

PCI Compliance: Still Work To Be Done

Smaller retailers need your guidance and education on compliance initiatives.

BY BRIAN ALBRIGHT

Retailers, whether they are brick-and-mortar or Web-based, worry about the security of their customers' payment information. Having that data hacked or stolen creates a public relations nightmare and erodes the trust between the merchant and consumer. That's why adopting the Payment Card Industry Data Security Standards (PCI DSS) has become such an important issue when it comes to processing credit card information.

So far, most large retailers are well on their way to full PCI compliance, but there are opportunities for VARs to help small and midsize retailers (who are largely behind the curve) achieve compliance. "Despite the uptick in compliance validation, the majority of small and medium enterprise merchants remain at risk for account data compromise because those merchants still use legacy systems to store card data," says Rick Allen, director of partner compliance at Payment Processing, Inc. (PPI).

These smaller merchants require guidance and education to achieve compliance. "PCI is like an insurance policy against data breaches and should be considered an essential part of conducting business," says Marianne Rocco, director of marketing and communications at Merchant Warehouse. "VARs and independent software vendors (ISVs) should become the go-to place for their merchants when it comes to understanding PCI requirements."

VARs can help by partnering with a PCI security vendor that can deliver a range of solutions, from self-assessment questionnaire (SAQ) wizards to comprehensive on-site assessments. VARs can also help smaller merchants find ways to limit their exposure and the scope of their required assessments. "PCI DSS services

are really treating the symptom rather than the cause when it comes to merchant compliance," says Robert Cortopassi, senior VP of product development at Accelerated Payment Technologies. "Providing technology solutions that directly impact the merchant's security environment is much more effective at reducing risk and limiting the scope of an assessment."

VARs should also evaluate their own processes and products in the context of compliance. "Resellers should complete the SAQ to ensure they understand the PCI requirements," says Lucas Zaichkowsky, senior compliance technologist, Mercury Payment Systems. "Setting up merchant systems in a noncompliant fashion can introduce risk and liability."

Small Merchants Pose A Challenge

One of the major problems with PCI compliance among smaller merchants is that they either dismiss the need for compliance altogether, or assume because their point of sale software is compliant, that they don't need to do any more work to secure customer data. VARs should approach these clients with a full-blown compliance program, not just a software or hardware fix.

"The first common mistake is buying into a false sense of security that 'it can never happen to me,'" says Rocco. "The second common mistake is thinking that their business is too small to attract hackers. And the third common mistake is that they do not have a shopping cart business (i.e. a website), so they aren't really at risk."

VARs should determine if these merchants have a firewall in place, password-protected systems installed, and the extent to which employees have access to card data.



MARIANNE ROCCO,
DIRECTOR OF MARKETING
& COMMUNICATIONS



ROBERT CORTOPASSI,
SENIOR VP OF PRODUCT
DEVELOPMENT



LUCAS ZAICHKOWSKY,
SENIOR COMPLIANCE
TECHNOLOGIST



RICK ALLEN,
DIRECTOR OF PARTNER
COMPLIANCE



From there, they have to get the merchant to move beyond the technology-only side of compliance. “Merchant compliance depends as much on providing employee education, restricting data access to those with a business need to know, and managing in-store antivirus and firewall systems as it does on selecting the right POS application or purchasing a compliant PIN pad,” Cortopassi says.

The SAQs are used by merchants and service providers that are not required to undergo an on-site assessment under the PCI DSS procedures. Both merchants and VARs should take these assessments seriously. “Should the merchant get breached, the forensic auditors are going to take a hard look at compliance of each and every requirement at the time of breach,” Zaichkowsky says. “Large merchants processing more than 1 million transactions per year will need to hire a Qualified Security Assessor [QSA] to validate their compliance on-site. If they became compliant and used the SAQ to self-validate, the validation performed by the QSA will likely go more smoothly.”

Online Retailers Also Require Compliance

E-tailers present some special challenges when it comes to PCI compliance, but the solutions they require largely mirror those used by their brick-and-mortar cousins. “E-commerce merchants typically rely more on outsourced solutions such as shopping carts/content management systems, hosting companies, and open source technologies, and need to pay special attention that the solutions they are using are validated and secure,” Rocco says. “Some minor differences include the need for supplemental security controls for POS systems that access the Internet, as well as limiting Web access to employees.”

There are noncompliant shopping cart systems and online ordering systems on the market, so VARs and merchants should take care to evaluate these vendors. “These systems slip past mandate requirements because the payment gateway is specified as the ‘payment application’ when asked by their processor about compliance,” Zaichkowsky says. “Thankfully, there are a few fully PCI-compliant systems and providers out there. They are raising awareness through market pressure.”

Another issue for PCI is the increased interest in mobile solutions, in which customers can use their smartphones or other devices to conduct business. While mobile payments aren’t officially part of the current standard (PCI will address these payments specifically next year), merchants can still ensure mobile payment security by adhering to PCI’s guidance. “A merchant who is interested in mobile payment acceptance should seek out those vendors who are proactive in complying with the data security standards, submit their mobile payment applications for PA-DSS assessment, and remain deeply committed to security,” Cortopassi says.

Reduce Scope Of PCI Compliance Needs

One way to help smaller merchants with compliance is to reduce the scope of the affected systems by removing sensitive transaction information from the POS system. By reducing the number of vulnerable points in the card data environment, the likelihood of a breach is reduced. “This may mean implementing point-to-point encryption through sophisticated payment applications, segregating the point of sale devices from other computers on the network, limiting or eliminating the use of wireless networking, or using a tokenization provider to outsource sensitive cardholder data which may be desired for reuse or analytics,” Cortopassi says.

Web-based applications can also remove all credit card data from the POS system, which can minimize the cost and headaches associated with merchant-level

PCI compliance. “These solutions do require an investment of time and money,” Zaichkowsky says. “But, when you compare that to the time and cost of meeting all the PCI DSS requirements with all systems at all times, the investment seems worthwhile.”

Scope reduction doesn’t remove the need for compliance. “Even companies who use POS systems/services that are deemed out of scope must implement them in a PCI-compliant manner,” Allen says. “The biggest drawback of scope reduction is when merchants believe that reducing the scope frees them from having to be compliant. Even if the system doesn’t store card data, a number of data compromise incidents occur because malware or key loggers can intercept card data before encryption.”

Focus On PCI Education

With the release of PCI DSS v2.0, PCI has cleared up some confusion in the previous standard that should help merchants complete their audits without as much ad hoc interpretation of the standard. No other major upgrades are expected until 2014, so smaller merchants may face additional scrutiny, particularly since smaller retailers have suffered more data breaches as of late.

For VARs hoping to take advantage of opportunities presented by PCI compliance for smaller retailers, the vendors interviewed for this story encourage resellers to combine education with a risk-based approach to compliance. VARs can be one-source providers that offer technology, merchant acquiring, and PCI assistance programs that can help small merchants improve data security.

“Understand that PCI compliance can’t be purchased with one product or technology,” Allen says. “Educate your customers that compliance only represents a point in time; the real problem to solve is how to implement effective security at the network, host, and application levels without adding complexity. VARs who take responsibility to implement secure technology can facilitate the merchant’s compliance with PCI DSS and become a trusted partner.” ●

“PCI compliance can’t be purchased with one product or technology.”

RICK ALLEN, PAYMENT PROCESSING, INC.