Media Contacts

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

Security
Standards Council

Payment Card Industry
Security Standards Council, LLC

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

PCI COUNCIL HIGHLIGHTS EXPECTED CHANGES TO PCI DSS AND PA-DSS

—Version 3.0 to focus on flexibility, education and awareness, and security as a shared responsibility—

WAKEFIELD, Mass., 15 August 2013 — Today the PCI Security Standards Council (PCI SSC), an open, global forum for the development of payment card security standards published *PCI Data Security Standard (PCI DSS) and Payment Application Data Security Standard (PA-DSS) 3.0 Change Highlights* as a preview of the new version of the standards coming in November 2013. The changes will help companies make PCI DSS part of their business-as-usual activities by introducing more flexibility, and an increased focus on education, awareness and security as a shared responsibility.

The seven-page document is part of the Council's commitment to provide as much information as possible during the development process and eliminate any perceived surprises for organizations in their PCI security planning. Specifically, the summary will help PCI Participating Organizations and the assessment community as they prepare to review and discuss draft versions of the standards at the 2013 Community Meetings in September and October.

Changes to the standards are made based on feedback from the Council's global constituents per the PCI DSS and PA-DSS development lifecycle and in response to market needs. Key drivers for version 3.0 updates include: lack of education and awareness; weak passwords and authentication challenges; third party security challenges; slow self-detection in response to malware and other threats; inconsistency in assessments.

"Today, most organizations have a good understanding of PCI DSS and its importance in securing card data, but implementation and maintenance remains a struggle – especially in light of increasingly complex business and technology environments," said Bob Russo, PCI SSC general manager. "The challenge for us now is providing the right balance of flexibility, rigor and consistency within the standards to help organizations make payment security business-as-usual. And that's the focus of the changes we're making with version 3.0."

Based on feedback from the industry, in 2010 the Council moved from a two-year to a three-year standards development lifecycle. The additional year provides a longer period to gather feedback and more time for organizations to implement changes before a new version is released. Version 3.0 will introduce more changes than version 2.0, with several new sub-requirements. Proposed updates include:

- Recommendations on making PCI DSS business-as-usual and best practices for maintaining ongoing PCI DSS compliance
- Security policy and operational procedures built into each requirement
- Guidance for all requirements with content from Navigating PCI DSS Guide
- Increased flexibility and education around password strength and complexity
- New requirements for point-of-sale terminal security
- More robust requirements for penetration testing and validating segmentation
- Considerations for cardholder data in memory
- Enhanced testing procedures to clarify the level of validation expected for each requirement
- Expanded software development lifecycle security requirements for PA-DSS application vendors, including threat modeling

Note that these updates are still under review by the PCI community. Final changes will be determined after the PCI Community Meetings and incorporated into the final versions of the PCI DSS and PA-DSS published in November.

The change highlights document with tables outlining anticipated updates is available on the PCI SSC website: https://www.pcisecuritystandards.org/security_standards/documents.php

The Council will host a webinar series for the PCI community and the general public to outline the proposed changes. To register, visit:
https://www.pcisecuritystandards.org/training/webinars.php

“PCI DSS and PA-DSS 3.0 will provide organizations the framework for assessing the risk involved with technologies and platforms and the flexibility to apply these principles to their unique payment and business environments, such as e-commerce, mobile acceptance or cloud computing,” added Troy Leach, PCI SSC chief technology officer.

PCI DSS and PA-DSS 3.0 will be published on 7 November 2013. The standards become effective 1 January 2014, but to ensure adequate time for the transition, version 2.0 will remain active until 31 December 2014.

For more information and to register for the 2013 Community Meetings, please visit:
https://www.pcisecuritystandards.org/communitymeeting/2013/

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 Financial Services, JCB International, MasterCard Worldwide 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