

Compliant... *and*

PCI compliance represents only the first step in the constant quest for data security

By Richard H. Gamble

After several years of high-profile data security breaches, electronic payments professionals are reminding any less-vigilant peers that risk management is an ongoing process. Becoming PCI compliant is only the first step in an ever-evolving challenge.

The focus going forward should be a more broad focus on data security, not just PCI compliance, says Phil Neray, vice president for strategy at Guardium in Waltham, Massachusetts. "You can be compliant but not secure. The PCI specs are pretty detailed, but they can't cover everything, and there's a lot of interpretation involved."

For example, Requirement 10 says you must track and monitor all access to cardholder data, he explains. But how often do you look at the logs? And do you monitor activity, occasionally or continuously? Manually or automatically?



Secure

KEY NOTES

- ▶ Over the past several years, PCI compliance has gone a long way in improving the security of cardholder data and is now a core part of the business process. But it's only one step of ongoing risk management.
- ▶ Ensuring security requires vigilant people, solid processes, tighter standards, reengineering architecture, and more.
- ▶ Most businesses are trying to balance what it takes to secure data with what it takes to sell and service an account profitably.
- ▶ Whatever the business case for spending on data security, selling data security services is a powerful opportunity for ISOs.

“Those are conversations management teams need to have,” Neray says. “You can’t rely on auditors for the PCI organization to tell you what to do. Your own data security people are better positioned to know your exposures and what you need to do about them.”

Complying with PCI standards has been a huge step toward achieving data security. “PCI has laid a good foundation,” says Michael Petitti, chief marketing officer at Trustwave, a provider of data security services. “It has done a lot in five or six years to improve the security of cardholder data. It’s no longer an ad hoc component but a core part of the business process.”

But it is only a step. “PCI compliance is a snapshot. If an auditor examines your data security provisions and finds them compliant, then you are compliant at that moment but not necessarily the next week or the next month,” reminds Greg Cohen, president of Moneris Solutions Inc. in Chicago. “We’ve learned from experience that there is no safe harbor for data security. If the data are valuable enough, someone will find a way to get them.”

Creating a Plan of Attack

So how does an acquirer, processor, or ISO rise to that next level of data security? After carefully studying PCI SSC’s roadmap to addressing risks in priority order (www.pcisecuritystandards.org), consider these suggestions:

1. Rely on vigilant people. PCI creates a useful policy baseline, but it takes good people to make it operationally effective, says Cliff Gray, an associate at the Strawhecker Group in Omaha, Nebraska. While some companies emphasize systems over people, Gray says it is cheaper and ultimately unavoidable to rely on vigilant people, even if it means paying higher salaries and providing more intensive training. “Systems may be reliable, but someone has to tell them what to do,” he says.

Recent breaches were a result of human error, he says. “Someone fell asleep at the wheel. Data security can get com-

PCI standards are “no longer an ad hoc component but a core part of the business process.”

—Michael Petitti, Trustwave

.....

plicated with a sophisticated infrastructure, a large IT department, and high transaction volume, but the fundamental rule still holds: If you have the right rules and if the people running the network are competent, trustworthy, and follow all the rules all the time, you have a secure network.”

2. Ensure all systems are up-to-date. For many companies, data security still means perimeter firewalls and antivirus programs, goals that have been largely achieved, says Neray. But the firewall concept is 15 to 20 years old and seriously outdated. “In the world of Web 2.0, it’s easy to bypass firewalls and get into databases,” he says.

Firewalls were built to close off internal networks and only allow certain trusted people to get in, but now systems are designed to allow Web traffic to get through. Companies have essentially opened their data centers to customers, business partners, and others on the outside, making firewalls very porous. “A firewall is not smart enough to tell which traffic is legitimate and which is not. For that, you need a system that provides real-time monitoring,” Neray insists.

Due largely to inertia, the vast majority of companies involved with merchant card payments still use manual monitoring, which Neray argues is increasingly inadequate. “The average breach happens in a few seconds,” he notes. “There’s no way a company could block a breach in time with manual monitoring.” Yet de-

spite an attractive payback (six-month ROI over 200 percent) and ease of installation (it could be done over a weekend), automated monitoring has not become a board-level issue at most companies, he claims. In a down economy where companies are looking to automation to reduce the cost of manual processes and looking to shore up fraud protection, going high-tech should be a no-brainer, he insists.

3. Implement tighter security processes.

One way to move beyond simple PCI compliance is to have dual custody over access to critical data. Dual custody means that it takes two keys to open the door and two people to operate the keys. “It’s unlikely that you’d have two people who would work together to commit fraud or ignore it,” Gray points out.

