InformationWeek :: analytics
techSTRATEGY

[STRATEGIC SECURITY]

Inside PCI Compliance

Assessors reveal mistakes companies make with data security standard

By Andrew Conry-Murray

Whether you think PCI is a useful standard that makes our credit card data safer or a credit card industry whitewash that merely creates the illusion of security, PCI compliance is a fact of life.

As part of PCI compliance, companies that process a high volume of credit card transactions must submit to an annual assessment by a qualified security assessor, or QSA. For example, Visa requires it of merchants that process 6 million or more transactions. Assessors work for third-party organizations and generally visit companies to examine their processes and determine whether they comply with PCI rules.

To help companies get ready for a an evaluation, we asked QSAs to describe common problems they encounter when working with IT groups on PCI compliance. What follows are five best practices to help companies better prepare for an assessment and maintain compliance.

1. Know Where Data Lives

First off, you must know how credit card data flows through your system, where the data resides in the enterprise, and who has access to it. Assessors ask for this information at the outset of an assessment because it determines the scope of the project. They aren't there to review your entire security infrastructure, just the systems that collect, process, transport, and store credit card data. A surprising number of companies don't have a good grasp of this information. "It's common for a client to completely miss a particular data flow and have no idea that credit card data is being forked off to system X, Y, or Z," says a QSA at Neohapsis, who asked to remain anonymous.

3 TYPICAL PCI COMPLIANCE ERRORS

> PCI requires companies to maintain a network diagram that shows how card data flows through IT systems, but assessors say companies often don't have one or it lacks critical details.

> According to PCI, companies must install critical security patches, but patches sometimes break systems, or one IT group requests a patch but another forgets to install it.

> Sometimes IT runs external scans but neglects to scan inside the firewall, which PCI requires. Organizations also must show that vulnerabilities have been remediated by running a scan after patches are deployed, but many skip this step.

Companies express an "extreme amount of frustration" over the amount of effort they have to put in to put the full picture together, says Ted Keniston, a QSA and managing consultant with the global compliances group at Trustwave. "We should be validating this information, not determining it."

Having a complete picture of credit card data isn't just a courtesy to your assessor; it also affects your ability to protect customer information, because you can't secure what you don't know about.

2. PCI Is A Moving Target

Let's say your assessor has just stamped you "compliant." You breathe a sigh of relief. The PCI assessment is annual, so you don't have to worry about it for another 12 months, right? Not so.

PCI compliance is only valid and only applies to the state of the network and systems at the time of the assessment. The moment you make changes to systems that fall under the scope of PCI, your compliance status is in question.

Of course, no network or computer system remains unchanged, so companies must account for how those changes will affect compliance. All of the controls and processes you put in place to demonstrate compliance at the assessment must be carried forward.

"Change management, log management, system configuration changes—it all has to adhere to PCI requirements," says Trustwave's Keniston.

A related issue is that PCI rules are intended to be adopted as part of ongoing operations. Compliance isn't an annual flu shot that you only think about once a year. It's more like exercise—it has to be done regularly.

For example, PCI requires companies to review firewall rulesets, but this can be a tedious and time-consuming task, easily put aside by busy IT pros. To prevent this from falling by the wayside, one QSA suggests creating sched-

uled tasks that get assigned to administrators as part of their regular workflow.

Many companies try to bolt on PCI compliance instead of embedding the practices dictated by the standards into their everyday operations. Often they don't want to hear about compliance when developing projects, particularly revenue-generating ones, because any delay in deployment means a delay in income, says the Neohapsis QSA. "They wait until the audit to find out what they need to change, and the cost is always higher to fix it on the back end instead of building it right from the get-go."

If your organization has incorporated PCI requirements into daily operations, be sure you document it so you can get credit. A lot of companies do what they're supposed to for PCI, "but they've never put it in a policy or have anything formal that says 'This is what we do,'" says Trustwave's Keniston.

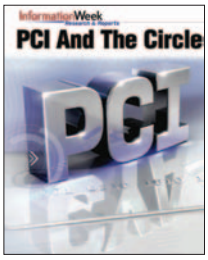
3. Take Advantage Of Overlaps

Companies large enough to process millions of credit card transactions are likely to be subject to other regulations, such as Sarbanes-Oxley, or standards such as ISO and the SAS 70 security audit, as well as state laws that mandate the protection of consumer information. Many companies treat each requirement separately, so that every audit becomes a disruptive event, says the Neohapsis QSA. A more proactive approach is to dovetail as many requirements as possible so that audits are less of an issue.

For instance, regulation X might mandate seven-character passwords, while regulation Y says eight. "Set it to nine and satisfy all those controls," he says. "I haven't seen a lot of effort there. People wait for the auditor to come through and correct you instead of doing it as a unified effort."

DIG DEEPER

PCI And The Circle Of Blame



PCI is a flawed exercise in protecting credit data. The requirements are sound, but complying is costly, creating an incentive to seek the least expensive path to compliance. The process can be manipulated so merchants seem compliant without actually making their data more secure. And credit card issuers have little reason to make any changes. It's a process in need of improvement.

Get this at *informationweek.com/analytic/pci*

See all our Analytics Reports at analytics.informationweek.com

4. Your Assessor Isn't The Enemy

It's hard for overworked and underfunded IT and security teams to watch some dude stroll in with a scorecard and tell them where they've failed—and then send a bill. A certain coolness, if not downright animosity, is to be expected.

But your company has an obligation to protect cardholder data, and the assessor can help achieve that goal. Companies should view assessors "not as opponents, but as partners in developing sound security programs," says Fabian J. Olivia, a QSA and global PCI competency leader at IBM.

Some IT teams realize that they can use the findings from an assessment to get funding they've been asking for to implement critical projects, says Branden Williams, a QSA and senior director of consulting at AT&T Consulting's PCI group. If you know a PCI assessment is coming, document areas where your controls are weak, outline a plan to address them, and get that information in front of management immediately. Once the assessment is over, you'll have third-party validation that the issues you've raised are important, and funding may come your way.

5. This Is A Pass/Fail Test

Unlike many regulations that emphasize risk management, PCI is a prescriptive compliance standard. It requires specific controls and processes, and organizations have to meet all the requirements, or they won't pass. "There is no partial compliance," says the Neohapsis QSA. "You either are, or you are not. It's not something the QSA can change for you."

PCI critics say the standard is complex and costly, and that compliant companies can still lose data. We agree. But despite its flaws, PCI is an opportunity for companies to get serious about their obligation to protect cardholder data and implement sensible controls. "PCI compliance should be a by-product of sound security practices and programs," says IBM's Olivia. We also agree.

Write to Andrew Conry-Murray at *acmurray@techweb.com.*