Reprint courtesy of *NACS Magazine*, free to employees of NACS member companies. E-mail Erin at epressley@nacsonline.com for a subscription.

BITE THE BULLET

PCI compliance — you gotta do it. And recent security breaches at other companies don't change that simple fact.

BY JERRY SOVERINSKY

I suspect the only thing more maddening than watching kindergartners play soccer is being a kindergartner playing soccer.

I attended my nephew's soccer game last month, and his team had fallen mercilessly behind (though the teams didn't officially keep score). During a kicked-shin timeout, my nephew skipped over to his mother, pleading with her to end the humiliation.

"Can we please go home!" he begged.

"Honey, there's still a lot of time left," she replied, feigning optimism. "You're doing great."

"What's the point!" he shot back. "We're still gonna lose!"

"You're doing great," replied my sister-in-law unconvincingly, gently leading my nephew back to the game. "You're doing great."

I thought of my nephew's soccer game as I considered the recent Heartland data breach.

Credit card processor Heartland Payment Systems announced in mid-January that hackers had breached its computer systems in 2008, accessing an untold number of credit card accounts. The company handles an average 100 million transactions each month for 175,000 small- and medium-sized businesses, and investigators are speculating that the size and scope of the compromise could be one of the largest and most severe ever reported (for more on the data breach, visit www.2008breach.com).

MASTERFILE

DID YOU KNOW?

For more information on the basics of PCI compliance, check out "The PCI ABCs" from the September 2008 issue of *NACS Magazine*.

IS THE ENDEAVOR OF BECOMING PCI COMPLIANT AN EXERCISE IN FUTILITY, TOO, ONE DOOMED TO DEFEAT?

To date, separate class action suits have been filed on behalf of consumers and financial institutions.

All of this spells a protracted legal and financial mess for Heartland, as well as untold headaches and expenses for thousands (and perhaps millions) of consumers and businesses. You might question whether Heartland had taken the appropriate data security protective measures — but here's the kicker: At the time of the data breach, Heartland *was* PCI compliant.

As a credit card processor, Heartland was subject to some of the most stringent data security standards, and during its most recent audit in April 2008 — and as reported by Visa — it had "successfully completed an assessment based on the PCI Data Security Standard (PCI DSS)" by Trustwave, a Qualified Security Assessor (QSA) that has helped 30,000 organizations manage their compliance and security protocols.

On paper, Heartland seems to have done everything by the book. And yet a data breach — a massive, unprecedented breach — compromised its system.

As a retailer, you've been hearing for several years now the importance of becoming PCI compliant and the potential consequences if you don't. But in light of Heartland's data breach, the obvious question is why should you become PCI compliant if the approved standards, as attained by Heartland, still subject systems to security vulnerabilities and legal trouble?

"It would be really easy to get discouraged," conceded Gray Taylor, former NACS vice president of technology and research and now a NACS consultant. "Heartland is one of the most secure processors, and they've taken [security] seriously from day one."

It's not an isolated accolade, but one shared generally by industry insiders.

Like my nephew heading back into the soccer game with the outcome all-but-certain, is the endeavor of becoming PCI compliant an exercise in futility, too, one doomed to defeat? Is there *anything* you can do, PCI or not, to protect your customers and business?

The answer to these questions, NACS maintains, is that the fight for data security is relevant; you're still very much in the game and there are steps you can take to control the outcome.

Standards Recap

Unless you've been living in a retailing spider hole for the past few years, you're no doubt aware of PCI standards: the 12-steps of compliance, retailer classification levels and the penalties if you are either in non-compliance or subject to a data breach.

In a nutshell, the Payment Card Industry (PCI) Security Standards Council, comprised of the five major credit card companies, established (and continues to revise) Data Security Standards (DSS), which are designed to protect personal data from your consumers' credit cards. The measures that merchants must take to secure that data are a reflection of your retailer classification level, as determined by your sales volume.

Performance of regular audits helps ensure that you're compliant with the DSS, and if you're not, depending on your retailer classification level, you're subject to heavy fines ($25,000 per month for Level 1 and Level 2 merchants) and the revocation of your right to accept credit cards, among other card brand-imposed penalties — and this is regardless of whether a data breach actually occurs.

If you incur a data breach *and* you are found to be non-compliant, the results can be disastrous for your business — not to mention the harm your customers could suffer. Not only do you risk card brand-imposed penalties (Level 1 and Level 2 merchants can be fined $500,000), you'll likely face high costs associated with the following: notifying all suspected cardholders that their information might be compromised, defending yourself against inevitable lawsuits and controlling the PR damage from publicly announcing the data breach — all of which could threaten your company's survival.

"Because I Said So!"

This all comes back to the Heartland case and the pursuit of data security: If becoming compliant doesn't guarantee security and eliminate data breach-related threats to your operations, why the emphasis on PCI standards and compliance?

Here's the blunt answer, and you probably won't like it: The credit card companies require it.

