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 to 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 DSS compliance. No single vendor or product, however, fully addresses all 12 requirements of PCI DSS. When marketing focuses on one product's capabilities to the exclusion of other PCI DSS requirements, the resulting perception of a "silver bullet" might lead some to believe that a point product provides "compliance," when it really only addresses just one or a few elements of the standard.

The PCI Security Standards Council urges merchants, service providers and processors to avoid focusing on point products for data security and PCI DSS 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. This approach includes people and processes, not just technology.

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 when you 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 proof of compliance annually from providers.

Myth 3 – PCI DSS 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.

Myth 4 – PCI DSS will make us secure

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

Myth 5 – PCI DSS 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 of using compensating controls to meet most 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 DSS 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 assesses and validates compensating controls. However, the payment card brands provide the option of doing an internal assessment with an officer sign-off if your acquirer and/or merchant bank agrees. The PCI SSC also provides training for Internal Security Assessors (ISAs). Smaller merchants may be eligible to self-assess their compliance and validate using the Self-Assessment Questionnaire (SAQ) found on the PCI SSC web site.

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

PCI DSS 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

SAQs are validation tools for eligible merchants and service providers to report that they have evaluated their PCI DSS compliance through a self-assessment. It represents a snapshot of the particular moment in time when the Self-Assessment Questionnaire and associated vulnerability scan (if applicable) is completed. After that moment, only another assessment or post-breach forensic analysis can prove PCI DSS compliance. But a single system change can make you non-compliant in an instant. True security of cardholder data requires non-stop assessment and remediation to ensure that the likelihood of a breach is kept as low as possible.

Myth 9 – PCI DSS 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, or equivalent data from a chip. If merchants or processors have a business reason to store front-of-card information, such as cardholder name and primary account number (PAN), PCI DSS requires this data to be protected, and the PAN to be encrypted or otherwise made unreadable.

Myth 10 – PCI DSS is too hard

Understanding and implementing the 12 requirements of PCI DSS can seem daunting, especially for merchants without a large security or IT department. However, PCI DSS mostly calls for good, basic security. Even if there was no requirement for PCI DSS 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 DSS compliance.

When people say PCI DSS 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.