Media Contacts

Laura K. Johnson, Lindsay Goodspeed
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 COUNCIL PUBLISHES GUIDANCE ON PENETRATION TESTING

— Recommendations to help organizations address top security challenge area —

WAKEFIELD, **Mass**., 26 March 2015 – According to a 2015 report on PCI compliance from Verizon, testing security systems is the only area within the PCI Data Security Standard (PCI DSS) where compliance fell over the past year. Today the PCI Security Standards Council published *Penetration Testing Guidance* to help organizations establish a strong methodology for regularly testing security controls and processes to protect the cardholder data environment in accordance with PCI DSS Requirement 11.3.

Organizations can use penetration testing to identify and exploit vulnerabilities to determine whether unauthorized access to their systems or other malicious activity is possible. It is also a critical tool for verifying that segmentation is appropriately in place to isolate the cardholder data environment from other networks and to reduce PCI DSS scope. Often times, networks considered out of scope are compromised because of poor segmentation methods.

Developed by a PCI Special Interest Group of industry experts, the new guidance aims to help organizations of all sizes, budgets and sectors evaluate, implement and maintain a penetration testing methodology. Best practices address:

- **Penetration Testing Components:** Understanding of the different components that make up a penetration test.
- **Qualifications of a Penetration Tester:** Determining the qualifications of a penetration tester, whether internal or external, through their past experience and certifications.
- **Penetration Testing Methodologies:** Detailed information related to the three primary parts of a penetration test: pre-engagement, engagement, and post-engagement.
- **Penetration Testing Reporting Guidelines:** Guidance for developing a comprehensive penetration test report.

An update to PCI guidance published in 2008, the document also includes three case studies which illustrate the various concepts presented within the document, as well as a quick-reference guide to assist in navigating the penetration testing requirements. The *Penetration Testing Guidance* is available for download on the PCI SSC website here.

“Penetration testing is a critical component of the PCI DSS,” said PCI SSC Chief Technology Officer Troy Leach. “It shines a light on weak points within an organization’s payment security environment which, if unchecked, could leave payment card data vulnerable.”

PCI Special Interest Groups are PCI community-selected and developed initiatives that provide additional guidance and clarifications or improvements to the PCI Standards and supporting programs. As with all PCI Council information supplements, the guidance provided in this document is supplemental and does not supersede or replace any PCI DSS requirements.

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 other standards that increase payment data security. Founded in 2006 by the major payment card brands American Express, Discover, JCB International, MasterCard and Visa Inc., the Council has more than 700 Participating Organizations representing merchants, banks, processors and vendors worldwide. To learn more about playing a part in securing payment card data globally, please visit: 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