GETTY IMAGES

The PCI ABC's

If you collect, transmit or store credit card data, you need to act now — or be subject to the consequences.

BY JERRY SOVERINSKY

You know the initials, of course — you see and hear them everywhere. Industry magazines. Workshops. Vendors (oh, those sales calls).

You're sure a deadline is approaching. Or has it already passed? You're not quite sure. Besides which, even if you knew, you're still not sure what you need to do (or what happens if you don't).

PCI compliance.

Does it apply to you? Here's a hint if you're not sure: If you collect, transmit and/or store cardholder information, then it does.

WHY

In December 2006, international apparel and home fashions retail giant TJX Companies (parent company of T.J. Maxx, Marshalls and HomeGoods) incurred one of the world's most severe and widespread data security breaches in history, when computer hackers accessed a TJX computer system that stored credit card, check and merchandise return transactions for more than 45 million TJX customers. The hackers stole detailed customer information, including credit card information, social security numbers and driver's licenses — a nightmare for the affected consumers and a legal and financial setback for TJX.

"The $17.4-billion retailer's wireless network had less security than many people have on their home networks," reported *The Wall Street Journal* in a May 4, 2007, analysis. "And for 18 months the company had no idea what was going on." The article speculated that because of the breach, banks would have to pay up to $300 million in card replacement costs, while TJX would have to pay up to $1 billion for security upgrades, attorney fees and rebranding efforts. Internally, TJX projected more than $20 million in fraudulent transactions.

WHO

On September 7, 2006, in an effort to counter mounting security transgressions (the TJX case was one in a rapidly expanding list), the major credit companies — Visa, MasterCard, American Express, Discover and JCB — formed the Payment Card Industry Security Standards Council (PCI SSC) "to enhance payment account data security by fostering broad adoption of the PCI Data Security Standards (PCI DSS)."

The coalition was several years in the making. Responding to a pandemic of data security breaches in the 1990s, each of the credit card companies began developing safeguards for the storage, processing and transmission of cardholder information. Recognizing the merits of a collective attempt at standardization, the companies eventually aligned in December 2004, creating PCI DSS.

WHAT

These standards — PCI DSS — are a set of formal requirements with which affected merchants (again, *any entity that collects, transmits and/or stores cardholder information*) must comply. The 12 requirements, centered around six goals, are as follows:

GOAL 1: Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

GOAL 2: Protect Cardholder Data

Requirement 3: Protect stored cardholder data.

Requirement 4: Encrypt transmission of cardholder data across open, public networks.

GOAL 3: Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software.

Requirement 6: Develop and maintain secure systems and applications.

GOAL 4: Implement Strong Access Control Measures
Requirement 7: Restrict access to cardholder data by business need-to-know.
Requirement 8: Assign a unique ID to each person with computer access.
Requirement 9: Restrict physical access to cardholder data.

GOAL 5: Regularly Monitor and Test Networks
Requirement 10: Track and monitor all access to network resources and cardholder data.
Requirement 11: Regularly test security systems and processes.

GOAL 6: Maintain an Information Security Policy
Requirement 12: Maintain a policy that addresses information security.

HOW

To pursue compliance, PCI SSC outlines a three-phase process: assess, remediate and report.

■ Step 1: Assess

During this phase, merchants identify data security vulnerabilities (a reflection of how credit card data is processed, stored and transmitted — the above 12 requirements). Depending on the number of credit card transactions that you process, assessment may be either on-site or via self-assessment questionnaire. If an on-site assessment is required, Qualified Security Assessors (QSA) and Approved Scanning Vendors (ASV), both aligned with PCI SSC, can perform recognized certification assessments.

■ Step 2: Remediate

Once vulnerabilities are identified, merchants must fix the problems. PCI SSC recommends a triage approach, prioritizing fixes based on their threat implications. Fixes might include instituting changes in processes as well as hardware and software modifications.

■ Step 3: Report

Merchants must file *regular* reports with their acquiring banks and card companies that detail their compliance efforts, along with quarterly network scan reports. Larger retailers must work with on-site assessors, while smaller marketers can submit a self-assessment questionnaire.

With an acknowledgment of the challenges that small retailers face, card companies modify their compliance requirements based on the number of transactions processed. These vary by card issuer; below are those for Visa and MasterCard.

