

## Can Mid-Market Merchants Comply with PCI Standards In Time?

If you want to transact business with credit cards, you have to follow the rules: the payment card industry security standards. Companies that don't comply face fines or worse. So why aren't more mid-market merchants already in compliance?

By Michael Jackman

December 06, 2007 — CIO — Nearly a year after TJX Companies suffered what is believed to be the largest identity theft to have hit a retailer, credit card companies are laying down the law for any merchant who transacts business with plastic. By New Year's Eve, all businesses that handle between 1 million and 6 million credit card transactions a year (primarily mid-market companies) must comply with the payment card industry's new Data Security Standard (PCI DSS).

Companies that fail to comply with the standard's 12-point specification risk thousands of dollars in fines (from Visa, \$5,000 to \$25,000 a month), though it's hard to predict what noncompliance will really cost because the penalty structure is complex. Ultimately, Visa, MasterCard and the other payment card companies could revoke merchants' rights to make credit card transactions—a mortal wound for any consumer-oriented business. And yet despite the threat of penalties, experts believe that most mid-size companies won't make the deadline (larger companies with a higher transaction volume are already supposed to be compliant).

Compliance is hardly rocket science—or is it? Directives to use firewalls and change vendor-supplied default passwords are simply security best practices. But in other areas, merchants struggle to interpret the standards, haggling with auditors, consultants and sometimes the PCI Council itself over exactly how to protect cardholder data. And they often have to reach deep into cash-strapped pockets to come up with the funds for conducting a top-to-bottom security review.

Brian Shneiderman, a director at Deloitte Consulting, estimates that 40 percent to 45 percent of merchants might need to overhaul everything from access management, ID control and physical security, to infrastructure, firewalls and antivirus measures.

"The industry is not sitting in a stable position with regard to PCI standards," he says.

### Lessons from TJX

Version 1.1 of the PCI Data Security Standard (PCI DSS 1.1) was on the books in January 2007, when TJX Companies—operator of A.J. Wright, Bob's Stores, HomeGoods, Marshalls and T.J. Maxx—announced that hackers had breached its network. Estimates of the damage vary, but data thieves may have copped anywhere from 45 million to more than 100 million user accounts, from customer transactions going back to 2003.

According to *The Wall Street Journal*, the thieves may have begun their odyssey in a van parked near a St. Paul, Minn., Marshalls store, at which they pointed an antenna and picked up wireless data beamed across the store from registers and handheld scanners. The intercepted data allowed thieves to hack the main network in Framingham, Mass. and allowed them to download megabytes of stored customer records. At least three class-action lawsuits seeking damages on behalf of customers and banks are pending in federal court. (TJX is awaiting court approval of a proposed settlement with customers worth an estimated \$256 million. On Nov. 30, 2007, the company announced a \$40.9 million settlement with Visa through which it would pay banks for their claimed losses, provided banks agree not to pursue further legal action.)

Among the 11 security deficiencies with which TJX was charged: It failed to comply with the PCI standards for data and computer security. This global security standard is a product of the PCI Security Standards Council, created in September 2006 by the five major card brands: American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa. According to Bob Russo, PCI's general manager, the council's main goal was to create "one answer for all five brands." It also seeks to educate companies and has taken on the vital tasks of qualifying and managing the auditors who must certify merchants' compliance (known as qualified security assessors or QSAs), and qualifying approved scanning vendors (ASVs), who test system security by running simulated customer transactions. The council is also building a lab to test and validate the security of pin-entry devices.

Despite any relief merchants may feel by only being held to one merged standard, DSS remains a throbbing toothache for many CIOs in charge of payment card transaction systems. Compliance, verified by stated deadlines, is mandatory. The New Year's Eve deadline looms for full compliance by mid-market merchants. Fines threaten, but it's hard for merchants to predict just what they might cost because they are levied by the individual card companies who have their own rules and rates (Visa may fine one amount and MasterCard another). Complicating matters further, these fines are not directly charged to merchants but to their card-processing banks. The banks then choose to either pass them along, absorb them or, in some cases, even increase them.

