Compliant—But Secure?

According to the Identity Theft Resource Center, the number of data breaches rose nearly 50% in 2008, compromising the personal records of at least 35.7 million Americans. With fines, lawsuits, damage to brands and very unhappy customers, this is serious.

Notable security breaches include TJX, Hannaford Bros. and Heartland Payment Systems. TJX suffered a breach starting in 2005, when a vulnerable wireless network was used to download tens of millions of credit-card numbers. Estimated total impact to TJX is more than $100 million.

Hannaford Bros. Supermarkets suffered a breach of debit- and credit-card information from more than 200 stores. And after being alerted by Visa and MasterCard of suspicious processing-system intrusion activity in 2008 and early 2009, Heartland Payment Systems launched an investigation that revealed "malicious software" had compromised data in Heartland's network. Heartland's systems breach has cost the company more than $12.6 million in fines from Visa and MasterCard, legal bills and administrative costs, plus untold losses from clients switching to competitors as a result of the breach.

Closer to home, at NACStech a few months ago, two out of three speakers in one of the PCI panel sessions had experienced a compromise of their card information. Examples such as these have driven PCI awareness and IT investing in solutions for compliance to all-time highs.

Yet instances of security breach are on the rise. Why?

Baseline Definition, Not Breach-Proof

As a starting point, what does being PCI compliant mean? It simply means that through an audit process the data environment has been deemed compliant with the guidelines set forth in the Payment Card Industry (PCI) Data Security Standard (DSS). The PCI-DSS is an effort by the payment-card industry to provide businesses that process card payments a baseline with which to prevent fraud through increased controls around data and its exposure to compromise.

PCI compliance, however, does not, and cannot, ensure data security under all circumstances. By focusing on the minimum check-box compliance, a merchant may pass a compliance audit, but that doesn't necessarily mean that it is free from risk.

Change Is Constant

One misconception among merchants is the notion that achieving compliance means data is secure now and forever more. While compliance does mean that certain security guidelines have been met, there is no guarantee. Further, an audit takes place only at a specific point in time. However, all application, network and data environments evolve over time. Employees come and go, requiring new user accounts, systems get upgraded, applications are added, etc. To manage the change, and potential vulnerabilities, implementation of security tracking and reporting software, along with change-management policies, are highly recommended.

The Threat Within

Many devices can be physically attached to an open network port and used to collect the data traveling between the point-of-sale (POS) terminal and the data processor. This can happen from an outside source, but it often occurs when someone on the outside is connected to an employee on the inside. This is exactly what happened to TJX, which is still dealing with the fallout from its breach.

Any new applications or devices added to the network can represent a potential threat: an employee plugging in a laptop to download a music file, Wi-Fi access for visiting regional managers or customers, etc. All have the potential to compromise the security of the network. While it is possible to add these local-access technologies, appropriate firewall and Intrusion Detection and Prevention (IDP) capabilities are required.

Complexity Perplexity

Security and compliance solutions can be complex and costly if a merchant chooses to set up and maintain technology itself. One example is a firewall used to segment a network, but it's an effective security solution only if it is properly configured *at all times*. Many merchants look at investing thousands of dollars for firewall solutions at each site, only to find that the ongoing management of the configuration in each store is a full-time job for a highly qualified network or security specialist. For most, this simply isn't feasible. A good start is upgrading the POS system, but even this does not address all the potential security holes.

> PCI compliance does not, and cannot, ensure data security under all circumstances.

Don't Fly Solo

While the latest-generation POS systems have the ability to be PCI compliant from the get-go, the POS system (and vendor) can't do it all. Inevitable changes to the environment and lack of oversight can lead to a vulnerable and unsecure environment for your data. Far from being complicit, the internal IT resources responsible for the systems and data are often stretched as thin as possible.

So what's the answer? Increasingly, outsourcing security and network solutions has become attractive as a way to save both time and money while providing additional expertise and independent oversight. The managed service providers themselves are held to strict guidelines for PCI compliance. The current status of any vendor can be checked on Visa's Web site. Merchants also benefit from a lower total cost of ownership through better buying power from providers and technology vendors, consolidating vendor management, faster issue resolution and availability of subject-matter expertise.

With security breaches on the rise, smart merchants are realizing that a 24/7 approach to network security, in addition to becoming PCI compliant, is the best way to protect customers' critical data. This also frees up the internal IT staff to support the applications and in-store user community to ensure a superior customer experience. And happy customers are definitely a good thing. ■

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. Call 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, branded and market-leading customer loyalty rewards program solutions. CFSG is partnered with Cybera for the delivery of PCI compliance, network and connectivity applications. Call him at (760) 250-7791, or visit the CFSG Web site at www.CFStrategy.com.