Ten Common Myths of PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) secures cardholder data that is stored, processed or transmitted by merchants and processors. PCI DSS specifies 12 requirements entailing many security technologies and business processes, and reflects most of the usual best practices for securing sensitive information. The resulting scope is comprehensive and may seem daunting – especially for smaller merchants who have no existing security processes or IT professionals who help guide them through what is required and what is not. To complicate matters, some vendors who sell security products or services market their products in a broader context than just the PCI DSS requirements. As a result, retailers who are new to security may harbor myths about the PCI DSS. The PCI Security Standards Council presents ten common myths about PCI DSS to help your business optimize protection of cardholder data and ensure compliance with the standard.

GOALS OF PCI DSS

Build and maintain a secure network

Protect cardholder data

Maintain a vulnerability management program

Implement strong access control measures

Regularly monitor and test networks

Maintain an information security policy

Myth 1 – One vendor and product will make us compliant

Many vendors offer an array of software and services for PCI compliance. No single vendor or product, however, fully addresses all 12 requirements of PCI DSS. When marketing focuses on one product's capabilities and excludes positioning these with other requirements of PCI DSS, the resulting perception of a "silver bullet" might lead some to believe that the point product provides "compliance," when it's really implementing just one or a few pieces of the standard.

The PCI Security Standards Council urges merchants and processors to avoid focusing on point products for PCI security and compliance. Instead of relying on a single product or vendor, you should implement a holistic security strategy that focuses on the "big picture" related to the intent of PCI DSS requirements.

Myth 2 – Outsourcing card processing makes us compliant

Outsourcing simplifies payment card processing but does not provide automatic compliance. Don't forget to address policies and procedures for cardholder transactions and data processing. Your business must protect cardholder data when you receive it, and process charge backs and refunds. You must also ensure that providers' applications and card payment terminals comply with respective PCI standards and do not store sensitive cardholder data. You should request a certificate of compliance annually from providers.

Myth 3 – PCI compliance is an IT project

The IT staff implements technical and operational aspects of PCI-related systems, but compliance to the payment brand's programs is much more than a "project" with a beginning and end – it's an ongoing process of assessment, remediation and reporting. PCI compliance is a business issue that is best addressed by a multi-disciplinary team. The risks of compromise are financial and reputational, so they affect the whole organization. Be sure your business addresses policies and procedures as they apply to the entire card payment acceptance and processing workflow.

PCI AT-A-GLANCE

(visit www.pcisecuritystandards.org for more information)

Overview

Getting Started with PCI DSS

10 Common Myths of PCI DSS

Data Security Do's and Don'ts

Getting Started with PA-DSS

Getting Started with PCI PED

Myth 4 – PCI will make us secure

Successful completion of a system scan or assesssment for PCI is but a snapshot in time. Security exploits are non-stop and get stronger every day, which is why PCI compliance efforts must be a continuous process of assessment and remediation to ensure safety of cardholder data.

Myth 5 – PCI is unreasonable; it requires too much

Most aspects of the PCI DSS are already a common best practice for security. The standard also permits the option using compensating controls to meet some requirements. The standard provides significant detail, which benefits merchants and processors by not leaving them to wonder, "Where do I go from here?" This scope and flexibility leads some to view PCI DSS as an effective standard for securing *all* sensitive information.

Myth 6 – PCI requires us to hire a Qualified Security Assessor

Because most large merchants have complex IT environments, many hire a QSA to glean their specialized value for on-site security assessments required by PCI DSS. The QSA also makes it easier to develop and get approval for a compensating control. However, PCI DSS provides the option of doing an internal assessment with an officer sign-off if your acquirer and/or merchant bank agrees. Mid-sized and smaller merchants may use the Self-Assessment Questionnaire found on the PCI SSC Web site to assess themselves.

Myth 7 – We don't take enough credit cards to be compliant

PCI compliance is required for any business that accepts payment cards – even if the quantity of transactions is just one.

Myth 8 – We completed a SAQ so we're compliant

Technically, this is true for merchants who are not required to do on-site assessments for PCI DSS compliance – for that particular moment in time when the Self-Assessment Questionnaire and associated vulnerability scan (if applicable) is completed. After that moment, only a post-breach forensic analysis can prove PCI compliance. But a bad system change can make you non-compliant in an instant. True security of cardholder data requires non-stop assessment and remediation to ensure that likelihood of a breach is kept as low as possible.

Myth 9 – PCI makes us store cardholder data

Both PCI DSS and the payment card brands *strongly* discourage storage of cardholder data by merchants and processors. There is no need, nor is it allowed, to store data from the magnetic stripe on the back of a payment card. If merchants or processors have a business reason to store front-card information, such as name and account number, PCI DSS requires this data to be encrypted or made otherwise unreadable.

Myth 10 – PCI is too hard

Understanding and implementing the 12 requirements of PCI DSS can seem daunting, especially for merchants without security or a large IT department. However, PCI DSS mostly calls for good, basic security. Even if there was no requirement for PCI compliance, the best practices for security contained in the standard are steps that every business would want to take anyway to protect sensitive data and continuity of operations. There are many products and services available to help meet the requirements for security – and PCI compliance.

When people say PCI is too hard, many really mean to say compliance is not cheap. The business risks and ultimate costs of non-compliance, however, can vastly exceed implementing PCI DSS – such as fines, legal fees, decreases in stock equity, and especially lost business. Implementing PCI DSS should be part of a sound, basic enterprise security strategy, which requires making this activity part of your ongoing business plan and budget.