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 RELEASES PCI DSS E-COMMERCE SECURITY GUIDELINES

— PCI Special Interest Group offers guidance to merchants to help secure payments accepted over the Internet—

WAKEFIELD, Mass., January 31, 2013 — Today the PCI Security Standards Council (PCI SSC), an open, global forum for the development of payment card security standards published the *PCI DSS E-commerce Guidelines Information Supplement*, a product of the E-commerce Security Special Interest Group (SIG). Businesses selling goods and services over the Internet can use this resource as a guide for choosing e-commerce technologies and third-party service providers that will help them secure customer payment data and support PCI DSS compliance efforts.

PCI Special Interest Groups (SIGs) are community-driven initiatives that provide additional guidance and clarifications or improvements to the PCI Standards and supporting programs.

In 2012, PCI Participating Organizations selected e-commerce security as a key area to address via the SIG process. More than 60 global organizations representing banks, merchants, security assessors and technology vendors collaborated to produce guidance that will help organizations better understand their responsibilities when it comes to PCI DSS; the risks they need to evaluate when considering ecommerce solutions; and how to determine their PCI DSS scope.

“Take SQL injections as an example. This is not a new attack, and something we’ve known about in the industry for years. Yet it continues to be one of the most common methods by which e-commerce websites are compromised, said Bob Russo, general manager, PCI Security Standards Council. “This can be addressed through simple, prudent coding practices, but merchants often don’t know where to start. These guidelines will help them better understand their responsibilities and the kinds of questions they need to ask of their service providers. In the case of SQL injections, one of the most important items to request of an e-commerce service provider is a description of the security controls and methods it has in place to protect websites against these vulnerabilities.”

The *PCI DSS E-commerce Guidelines Information Supplement* provides an introduction to e-commerce security and guidance around the following primary areas and objectives:

- **E-commerce Overview** – provides merchants and third parties with explanation of typical e-commerce components and common implementations and outlines high-level PCI DSS scoping guidance to be considered for each.

- **Common Vulnerabilities in E-commerce Environments** – educates merchants on vulnerabilities often found in web applications (such as e-commerce shopping carts) so they can emphasize security when developing or choosing e-commerce software and services.

- **Recommendations** - provides merchants with best practices to secure their e-commerce environments, as well as list of recommended industry and PCI SSC resources to leverage in e-commerce security efforts.

The document also includes two appendices to address specific PCI DSS requirements and implementation scenarios:

- **PCI DSS Guidance for E-commerce Environments** – provides high-level e-commerce guidance that corresponds to the main categories of PCI DSS requirements; includes chart to help organizations identify and document which PCI DSS responsibilities are those of the merchant and which are the responsibility of any e-commerce payment processor.

- **Merchant and Third-Party PCI DSS Responsibilities** – for outsourced or "hybrid" e-commerce environments, includes sample checklist that merchants can use to identify which party is responsible for compliance and specify the details on the evidence of compliance.

The information supplement can be downloaded from the documents library on the PCI SSC website at https://www.pcisecuritystandards.org/security_standards/documents.php.

Merchants who use or are considering use of e-commerce technologies in their cardholder data environment, and any third-party service providers that provide e-commerce services, e-commerce products, or hosting/cloud services for merchants can benefit from this guidance. This document may also be of value for assessors reviewing e-commerce environments as part of a PCI DSS assessment.

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.

"E-commerce continues to be a target for attacks on card data, especially with EMV technology helping drive so much of the face-to-face fraud down in Europe and other parts of the world, said Jeremy King, European director, PCI Security Standards Council. "We are pleased with this guidance that will help merchants and others better understand how to secure this critical environment using the PCI Standards."

Those interested in learning more about this guidance and how to use it are invited to join the PCI Council for a webinar on February 7 and 14, 2013. Visit the PCI SSC website for more information and to register: https://www.pcisecuritystandards.org/training/webinars.php.

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 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: 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