Payment Card Security Compliance

What it is and why you should care

BY CHRIS VON RABENAU

In 2006, the major payment card vendors agreed to cooperate on a single standard for electronic data security that would be enforceable across the payment card industry. This agreement led to the creation of the Payment Card Industry Security Standards Council (PCI-SSC). Beside payment card vendors, the Council includes stakeholder representation from payment processors, merchants, banks and equipment manufacturers. The work of the Council ultimately created the Payment Card Industry Data Security Standard (PCI-DSS). Each of the founding members agreed to incorporate the PCI-DSS into the technical requirements for its own data security programs.

PCI-DSS ACRONYMS

PCI-DSS: Payment Card Industry Data Security Standard

PCI-SSC: Payment Card Industry Security Standards Council

PCI-PED: Payment Card Industry PIN Entry Device

VISA CISP: Visa Cardholder Information Security Program

PABP: Payment Application Best Practices

MasterCard PTS: POS Terminal Security standard

PCI-DSS is a security standard for electronic payment card data. It is outlined in a 12-point list of requirements within six principles of security concern: security management, policies, procedures, network architecture, software design, and other critical protective measures (see www.pcisecurity standards.org/tech/index.htm for more information).

Payment card vendors (MasterCard Worldwide, Visa International, American Express, Discover Financial Services and JBC) consider compliance with PCI-DSS mandatory if a merchant accepts credit cards. Failing to abide by this standard is not illegal, but opens any merchant failing to follow the standard to legal liability for any security breach resulting in stolen payment card information. In addition to being financially liable for the direct costs of a security breach, the merchant may be liable for penalties assessed by the payment card vendors, costs which are assigned to payment card processors but passed on to the merchant.

The cost of non-compliance

The estimated direct cost of a security breach is in the neighborhood of $180 per compromised card. This cost includes credit monitoring, notifying those affected (a legal responsibility in most states), and fielding customer queries. This does not include the cost of forced equipment replacement, damage to your brand, or potential fines. Using an example of a merchant handling 1000 cards per day, a breach of a single day's system could result in a direct cost of over $180,000. Considering that forensic investigations typically take 20–30 days to trace a breach back to a specific merchant, the direct cost for a single breach can inflate quite rapidly from hundreds of thousands to millions of dollars.

Just as security is not a static field, neither is the PCI-DSS. There are sunrise and sunset dates for each version of the standard. In other words, you may be compliant today, but that does not mean you will be compliant tomorrow. It is important to understand the PCI-DSS expectations for your organization as well as the sunrise/sunset dates that are relevant to you. Though compliance with PCI-DSS does not guarantee shelter from a security breach, it does demonstrate a good faith effort to protect your customers' electronic data. This good faith effort will be considered by any payment card vendor if and when levying fines.

The majority of co-ops are "Tier IV" operators. Tier IV operators process fewer than 1,000,000 bank card transactions (or fewer than 20,000 e-commerce transactions) per year. At present, in addition to POS-related hardware and software compliance, Tier IV operators are only required to annually complete the Self Assessment Questionnaire and to quarterly perform a network scan. Outside consultants may be hired to support both activities and are available. However, completion of this questionnaire will still require the integral support of internal staff, because it focuses not only on systems that are in place to protect electronic resources but also on business processes.

In the case of the quarterly network scan, assistance from external network security organizations provide the benefit of audited finding and remediation recommendations. There are also intrusion detection systems, such as ARUBA Network's Network Chemistry, that constantly monitor and protect the network and hence fulfill the obligation of quarterly network scans.

Where to start?

The first step is to contact your point of sale (POS) vendor and directly ask about the PCI compliance status of the system and, if necessary, begin to remedy the state of your POS. The second step is to contact your bank card vendor to determine the PCI status of your bank card terminals. These two items are the most pressing to address, because fixing PCI non-compliance with these systems will require a direct outlay of capital. As a side note to these items, be sure to query vendors on the PCI compliance status of any new equipment or software involved in the processing of bank cards.

The next step, the Self Assessment Questionnaire, has been shown to be the most time

INFORMATION RESOURCES

The PCI-DSS standard: www.pcisecuritystandards.org/tech/download_the_pci_dss.htm

This is a link to the actual standard. You will need to agree to abide by its policies before you gain access to the standard.

PCI-DSS User Group: www.forum.aegenis.com

This is a user group focused on PCI standards implementation.

Verifone Sercurity Retail Payments site: www.secureretailpayments.com/

Verifone is one the largest credit card terminal companies in the world and has taken a very strong stand in support of the PCI-DSS standards. It is the only vendor on the PCI-SSC.

Five Myths of PCI compliance: www.tinyurl.com/2qywly

This is a great set of articles on PCI compliance.

PCIRisk video from Retail System Provider Association (RSPA): www.youtube.com/profile?user=PCIRisk

Anyone not convinced about the need to implement PCI-DSS should watch this two-part series. It is an excellent explanation of what PCI compliance is and the ramifications of not being compliant.

PCI SELF ASSESSMENT QUESTIONNAIRE

Section 1: Build and maintain a secure network
Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Section 2: Protect cardholder data
Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Section 3: Maintain a vulnerability management program
Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

Section 4: Implement strong access control measures
Requirement 7: Restrict access to cardholder data by business need-to-know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

Section 5: Regularly monitor and test networks
Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Section 6: Maintain an information security policy
Requirement 12: Maintain a policy that addresses information security

consuming and controversial of the steps. Its purpose is to challenge internal systems and force correction where systems fail to meet a standard of PCI compliance. The Self Assessment Questionnaire steps out of the POS front end and looks at processes and security on the back side of the operation as well. The initial self assessment may take some time, not only for completion but in remediation.

The most challenging aspect of the self assessment is that there are no silver bullets. The implementation of PCI, in this sense, is in the eye of the beholder. Only in the instance of a breach will an entity that has completed its Self Assessment Questionnaire know whether it has fulfilled the obligation implied by the PCI standard.

As director of information technology for National Cooperative Grocers Association, it is my goal to make you aware of PCI-DSS so that your co-op will research the issue and take the steps necessary to ensure compliance. ■