While they address uniform standards, ensuring compliance (and assessing fines and penalties for those found to be non-compliant) remains the responsibility of the individual payment brands. As of September 2007, merchants are required to file proof of compliance to each payment brand with whom they cooperate. Failure to do so could mean financial liability for the merchant, a substantial risk that should provide incentive to meet compliance standards.

HOW: The Basics

Acknowledging the three-step overarching process, Rick Dakin, president of Coalfire Systems, which provides IT security, governance and regulatory compliance services, recommends a more basic starting point, one that requires retailers to make just two phone calls. "First, go back to the people you trust, the POS vendors," Dakin said. "Ask them whether

MERCHANT CLASSIFICATION LEVEL	NUMBER OF ANNUAL TRANSACTIONS	VALIDATION REQUIREMENT
1	6 million+	■ On-site review by either internal auditor, QSA or internal audit (if signed by company officer) ■ Quarterly network scan via approved scanning vendor (ASV)
2	1 million to 5,999,999	■ Annual self-assessment questionnaire ■ Quarterly network security scan via approved ASV
3	20,000 to 999,999	■ Annual self-assessment questionnaire ■ Quarterly network security scan via approved ASV
4	Less than 20,000	■ Annual self-assessment questionnaire ■ Quarterly network security scan via approved ASV

their applications are certified." If merchants are already working with specific POS equipment that is not certified, their vendors have until July 2010 to correct the deficiency.

"Second, call your acquiring bank," Dakin continued. "Ask your payment gateway or acquiring bank what information is needed by them to validate [your] compliance. The 12 requirements don't apply to every merchant, and their banks will [be able to help guide them]."

Jenny Bullard, CIO of Flash Foods (Waycross, Georgia), has been involved in her company's two-year ongoing pursuit of PCI compliance, and recommends placing a priority on the quarterly scan requirement. "Contact your bank, and ask them to put you in touch with a company that will do your quarterly scan," she advised. "You may have holes in your network that you're not aware of, and the scans are [vital] for determining those deficiencies."

After these basic steps, Dakin recommends engaging a QSA. Companies like Coalfire or Check Point Software offer everything from online assistance to on-site guidance, solutions that cater to a variety of budgets and system complexities. The most basic assistance starts at $300, a downloadable set of policies that Coalfire offers small retailers. The largest retailers could pay significantly more than that — fees of "$1 million in infrastructure changes" are common, noted Dakin.

These costs are a particular challenge for retailers, who "are finding it hard to calculate a return on this investment," noted Scott McDowell, Marketing Manager for Gilbarco Veeder-Root, a supplier of fuel marketer resources, "and realize it is a cost of doing business."

But think of it this way, if a data breach occurs, you are required to notify a consumer by written letter explaining that their personal data has been jeopardized. Think of the cost of trying to reach those tens of thousands of consumers.

And "the real cost," noted McDowell, "is associated with the PR damage. Sites that have been compromised have seen as much as a 50 percent drop in business after an attack. This results in [lost] revenue and potential store closings."

Several thousand dollars invested in PCI compliance might not seem so hefty when these other factors are taken into consideration.

HOW Often

Meeting PCI compliance requirements is not a one-time venture explained Alan Thiemann, an Alexandria, Virginia-based attorney who works with NACS on PCI compliance issues. "It's a lot like a smoke detector in your house. The battery may work at night, but not in the morning. You have no recourse in the morning if your house burns down because the battery died at night."

Case-in-point: New England grocery retailer Hannaford Brothers. They met all audit requirements during their PCI compliance process, but they were found to have non-compliant processes updating their antivirus software.

"Compliance today doesn't mean compliance tomorrow," Thiemann said. "[You must pay attention] to everything on a day-to-day basis." Too many organizations meet their assessment requirements and then don't think about security for another six months. All those who handle credit card or personal data must make a commitment to protect against breaches by establishing a security-centric foundation that is monitored and self-assessed routinely, not just at implementation.

HOW Much

Credit card companies are introducing audits (and assessing penalties) as a means of ensuring compliance. These on-site visits include a PCI-authorized auditor who performs a network scan, measuring a company's adherence to the 12 requirements. Retailers who are non-compliant — regardless of whether an actual security breach has occurred — are subject to harsh penalties: substantial fines, sole liability for electronic data theft and the revocation of its license to accept credit cards.