4. Revise systems architecture.

The alternative to spending too much time on constant monitoring is “to rearchitect your systems to make them less vulnerable,” says Donna Embry, senior vice president for strategic product development at Payment Alliance International in Louisville, Kentucky. “If you have four parts of your business that touch card numbers, combine them into a star configuration where you have only one exposure.” That might cost more upfront but less in the long run, not even counting the cost of a breach, she says.

5. Expand your security coverage.

The list of sites to be protected must be enlarged, Petitti says. An online retailer typically has a Web site where credit card payments are accepted, and that Web site now typically would be protected according to the PCI standards. But that retailer may have other public-facing portals that don’t handle credit card payments and have been considered low risk. “We’ve seen cases where someone hacked into a supposedly low-risk portal and used that doorway to gain access to a corporate network and ultimately to stored credit card data,” he reports. “People need to expand their security to all sites and portals.”

6. Shorten and simplify the communications chain.

Five or six years ago, the threat was hackers getting into databases, but companies involved in card payments have moved away from storing sensitive data in databases, so now thieves are more likely to steal data in transit, Petitti explains. "That's why we're seeing more malware," he observes. "The standard will have to evolve to combat that threat. That will be the next challenge for the PCI standard."

"Card numbers, addresses, and bank account numbers are all moving through the current system in the clear," Gray notes. A processor still has to see the card number to route it properly in most cases. Eventually, that will all change with smart cards and end-to-end encryption, he says, but until it does, payment processors will be vulnerable to data breaches. Why not have the merchant send the transaction straight to

the card issuer? That would reduce risk, but it would take a huge rebuilding of the communications infrastructure. "It may happen eventually, but not soon," he concludes.

7. Go after players who are still not PCI compliant.

PCI compliance is still spotty among small (Level 4) companies. "If you're Level 4, you self-assess, which translates into many companies simply saying they're compliant. There's a big enforcement problem, Gray says. "The ISOs are begging, pleading, and demanding that merchants comply, but they're offering them no financial incentive and compliance costs money," so merchants are looking at alternatives like using an intermediary token so the merchant never sees card numbers. "They may conclude that if there are no sensitive data to see, there's no threat of a breach," he reports.

Small merchants have heard from ISOs and acquirers that they have to use a PCI-compliant point-of-sale system, but that probably is not enough, Gray says. Really small merchants, like people selling at craft fairs, create paper slips with card numbers and come back to their homes or offices and manually enter the transactions with their processor through a secure Web portal. As long as they use a PCI-compliant processor and shred the paper slips after they have been entered, that's PCI compliance for this group, he explains.

Fines are too small to get large merchants to comply, but reputation risk is a sufficient motivator for most. For small merchants, a \$5,000 fine could be a backbreaker and might cause them to pay attention to compliance, Gray says.

And, according to PCI SCC chief Bob Russo, a breach can cost 20 times the cost of compliance.



Wanted: ISO Startups

Is someone you know starting up a new ISO?

Transaction Trends wants to know.

A new series will follow several ISOs as they navigate a new startup. Please contact editor Angela Brady at abrady@strattonpublishing.com for more information.

The Payment Gateway with the RIGHT solutions for your merchants.

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

8. Support updated and improved PCI standards. PCI started with data security around merchant transactions, Embry points out, but it will expand to include ATMs and kiosk processing. “The definitions of a ‘merchant’ and of ‘processing’ are expanding to include types of transactions not envisioned in the original PCI concept,” she says.

But because PCI standard-setting is very collegial—involving lots of discussion, buy-in, and consensus—the council needs time to study and update the standard, something done every two years, Petitti notes. Right now, the council is looking at developing standards around emerging technologies.

9. Address the security issues PCI doesn’t cover. Identification validation for online commerce (verifying that buyers are dealing with the sites they think they are dealing with) has important ramifications for cardholder data security but lies outside the scope of PCI, so it’s another exposure that needs to be addressed,

Petitti notes. PCI also doesn’t address breaches caused by cardholder mistakes, like responding to phishing scams, he says. Issuers face a continuous challenge to educate cardholders and encourage them to prevent fraud.

10. Go European. “Eventually, we’ll look like Europe, where cardholders use smart cards and punch in a PIN. It will take years to get there, but that’s what is coming,” Gray concludes.

