Reprint courtesy of *NACS Magazine*. For more information, please contact Erin Pressley at 703-518-4208, or epressley@nacsonline.com.

[IDEAS 2 GO]

PCI Myths Debunked!

Protect your company by knowing what's fact and what's fiction about PCI compliance.

BY DREW MIZE

Protecting cardholder data is more important than ever. The costs of that data falling into the wrong hands have become an enormous expense — not only to the cardholder, but to retailers as well. Fines can be very high for non-compliance to PCI standards, and at some point your processor could take you off the network completely if you aren't processing cards on a secure network that meets compliance standards.

PCI compliance is a complicated topic, and one that we're all learning about as we go along. It isn't going away, and Visa and MasterCard are leading the efforts and strictly enforcing the rules.

Many myths are floating around about what will solve the challenges. Some of the most common misstatements:

My technology provider provided the hardware/software, so they'll get the heat if a PCI-related issue occurs.

Not so. If a PCI-related breach occurs and it is found that the theft originated from one of your systems, it's *you* who pays the fines and ongoing penalties. Do your research and understand PCI and surrounding requirements. Make the investment to have a qualified PCI auditor assess your organization.

My technology provider said it's compliant, so I'm safe.

There is a significant difference between Visa-approved PCI compliance, and hardware and software that a technology provider has deemed PCI compliant. PCI compliant means that the hardware and software have been thoroughly evaluated by a PCI Security Standards Council approved qualified security assessor (QSA) and the solution certified as safe and secure.

My technology provider will take care of me.

Nothing could be further from the truth! Your technology provider is an excellent source for education and information, but should not be thought of as the magic cure. Any technology provider that has gone through a formal PCI audit for the technology they are selling should have at least one certified PCI auditor they can recommend to you. If they can't do this, start asking the hard questions. You pay the fines and penalties if a breach occurs, not your technology provider.

My point of sale is compliant, so my company is compliant.

The point-of-sale solution is a central component to payment transactions, but a whole slew of other devices should be considered. Dispenser CRINDS, ATMs, pin pads, routers, firewalls, wireless networks, the USB port on your back-office PC and so on. And don't forget about the home office: databases, LANs, WANs, the box of credit card numbers that accounting has on their desk for local accounts, physical access to servers and so on.

If the technology is PCI compliant, I'm compliant.

One of the critical aspects of PCI compliance isn't just that the technology itself is compliant, but that it is implemented in a PCI compliant environment and is managed by human processes and

YOU PAY THE FINES AND PENALTIES IF A BREACH OCCURS, NOT YOUR TECHNOLOGY PROVIDER.

controls to ensure ongoing security. As an example, your point of sale may be PCI compliant, but if it is on the same IP network as a wireless LAN you are likely no longer compliant. Or, if adequate processes aren't in place to manage the logins and passwords for accessing the point-of-sale systems across your organization you face the same issues.

Today I'm PCI compliant, so I'm PCI compliant forever!
False. The Hannaford Brothers incident in March is the first cardholder data breach at a company that was deemed PCI compliant by a certified PCI auditor. As fast as you close the open holes to cardholder data theft, smart thieves are finding new ways to create new holes. PCI compliance is a journey, not a destination. Don't stop with initial PCI-compliance success, and definitely don't limit your organization to the once per year renewal of PCI compliance.

In short: Don't get your company caught up in the middle of a breach. If you haven't already done so, contact a PCI Security Standards Council certified QSA to audit your organization. (That auditor will be a heck of a lot cheaper than the fines you will pay if you get hacked.) Even if your technology supplier has provided proof of PCI compliance, and those solutions status' are evidenced on Visa's Web site, your provider only knows a small percentage of your organization.

Above all, don't stop when you achieve PCI compliance. As long as there are thieves out there you are subject to their creative deviousness. Make the relationship with your QSA a long-term commitment. ■

Drew Mize is the vice president of product management and marketing at The Pinnacle Corporation.

The views expressed here are those of the vendor and not necessarily the views of NACS.