Other punitive measures are possible, including having card processing privileges revoked or, as in the TJX example, justification for lawsuits.

Most analysts agree that the majority of companies are not yet certified, though the exact numbers are hard to pin down. In an October news release, Visa announced that 65 percent of the largest merchants had been verified as compliant. Shniderman of Deloitte Consulting puts the level for midsize merchants at only 40 percent to 45 percent.

Payment card industry security standards provide a list of best practices

#### **Build and Maintain a Secure Network**

- Install and maintain a firewall.
- Change vendor-supplied defaults for system passwords and other security parameters.

#### **Protect Cardholder Data**

- Protect stored transaction data.
- Encrypt data transmitted across open, public networks.

#### **Maintain a Vulnerability Management Program**

- Keep antivirus software updated.
- Develop and maintain secure systems and applications.

#### **Implement Strong Access Control Measures**

- Restrict access to cardholder data by business need-to-know.
- Assign a unique ID to each person with computer access.
- Restrict physical access to cardholder data.

#### **Monitor and Test Networks**

- Track and monitor all access to network resources and cardholder data.
- Regularly test security systems and processes.

#### **Maintain an Information Security Policy**

#### **Common Sense Standards**

So merchants have little choice. But how good is the standard and how bad are the obstacles to achieving the sought-after verification? Hans Keller, CTO since 1999 of the National

Aquarium in Baltimore, says that most of the requirements are common sense. "A lot of pieces of PCI are things you should be doing." The PCI council's Russo concurs. "There really isn't anything mysterious about these standards. They are all security best practices."

Those who gritted their teeth over earlier standards, such as Visa's Account Information Security and Cardholder Information Security Program, or MasterCard's Site Data Protection—and who then found the first version of the PCI security standard confusing—should at least find the latest incarnation much improved. Russo says that among the issues solved by version 1.1 are inconsistencies in terminology and language. For instance, words like the vague "periodically" and "regularly" have been replaced with specifics, such as annually, quarterly and monthly. Other changes ironed out distinctions between cardholder data, which merchants store and must protect, and data so sensitive that it should never be stored.

### **Implementation Challenges**

Neat as that sounds, don't put away the aspirin yet. Unless you run a large business, you'll face several implementation challenges.

**1. Tight budgets.** While larger companies (which PCI calls Level 1) often have dedicated security resources, midsize merchants may find themselves in that jaw-clenching budget bind.

**2. Complex environments.** Cathy Hotka, a retail technology consultant, says even mid-market merchants may be running more than 500 applications at a time in "highly customized environments with hand-written code" that has been around for years. Old code is often poorly documented, and even small changes are complicated just as they were to fix the Y2K bug. The DSS standards are more comprehensive than replacing two-digit years with four-digit years, and they constantly change. Hotka compares complying to PCI with "fixing the windshield of a plane while it's in the air."

**3. Conflicting interpretations.** Individual auditors may interpret the rules differently. "The auditor you bring in today will tell you something different than the auditor you bring in next week," says The National Aquarium of Baltimore's Keller. Disagreements can arise over the proper way to divide up networks and secure them with firewalls.

### **How One CIO Is Meeting the PCI Compliance Challenge**

Though it qualifies as a small merchant, The National Aquarium in Baltimore (which earns about \$40.5 million in annual revenue) has encountered most of these mid-level difficulties. Reporting to the CFO, Keller oversees an IT staff of 10. He's responsible for application development as well as support for 500 users and 300 PCs. Keller devotes approximately one percent of his annual \$2.5 million IT budget to PCI compliance.

The aquarium's road to compliance began in September 2006, when its merchant bank asked for an update. Merchant banks process payment cards and are the middlemen between the payment card companies and the merchants.

