Ten myths muddling PCI mastery

By Ross Federgreen
CSRSI

Merchants are becoming acutely aware of the mandated requirements of the Payment Card Industry (PCI) Data Security Standard. Unfortunately, many misconceptions, or myths, are associated with this. It is important that members of the merchant services community fully understand PCI and assist their customers with the complexities of compliance.

Myth 1: I do not have to be PCI-compliant

Untrue. Every merchant who in any manner accepts, handles, stores or transmits credit card information must be compliant. This extends to all merchants regardless of their credit card environment. There are no exceptions for merchants who are in the card present environment.

Myth 2: If I have penetration scans, I am compliant

Wrong. Penetration (or vulnerability) scans represent only a fraction of PCI's requirements. While they are important, they are not all that is required. Merchants must also complete the 75 questions comprising the annual self-assessment questionnaire (SAQ).

Myth 3: To complete the SAQ, I can just answer yes to all the questions

Not true. Merchants should only answer yes if they both understand the question and possess documented evidence that the answer should be yes. Fabricating yes answers is inappropriate and opens merchants to severe penalties, including loss of credit card privileges.

Myth 4: No one will ever look at my answers to the SAQ

Untrue. PCI requirements dictate that all merchants must file SAQs with their acquirers annually. If merchants are compromised, risk rated, randomly audited or flagged for other reasons, their SAQ responses will be examined.

Myth 5: I don't need to examine my completed penetration scans

Wrong. It is vitally important to examine penetration scan results and note findings. Each abnormal finding must be addressed regardless of which of the four levels – from informational to severe – is listed. Findings in the severe category must be remediated within 30 days.

Myth 6: If my software or terminal is compliant, I am compliant

Not true. To answer SAQ questions correctly and honestly, every merchant must have written policies, procedures and auditable logs. And significant physical security requirements must be met. PCI-compliant software and terminals are critical, but they are not the entire answer.

Myth 7: A breach can't happen to me

Untrue. Security breaches happen everywhere and can happen to anyone at anytime.

Myth 8: All security breaches are caused by external sources

Wrong. Over 90% of security breaches occur because of employees or other people who have internal access to the merchant.

Myth 9: My processor is responsible for the fines, not me

Not true. Merchants are ultimately responsible for all financial penalties resulting from their PCI-compliance failures. Fines can be up to $25,000 per month per event.

Myth 10: I can complete the SAQ myself

True – but no one should. The 75 questions on the SAQ are complex. To answer them requires in-depth understanding of the meaning and intent of each question. Each merchant should obtain qualified assistance in achieving PCI compliance.

Focus on facts

All ISOs and merchant level salespeople need to fully understand PCI. And merchants need to know that they *must* comply with PCI: Noncompliance can lead to civil penalties, criminal prosecution and loss of credit card accepting privileges.

The payment brands have spent considerable sums attempting to educate the merchant population. A number of resources are available to assist in helping merchants achieve compliance. *The Green Sheet* has published many articles addressing PCI issues.

In addition, each card brand has information on its Web site defining requirements and merchant categories.

So, learn what it really takes to be PCI-compliant. This will help you maintain, retain and obtain merchant customers.

Ross Federgreen is founder of CSRSI, The Payment Advisors, a leading electronic payment consultancy specifically focused on the merchant. He can be reached at 866-462-7774, ext. 23, or rfedergreen@csrsi.com.