intronis
cloud backup + recovery

PCI Compliance is More Than a Matter of Dollars (and Sense)

Are Your Clients Properly Protected Against Lost or Stolen Data?

Overview

Every electronic transaction creates an opportunity for unscrupulous activities to occur. When these activities are corrupted, the damage can be significant; ranging from a simple one-time illegal purchase by a clerk or waitress using a customer's credit information, to a full-blown identity theft using thousands (even millions) of people's stolen personal data. Neither situation is desirable or tolerable in the business community, especially when both can be prevented or curtailed with the implementation of industry-proven security best practices and the proper systems.

That's why businesses that deal with credit transactions must remain particularly diligent, addressing each of the specific "danger areas" associated with processing. Without the proper security processes and technologies in place, their client data could be compromised or stolen, and the repercussions of a breach go much further than lost customer confidence. Lawsuits and financial restitution can be significant, especially if the activity is the result of the retailer not following well publicized best practices.

In order to provide greater guidance to businesses that accept credit cards and ensure that their clients are properly protected, the major payment card organizations established a set of standards that have been implemented over the past few years. American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. came together to create the Payment Card Industry Data Security Standard (PCI DSS). These rules provide an actionable framework for securing payment card data, including deterrence, discovery and the appropriate response to breaches and other security-related events.

PCI DSS version 2.0 (implemented January 1,′ 2012) applies equally to all businesses that store, process or transmit bank cardholder data. Failure to comply with these rules can result in hefty penalties, regardless of a merchant's intent or lack of awareness. The latest version extends the implementation, feedback, review and revision processes to a three-year cycle (previously two-years), and updates key security provisions including firewall protection, password and key management, and related documentation.

These standards impact a number of organizations that participate in retail operations, including merchants, payment card issuing banks, processors, developers and technology vendors. Of course, solution providers who support these businesses play a major part in PCI DSS, ensuring that their clients (as well as their end user customers) understand the systems and protection required to fulfill their obligations.

VARs and managed services providers have a tremendous opportunity with retailers, as long as they can offer solid guidance, implementation and support services needed to appropriately address these standards.

The Basics of PCI DSS

In order to help merchants navigate and better understand the conditions and implications of these standards, the PCI Security Standards Council has taken great pains to distribute the most critical information to everyone involved. Despite their efforts, the material can be cumbersome and hard for many retailers to comprehend. That's where solution providers can really excel, filtering out the critical details and offering sound advice to help merchants meet the compliance requirements that pertain to their particular organizations.

Even though the PCI Security Standards Council developed the specific standards addressed in this paper, compliance is actually mandated by the individual payment card companies. Visa, MasterCard, American Express, Discover and JCB International each have their own specific requirements and compliance levels. While many of these are minor, solution providers need to understand the nuances of each to ensure their clients are aptly protected.

For example, while PCI DSS compliance is divided into four general merchant categories, each credit card company may add their own stipulations to each. Solution providers who service the retail vertical need to not only understand the differences, but to ensure their clients payment processes adhere to those variations.

The general PCI DSS categories include:

- Compliance level 1: Those who process more than 6,000,000 transactions per year, as well as those with a previous security violation/data breach or who have been listed as category 1 by a particular credit card company. This status requires yearly on-site reviews by an internal auditor, as well as a network scan by an approved scanning vendor (ASV).

- Compliance Level 2: Businesses with between 150,000 to 6,000,000 transactions per year. Merchants must complete an annual Self-Assessment Questionnaire (SAQ) and submit to a network scan using an approved scanning vendor.

- Compliance Level 3: Retailers that process 20,000 to 150,000 transactions per year. Also requires annual completion of a SAQ and a network scan with an approved scanning vendor.

- Compliance Level 4: Merchants with less than 20,000 transactions per year. Same annual requirements as Level 2 and Level 3 merchants.