The 12 top-level standards quickly subdivide into finer levels of detail. For instance, Requirement 8: "Assign a Unique ID to Each Person with Computer Access" contains five sub-steps, with step 8.5 divided into 16 more. In response to this requirement, Keller moved his admissions system away from one common "extremely restricted" login used by everyone working the ticket booth, to separate IDs for each employee. Internally, he now tracks users by PC as well as by their job function, so that their network access across the system can be logged. As required by PCI, passwords change every 90 days. Keller also added an intrusion detection system and revised information security policies to make them more easily understandable.

Keller decided to do his own compliance work in-house, but it wasn't his first choice. First he approached consultants specializing in PCI DSS, but he had difficulty finding a firm willing to take full accountability for its decisions.

Many consultants claim to be working on behalf of PCI, but "none of them will sign next to you on your audit questionnaire," explains Keller. "So if they won't stand behind me and sign on the line in case of a breach, why should I pay them any money in the first place?" Keller does use an approved QSA, Fishnet Security, for the quarterly security scans and penetration testing required by PCI for all merchants with more than 10,000 transactions a month. The results are forwarded to the National Aquarium's merchant bank. As the company develops new applications, the QSA consultant will also analyze the code for security compliance as part of the development process. The requirement to test new code has a deadline of June 30, 2008.

When it came to interpreting the standard, one area in which he and the auditors disagreed was with the proper way to secure a proprietary wireless bridge between two buildings.

"Some [auditors] will say even though there's no credit card traffic passing through that it still needs to be segmented off with hardware firewalls. And to me, I cannot see a valid need for doing that when the wireless network itself is proprietary. So I think there are opportunities where the standard can be taken a little bit too far."

Despite the difficulties, Keller seems satisfied with the standard and the process. "PCI gave us a great security checklist and a great place to start. And by going through the 12 different requirements, it allowed us to ensure that we have adequate protection around the data that we have."

### **Never-Ending Deadlines**

You'll never be finished with compliance. Even after your company meets the current standards and sets up the quarterly cycle of scans and reports, you can expect new requirements to address new threats. And with them, new deadlines.

Russo explains that the PCI Council will "make changes in the standard on the fly" as a way of responding flexibly to new threats. How long merchants will have to respond depends on the type of change. A simple patch might be required immediately. Major changes, such as the new Web and enterprise application code audit requirement due June 30, 2008, will get companies a year to 18 months' grace period. "The object of releasing a new standard is not to put anyone out of compliance when we release it," assures Russo.

While penalties are the stick of PCI, brand confidence may be the carrot. In the event of a security breach, you have your customers and your brand suffering a tremendous amount of damage. Or so runs conventional wisdom.

But customer confidence proves to be notoriously fickle. Take TJX. Following its data breach disclosure, the company reported two consecutive, highly successful quarters. To some observers, the fact that TJX has not suffered serious consequences makes the carrot of customer confidence a harder sell. Says Keller: "Think of the PR, especially for an organization like ours. What if we have this huge data breach? Yet here's TJ Maxx, a well-known brand. They have this huge breach and yet they have one of their best quarters ever."

Shniderman cautions IT leaders to be careful of how they interpret TJX's good fortune. "You can read a couple of things into that," he says. "Some consumers are willing to increase their vulnerability to get a good discount," he says.

TJX might have changed their pricing or promotions during the period after the breach, or they may simply have addressed the crisis effectively, continues Shniderman. "If you have a

fraud-compromising event, it's a moment of truth. The trust level goes down significantly if you don't address it well."

Whether or not customer confidence can be managed after a breach, it's a safe bet that no company wants to suffer one. And while PCI DSS 1.1 will not plug all potential security leaks, it's now a necessary cost of doing business.

*Michael Jackman writes frequently about computer security. Contact him at [mjackman@mjfreelancer.com](mailto:mjackman@mjfreelancer.com).*

© 2007 CXO Media Inc.