

PCI White Paper Series

Compliance Driven Security



1 Table of Contents

- 1 Table of contents2
- 2 Compliance Driven Security3
 - 2.1 The threat3
 - 2.2 The solution3
- 3 Why comply?3
 - 3.1 The threat3
 - 3.2 Benefits3
 - 3.3 Efficiencies4
 - 3.4 Meeting the intent of the standard4
- 4 Requirements cannot be implemented in isolation5
 - 4.1 PCI DSS is not a checklist5
 - 4.2 Ask for help5
 - 4.3 Compliance is for life not just for audit5
 - 4.4 Compliance cannot be achieved by buying appliances5
 - 4.5 Compliance is not security5
 - 4.6 Achieving compliance through security6

2 Compliance Driven Security

2.1 The threat

Information security has been a necessity ever since people realised that information assets had value. In modern times, computer systems allow for the storage and processing of large volumes of data that present rich targets to organised crime, foreign intelligence and opportunists. This is exactly the problem faced by organisations that conduct electronic financial transactions, in particular, credit card transactions.

Customer credit card data has become a major target globally with well resourced organised crime syndicates and freelancers eager to meet demand by hacking into the databases and computer networks of major businesses, particularly in the retail sector, to extract credit card data for financial gain. A simple internet search returns hundreds of rows of consumer credit card data offered as a sample of vast databases of stolen records.

2.2 The solution

To combat this threat, the five major credit card brands have introduced various schemes requiring their partners to implement information security controls. The most recent evolution being the Payment Card Industry Data Security Standard (PCI DSS).

Complying with the PCI DSS is a requirement for any organisation that processes, transmits or stores credit card data. In fact the scope can even include third parties that provide service that could impact on another organisation's credit card processing systems.

3 Why comply?

3.1 The threat

PCI DSS provides organisations with a direct business driver for implementing a robust level of baseline information security controls across their organisation, at least within the parts of the business that deal with credit card transactions. The options for an organisation are to either comply with the standard or cease to process credit card transactions and if you are the victim of a breach, endure heavy fines, financial fallout and reputation damage.

3.2 Benefits

While it is possible to focus on the downside of non-compliance as a driver, in reality there are many positive sides to PCI compliance. The PCI DSS provides a comprehensive information security framework that details technical controls interwoven with the policies, procedures and standards to make the controls effective on a day-to-day basis.

By properly implementing the PCI DSS and achieving and maintaining compliance, an organisation is better prepared to prevent and detect a host of attacks against their information assets both at the network and physical level. PCI compliance can improve operational efficiency by ensuring that policies are defined and procedures are documented so that employees know what they should be doing and how to do it. Controls, policies and procedures developed for PCI can be rolled out across the organisation to spread the security benefits and reap the greatest return on investment from a PCI compliance project.

In addition, the PCI-DSS has been developed and is maintained, to protect against the most prevalent threats to data security in general. Many of the controls required can be applied in other areas of the business which would help secure sensitive corporate data sets and intellectual property. For instance, by applying the same set of standards to company firewalls protecting the cardholder data environment, an organisation can improve the awareness of their attack surface, reduce the administrative burden of managing bloated rule sets and lead to increased resistance to attack. Having already developed the policies, procedures, configuration standards and administrative expertise for compliance purposes, the incremental cost of extending the controls to other parts of the business is often marginal.

3.3 Efficiencies

Automation of processes such as patching, AV updates and log review free up internal resources to tackle the more challenging problems rather than wasting their time fire fighting from one incident to the next. Improved internal monitoring makes it easier to spot potential incidents developing and provides better quality data for investigation and troubleshooting, reducing the time taken to perform these activities.

Good quality information security reporting can identify controls that are effective and highlight trouble spots that need attention, for example “why does this branch office have so many virus outbreaks?” or “why is this user regularly logging in out of hours and making large data transfers?” Many times IT managers realise that they could be more efficient by adding layers of controls, but cannot get the budget or resources. With PCI compliance as an additional driver, the manager can often get the resources or spend approved.

3.4 Meeting the intent of the standard

Unlike other standards in the IT industry, the PCI DSS makes very prescriptive statements about what an organisation is required to do to protect their systems. Certain requirements could appear onerous and may require a large investment. Ultimately, the standard is about achieving a robust baseline level of data security. Ideally, all of these requirements would already be standard practice and most are based on best practice advice that has been around for years. Where a requirement can't be met for a legitimate business reason, a compensating control that provides an equivalent or better level of protection can be implemented.

Determining the acceptability of a compensating control requires negotiation with your PCI QSA (Qualified Security Assessor) and your Acquirer. It is more important to meet the intent of a requirement than to follow the standard to the letter. The ultimate aim is to improve the security of your systems and protect the valuable and sensitive cardholder data that your customers have entrusted to you.