"Forget about 'standards,'" said Michael Davis, NACS vice president of member services. "These are mandates, another form of interchange, driven by the five major card payment brands to relieve themselves of any risk, passing it down to the retailer under the auspices of protecting consumer data and the retailer is in the middle here."

Davis said that the PCI Security Standards Council, which is fully staffed solely by the card brands, pushes through the PCI compliance standards without having to answer to anyone, including those who are responsible for enforcing and implementing the standards.

"There is not one retailer, not one processor, not one issuing bank, not one auditor, not one technology company sitting on the council," said Davis.

While the PCI Security Standards Council has developed a Board of Advisors that "provides input to the organization and feedback on the evolution of the PCI DSS," according to the Council, in reality, the board has very little influence.

"The plain truth is that the Board of Advisors review 'standards' a month before issuing and can 'comment' but have no input on the standards themselves," explained Davis. "In essence, the card brands run the Council, the card brands man the committees that develop the standards, and the card brands are the ones that interpret and enforce the standards."

Leaning On the Council

So while the process might be unfair, as long as you accept credit cards, there is not much you can do about the standards and compliance penalties. However, lest you feel completely helpless, understand that NACS has been and continues to be an outspoken critic of the process, and is committed to helping bring about change.

"NACS has joined the PCI Security Standards Council as a Participating Organization," said Davis, "and is lobbying for a Board of Advisors seat. Over 40 NACS members are already Participating Organizations and we are looking to use our size to apply greater pressure through the Council. We have engaged PCATS [Petroleum and Convenience Alliance for Technology Standards] to assist in any future standards of development."

One standard that NACS would like to see implemented is the requirement of PIN-based technology for card transactions — not just ones that are debit-based.

"Putting a four-digit PIN on every card transaction might have made the Heartland breach meaningless," said Taylor, who said that the Council's resistance to PIN-based transactions is a financial one.

"It boils down to transaction pricing," said Taylor, referring to the cost differential between credit and debit transactions. However, that may change, as the costs of PIN-based transactions rise. "As soon as [PIN-based transactions] become as expensive as credit card transactions, you'll see the adoption of PIN-based cards," predicted Taylor. "The trend is clearly there."

However, this added level of security would not come without cost to retailers. "Requiring a PIN for all debit and credit transactions would undoubtedly improve the security of card transactions significantly," said Jim Huguelet from The Huguelet Group LLC, a strategic IT consulting firm. "However, the amount of money and effort involved to make a fundamental change in the way

Top Six List

As part of a "prioritized approach" framework for achieving compliance (and separate from the NACS Eight-Step plan), the PCI SSC has released a list of six milestones — a best practices checklist — to help merchants protect against the most serious data security risk factors.

"The Prioritized Approach framework will help stakeholders understand where they can act to reduce risk earlier in their journey toward PCI DSS compliance," said Bob Russo, general manager of the PCI Security Standards Council.

The milestones are as follows:

1. Remove sensitive authentication data and limit data retention. If you don't need it, don't store it.

2. Protect the perimeter, internal and wireless networks. Weaknesses in these areas offer easy prey for compromising systems and obtaining access to cardholder data.

3. Secure payment card applications, focusing on controls for applications, application processes and application servers.

4. Monitor and control access to your systems. Detect the who, what, when and how concerning access to your network and cardholder data environment.

5. If you must store primary account numbers, protect stored cardholder data.

6. Complete PCI DSS requirements and ensure that all controls are in place.

WHILE SOME OF THE STEPS MIGHT BE FINANCIALLY IMPRACTICAL FOR SMALL RETAILERS, THEY REPRESENT A BEST PRACTICES APPROACH FOR ENSURING MAXIMUM PROTECTION.

consumers use credit cards across both brick-and-mortar as well as online merchants would be staggering."

In the meantime, NACS continues to advocate on behalf of retailers, continually pushing for change, at the very least in terms of the decision-making process.

"We have a shared interest and responsibility in customer [data security], but we don't have a shared involvement in how we do it," said Taylor. "We represent the industry to say that there might be a better way to do it, and we're trying to build those security walls to make [breaches] more difficult."

The Eight-Step Program

While the overall focus for NACS is on data security, that doesn't rest solely with PCI compliance.

"We're missing a broader point," said Lisa Stewart, president of Impact 21 Group LLC, and a NACStech workshop moderator. "We have found over and over again that retailers do not have an appropriate level of IT infrastructure to protect their own data and systems. My biggest concern is that they have to start down the [data protection] path . . . that we're at significant risk even without PCI [compliance]."

Toward that end, NACS, in partnership with PCATS, W. Capra, and Coalfire Systems, has developed an eight-step plan designed to help retailers achieve data security. While some of the steps might be financially impractical for small retailers, they represent a best practices approach for ensuring maximum protection.

Step 1:

Learn About PCI DSS, PCI PED and PCI PA-DSS

As you've already recognized, PCI compliance is replete with acronyms. In addition to DSS (see discussion above), there's PCI PED — that addresses security measures for maintaining pin entry devices; and there's PCI PA-DSS — that concerns payment application systems (POS systems and payment terminals, among other items). Not surprisingly, each comes commensurate with specific PCI standards (mandates) that govern retailer operations.

