

Q&A: Cash In On PCI Compliance Opportunities

As the July 1, 2010 PCI (payment card industry) deadline looms, VARs and ISVs (independent software vendors) are presented with a great, yet time-sensitive, business opportunity.

BY MIKE MONOCELLO

What trends are you seeing with ISVs concerning the July 1, 2010 deadline?

Sean Kramer, president and CEO, Element Payment Services: First, PA-DSS (Payment Application Data Security Standard) was launched with a two-pronged approach: one targeting new merchants, or merchants that switch processors, and the other targeting merchants that have been processing on the same platform before the adoption of PA-DSS (these merchants were grandfathered in). On Oct. 1, 2008, newly boarded Level 3 and 4 merchants were required to be PCI DSS-compliant or use PA-DSS-compliant applications. The July 1 date is significant because it will require all merchants (not just those who switch processing providers) to use only PA-DSS-compliant payment applications or software applications that are out of scope.

We're seeing two separate scenarios with our ISV partners. ISVs with large merchant customers are being driven to provide PA-DSS-validated or out-of-scope enterprise management applications. The reason for this is that larger merchants are receiving pressure from either their merchant service providers (MSPs) or the card brands (Visa, MasterCard) to validate PCI DSS compliance. Large merchants understand that they themselves cannot be PCI DSS-compliant if the payment applications they are using are not validated for PA-DSS compliance. These merchants are also looking to their ISVs to help reduce the scope of their own PCI DSS compliance requirements through tokenization, encryption, and hosted processing technologies. For example, when ISVs elect to employ tokenization and

remove cardholder data storage from their software applications, merchants using these applications qualify to answer a shortened version of the Self Assessment Questionnaire (SAQ C vs. SAQ D), which essentially eliminates the need for the merchant to answer more than 180 additional questions geared towards the controls around cardholder data storage.

In the second scenario, ISVs aren't receiving the same pressure from customers because of merchant size. Smaller merchants haven't yet felt from MSPs or the card brands the same pressure to prove compliance as their larger merchant counterparts and therefore, aren't demanding compliance from ISV providers yet. And, unfortunately, many of these ISVs are still in denial. They are either choosing not to believe that PA-DSS requirements apply to them or that the July 1 date will have no implications for their customers. It's unfortunate for merchants who will no longer be "grandfathered in" after the July 1 deadline and will risk fines and/or lose their ability to accept credit cards as a form of payment.

What risks does a VAR face by selling noncompliant software?

Chuck Riegel, executive VP, Payment Processing, Inc.: Recent cases involving compromised payment card data are naming the VAR who sold and installed the system. The VAR is no longer immune from financial risk and loss when the customer organization suffers a compromise of payment card account data. Customers using stand-alone, integrated POS (point of sale) or e-Commerce solutions expect that their software purchase is secure when, in fact, it's an accident waiting to happen because the VAR has sold non-validated software and installed it without the most basic security controls necessary to keep customers from harm's way. Recent forensic cases of compromised card data clearly show that the majority of VARs are simply unaware that their actions (or lack of action) put the customer in peril rather than protecting the organization.

Additionally, compliance does not mean one is secure. VARs are in a great position to become a trusted advisor to businesses relying upon the VAR's expertise to keep safe. To remain secure relative to risk, all stakeholders need to understand that security is a continuous process not a "set-it-and-forget-it" task. Once the VAR helps an organization become compliant, they



SEAN KRAMER,
PRESIDENT & CEO



CHUCK RIEGEL,
EXECUTIVE VP



LUCAS ZAICHKOWSKY,
SENIOR COMPLIANCE
TECHNOLOGIST



have reasonable assurance that basic security controls are in place to protect them; however, it only takes a mouse click or change in setup to immediately become noncompliant and at risk. Resellers add real value when they have the right people, processes, and technology in place to maintain security.

Once the July 1, 2010 deadline passes, will VARs and ISVs still have to spend time and resources on PCI?

