



PCI SSC broaches possible changes

July 13, 2009

Though the **PCI Security Standards Council (PCI SSC)** has historically resisted major reforms to the Payment Card Industry (PCI) Data Security Standard (DSS), a new partnership to explore possible changes in the use of security technology may signal a shift toward a more flexible approach.

In June 2009, the council revealed it had commissioned the consulting firm **PricewaterhouseCoopers** to research new approaches to the adoption of security technology by merchants, processors and acquirers. The decision comes in light of the growing contention that, for some, compliance with existing standards is too expensive and difficult.

"I'm very encouraged and pleased that ... [PCI SSC members] realize that some additional things need to be put in place," said Paul Rasori, Senior Vice President, Global Marketing for the payment processing vendor VeriFone and Secretary of the **Secure POS Vendor Alliance**.

The SPVA was founded in early 2009 by a group of industry executives seeking to strengthen payment security standards and simplify their implementation. Rasori said the organization was not involved in the PCI SSC's decision to take on its latest project, but that the undertaking reflected the kind of innovations the SPVA aims to help spur.

"Investing in this third-party review is important both from the standpoint of improving security, but also showing the rest of the world that they're open to modifying it to be better for everyone," Rasori said.

The task

Specifically, PricewaterhouseCoopers is charged with identifying and determining the viability of technologies that can reduce and fortify the storage and transmission of consumer card data. The company will recommend to the PCI SSC the technologies considered most likely to improve adoption rates and reduce the costs of implementing mandated security measures.

The PCI SSC has been getting "a lot of pressure from retailers and acquirers to augment the current rules to be more end-to-end in nature," Rasori said. "Pretty much all the PCI

guidelines today are about building walls around your data, but the problem that exists out there is that retailers, merchants and infrastructures are all completely different.

"The decision to protect your data is very unique per retailer, and it's very expensive, so their willingness to look at encryption from the point of swipe all the way through to some end point - which I think is something to be defined as part of this research - will go a long way in helping protect the information in the event that it's breached."

PricewaterhouseCoopers has served as a security and image consultant for a number of Fortune 500 companies, including 15 that are ranked among the world's 25 most profitable firms.

A larger effort

Bob Russo, General Manager for the PCI SCC, said the study's findings would be part of a larger discussion about possible changes to industry standards when the PCI SSC reconvenes later this year.

"The PCI Security Standards Council has commissioned a study ... to research the impact specific technologies have on the PCI [DSS], such as tokenization, Chip and PIN, and end-to-end encryption," he said. "The study's findings will be presented and discussed at the North American and European community meetings this September and October.

"Another major focus at the community meetings this year will be gathering more feedback on PCI standards in a face to face setting from our participating organizations. ... We are always open to feedback from merchants, retailers, processors, banks, [qualified security assessors] and [approved scanning vendors] and are looking forward to a productive discussion," Russo added.