The Evolution of Security in the Payments Industry

Over the past few years, high-profile data security breaches have resulted in a new mantra for merchants, VARs and ISOs everywhere: "Get it Out!"; meaning "out of my store," "off my property," out of my business." And for good reason; the risks and overhead associated with protecting cardholder data have resulted in excessive time, labor and expense for everyone in the payments industry.

By Michelle G. Wagner

Mitigate Risk & Reduce Cost

In 2010, the mantra isn't likely to change as businesses look to implement solutions to better secure and manage the storage, processing and retrieval of transaction data. Everything from how an account number enters the payment stream, to where and how it is stored for reconciliation and record-keeping, is being analyzed in an effort to mitigate risk and reduce the costs and scope associated with PCI compliance measures and audits.

The Industry Responds

As a whole, the payments industry has done a good job of coming together to combat fraud by creating best practices and new solutions that help protect the integrity of cardholder data. PCI and PA-DSS formed a solid baseline standard that forced businesses to take a close look at their systems that store, transmit or process card numbers and associated customer data. However, as was demonstrated through recent breach activity, PCI compliance itself will not prevent an attack from happening. As a result, many industry-wide initiatives have been undertaken to securely manage data and shift the associated liability and risk.

Have You Heard About. . .?

Buzz words like "tokenization," "pre-authorization pop-ups," and "E2EE" are now scattered throughout the payment industry's lexicon, yet it's important to note that there are no standards for implementation. Security is a not a product, but a process that must continuously be tested, implemented and enhanced. There's more to security than designing strong cryptography into a system; it's designing the entire system such that all security measures work together.

Additionally, while every new system coming to market promises to elicit a "wow" factor, the fact is many retailers are strapped with incompatible legacy systems; the reality of an enterprise-wide replacement is simply not feasible, especially in the current economic environment. And while many tout the benefits of true "end-to-end" solutions, it's also important to note that most merchants have implemented a multi-vendor strategy to handle payments across their enterprise — terminals, POS/PMS systems & software, gateways, front-end processors, back-end acquirers, and professional services providers all play a role in the end-to-end processing of transactions. Getting all these disparate systems to work together is not a plug-and-play solution; rather it requires collaboration, integration and certification from all providers.

Hard Costs, Hard to Swallow

The ugly truth is that merchants are faced with a real threat that, while too risky to ignore, results in significant organizational costs. As the average cost of a data breach increases, the costs of PCI compliance multiply in kind; often totaling millions of dollars per year for Tier 1 merchants. Businesses are faced with increased resource costs to monitor and maintain systems, as well as ongoing audit and system scanning costs to adhere to PCI compliance standards.

But that may pale in comparison to an actual security breach, with potential fines — investigation, communication, reissuance, fraud losses — applied per account affected. And the reputational damage can't be ignored; no merchant wants to be in the headlines when the topic deals with stolen customer data.

The Evolution of Security in the Payments Industry (continued)

Solution: Cut Costs, Not Corners

There is good news when it comes to facing the security challenge head-on: the cost of compliance can be off-set by shifting liability and risk and utilizing new security methods that either mask account numbers or entirely remove cardholder data from entering the payment stream, thus substantially reducing the scope of PCI audit requirements while simultaneously meeting stringent security standards.

The challenge often lies in finding the best vendor to get the job done. Merchants must weigh the promises of new technology against the reputational and financial stability of solution providers. Are they a company that will be there for the long haul? Do they have the deep pockets necessary to keep ahead of constantly changing security standards? Do their systems offer complete redundancy throughout every aspect of the process, ensuring maximum uptime; after all, the inability to retrieve information necessary to make adjustments, process chargebacks, or share with third-parties, will render a "whiz-bang security" promise neutral.

One Size Doesn't Fit All: Finding the Right Solution

Elavon understands that businesses can't wave a magic wand to instantly solve all the security challenges they face. The answer lies in implementing solutions that are realistically aligned with company goals. The best way to start is through a detailed analysis of all systems, processes and practices in place, taking into consideration the associated expense of upgrades, certifications and installations.

A conversation with Elavon's experienced Service and Support experts can result in the exploration and implementation of various solutions to mitigate risk and the associated liabilities and costs. Years of experience has led us to develop a comprehensive portfolio of solutions to support a wide variety of business environments, including:

- Hosted gateway solutions that move critical cardholder data from a merchant's location to a centrally-managed host within a secure data center at Elavon

- Tokenization, pop-up, and card-on-file solutions that replace account numbers with Unique IDs
- Secure Device Modules that support the removal of all cardholder information from the POS/PMS
- End-to-end solutions that protect data at every point in the transaction process through encryption / decryption technology
- Integration solutions for legacy POS/PMS systems that help reduce PCI liability, while avoiding the labor and costs of system-wide upgrades

Elavon understands that downtime is not an option. Our solutions are built on proven, dependable and redundant technology that delivers maximum uptime. And they are backed by a financially stable company that has been dedicated to the payments space for nearly 20 years. For more information, please visit www.elavon.com. ■

Michelle G. Wagner | Vice President, Global Marketing Solutions

Michelle Wagner is responsible for managing all aspects of product marketing, communications, and training for Elavon, a leading global payments company. She led the effort to rebrand the company in 2008, and oversees the delivery of all products and programs through Elavon's multiple direct and indirect sales channels.

Ms. Wagner joined Elavon in 2004. She has more than 20 years experience in the electronic payments industry. Prior to joining Elavon, she was vice president of delivery marketing at VeriFone, managing all global product launch and communication efforts. She has held various product and marketing positions for payment and loyalty companies throughout her tenure in the payments industry.