



PCI: Smaller Merchants Threatened

Criminals Now Picking Less Compliant Targets

October 19, 2010 - Linda McGlasson, Managing Editor

The Payment Card Industry's **Security Standards Council** may be doing a good job helping lock down larger retailers, but the smaller "Mom and Pop" merchants are becoming the new targets of **cyber criminals**, says a PCI expert.

A recent report on PCI compliance by Verizon Business shows some unsettling trends, says Jen Mack, Verizon's director of global PCI consulting services.

Mack says Level 3 and 4 retailers are now being targeted by cyber criminals for the theft of credit card data. Examples of these targets include restaurants in several states that were hit in the past several months -- the latest being one that had its **POS system breached** in Tallahassee, Fla.

Level 3 merchants are defined by those merchants that have 20,000 or more credit card transactions annually. Level 4 are those that have fewer than 20,000 credit card transactions per year.

The PCI report shows that businesses of every size "are better at planning, doing -- not at checking if they are compliant," says Mack, a former member of the PCI Security Standards Council. The overwhelming majority of data breaches occur because of failures to check things were in place. Despite arguments to the contrary, Mack says "There's no open hole causing data breaches that isn't covered by the PCI standards."

Smaller Merchants Need Education

Merchant levels 3 and 4 need more education about how to comply with PCI, Mack says, as they represent the largest group of merchants.

"The Level 3 and 4 challenge is daunting and very serious," she says. "Massive amounts of data are at these merchants, and they clearly don't have the same level of security as larger retailers do."

The size of a merchant, Mack says, doesn't preclude it from being a target. As an example she points out that street cart vendors in large cities are accepting credit card payments merely by using an iPhone and a card skimmer to process transactions. "The idea that security is included in this kind of transaction doesn't enter the street vendor's mind," Mack says. "They're doing business, and even though the transaction may only be a few dollars, the card data is still used."

Plans for further education and a compliance push by the PCI Security Standards Council include a microsite for these two groups of merchants. The microsite will launch at the same time the final draft of the **new PCI standard** is released at the end of October. Even with this push by the PCI SSC, Mack says financial institutions can also push for more education of the merchants they do business with and handle transactions. Above all, Mack says merchants need to avoid the failure to communicate with their bank about PCI compliance.



Tips for Merchants

Some ideas Mack says institutions can offer their merchants about meeting PCI compliance:

- Give them whatever education and information about PCI compliance, but keep it simple. Offer them the available tools to help meet compliance.
- Wherever possible, Level 4 merchants should outsource all parts of the card transaction process to a payment processor. Institutions should help compile a list of the vendors and give the merchants a range of options from which to choose.
- Institutions should categorize their riskier merchants, beginning with bars and restaurants, and begin talking to them. "Keep it simple," Mack says. "Often the changes that are needed won't be major efforts."

In addition to assessing the effectiveness of the PCI DSS, Mack says the PCI compliance report identifies which attack methods are most common and gives recommendations for all businesses on earning and maintaining PCI compliance.

By coupling PCI assessment data with the post-breach analysis, Verizon analysts were able to rank the top attack methods used to compromise payment card data in the report. The top attack vectors include malware and hacking (25 percent), SQL injections (24 percent) and exploitation of default or guessable credentials (21 percent).

PCI Best Practices

While there is no magic bullet for **PCI compliance**, fully compliant organizations serve as a model for other organizations looking to earn and maintain compliance. Best practices found in fully compliant organizations include:

- **Build in Security.** Security needs to be built into business processes from the very beginning, not added on. Organizations that adhere to this practice typically spend fewer resources and achieve more value from their compliance activities.
- **Do Not Separate Compliance and Security.** Both compliance and security activities are aimed at protecting data. Organizations that align compliance and security tend to more easily achieve compliance with security regulations such as PCI DSS. Compliant organizations also tend to have one compliance and security management team, or have two teams that are highly collaborative.
- **Treat Compliance as a Continuous Process.** Organizations should incorporate PCI activities into their daily business operations. Merchants get into trouble when they approach PCI as a monthly, quarterly or yearly project.
- **Control Data Closely.** Scope creep is a common problem with assessment activities. Discovering, tracking and managing data is essential. The larger the scope of the assessment, the more costly and difficult it is for the organization to perform.

EXPERIENCE THE *NPS* DIFFERENCE™