to the existing requirements that are likely to require considerable time and resources to address. Following is a more detailed review of the most notable changes.

A Higher Bar to Achieve "Segmentation"

The change to the scoping considerations possibly has the greatest implications, affecting several other compliance rules as discussed below. Specifically, scoping has been clarified to indicate that system components must include "Any component or device located within or connected to the cardholder data environment (CDE)." The new language also states that the "PCI DSS security requirements apply to all system components included in or connected to the CDE." Additionally, a new requirement has been added requiring that if segmentation is used, "penetration testing procedures must test all segmentation methods to confirm they are operational and effective, and isolate all out-of-scope systems from in-scope systems."

Offering further clarity, the standard states that, "To be considered out of scope for PCI DSS, a system component must be properly isolated (segmented) from the CDE such that even if the out-of-scope system component was compromised it could not impact the security of the CDE."

The additional focus on connected systems likely expands the number of systems considered in-scope for many organizations. If a compromise of systems traditionally located outside the CDE could impact the security of the CDE, then those systems are in scope. For example, in an Active Directory environment, every computer on the domain can be used to administer the domain. A compromise of any domain member could impact security of the CDE and now could be considered in-scope for the PCI assessment.

At recent PCI Community Meetings, the Council indicated that it would provide further clarification and direction on how to apply this scoping guidance for PCI DSS 3.0.

Companies with systems on the periphery of the CDE that could impact the security of the CDE should start re-thinking their scoping decisions and take appropriate actions to align the security of such systems to PCI DSS requirements.

Hosted Payment Pages Are No Longer a "Silver Bullet"

In PCI DSS 2.0, it was possible for online merchants to de-scope their Internet-facing web systems from PCI DSS validation if they outsourced the online payment processing to a third party. However, going forward, PCI DSS 3.0 offers a new definition of system components that brings Internet-facing e-commerce systems back into scope for compliance: "System components include systems that may impact the security of the CDE (for example web redirection servers)."

Up until now, e-commerce web servers have been considered out-of-scope if they use iFrames, hosted payment pages and other redirection technologies to prevent cardholder data from touching the merchant's systems. Under the new standard, all of these web servers and the systems connected to them fall in scope due to the new segmentation requirement. This likely brings the rest of a company's network into scope, as well. Why? Because web infrastructure is typically connected to back-end billing, accounting, content and other systems. The only "out" for companies that lack the ability internally to ensure the security of web servers remains fully outsourcing the web infrastructure.

Companies making use of third-party hosted payment pages should start considering steps they need to take to enhance security controls on their e-commerce web servers to align to PCI DSS 3.0 requirements.

No Reduction in Procedures for PA Applications

In PCI DSS 2.0, PA-validated applications must be implemented into a compliant environment according to the PA implementation guide. However, PCI DSS 3.0 states "all applications that store, process, or transmit cardholder data are in-scope for an entity's PCI DSS assessment, including applications that have been validated to the PA-DSS. The PCI DSS assessment should verify the PA-DSS validated payment application is properly configured and securely implemented per the PCI DSS

requirements." In environments being assessed by a third party, this means a higher level of effort could be required to validate compliance of PA-validated applications because there is less ability to rely on the PA-DSS validation.

Companies making use of PA-DSS validated payment applications within their environment will need to ensure these applications have been implemented in line with PCI DSS requirements.

Larger Samples

The new standard requires larger samples. Specifically, "Samples of system components must include every type and combination that is in use. For example, where applications are sampled, the sample must include all versions and platforms for each type of application." Again, for merchants undergoing a third-party assessment or Level 1 merchants that self-assess, the level of effort in the validation process is likely to increase.

Companies will need to prepare for larger sample size requests from their QSAs in future compliance validations.

POS Physical Controls

In response to recent attacks in which POS devices have been physically modified or systematically replaced by rogue devices to capture cardholder data, there is a new set of control requirements around physical security for POS devices. First, merchants must maintain an inventory of POS devices, which must be identified in detail, including the location and serial number of each device. Additionally, POS devices must be inspected periodically for tampering, and employees at POS locations must be trained in how to detect and prevent device tampering.

Retailers that have a physical POS presence need to start taking steps to create an inventory of POS devices in their environment and instill additional processes to validate their integrity on a periodic basis.

Third-Party Service Provider Management

PCI DSS 3.0 has introduced several new controls for managing third-party suppliers that include the need to gain greater transparency and formality with the roles, responsibilities and accountabilities of third-party suppliers engaged in supporting aspects of IT and business processes for companies involved in handling cardholder data.

Companies that rely on third parties for handling aspects of their IT and CDE need to ensure appropriate levels of transparency are achieved to document roles, responsibilities and accountabilities for security.

In addition to these major changes in PCI DSS 3.0, there are other updates that, while less likely to impact the payment processing structure within organizations significantly, are still noteworthy:

- **Default accounts** – The previous requirement stated only that default passwords should not be used. Now, default accounts have to be disabled or removed whenever possible.
- **Inventory of system components** – Companies must maintain an inventory of system components that are in-scope for PCI DSS. This would include all "connected" components that are in-scope.
- **Disk encryption** – In PCI DSS 3.0, logical access must be managed separately and independently of native operating system authentication and access control mechanisms, such as not using local user account databases or general network login credentials. One implication of this is that Active Directory credentials may no longer be acceptable to manage disk encryption.

