



adequate processes aren't in place to manage the logins and passwords for access of 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 was the first cardholder data breach at a company that was deemed PCI compliant by a Visa-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 Visa-certified qualified security assessor (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; consider this journey an ongoing one. ■

Drew Mize is Vice President of Product Management and Marketing at The Pinnacle Corporation.

PCI Myths Debunked!

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

By Drew Mize, Vice President of Product Management and Marketing, The Pinnacle Corporation

Protecting cardholder data is more important than ever. The cost of that data falling into fraudulent hands has 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 Visa 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 has been thoroughly evaluated by a Visa-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 auditor they can recommend to you — their own. 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 pieces at 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.

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

One of 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 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



Texas Petroleum and C-Store Journal is published for the **Texas Petroleum Marketers and Convenience Store Association (TPCA)**
401 West 15th Street, Suite 510
Austin, TX 78701
Phone: 512-476-9547
Fax: 512-477-4239
www.tpc.org

TPCA Staff
Chris Newton, President
Scott B. Fisher, Vice President of Policy and Public Affairs
Doug DuBois, Jr., Director of Membership Services and Governmental Affairs
Bill Duncan, Director of Finance and Information Services
Annette Hicks, CMP, Director of Meetings & Expositions
Kris Wallace, Assistant Director of Accounting

Published by:
naylor

Naylor, LLC
5950 N.W. 1st Place
Gainesville, FL 32607
Phone: 800-369-6220
Fax: 352-331-3525
www.naylor.com

Publisher: Kathleen Gardner

Editor: Shani Lyon

Marketing: Patti Callahan

Project Manager: Jason Dolder

Advertising Sales Director: Matthew Yates

Sales Representatives:
Adam Lingenfelter, Beth Palmer, Bill Lovett, Doug Pratt, Jamie Williams, Kevin Mizell, Leron Owens, Norbert Musial, Paul Walley, Shaun Greying, Shirley Luster

Layout & Design: Dan Proudley

Advertising Art: Glenn Domingo

©2010 Naylor, LLC. All rights reserved. The contents of this publication may not be reproduced by any means, in whole or in part, without the prior written consent of the publisher.

This information is being distributed to you by:

PUMP TEX

