THINKSTOCK

When it comes to passing a PCI audit, the key is in a familiar mantra: be prepared.

by Holly Doering

When "Big Joe" McGinnis stole $2.7 million from the Brink's Depot in Boston (now a parking garage) in 1950, he needed an ice pick to enter the building. Today's thieves only need to find a way to breach your online defenses. That's the reason for the rise of the Payment Card Industry (PCI) Council and its data security standards (DSS) for e-commerce.

PCI-DSS compliance is mandatory if your parking organization processes, stores, or transmits credit card information. The challenge we all face is that compliance is an ongoing process rather than a static checklist, and we have to follow a good roadmap to navigate changes such as employee turnover and network infrastructure upgrades. According to the Verizon 2011 PCI Compliance Report, only 21 percent of organizations met the must-pass requirements during their initial report on compliance (ROC) that year, "even though most were validated to be in compliance during their prior assessment."

Parking software provider OmniPark^{TM}, which maintains PCI-DSS Level 1 security certification through Imprezzio's TranZgate, successfully completed its annual PCI audit in January. Chief Architect Neil Taylor explains, "Because of the sheer volume of transactions we process, and in order to offer our clients better and more aggressive rates, we decided to go for the gold and become Level 1 certified. By going above and beyond, we can provide peace of mind for our clients and their customers. "

So how does an organization prepare for a Level 1 (the strictest) audit? OmniPark^{TM}'s experience provides a guide.

The Gap Analysis: A Dry Run

In December, experts from a qualified security assessment (QSA) company of PCI Council-certified experts performed a pre-audit assessment called a gap analysis. A gap analysis isn't required, but it's a good idea. Taylor explains, "The gap analysis is a mock audit. They look at everything and make sure you've been following your own policies and procedures, that they are reviewed and updated regularly, and that your systems are up to date."

"If problems are found, you have time for remediation," he says. "You can collect logs, update and review processes and procedures, and prove that you know what to do with the information."

There can be scheduling issues that push calendars back, Taylor says, but he normally finds a gap analysis that takes place 60 to 90 days before the audit to be the most effective—and cost-effective.

"The auditor does spot checks on everything from the way you deal with employees to the way you deal with data, technical documents, and implement checks and balances," he says. "They look at how you audit your firewalls, how you build your routers, and what you do with new machines when they're installed before credit card data is allowed to pass through them."

"They also check on how you manage personnel," he continues, "and that your developers can't write code allowing them to steal credit card numbers if they get fired three years from now, for example."

"The most difficult area of passing a PCI audit is the documentation," Taylor says, "because there are dozens of required documents." There are 12 major PCI-DSS requirement categories and 221 sub-requirements businesses must meet to protect credit card data from theft.

While it can be cumbersome to follow the rules with lots of steps to go through before any actual work happens on the audit itself, Taylor says, "If you are dedicated and diligent, you will have a secure environment by design. The controls are there for a reason."

Hiring the Right QSA

A PCI audit is a large investment. For widespread organizations with multiple locations or even multiple cities, the PCI audit can cost tens or hundreds of thousands of dollars. According to Network World, Inc., the low-cost end cost of the average PCI audit is $225,000.

Which payment card industry (PCI) requirements are hardest to meet? According to Verizon's PCI and RISK Intelligence Teams, organizations struggled most with:

- Protecting stored cardholder data.
- Tracking and monitoring all access.
- Regularly testing security systems and processes.
- Maintaining information security policies.

Verizon found the highest implementation levels on PCI requirements in the following areas:

- Encrypt transmissions over public networks.
- Use and update anti-virus software.
- Restrict access to need-to-know.
- Restrict physical access.

So choosing the right quality security assessment (QSA) company is essential. Taylor says a good QSA should:

- Understand your organizational scope.
- Be able to work with your staff so business doesn't come to a standstill during the audit.
- Be able to perform both a gap analysis and a PCI audit.
- Offer good solutions, remediation, and strategies if gaps are identified.
- Realize that it is in their best interest to help you pass legitimately.

If you fail audits, Taylor says, your business will suffer and you won't be able to afford more audits. "The ideal QSA will assist you to run a successful business operation. At the same time, they need to have internal and peer review processes in place within their firm to ensure you don't get a friendly auditor who just says everything is fine."

"Quality reports of compliance (ROC) have a much higher chance of being accepted by banks and credit card associations. If the quality of your ROC gets called into question, it is much harder to pass," he says. "It could get dicey."

Best Practices and Due Diligence

Best practices in the field of data security include limited access and separation of duties. "In our environment, for example," says Taylor, "no single employee can perform all aspects of credit card processing. Our development team writes and tests the software; their changes are code-reviewed by someone else without access to write software back to the archive. The code is deployed by yet another team in yet another process. The idea is to make it very difficult for one individual to maliciously compromise cardholder data.

How to Find a Qualified Security Assessment (QSA) Company:

- Ask for recommendations from your bank
- Visit the PCI Council's website at pcisecuritystandards.org. QSAs in remediation are marked on their listing.
- Check that any QSA firm you're considering is properly licensed and currently in good standing.
- Don't automatically choose the lowest bidder.

"We make sure multiple people are involved in software deployment and approval. Checklists, formalized test plans, and production checkout procedures help us make sure we haven't missed anything. It requires diligence," he says.

Of course, PCI-DSS compliance does not guarantee an organization will never be hacked, as Global Payments, a well-known processor for New York parking garages, learned in 2012, but it does help your parking company make informed decisions on how you use and protect customer data.

The Price Tag

Taylor's tips for reducing the cost of a PCI audit include limiting your operational scope and employee access and keeping it local. "The scope of the audit is one of the biggest factors in driving up the cost," Taylor says. "The bigger the cardholder data environment you maintain or number of systems or parts of systems that can access credit card numbers, expiration dates, swipe data, etc., the more your audit is going to cost.

"In our environment, we have limited the scope of our operation to cardholder data environments (CDEs) that contain all our TranZgate software and databases and two external laptops that can access it. The rest of our environment doesn't fall within the scope of the audit because it doesn't access the cardholder data. We also keep the number of staff with access very small, so we only need to train a handful of people. This also reduces cost," he says.

Hiring local QSAs can also cut down on expenses, Taylor says, noting that the company finds it significantly more cost-effective to work with Seattle QSAs than flying people in from California.

Ultimately, maintaining the rigorous standards of the PCI-DSS Level 1 security certification is worth it because of the extra comfort level of existing and future clients.

HOLLY DOERING is a technical writer with Imprezzio, Inc. She can be reached at hollyd@imprezzio.com or 866.847.4515.