- **Split knowledge/dual control** – For manual clear-text operations, two people are required to perform any key-management operations (such as rotating keys). Generally, this would mean not only that knowledge of the key must be split, but also that the account that provides access to any key management functionality must be split.
- **Custom developers** – Procedures for secure development and code review now "applies to all software developed internally as well as custom software developed by a third party." This means that any developers with whom a company works will need to be required contractually to comply with the updated PCI standard.
- **Vulnerability scans don't meet requirements for web application security** – We've been asked by many companies if vulnerability scans can be used to meet the PCI DSS requirements for web application security. PCI DSS 3.0 makes this clear – vulnerability scans are not sufficient.
- **Service providers must use a unique password for each customer** – This applies only to service providers, many of which still use the same password for the service account for every customer. This will not be permitted after June 30, 2015.
- **Unique certificates** – Merchants that use certificates, smart cards or tokens must ensure these security items are unique and tie to an individual account such that if employees were to swap tokens, they would not be able to log on.
- **Inventory of wireless access points** – Merchants and service providers must maintain an inventory of authorized wireless access points, along with a business justification for each.
- **More frequent risk assessments** – Risk assessments, which used to be required annually, must now be performed upon any significant changes to the environment, as well as annually.
- **Expansion of service providers required to be in compliance** – With PCI DSS 2.0, only service providers that have access to a merchant's cardholder data must be contractually bound to follow the PCI DSS. The new standard expands this requirement to include all service providers that could affect the security of the cardholder data. This expansion adds many more service providers to the list, including custom developers, hosting providers and managed security service providers. Additionally, companies must maintain information on which PCI DSS requirements are managed by each service provider and which are managed by the company.

In Closing

The changes in PCI DSS 3.0 are likely to result in significant additional effort for companies processing credit card payments. Additionally, as the bar for segmentation is raised, we see point-to-point encryption and tokenization becoming more valuable scope reduction strategies.

- **Point-to-point encryption** – Encrypts card data at the point of swipe and maintains that encryption all the way to the processor such that the merchant cannot ever decrypt the data. Use of point-to-point encryption remains one of the most effective ways to reduce PCI scope.
- **Tokenization** – Reduces the footprint for cardholder data loss by transforming cardholder data into data that cannot be used by attackers to perpetrate credit card fraud.

Merchants and service providers alike will need time to address these new requirements and expanded scoping. Nevertheless, those entities that are able to implement the new rules effectively can gain competitive advantage and ensure better protection of personal payment information, as well as avoid serious reputational harm caused by unauthorized exposure of customers' credit card data.

Those companies that are still working on gaining compliance to PCI DSS 2.0 should realign their efforts to PCI DSS 3.0 at their earliest convenience.

We will be watching for further developments on the new standard and will issue updates as new information is released. In addition, we are hosting a webinar on Wednesday, November 13, at 1:30 p.m. EST, 10:30 a.m. PST, during which Protiviti Managing Directors Scott Laliberte and Jeff Sanchez will discuss recent changes and upcoming developments in the PCI data security standards and their impact on companies. Register here.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that helps companies solve problems in finance, technology, operations, governance, risk and internal audit. Through our network of more than 70 offices in over 20 countries, we have served more than 35 percent of FORTUNE 1000® and FORTUNE Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies.

Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

About Protiviti's PCI DSS Compliance Services

As the business world's communications and commerce become more electronically integrated, activities and technology assets require more protection. Security threats, vulnerabilities and information exposures challenge every organization today, creating risks that must be controlled and managed. Often, organizations do not know what risks they face or how they will manage them in the event of a security breach.

Protiviti (www.protiviti.com/PCI) provides a wide variety of security assessment, architecture, transformation and management services to help organizations identify and address potential security exposures (e.g., loss of customer data, loss of revenue, or reputation impairment to a customer) before they become problems. Our professionals apply industry standards and tools to identify gaps in architecture and processes that pose risks. In the event of an incident, we can assist management to identify the source, reduce the risk, and remediate the exposure.

Protiviti holds the PCI Security Council's Qualified Security Assessor (QSA), Payment Application Qualified Security Assessor (PA-QSA), and Approved Scanning Vendor (ASV) certifications. In addition, Protiviti is a PCI Forensic Investigator (PFI). Fewer than 2 percent of PCI assessors hold all four certifications. We hold global certifications for QSA and ASV, and U.S. certifications for PFI and PA-QSA.

Contacts

Rocco Grillo
Managing Director
+1.212.603.8381
rocco.grillo@protiviti.com

Scott Laliberte
Managing Director
+1.267.256.8825
scott.laliberte@protiviti.com

Mark Lippman
Managing Director
+1.571.382.7807
mark.lippman@protiviti.com

Ryan Rubin
Managing Director
+44.207.389.0436
ryan.rubin@protiviti.co.uk

Jeffrey Sanchez
Managing Director
+1.213.327.1433
jeffrey.sanchez@protiviti.com

Cal Slemp
Managing Director
+1.203.905.2926
cal.slemp@protiviti.com

Michael Walter
Managing Director
+1.404.926.4301
michael.walter@protiviti.com

protiviti®
Risk & Business Consulting.
Internal Audit.