Although they conduct the fewest transactions, Compliance Level 4 retailers make up approximately 99% of the businesses that process credit cards in the United States and typically have the least amount of IT support. The lack of a dedicated onsite IT security professional presents a serious risk for retailers, and a significant opportunity for solution providers with PCI DSS skills.

With many businesses lessening their dependence on "cash only" policies, and others moving to "cashless" transactions, the focus on PCI DSS compliance is expected to intensify. Since every company that accepts credit must obey the standards, its prevalence presents a great new specialty practice opportunity for VARs and MSPs. Of course, the first thing solution providers need to know is the t**hree critical steps in PCI DSS compliance.**

1. PCI DSS compliance:

1. **Assess**: identify cardholder data, inventory the company's IT assets and business processes for payment card processing, and analyze each for security weaknesses.

2. **Remediate**: address perceived vulnerabilities and remove unneeded cardholder data.

3. **Report**: compile and submit remediation authentication records (if applicable), and provide compliance reports to each bank and payment card company they do business with.

PCI DSS standards mirror the practices that security-oriented solution providers already employ, following industry practices to properly protect the data and infrastructure of their business customers. While some of the terms and acronyms used by retailers and payment processing vendors may be unique, the basic processes and technologies required to secure their information and infrastructure don't differ significantly.

2. The Solution Provider Role (and Accountability)

While PCI DSS can be complicated for the novice solution provider, the payment card industry understands the important part they play in compliance. To help those who build and support secure payment applications, the PCI Security Council created a number of compliance-related resources and programs. That includes the Payment Application Data Security Standard (PA-DSS) and a list of "Validated Payment Applications" to select from, along with Self-Assessment Questionnaires that allow merchants to authenticate their current security procedures.

Compliance goes beyond credit card processing systems. It extends to the network, data storage infrastructure and any method involved in the management or transport of customer data, with responsibility falling on the merchant and those who support it. Solution providers who fail to implement PCI DSS compliant solutions may find themselves liable (at least in part) for any damages their clients and their customers suffer. Fines levied by banks and credit card institutions on noncompliant merchants can range from $5,000 to $500,000, and lawsuits from compromised end user data can push those costs much higher.

To be successful in the retail vertical, solution providers just need to follow the **six control objectives for PCI DSS:**

1. **Build and Maintain a Secure Network**
    - Install and maintain an effective firewall configuration to protect cardholder data
    - Avoid vendor-supplied defaults for system passwords and related protection measures

2. **Protect Cardholder Data**
    - Protect all stored cardholder data
    - Encrypt transmission of cardholder data across open, public networks

3. **Maintain a Vulnerability Management Program**

- Employ and update anti-virus software on a continual basis
- Develop and maintain secure systems and solutions

4. **Implement Strong Access Control Measures**
   - Restrict access to cardholder data by business necessity
   - Assign a unique identification to each person with system and network access
   - Restrict physical access to cardholder data (door locks, alarms and other safeguards)

5. **Regularly Monitor and Test Networks**
   - Track and monitor all access to networks, applications and cardholder data
   - Regularly test system protection and processes

6. **Maintain an Information Security Policy**
   - Maintain a policy that addresses data security

To address the specific requirements of PCI DSS, providers need to validate every procedure and technology solution their clients use in electronic payments, from the card swipe device to their data storage policies. That attention to detail must also include a continual review of all vendor offerings, verifying that their data protection methods are effective and identifying (and fixing) potential vulnerabilities. The same diligence is required when it comes to evaluating cloud applications and offsite storage services. By ensuring that vendor offerings are PCI DSS compliant when properly implemented, and periodically validating those systems' security settings, solution providers fulfill a big part of their responsibilities. Of course, they still need to work closely with suppliers to communicate potential risks, failures or other issues that could compromise the security of their clients' data.

3. Concerns and Opportunities Related to PCI DSS

Every new business practice comes with some risk. Solution providers who add a retail specialty to their portfolio have to pay careful attention to the specific hazards associated with credit transactions. Since the most important aspects of PCI DSS are data protection and network security, most channel professionals have at least the basic skills needed to support this market.