Media Contacts

Laura K. Johnson, Ella Nevill
PCI Security Standards Council
+1-781-876-6250
press@pcisecuritystandards.org
Twitter @PCISSC

Payment Card Industry
Security Standards Council, LLC

401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

PCI SECURITY STANDARDS COUNCIL PUBLISHES PCI DSS VIRTUALIZATION GUIDELINES

—Resource provides guidance for implementing PCI requirements in virtualized environments; specific recommendations on cloud computing—

WAKEFIELD, Mass., June 14, 2011 —The PCI Security Standards Council (PCI SSC), a global, open industry standards body providing management of the Payment Card Industry Data Security Standard (PCI DSS), PIN Transaction Security (PTS) requirements and the Payment Application Data Security Standard (PA-DSS), today announced the findings of the Council's Virtualization Special Interest Group. The *PCI DSS Virtualization Guidelines Information Supplement* provides guidance to those in the payment chain on the use of virtualization technology in cardholder data environments in accordance with PCI DSS.

The Council developed Special Interest Groups (SIGs) to help clarify elements of the PCI DSS that might be considered challenging, or open to interpretation for stakeholders seeking to secure cardholder data. The use of virtualization technology has been a chief area of interest for organizations considering its implementation in their cardholder data environments and assessors who evaluate virtualized environments as part of a PCI DSS assessment. While it provides many benefits, virtualization also introduces new and unique risks that must be considered carefully prior to deployment.

A product of months of collaborative efforts led by Virtualization SIG Chair Kurt Roemer, Chief Security Strategist, Citrix Systems, Inc, and more than 30 Participating Organizations in conjunction with the PCI Council, the information supplement helps merchants, service providers, processors and vendors understand how PCI DSS applies to virtual environments including:

—more—

- Explanation of the classes of virtualization often seen in payment environments including virtualized operating systems, hardware/platforms and networks
- Definition of the system components that constitute these types of virtual systems and high-level PCI DSS scoping guidance for each
- Practical methods and concepts for deployment of virtualization in payment card environments
- Suggested controls and best practices for meeting PCI DSS requirements in virtual environments
- Specific recommendations for mixed-mode and cloud computing environments
- Guidance for understanding and assessing risk in virtual environments

The supplement also includes an appendix that provides examples of virtualization implications for specific PCI DSS requirements and suggested best practices for addressing them.

“This information supplement provides a more detailed view into the definitions and boundaries where PCI intersects with virtualization,” said SIG Chair Kurt Roemer. “Now merchants can identify the range of questions to ask their providers and then determine the risk mitigation options available.”

The Special Interest Group’s findings highlight that there is no single method for securing virtualized systems. Virtual technologies have many applications and uses, and the security controls appropriate for one implementation may not be suitable for another. Using this resource, organizations can better understand and evaluate their own environments to identify the unique risks virtualization brings to the security of their cardholder data environment, and can plan deployments accordingly.

“Virtualization and cloud computing in relation to PCI have been topics of great interest among our stakeholders,” said Bob Russo, general manager, PCI Security Standards Council. “I want to recognize the Virtualization SIG and the tremendous amount of effort and collaboration that went into creating this guidance. It points to the critical importance of participation from the PCI community in helping us provide resources that help meet our stakeholders’ expectations of securing cardholder data.”

The Council will host a webinar for Participating Organizations and the public that highlights the key findings from the information supplement and how stakeholders can best use this resource within their organizations.

To register for the Tuesday, June 28th session, click here.

To register for the Thursday, June 30th session, click here.

Click to Tweet: PCI SSC releases PCI DSS Virtualization Guidelines http://bit.ly/m6YXAL

About the PCI Security Standards Council

The PCI Security Standards Council is an open, global forum that is responsible for the development, management, education, and awareness of the PCI Data Security Standard (PCI DSS) and related standards that increase payment data security. Founded in 2006 by the major payment card brands American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc., the Council has over 600 Participating Organizations representing merchants, banks, processors and vendors worldwide. To learn more about playing a part in securing payment card data globally, please visit: http://pcisecuritystandards.org.

Connect with the PCI Council on LinkedIn: http://www.linkedin.com/company/pci-security-standards-council
Join the conversation on Twitter: http://twitter.com/#!/PCISSC

###