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 GUIDANCE FOR MAINTAINING PCI DSS COMPLIANCE

— Guidance provides best practices for merchants to maintain culture of security to protect cardholder data —

WAKEFIELD, Mass., 28 August 2014 — Today, the PCI Security Standards Council, an open global forum for the development of payment card security standards, published guidance on building PCI Data Security Standard (PCI DSS) practices into daily business processes. Developed by a PCI SSC Special Interest Group (SIG) including merchants, banks and security assessors, the *Best Practices for Maintaining PCI DSS Compliance Information Supplement* will help organizations ensure ongoing security for cardholder data.

While adoption of PCI DSS has improved steadily over the years, industry reports highlight the challenge of ongoing maintenance of PCI DSS controls as part of a daily business process, with organizations often viewing PCI DSS compliance as a single annual event and unaware that compliance needs to have a 365 day-a-year focus[1]. Recent breach incidents highlight the danger of this approach and the increasing importance of building a culture of continuous security and vigilance to protect payment card data at all times.

In response to this challenge, the PCI community developed a dedicated Special Interest Group of more than 150 organizations to provide guidance on implementation and ongoing maintenance of PCI DSS as business-as-usual. The information supplement provides practical recommendations for dealing with key challenges in maintaining compliance - such as ever-increasing customer demands, rapidly changing technology and complacence - and offers solutions to help merchants and other organizations prevent pitfalls of compliance fall-off. Recommendations include:

- **Maintain the proper perspective:** Ongoing security of cardholder data should be the driving objective behind all PCI DSS compliance activities, as opposed to achieving a passing compliance report and then subsequently letting security practices fall-off.
- **Emphasize security and risk, not just compliance:** Build a culture of security and allow compliance to be achieved as a consequence.

[1] Verizon 2014 PCI Compliance Report

- **Continuously monitor security controls:** Develop strategies to continuously monitor and document the implementation, effectiveness, adequacy and status of all security controls.
- **Detect and respond to security control failures:** Put processes in place to respond to security control failures in a timely manner.
- **Develop performance metrics to measure success:** Quantify the ability to sustain security practices and PCI DSS compliance by developing a set of metrics that summarize the performances of their security controls.

The *Best Practices for Maintaining PCI DSS Compliance Information Supplement* is now available on the PCI SSC website at: https://www.pcisecuritystandards.org/security_standards/documents.php.

The supplement also includes examples of publically available governance framework resources that can be used to complement PCI DSS controls to enhance the overall effectiveness of an organization's cardholder data security program. Additionally, the document maps out the functional roles typically defined within organizations and provides guidance on associated PCI DSS assessment responsibilities.

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. It provides best practices for maintaining compliance after an organization has successfully completed an initial PCI DSS assessment and supports updates made with version 3.0 of the PCI DSS to help make payment security business-as-usual.

"Building a culture of continuous security and vigilance is vital to meet the intent of the PCI DSS, which is safeguarding payment card data at all times," said Bob Russo, general manager, PCI SSC. "Merchants and others can use this resource to help prioritize payment security as part of daily business processes, not just a once-a-year compliance exercise."

PCI Special Interest Groups are community-selected and developed initiatives that provide additional guidance and clarifications or improvements to the PCI Standards and supporting programs. To learn more about the Best Practices for Maintaining PCI DSS Compliance guidance and to participate in the 2015 SIG selection process, register to attend the PCI Community Meetings: http://community.pcisecuritystandards.org/

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 650 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

###