July 1, 2010, is a crucial deadline for *all* pin entry devices, after which they must utilize triple DES encryption (a sophisticated scrambling providing the highest levels of data security). NACS recommends that you engage your dispenser manufacturer to confirm that you will be in compliance and to ascertain the steps you might need to take — either upgrade or replace your dispensers — to get on track now.

Step 2:

Contact Your Bank Processor or Provider

While self-assessment familiarizes you with your systems, rely on your processor to help you wade through the details.

Ask for an explanation of your merchant level and how PCI affects your business, as well as the steps you need to take to achieve compliance. Repeat the process if you have multiple processors, asking them to verify *their* PCI compliance. *At every step, document your conversations.*

This step can be more complicated than it seems, and it may also require legal assistance to determine your responsibilities. We're an industry with an inherently complex system, one involving jobbers, dealers and owners. As such, the lines of liability are often difficult to ascertain.

"If you're branded, look at your jobber contract," said Davis. "If you're unbranded, look at your processor contract. There's a big difference — you need to check your contracts and get things in writing."

Not knowing that you were responsible is never a solid defense to liability.

Step 3:

Scrutinize Your Systems

Working with the details you uncovered during step two, conduct a thorough inventory of your payment systems, including PIN pads (inside and outside), POS and networks.

"Perform a visual inspection of every pin entry device, including their serial numbers," instructed Davis. "Skimmers are the biggest security risk we face." In fact, this part of the process cannot be overemphasized.

"Magnetic-stripe skimmers represent a significant threat to petroleum retailers," said Huguelet. "There have been numerous cases where a group of sophisticated criminals have engineered an overlay card reader that is tailored to the design of a particular dispenser or outside payment terminal model. They have then attached these skimmers to capture the card information of consumers using their payment cards for a legitimate transaction. This information is stored within the skimmer and then retrieved at a later date by the criminals."

For some, it's a game of cat-and-mouse that requires constant evaluation and proactive efforts.

"The crooks are definitely getting smarter and will go after processors, dispensers and points inside stores," said Pat Raycroft, founding partner at W. Capra, a retail technology consulting firm. "That means we need to keep operating smarter and stay in front of potential threats."

With innovation in mind, Huguelet cited companies such as Gilbarco as having developed a secure card reader, Secure FlexPay, that thwarts skimming attacks. But for now, they're optional.

"These secure card readers are not currently required by any PCI rule or card brand mandate," said Huguelet. "However, with the forthcoming announcement of the new PCI Unattended Payment Terminal (UPT) specifications, there will then be requirements that outline necessary protections for the card reader itself. [Because of that, before] retailers invest in any data security-related remediation for their dispensers, they should engage in a detailed dialog with their dispenser and OPT manufacturers so they can fully understand how their products will (or won't) meet the upcoming PCI UPT requirements."

A PCI UPT standard has been discussed for two years but has not yet been released by the card brands.

Step 4:
Contact Your System Vendors

Obtain written verification from your vendors that your entire system is PCI compliant (depending on the component, PCI DSS, PCI PED or PCI PA-DSS will apply).

For those items that are not compliant, obtain written instructions as to what steps you must take to attain compliance.

Step 5:
Self-Assess

The PCI Security Standards Council Web site — www.pcisecuritystandards.org — provides a self-assessment form that you can use to analyze your system. In addition, NACS has partnered with TurboPCI to offer its TurboPCI Easy Workbook (see page 16 for more information).

Step 6:
Remedy Security Gaps ASAP

After completing the self-assessment in Step 5, consult an experienced PCI expert to help you plug any security gaps in your system.

Step 7:
Obtain an External Audit and Security Scan

Hire a QSA to perform an audit and security scan of your system. They will ensure that the most up-to-date procedures (and those required by the card brands) are in place.

Step 8:
Fix Any Remaining Items

Fix any remaining vulnerabilities and plan for *continual* adherence to the security standards — data security requires your ongoing attention.

"PCI is a circle, you can't do it one time," suggested Stewart. "Building a secure infrastructure is ongoing, the assessments are ongoing and are required to secure your data." She explained that the standards (mandates) are constantly evolving to reflect new technologies and practices.

"We have to be careful because it's changing so fast and the liability is on us at every level," said Stewart. "The self-assessment has already changed multiple times. Somebody at your company has to be responsible for keeping up, or you should outsource the job. [Always] protect your data."

Back to the Game

In the meantime, details of the Heartland breach will continue to unfold, and news of legal settlements and verdicts will cast public scrutiny on practices that involve your operations.

While things might look daunting — as they undoubtedly do in the soccer world for my nephew and his teammates — you can gain experience and develop skills that will enable you to expect — and not just hope for — victory.

Everyone's rooting for you.

Jerry Soverinsky is a Chicago-based freelance writer and a NACS Magazine *contributing writer.*

DID YOU KNOW?

At NACStech this year, May 18-20 in Grapevine, Texas, a total of seven PCI workshops will be held.