Making the Business Case

Data security discussions are often framed by absolutes, as if the goal were to prevent all data security breaches and end all fraud. But, at the end of the day, how data are secured is a business decision. Businesspeople understand the law of diminishing returns, Cohen points out. “Is there a silver bullet? Would end-to-end encryption really prevent breaches? Maybe, but would the cost of the prevention be greater than the cost of a few breaches? Most people are trying to balance what it

takes to secure data with what it takes to sell and service an account profitably.”

For banks, the business case for very high levels of data protection is persuasive, which may explain why we’ve never seen a security breach of the firewall at a major processor or bank-owned acquirer, Cohen says. Banks, he notes, have a big stake in maintaining secure systems and protecting their reputations. To find the best data security around card payments, look at the large bank acquirers, he suggests.

Large merchants also see great value in defending their brand and not letting a security breach tarnish their reputations, Petitti says. For small retailers, the cost of not preventing a security breach could be the fine they would pay if they are responsible for one, he explains.

The business case for ISOs depends on how much data they handle, Petitti says. An ISO could concentrate on sales and customer service and never touch the actual card data, but it’s still the responsible party between merchants and processors. If a breach occurs, fines flow from

Learning Anytime, Anywhere

escape

The Aegenis Group's eLearning was developed by both industry and educational experts to provide comprehensive Payment Security training. The CPISM eLearning program consists of 9 modules the learner can complete at their own pace. To assist with interest and retention, each module has interactive elements.

For more information please contact info@paymentsecuritypros.com.

spssp Society of Payment Security Professionals

THE AEGENIS GROUP

the card brand to the acquirer to the ISO to the merchant, he points out. "They still have some risk," he notes.

But a small ISO has much less at stake than a large acquiring bank. "If an ISO is small but growing and just hitting profitability, its owners probably are paying more attention to sales and marketing than data security," Cohen points out. "They have less to spend on data security and less motivation to make the effort," he notes. So rather than build the data security, they take shortcuts or simply refuse to board a merchant that is not PCI compliant.

Even small ISOs that specialize in customer service touch more card data than they may realize, Embry warns. "If you put a new terminal in a merchant location and the merchant pays with his or her card, you touch cardholder data. If you help a merchant with training, you may touch cards and cardholder data in that process. When you take the merchant's bank account number or Social Security number, you collect cardholder data that must be protected.

"Every touch point has its own level of responsibility," Embry continues. "The higher you are in the processing food chain, the more responsibility you have for monitoring all the players below you. You have to see that the chain is safe. You can't use contracts to shift liability."

Selling Data Security

Whatever the business case for spending on data security, the business case for selling data security services is powerful. "This is definitely an opportunity for an ISO to make money," Embry notes. "They can sell solutions that automate processes in secure ways. They can provide insurance that protects merchants from data theft. There are a lot of insurance programs out there. The right terminals and applications can reduce the merchant's exposure and add revenue for the ISO. And it's a real opportunity for processors and equipment manufacturers to come up with solutions that provide greater security. Such improvements would be doing merchants a favor and making more revenue for the

ISO, processor, or manufacturer at the same time."

Data security is an issue that's here to stay, Petitti agrees. No matter what comes—contactless, chip, PIN, mobile—protecting cardholder data will be part of the process. "The ISO or acquirer that can make data security affordable, easy to use, and understandable to laymen will do well," he predicts. "They will have significant value to add that merchants will appreciate."

While data security decisions aren't being driven by economic conditions, the economy is certainly a factor this year. Fraud always increases in a bad economy, Petitti notes.

But although merchants and those who help them accept card payments have also seen a downturn in revenue and are cutting costs, investments in protecting data haven't slowed down, Petitti says. **TT**

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

100%
PCI/DSS Compliant.
Virtual credit card POS gateway.

Available NOW

PERIOD!

- \$79.95 annually.
- No per-transaction based fees AND unlimited use within license.*
- Accept Visa, MC, Amex and Discover.**
- Self Installing internet download & updates.***
- Free API to developers.
- Can be integrated as a seamless back-end gateway into any POS system or operate as a stand-alone application.

Carpé Charge™



PCI/DSS Compliance
Seize the Charge!

Find out more at:
www.carpecharge.com

* CarpeCharge does not charge transaction fees. Only the normal credit card processor fees apply as set forth by the card processor. ** Pending your choice of merchant accounts. *** CarpeCharge requires an annual subscription and a valid merchant account. See your CarpeCharge sales rep or contact CarpeCharge.com for a list of approved merchant processing gateways. CarpeCharge is a Splyce / Payment Pro owned company. All rights reserved.