Lucas Zaichkowsky, senior compliance technologist, Mercury Payment Systems: Trying to secure every merchant system and network to all PCI requirements may always be an uphill battle. Merchant systems will always deal with malware and hacking incidents. As long as there is card data passing through the system in plain text, they will be heavily targeted by criminal hackers all over the world stealing card data from business systems.

It's much easier and safer for ISVs and VARs to deploy encrypting card readers, keypads, and PIN pads supported by the payment processor. The advantages to this strategy are that ISV and VAR involvement and liability is significantly lowered, and merchants can focus on addressing other security points, such as employee skimming, and making sure any third-party companies handling card data (e.g. online ordering) for them are compliant.

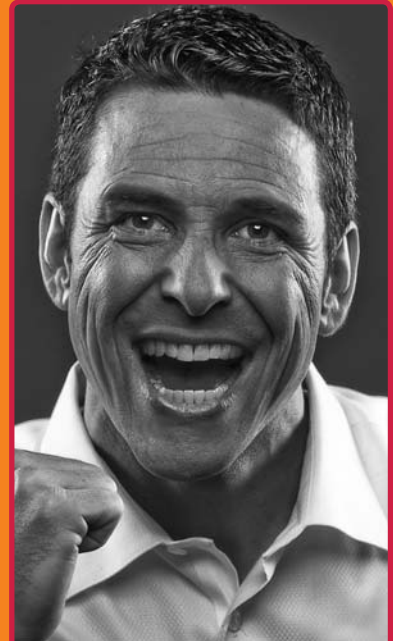
Additionally, one of the most misunderstood and underestimated PCI DSS requirements is requirement 12, "Maintain an Information Security Policy." A policy is designed to specify "what" is being accomplished. Procedures spell out "how" policies are implemented. All businesses need policies, procedures, and the will to follow them consistently. PCI DSS compliance can only be maintained as a business operates by following procedures designed to maintain compliance as set forth by a policy. Even companies that are validated can fall out of compliance easily by not adhering to their policies and procedures. This is how PCI-validated companies can end up being compromised. Historically, small businesses that have lost card data have paid an average of \$36,000.

What should VARs be doing in the short time remaining until the deadline?

Riegel: First, have a plan with your ISVs to ensure that a validated version of the software is available. Second, install the system per the secure implementation guide, paying particular attention to the following areas from which a number of compromise cases resulted:

- Microsoft Windows systems ship with default settings and unnecessary services. Take proactive responsibility for applying critical security updates and patches.
- Unsecured remote access, running RDP (remote desktop protocol) and/or VNC (virtual network computing)-type remote access methods, are rife with vulnerabilities that are easily exploited.
- Failure to securely delete previous installations of software that leave card data unprotected. Use secure delete software to wipe the system prior to the new install and going live in production.
- Lack of antivirus software and automated updates to protect from common forms of malware, including key loggers and sniffers designed to harvest payment card data.

Third, make sure your customer understands that three things must be in place to make them PCI-compliant: use of a validated payment application, passing a quarterly PCI security scan, and filing the appropriate version of the self-assessment questions. Make sure that your payment processor and/or acquiring bank has a record of these actions. Failure to do so places your customer at direct risk of maintaining consumer goodwill and becoming a compromised merchant that's liable for costs associated with forensic reviews and noncompliance fines. ●



Why do three out of four Avaya partners trust Catalyst Telecom with their business?

Because no matter what challenges they face, we've got a solution for that.

There's never been a better time to become an Avaya partner. And if you're ready to grow with Avaya's innovative product line, there's no better partner than Catalyst Telecom. Take advantage of our powerful lineup of resources designed to help you succeed, including our Avaya Enterprise & SME certification trainings.

Download our Avaya Solutions Guide at www.catalysttelecom.com/avaya. If you're ready to grow with Avaya, we've got a solution for that!



CatalystTelecom.

We've got a solution for that.™

|800.790.2029|