

Wake up call for Acquirers and Merchants



The Payment Card Industry (PCI) Data Security Standard has evolved to its current release level of Version 1.1 Release: September 2006. It defines a set of twelve requirements that must be met by each entity in the payment transaction lifecycle. These requirements apply to all system components included in or connected to the cardholder environment. This whitepaper provides the background to the standard, to whom it applies, and how a business should approach compliance with the standard.

How can O-C Group Help?

O-C Group has been founded by a team of Payment Industry experts with decades of experience in the industry. Through their management of the full development lifecycle of mission critical systems, supporting real-time transaction processing, the team is uniquely skilled and experienced to provide your organisation with the knowledge and know how to refine your systems and procedures to prepare your organisation for a PCI audit.



For more information see our web site at <http://www.o-cgroup.com> or contact us at info@o-cgroup.com.

Phone: +353 1 415 1205

Who is affected

The much published T.J.Maxx credit card data compromise combined with the Hannafords compromise highlights the need for more vigilance in Data Security at all points in the transaction chain. The card schemes are empowered to fine members for any compromise for which they were responsible. This places the onus on the acquirer to ensure that they continue to meet the PCI Data Security Standard. To avoid guilt by association, acquirers should be working with their service processors, merchants and payment service providers to ensure compliance across all entities that touch the credit card transaction.

As T.J.Maxx recover after the compromise and recede from the glare of publicity, it is timely that we consider the potential sources of such compromises.

Already one state is considering legislation that will make companies, responsible for a data breach, liable for all costs associated with the breach. e.g. Companies would have to cover the cost of issuers re-issuing a card portfolio.

Massachusetts Bill Would Make Companies Pay for Poor Data Security

http://www.darkreading.com/document.asp?doc_id=118059

February 23, 2007 Companies doing business in the Bay State may soon face stiff penalties for wayward security practices as Massachusetts is now considering legislation that would place these companies on the hook to pay for any costs associated with a data breach of their IT systems.

External Risk - The use of third parties

In this interdependent world, where every company utilises the services of multiple companies in the delivery of their product or service, ensuring that all entities with access to the sensitive card data are PCI compliant is a challenge. Acquirers need to develop a process to ensure that all their third parties are PCI compliant, including their service processors, merchants, call centres and payment service providers. This needs to be an on-going process that ensures that each entity provides an annual update on their compliance status. The process should be integrated into the contract review so that all new third party relationships have this obligation reflected in their contracts.

Internal Risk – The Human Element

Affording access to sensitive data, however necessary to support business operations, represents a significant risk. While Security Awareness Programs within organisations have helped enormously, the frequency of such training can be an issue. Annual programs need to be put in place to re-iterate the message, and special provision needs to be made for new employees throughout the year.

Internal Risk – Data Stores

The internal risks reflect those risks that are directly under the control of each company subject to PCI Compliance. The principle means of a bulk compromise is use and manipulation of data outside the controlled environment of an application.

Internal Risk - Data in transit

Much of the focus of data security has been around the database, however there are many other sources where data can be compromised. All organisations, involved in credit card processing need to inventorise where data lands and transits.

An often overlooked area for consideration is the various file receiving and sending activity in which your company engages. Here we are talking about transaction files either from merchants or indeed the various transactions files to and from the card schemes. Seldom are these files encrypted. In fact the card schemes require you to send these files in the clear to their processing centres. Ask yourself, where do these files reside in your organisation after transmission and are they encrypted?

Off-host analysis is another source of compromise. This may take the form of receiving a file extract from the central datasource and performing desktop analysis on it either using a spreadsheet package or a local desktop database. Worst case is that this is performed on a laptop which is later stolen or a desktop that is compromised.

Internal Risk – Web Services

As web services grow in their deployment and use both internally and externally in organisations, users are availing of many download capabilities. Some of these downloads can contain sensitive data.

Some Questions to consider

Whilst there is wide-spread acceptance of the importance and need for the PCI standard, there is increasing evidence that companies successfully achieving PCI compliance sign off, are falling down on its on-going application. Astute acquirers are asking the following key questions.

Are you sure that all entities in the transaction chain are PCI certified and audited?

Are all current staff aware of their data security obligations?

Is any card data transmitted over unsecured channels e.g. Email, Internet?

Is any card data (normally resident in a database) extracted to be further analysed?

What happens sensitive data files after transmission/receipt?

Do web services permit the download of card data (either internally or externally)?

Benefits of Compliance

The PCI Security Standards comprise a number of security best practices. The implementation of these requirements does improve the overall security of your environment and improves the security awareness of your employees. In an environment, where business reputation is of paramount importance, the successful implementation of the PCI standard is a further endorsement of your policies and procedures. Beyond that the key benefits are:

- Protects your customer data.
- Improves customer confidence through higher levels of data security.
- Protects your organisation from financial losses.
- Derive benefit from an annual health check of your systems security.