"A retailer is taking a real risk with their business by deciding to be non-compliant," explained McDowell. "If a retailer has a security breach during their noncompliance, they are assuming all liability for that breach. Breaches can range from $250 to $250,000, depending on the severity."

But McDowell's $250,000 estimate may be just a starting point. Earlier this year, Iowa passed a data breach law that, in addition to requiring giving notice to residents whose data may have

PCI's Other Standards

In addition to the Data Security Standards, within the PCI Council's first year, it also adopted PIN Entry Device (PED) security requirements and Payment Application Data Security Standards (PA-DSS). PCI PED is directed at manufacturers of personal identification number entry terminals, and PA-DSS are aimed at software developers of applications dealing with payment storage, processing, or transmission (i.e. magnetic stripe data applications). PCI compliance mandates that merchants must use certified PED and PA-DSS devices; all merchants must use payment applications that are certified as payment application best practices-compliant (PABP) by July 10, 2010.

NACS has joined the PCI SSC to work with more 20 other NACS members to ensure that mandates, such as PIN Entry Device Security Requirements, evolve to account for the financial implications to the retailers and, ultimately, the consumers whose data we're trying to protect. For more information on getting involved, contact Michael Davis at mdavis@nacsonline.com or (703) 518-4246.

IF A RETAILER IS FOUND TO HAVE DELIBERATELY COMPROMISED DATA, HE COULD POTENTIALLY FACE JAIL TIME.

been compromised (the 43rd state with such a requirement), allows the state to pursue actual damages incurred per individual, as a result of that breach. As such, the potential noncompliance costs can be huge, affecting the survival of the non-compliant entity.

Penalties are not only for those entities incurring a security breach. Non-compliant companies are also subject to penalties, determined by the individual card companies. These can range from "$5,000 to $100,000 in fines per month," noted McDowell, "or networks deciding to turn off a store's capability to process any credit or debit transactions."

Beyond the monetary, Barrie VanBrackle, legal consultant for Gilbarco Veeder-Root, says that other more restrictive penalties are not out of the question. "If the retailer is found to have internal employees or [if he has] deliberately compromised data," he noted, "the specific person found guilty of this offense will potentially face jail time."

HOW Effective

Implementing security standards is one thing; meeting compliance standards is quite another. According to a recent VeriSign report that reviewed 112 PCI assessments, the company found that more than 73% did not pass the PCI requirements. But the failure is not one of intention. Rather, while the PCI DSS "prevails as one of the most preeminent achievements in the information security industry," it reports, "many merchants and service providers are struggling with the increased complexity associated with the PCI Data Security Standard."

Coalfire's Dakin cites his company's own findings, with results that vary according to the merchant classification. "In level ones," he said, "everyone understands the requirements, but only 30 percent are compliant." By contrast, he notes, "20-30 percent of the merchants below level one" understand the requirements, "and only five percent are in compliance."

Confusion over the details surrounding PCI compliance has likely stalled the efforts of many retailers and dampened their enthusiasm for the process. And while the security goals of the PCI SSC are a welcome development for cardholders, retailers have also been less than enthusiastic about whether the PCI DSS are meeting the stated objectives.

The National Retail Federation believes the PCI SSC is overlooking basic operational requirements that subject cardholders to undue risk. In a letter to the PCI SSC, NRF Chief Information Officer David Hogan writes, "All of us...want to eliminate credit card fraud. But if the goal is to make credit card data less vulnerable, the ultimate solution is to stop requiring merchants to store card data in the first place... Instead of making the industry jump through [compliance] hoops to create an impenetrable fortress, retailers want to eliminate the incentive for hackers to break into their systems in the first place."

Hogan is referring to the credit card companies' requirement that merchants retain transaction credit card numbers for up to 18 months (in order to satisfy future retrieval requests). NRF's solution? Storing credit card numbers should be discretionary, not mandatory, a move the PCI SSC has yet to address.

WHEN

As of September 2007, merchants were required to file proof of compliance to each payment brand with whom they cooperate. But just because you might have already missed the deadline, it doesn't mean it's too late to now comply. Indeed, if you're non-compliant and haven't yet faced any repercussions (or a data security breach), consider yourself lucky.

And get to work. ■

Jerry Soverinsky is a Chicago-based freelance writer.