PCI DSS Compliance in the Cloud – A Primer on New Guidelines

Michael Peters | July 18, 2011

The PCI Security Standards Council's Virtualization Special Interest Group recently published its "Information Supplement: PCI DSS Virtualization Guidelines"(the "Guidelines") to Version 2.0 of the PCI Data Security Standard ("PCI DSS"). The Guidelines provide context for the application of the PCI DSS to cloud and other virtual environments, and offer at least three critical reminders:

- The PCI DSS applies to cloud environments without exception;
- Critical analysis of the application of the PCI DSS to rapidly evolving cloud offerings is essential to compliance; and
- Cloud providers must be prepared to document and contract for necessary controls.

Although the application of the PCI DSS to cloud and other virtual environments is not controversial, the guidelines make clear that unquestioning reliance on a vendor's assertion that it is PCI compliant may be inadequate and risky. Of course, failure to comply with the PCI DSS not only increases the risks to sensitive customer payment card data, but may also jeopardize a merchant's ability to process credit card transactions.

Speaking the Same Language

The guidelines include high-level vocabulary and technical advice, cataloging common components of virtualized environments and identifying those that are likely to be "in scope" for purposes of the PCI DSS. The guidelines also identify key risks unique to virtual and cloud environments. For example, the consolidation of resources inherent in all virtual environments increases the damage that may be caused by a single point of failure, such as the misconfiguration of the hypervisor in a public cloud which exposes the virtual environments of multiple customers. The guidelines include a number of recommendations and suggested best practices, most of which focus on the critical need to understand the precise technical operation of each virtual environment and its treatment of cardholder data as essential first steps in assessing PCI DSS compliance. Importantly for cloud offerings, the guidelines emphasize the need to ensure that the service offering enforces administrative, process and technical segmentation to isolate each customer's environment from those of other entities. The council recommends that this isolation encompass, at a minimum, all PCI DSS controls, including segmented authentication, network and access controls, encryption and logging.

A High Standard

The guidelines would hold cloud providers to a higher standard. One example would be the requirement to inform customers of the limited access allowed into the cloud's shared infrastructure. Moreover, the inherent risks of shared environments require the implementation of "more stringent preventive, detective, and corrective controls" to offset the additional risk that a public cloud, or similar environment, may introduce. Notably, the document concludes by indicating that "…these challenges may make it impossible for some cloud-based services to operate in a PCI DSS compliant manner." As a result, the guidelines put the burden of proving compliance squarely on the cloud provider and require "rigorous evidence of adequate controls." In particular, the guidelines state that "…the cloud provider should be prepared to provide their hosted customers with evidence that clearly indicates what was included in the scope of their PCI DSS assessment as well as what was not in scope. Other details that need to be provided include:

- Details of controls that were not covered and are therefore the customer's responsibility to address in their own PCI DSS assessment;
- Details of which PCI DSS requirements were reviewed and considered to be "in place" and "not in place";
- Confirmation of when the assessment was conducted."

These recommendations are important for contract drafting purposes, but the guidelines also will be helpful to those seeking to assure compliance with Nevada's 2010 amended law on the security of personal information, which requires that merchants doing business in Nevada and accepting payment cards must comply "…with the current version of the Payment Card Industry (PCI) Data Security Standard, as adopted by the PCI Security Standards Council." To facilitate compliance, the Guidelines include an appendix summarizing the 12 PCI DSS requirements, and providing a detailed list of virtualization considerations for each.

Lifting the Burden

PCI compliance is one of the core tenants of CrossView Security Services. We are experts in commerce security and compliance. Because of our unique position in the industry, your organization has the opportunity to leverage this expertise lifting the burden imposed by your auditors.