

## Media Contacts

Laura K. Johnson, Ella Nevill
PCI Security Standards Council
+1-781-876-6250
<a href="mailto:press@pcisecuritystandards.org">press@pcisecuritystandards.org</a>
Twitter @PCISSC

## PCI SECURITY STANDARDS COUNCIL PUBLISHES SECURITY AWARENESS GUIDANCE

— Resource to help organizations better educate personnel on importance of cardholder data security —

Wakefield, MA., 30 October 2014 – Today the [PCI](#) Security Standards Council, an open global forum for the development of payment card security standards, published guidance to help organizations improve company-wide information security awareness with a dedicated program. Developed by a PCI Special Interest Group, the [Best Practices for Implementing Security Awareness Program](#) information supplement provides recommendations for educating staff on protecting sensitive payment information.

Breach reports continue to point to the critical role that employee security understanding and awareness plays in identifying, protecting against and mitigating data compromise. PCI DSS Requirement 12.6 highlights the necessity for organizations to have a security awareness program in place to educate personnel on the importance of protecting sensitive payment information and how to do so securely.

Developed by retailers, banks, and technology providers, the new guidance can help organizations of all sizes, budgets and industries in this effort by providing detailed recommendations for developing, implementing and maintaining a security awareness program that supports PCI DSS requirements and meets their unique business focus and needs. The *Best Practices for Implementing a Security Awareness Program* information supplement focuses on three key areas:

- **Assemble a security awareness team.** The first step in the development of a formal security awareness program is assembling a security awareness team. The size and membership of the security awareness team will depend on the specific needs of each organization and its culture. This team is responsible for the development, delivery, and maintenance of the security awareness program.
- **Develop appropriate security awareness content for your organization:** A critical aspect of training is the determination of the type of content. Determining the different roles within an organization is the first step to developing the appropriate type of content and will also help determine the information that should be included in the training.
- **Create a security awareness checklist.** Establish a checklist to help when developing, monitoring, and/or maintaining a security awareness training program.

The guidance also includes two appendices organizations can reference in their security awareness program efforts: A sample mapping of PCI DSS Requirements to different roles, materials and metrics, for documenting how PCI DSS requirements could be incorporated into their training program frameworks, and a sample checklist for recording how a security program is being managed.

The *Best Practices for Implementing a Security Awareness Program* information supplement is available for download on the PCI SSC [website](#).

“Whether it’s, POODLE, Shellshock or the latest variant of malware, businesses and employees are exposed to threats every day that can put sensitive information at risk,” said PCI SSC Chief Technology Officer, Troy Leach. “PCI Standards emphasize the importance of people, process and technology when it comes to protecting payment information. This guidance can help businesses focus on the ‘people’ part of the equation and build a greater culture of security awareness and vigilance across their organizations.”

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](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>

###