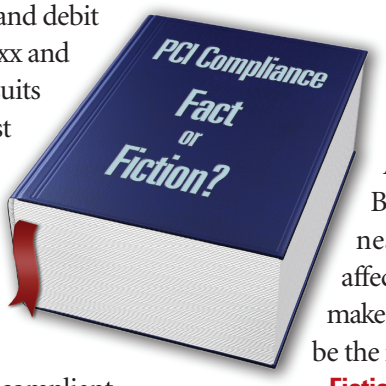
PCI Compliance: Fact vs. Fiction

By now, most of us understand that the Payment Card Industry (PCI) created the Data Security Standard (DSS) and others to better protect customers, payment card data and merchant data. However, as a managed service provider of security and networking solutions for PCI compliance, we routinely speak to organizations that have misconceptions regarding compliance and their need for action. Importantly, the cost of these false notions can outweigh the costs of compliance.

With 45 million and 4 million credit and debit cards compromised, respectively, T.J. Maxx and Hannaford have been battling fines, lawsuits and, more important, the soft costs of lost business and brand damage. Estimated financial effects on a merchant range from $100 to $300 per compromised card. So understanding fact vs. fiction can save a retailer money and, in some cases, even their business.



Fiction: Only the big guys need to be compliant.

Fact: PCI compliance is required for any business that accepts payment cards, starting with only one transaction. As a provider of certified secure network solutions to Shell Oil, we often work with both big and small organizations. Firms such as Green Valley Grocery, with 39 Shell-branded locations, or even companies with just one site face the same risks as the big guys.

Fiction: I'm small; hackers wouldn't target me.

Fact: The reality is, small organizations are targeted just as frequently as larger firms. Recently published statistics show that about one-third of all PCI breaches occurred at firms with fewer than 100 employees. Typically, smaller firms also have the least-sophisticated technology, making them actually easier to compromise.

Fiction: IT can handle it.

Fact: Many IT organizations can barely keep up with the applications they support. Add PCI to this and they're overloaded. Beyond IT, PCI requirements state that a business must maintain a security policy, which affects every level and function of a company. To make it all work, outside help from a specialist could be the right, timely answer.

Fiction: PCI compliance is too costly.

Fact: While the upfront costs could run into the thousands, compliance solutions do not have to be complex and costly to maintain. Actually lowering ongoing costs is generally what drives an organization to outsourced managed solutions. And remember, the financial risks associated with noncompliance such as loss of business, fines and legal fees can easily exceed compliance costs.

Fiction: We're PCI compliant, so we're secure.

Fact: PCI compliance is an assessment made at a point in time, not a guarantee. Security exploits are constant, making compliance a continual process to ensure safety to cardholder data. Also, PCI compliance is specific to payment data. The data associated with all other in-store applications may not be addressed by your current solution.

PCI requirements will continue to evolve just as the threats to your customer and company data will. Your best approach is to get the facts and not rely on false assumptions.

The continued viability of your business could rest with the actions you do or don't take. Fortunately, the card industry has published numerous resources online, and solutions providers stand ready to assist if you still have questions and are in need of proven, cost-effective solutions. ■

Dan Glennon is senior vice president of marketing and strategy for Cybera Inc. Cybera's solutions integrate all enterprise applications with a single managed security and network solution. Contact him at (866) 4CYBERA, or visit the Cybera Web site at www.Cybera.net.

Maurice P. Minno is a partner of CFSG, focused on providing unique, compelling and market-leading branded customer loyalty programs. CFSG partners with Cybera for the delivery of PCI Compliance and connectivity option solutions. Contact him at (760) 250-7791, or visit the CFSG Web site at www.CFStrategy.com.