4 Requirements cannot be implemented in isolation

4.1 PCI DSS is not a checklist

Often the approach taken to implementing an IT standard is to develop a checklist of audit items and work through them so you can be confident that come audit time, you will pass with flying colours. The strict audit checklist approach can set you down the wrong path when approaching the PCI DSS. The standard describes an eco-system of policies, procedures and controls that work together to improve security by preventing and detecting attacks on your network and data. To start with Requirement One and work down the list will create extra work and require systems to be repeatedly revisited and modified.

The optimal approach is to deconstruct the DSS and follow a phased approach to implementation. The PCI Standards Council helps in this area by providing documentation and workbooks on a recommended prioritised approach. See here for further details: https://www.pcisecuritystandards.org/education/docs/Prioritized_Approach_PCI_DSS_1_2.pdf

Controls must be implemented effectively, according to both the PCI-DSS and in a way that the organisation can manage on a day to day basis. Security activities must be conducted regularly and continuously. As soon as an organisation stops performing the maintenance, monitoring and review activities required by the PCI DSS they become non-compliant, no matter what the result of their last audit. For some organisations this can involve a major culture change, and this is often the hardest part of the compliance exercise.

4.2 Ask for help

Getting expert advice from the very start can significantly reduce the pain and effort of creating a strategy for achieving compliance. SecureWorks offer clients expert consultancy via our team of experienced PCI certified Qualified Security Assessors to identify gaps in your existing information security policies, procedures and controls and planning the most effective method to remediate the required issues. Some issues are more complex and take longer than others, so getting started early is key.

For example

- The PCI DSS requires (Requirement 12.1.1) that the information security policy addresses all of the items within the PCI DSS but leaving this until last requires going back over everything that has been done before and documenting it. Designing the high-level policy in advance and filling in the gaps throughout the project provides a guide to implementation from the very beginning and ensures that accurate information is captured at the time of a system being deployed.
- The PCI DSS requires a vulnerability management policy and associated procedures and this will influence various other requirements such as those for vulnerability scanning, penetration testing, secure development, secure coding training and review of industry threat intelligence. All of which are scattered through different requirements in the PCI DSS.

When creating an implementation plan group tasks in related areas. Often the DSS requires a policy statement for a specific control or system component, implementation of a control, documentation of the control configuration, documented procedures for monitoring and management. Producing these items in parallel improves the fidelity of captured information and reduces the overall effort.

4.3 Compliance is for life not just for audit

While compliance with some IT standards means passing a yearly audit, PCI requires you to be compliant all of the time. The audit is a verification of compliance but if you don't follow the procedures you create, don't update configuration documentation, don't update anti-virus or patch servers, don't monitor logs and IDS systems you are not compliant. Any previously produced "report on compliance" will be invalid and fines for any breaches will be heavy.

Getting compliant is only the beginning. While many organisations struggle to achieve a compliant state the real difficulty is maintaining compliance. It is relatively easy to install a firewall, or IDS or log management system but without trained experience people to monitor them and respond when necessary you are not compliant and have wasted a lot of money.

Managed services can be a massive help in this area. A managed service provider removes the burden of having the staff with vendor specific skills to manage each appliance and brings the added ability to provide 24/7 monitoring and response capability using specialist security personnel who are both skilled and experienced.

4.4 Compliance cannot be achieved by buying appliances

Point solutions such as security appliances and computer software are only the first step to compliance. For an organisation without dedicated security staff, that are trained and experience in managing firewalls, IDS, log management systems, SIEM system and all of the other controls that PCI require, managed services provide a simple route to compliance.

Managed service providers help you stay compliant by meeting the PCI requirements for ongoing maintenance, configuration review, log review and network monitoring, only alerting you when there is a genuine need. This frees up the valuable time of your staff to handle the other one hundred and one responsibilities that they have. Not only does a managed service help you achieve and maintain compliance but reportable security metrics allow you to easily demonstrate compliance resulting in a huge reduction in effort when the next annual audit comes around.

4.5 Compliance is not security

PCI can seem like a lot of work and the temptation is to try to do the minimum required to pass an audit. However, this is a false economy. This approach will likely result in your investment in time and money failing to provide the security expected by you and the PCI DSS. A post-breach investigation will likely find you to have been non-compliant at the time of breach as has been the case for every breach to date. Which is as good as having done nothing from the start. You'll still have to make the same or greater expenditure after the fact, but with a much higher cost – in terms of money and your reputation.

4.6 Achieving compliance through security

Use the PCI DSS as a framework for implementing robust security controls that protect your valuable data and, as a side effect, ensure that you are compliant. Security is an ongoing process that involves all aspects of a business and cannot be delegated to appliances that run quietly in the data centre or to third parties who stamp you compliant. Consider the aspects of the standard that you are best placed to meet on your own and ask for help with the rest.