February 24, 2011

PCI-DSS Version 2.0: What do I need to know?

By Kathy Argall
Associate Auditor of Candela Solutions LLC

The Payment Card Industry (PCI) Council issued version 2.0 of the Data Security Standards (PCI-DSS) entitled *Understanding the Intent of the Requirements* in October 2010. Organizations that need to comply with the standard can relax as the changes are relatively minor, but they are still worth understanding. The PCI Council divided the changes into 3 types; clarification, additional guidance, and evolving requirement.

"Using PCI-DSS as a basis for your security program means that customers can have confidence in doing business with you. This in turn protects and strengthens your reputation with business partners."

Clarification

Further details are offered to clear up misunderstandings as to the intent of the requirements. These clarifications do not change the intent of the requirements but provide additional information and more explicit wording regarding the requirements. A significant number of clarifications were made throughout version 2.0. In most instances, the end result was a minor wording change to clear up ambiguity as to the controls necessary to fulfill the requirements.

There are a couple of clarifications worth mentioning, such as the applicability of PCI-DSS. Version 2.0 specifically states that the primary account number is the "*defining factor in the applicability of PCI DSS requirements*." If a primary account number (PAN) is not collected, managed, or transmitted, the requirements do not apply. For example, if your organization retains cardholders' name and address but not the PAN, PCI-DSS does not apply.

In version 1.2, requirement 3.2 indicated that sensitive authentication data, i.e., magnetic strip data, PIN or CAV2 data, was not to be stored. Version 2.0 recognizes that there are instances when issuers have a legitimate business reason for retaining this data. In those cases, the requirement indicates the data should be stored securely.

Another noteworthy clarification in version 2.0 was the scope of requirements 3.3 (masking of PAN data) and 3.4 (rendering PAN data unreadable when stored). These requirements only apply to the account number. If information such as cardholder name, service code, or expiration date is processed, they need to be protected in accordance with all PCI-DSS requirements, except for sections 3.3 and 3.4 which only apply to the PAN. So, cardholders' name can be displayed or stored in clear text.

Additional Guidance

The additional guidance improves the understanding of particular issues. In this case, the new version provides 'additional guidance' for defining the scope of the cardholder data environment (CDE). The cardholder data environment is the portion of the network storing cardholder data or sensitive

authentication data. Version 2.0 of PCI-DSS indicates that organizations should confirm the accuracy of their scope annually by identifying all locations and flows of cardholder data. This scope evaluation is suggested to ensure the cardholder data environment is accurately defined.

The PCI Council through Version 2.0 suggests the following to complete this evaluation:

- The entity identifies and documents the existence of all cardholder data in their environment.
- Once all locations of cardholder data are identified and documented, the entity uses the results to verify that the PCI-DSS scope is appropriate.
- The entity considers any cardholder data found to be in scope for the PCI-DSS assessment. In addition, the related system components are considered part of the CDE.
- The entity retains documentation that shows how PCI-DSS scope was confirmed. Also, results are displayed for assessor review and/or for reference during the next annual PCI SSC (PCI Security Standards Council) scope confirmation activity. The importance of capturing the scoping and results documentation can't be overemphasized. It's critical to document that your team has conducted the assessment.

Another notable change under the type "Additional Guidance" is the expanded definition of system components to address virtual systems. The new version indicates that if virtualization is implemented, all virtual network components, servers or applications within the virtual CDE are considered in scope for the review.

The PCI-DSS requirements apply to each virtual system component. Therefore, virtualized components can effectively be regarded as separate hardware. When operating a virtualized environment, ensure clear segmentation of functions and networks that have different security levels as well as segmentation of test versus production environments. Virtual configurations should be secured such that vulnerabilities in one function cannot impact the security of other functions.

If your organization captures and stores card information in the cloud then this issue is complicated even more. You can use a cloud environment and be PCI-DSS compliant; however, it is critical to verify that your vendor has clearly defined the scope of the CDE and to assess the controls in the cloud cardholder data environment. In some cases the implementation uses a separate payment gateway provider to process cardholder data. Since this is not the same as a cloud environment, this type of implementation is often recommended to minimize the complexity of implementing PCI-DSS.

Evolving Requirement

Evolving requirement changes are made to ensure the standard stays up to date with emerging threats and best practices. While the other two categories serve largely to clear up misunderstandings, this category can represent actual changes to the intent or implementation of the requirements.

Requirement six of the PCI-DSS standards is to "*Develop and maintain secure systems and applications*". The previous requirement to identify and address new vulnerabilities has been expanded to encourage the prioritization of the vulnerabilities to ensure the most critical issues are addressed first. Version 2.0 of PCI-DSS requires prioritization in section 6.2 after June 30, 2012 and it's a recommended best practice until then.

The importance of maintaining compliance with these standards has not changed. Using PCI-DSS as a basis for your security program means that customers can have confidence in doing business with you.

This in turn protects and strengthens your reputation with business partners. It only takes a single incident to severely damage your reputation and your ability to conduct business. Don't make the mistake of thinking it won't happen to you, protect your company now. PCI-DSS version 2.0 is a good step forward and we encourage our readers and clients to embrace this refined standard.

*****

In MEMORY of Kathy Argall. She is missed by all of us at Candela Solutions.

Candela Solutions LLC is a strategic CPA firm in providing services to US public companies that external auditors cannot due to independence concerns. Visit our website at www.CandelaSolutions.com

This is an article reprint from the Governance Issues™ Newsletter, Volume 2011, Number 1, published on February 24, 2011