

## PUTTING PCI INTO PRACTICE

While it is unclear how much it would have cost TJX to comply with PCI and put preventive measures in place, it undoubtedly would have been less than the resulting remediation costs, fines and litigation settlements. The takeaway for similar retailers is that preventive measures clearly hit the bottom line less dramatically than the costs of delaying or ignoring security improvements or compliance.

PCI isn't a radical reinvention of security schema; rather, it's a codification of security best practices, many of which should be used regularly by organizations of any stature. The dozen PCI requirements include such standard security practices as installing and maintaining a firewall, encrypting credit card data when transmitted over public networks, restricting access to sensitive data, routinely testing security measures, and installing and regularly updating antivirus software.

PCI costs are heavily reliant on the security measures already in place before compliance efforts begin. Gartner estimates that Level 1 merchants—those processing more than six million credit card transactions a year—have spent about \$68,000 on average to meet PCI standards. Javelin estimates that 30 percent to 40 percent of PCI compliance spending is dedicated to reprocessing and re-engineering a merchant's security infrastructure and determining where sensitive data is being stored. Documenting compliance efforts and security measures alone consume much of the cost.

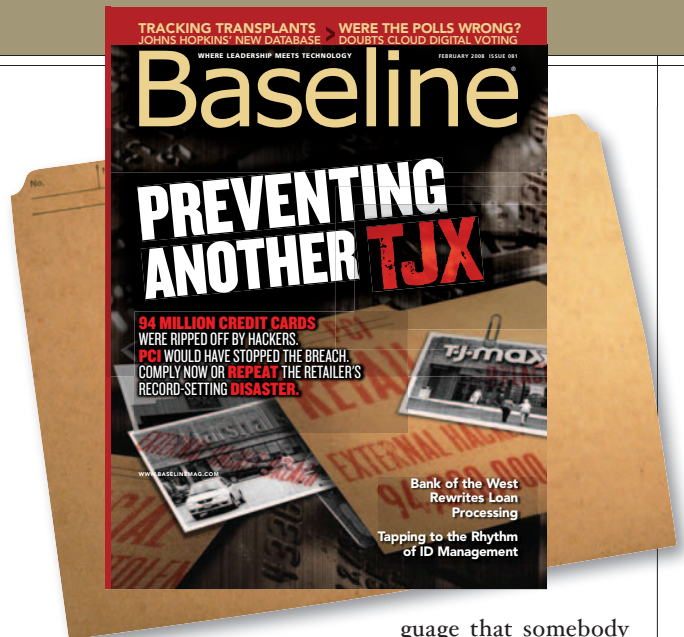
"If you have a basic information security program in place, broadly speaking, you're following what PCI says you ought to be doing, because you've got [a set] of good procedures," says Michael Barrett, chief information security officer at online payment service PayPal, a division of eBay. "Passing PCI is mostly a question of demonstrating compliance. So it's mostly fishing out documentation and making sure that when your operations people run quarterly scans, they keep those logs so you can later show them to the auditors."

This was the case for Hughes Network Systems, which acts as a managed-services provider for BP Corp. North America, Blockbuster, Yum! Brands and other major merchant brands. Hughes' clients demanded the provider adopt PCI standards to ensure their own compliance. Much of Hughes' security infrastructure was already compliant, but certain tweaks needed to be made with transport encryption over untrusted, public networks, says Matt Kenyon, the company's senior director of network operations and security.

"From the main front-door security, if you will, it didn't change much," Kenyon says. "But PCI has some specific mandates about encryption on the actual transport. So we added some new architectures to put further encryption on top of what we already had, and on our base transport, to get up to spec on compliance."

Beyond that, the most resource-intensive part of complying was getting ready for the auditors, a process for which Hughes enlisted the help of IBM security consultants.

"We already had documents and policies and procedures," Kenyon says, "but in order to get through the PCI compliance, what IBM helped us with was putting that into a lan-



guage that somebody outside of our own organization understands. And so it makes the compliance auditing process much easier."

Even with security methods already in place, many organizations have still needed to make major infrastructure changes to meet specific PCI standards. For example, Bwin, a European gambling site, had to rebuild its payment infrastructure to more cleanly organize and segment it from the rest of Bwin's systems. It was an intensive 10-month process.

"We took the whole payment infrastructure out of the Bwin infrastructure and rebuilt it," says Oliver Eckel, Bwin's head of corporate security. "The big challenge was to do it in a PCI-compliant way, which basically was a really big task on the documentation side."

Of course, department stores, restaurants and e-commerce portals are affected by PCI compliance requirements. Also under the PCI umbrella are movie theaters, sports stadiums, museums and hospitals. Even an organization such as the National Aquarium in Baltimore must comply, because it accepts credit cards for tickets, concessions and donations. While caring for aquatic animals is the aquarium's primary mission, PCI gave its IT staff justification for security spending.

"The benefit of PCI is that it usually helps in freeing up dollars for what were perceived as risk points that you couldn't necessarily get the budget for in the past," says Hans Keller, the aquarium's chief technical officer.

Prior to getting a call from the bank about PCI, Keller and his staff had been hoping to pick up a security information management system to fill in some holes within the aquarium's security program, but they couldn't convince management to allocate the cash. PCI changed the situation, and now the organization is running the TriGeo Information Manager System, which greatly aided its compliance effort.

"When you look at the PCI standards, for the most part 90 percent of those things are things that companies should be doing anyway," Keller says. "Most of the areas we were already fairly well compliant with, but there were six or seven areas where we weren't compliant, and TriGeo perfectly plugged all those holes."