



PCI's EVOLUTIONARY PROCESS

New technologies, business feedback bring new layers of strength

By Richard H. Gamble

It's review time for the data security standards set by the Payment Card Industry Security Standards Council (PCI SSC). Among the likely changes that will affect merchants, processors, and payment service providers will be greater integration of innovative, technology-based security tools like end-to-end encryption, tokenization, and mag-stripe imaging into the process in ways that could streamline compliance and make it easier and less expensive for merchants to comply.

KEY NOTES

- ▶▶ PCI Council is adapting new technologies to the standard and providing guidance on how they might reduce the scope of compliance.
- ▶▶ After commissioning a PwC study and asking interested parties to comment on new standards, the Council is now reviewing data before issuing a report.
- ▶▶ The best data security professionals are smarter than the criminals. "We know how to stop them," says the PCI Council's Bob Russo.



No silver bullets can exempt any party handling sensitive data from PCI compliance, says Bob Russo, PCI SSC general manager, “but each technology brings one more layer that helps to strengthen security. There are 30 or so technologies out there, and we won’t be endorsing any of them, but we will be looking at just what they do and how that should affect compliance.”

If, for example, a merchant or processor adopted a particular technology that did six specific things, that merchant or processor might be deemed to have complied with rules 2, 6, and 8 of the PCI standard and wouldn’t have to provide additional documentation of compliance with those rules, he explains. “We need to map these new technologies to the standard and provide guidance as to how they might reduce the scope of compliance.”

Gathering Intelligence

To get a handle on just how these technologies might interact with PCI standards, the Council commissioned a study by PricewaterhouseCoopers. Some of the findings of that study were discussed at annual community meetings held this year in Las Vegas in September and Prague in October. About 750 merchants, acquirers, processors, compliance professionals, and others most affected by PCI standards attended the Las Vegas meeting, while about 200 showed up for the one in Prague. That PwC study is not available to the general public and won’t be until the Council has had a chance to digest it and issue a summary some time next year.

The Council also invited interested parties to comment, criticize, suggest, and question the PCI standards in a comment period that closed in early November. Several hundred merchants, acquirers, processors, and data security firms provided comments on two key standards. Now the Council will spend six to eight months reading, sorting, and discussing the comments before issuing a report, then presenting the revised standards to the community meetings next fall, Russo explains.

“It was obvious at the last community meeting in Las Vegas that the Council is encouraging and listening to feedback,” says Brad Caldwell, CEO of the data security and PCI compliance firm SecurityMetrics in Orem, Utah. “There were more notifications about this last comment period than I’ve ever seen before. They are doing a good job of reaching out to more interest groups and getting industry leaders to help them shape the standards. This will help merchants with compliance.”

The feedback, both through comments and suggestions made at the community meetings, goes to various working groups who wrestle with how the standard can be improved in response to the feedback and then propose a new and hopefully improved version of the standard. “It’s all done in collaboration with the businesses that have the data that have to be protected,” Russo says.

“The goal is to make the standards robust without making them so draconian that they are difficult to comply with.”

—Bob Russo, PCI Council

Reaching Consensus

The Council oversees three data security standards. Two of them—the all-important Data Security Standard (DSS) and the Payment Application Data Security Standard (PA-DSS)—have two-year life cycles. Every two years they go through the same basic feedback and revision process. A third standard, the PIN Transaction Security Standard, has a three-year life cycle, Russo explains.

PCI and the Council, which has a staff and headquarters building in Wakefield, Massachusetts, are 2006 creations of the five major card brands, Visa, MasterCard, American Express, Discover and JCP. Leadership comes from a five-member Executive Committee, and execution is supervised by a five-member Management Committee, with each card brand



comes a rule so that companies have time to make an orderly transition to the new way of doing things, Russo explains.

The goal is always to reach a consensus, but there are times when a security step is controversial and polarizes those affected into conflicting camps, forcing the Council to act as referee. It's too soon to say, Russo says, whether the current revision process will involve any controversies.

Anticipating what the hackers and fraudsters will do next is not a big problem for the Council, according to Russo. The best data security professionals are smarter than the criminals, he insists. "Most of the attacks come in ways that are well-known," he observes. "The technology like malware is getting more sophisticated, but nine times out of 10, they just use the old, familiar ways of getting the malware into a system. We know where we have to stop them." The large, well-publicized security breaches would never have occurred if the parties had been PCI compliant at the time of the breach, he insists. **TT**

Richard H. Gamble is a contributing writer to Transaction Trends. Reach him at gamble10@earthblink.net.

providing one member of each committee. PCI crafts the standards, but enforcement is left to each card brand, Russo reports.

In addition to the brand-dominated leadership, the Council has some 600 participating organizations that include merchants, banks, processors, security firms, and other interested parties. They handle the data and have to incorporate the standards into practical business operations. "We go to them for the information to evolve our standards," Russo says. The participating organizations choose a 21-member board of advisors, which reports directly to the executive committee about what's working and what is not, he explains.

Besides incorporating emerging security technologies into the standards, much of the revision work involves clarification of just what certain language means at a nitty-gritty operational level.

The community meetings, as usual, featured presentations on standards by Council staff and open forum sessions where people attending would exchange ideas and suggest what needs to be incorporated in the next versions of the standards, Russo reports. "We've read some of the comments already," he says, "but now we have to categorize them, organize them in various buckets, and then figure out how to incorporate them in a revised standard. The goal is to make the standards robust without making them so draconian that they are difficult to comply with."

Many of the changes are small and technical, but when a standard revision is likely to change the way companies fundamentally do business, then complying with that standard is introduced as a best practice about 18 months before it be-

USAePAY
The Payment Gateway with the RIGHT solutions for your merchants.

Solutions
NEXT EXIT →

Solutions For:

- eCommerce/MOTO
- Retail
- Check Processing
- Mobile Processing
- Integrated Terminals
- QuickBooks
- Customer Database/Billing
- Payment Forms/Carts
- Multi-Currency Processing
- Satisfaction Guarantee Program

1-866-490-0042
resellers@usaepay.com • www.usaepay.com