



A CORSAIRE WHITE PAPER  
THE PAYMENT CARD INDUSTRY  
DATA SECURITY STANDARD

<b>Author</b>	Chris Leppard
<b>Document Reference</b>	The Payment Card Industry Data Security Stand v1.0.doc
<b>Document Revision</b>	1.0
<b>Date</b>	06/02/2007



# PCI Data Security Standard

---

## Table of Contents

<b>TABLE OF CONTENTS</b> .....	<b>2</b>
<b>THE SITUATION:</b> .....	<b>3</b>
<b>Introduction</b> .....	<b>3</b>
<b>What is the PCI DSS?</b> .....	<b>3</b>
<b>THE PROBLEM:</b> .....	<b>6</b>
<b>THE IMPLICATION:</b> .....	<b>8</b>
<b>Company Director Responsibilities</b> .....	<b>8</b>
<b>Managing Director Responsibilities</b> .....	<b>9</b>
<b>Finance Director Responsibilities</b> .....	<b>10</b>
<b>Chief Information Officer Responsibilities</b> .....	<b>12</b>
<b>Operations Director Responsibilities</b> .....	<b>14</b>
<b>Human Resources Director Responsibilities</b> .....	<b>15</b>
<b>CONCLUSION</b> .....	<b>16</b>
<b>The Benefits of the PCI DSS</b> .....	<b>16</b>
<b>REFERENCES</b> .....	<b>18</b>
<b>ACKNOWLEDGEMENTS</b> .....	<b>18</b>
<b>About The Author</b> .....	<b>18</b>
<b>About Corsaire</b> .....	<b>18</b>



# PCI Data Security Standard

---

## The Situation:

### Introduction

The Payment Card Industry (PCI) Data Security Standard (DSS) is a requirement for all organisations that process payments, develop products for payment or store payment card details. The PCI compliance standards were developed to establish a 'minimum security standard' with regards to the protection of cardholders' account and transaction information.

Many vendors are unclear as to their roles and responsibilities with regard to compliance to the PCI DSS. This paper is aimed at senior and executive management and is designed to show how the various elements of the PCI DSS will affect your organisation and what you will need to do to achieve compliance.

### What is the PCI DSS?

The PCI DSS is a worldwide benchmark for payment card security. It was initially developed by MasterCard and Visa in 2004. Since then, it has been adopted by all the major card issuers and is now under the guidance and control of the PCI Security Standards Council (known as 'PCICo'), which was formed by the major card issuers. The PCI DSS version 1.1 (September 2006), specifies 12 requirements in 6 areas for compliance:

#### *Build and Maintain a Secure Network*

- 1: Install and maintain a firewall configuration to protect cardholder data
- 2: Do not use vendor-supplied defaults for system passwords and other security parameters

#### *Protect Cardholder Data*

- 3: Protect stored cardholder data
- 4: Encrypt transmission of cardholder data across open, public networks

#### *Maintain a Vulnerability Management Program*

- 5: Use and regularly update anti virus software
- 6: Develop and maintain secure systems and applications



# PCI Data Security Standard

---

## *Implement Strong Access Controls Measures*

- 7: Restrict access to cardholder data by business need-to-know
- 8: Assign a unique ID to each person with computer access
- 9: Restrict physical access to cardholder data

## *Regularly Monitor and Test Networks*

- 10: Track and monitor all access to network resources and cardholder data
- 11: Regularly test security systems and processes

## *Maintain an Information Security Policy*

- 12: Maintain a policy that addresses information security

Each of the requirements is further subdivided to introduce a level of granularity and detail. For instance, Requirement 1 specifies that you must 'install and maintain a firewall configuration to protect cardholder data.' Section 1.1 specifies that the firewall configuration standards should include 'a formal process for approving and testing all external network connections and changes to the firewall configuration' (1.1.1) and 'a current network diagram with all connections to cardholder data, including any wireless networks' be maintained (1.1.2)

It should also be noted that while MasterCard and Visa have aligned behind the PCI standard (merchant levels, security audit & scan procedures and QSAs); they each have specific requirements for compliance validation reporting, enforcement procedures and fines. Each company individually issues compliance notices and holds lists of approvals granted.

## *Merchant Levels*

The PCI DSS categorises merchants according to the number of card transactions processed. It is important to understand this as it identifies the steps that need to be taken each year to maintain adherence to the standard. PCI DSS specifies 4 levels:

### *Level 1 Merchant*

- Over 6 million transactions a year
- Merchants who have suffered an attack that resulted in account data compromise



# PCI Data Security Standard

---

- Any merchant, at the discretion of the card schemes, who is deemed to require Level 1 compliance

## *Level 1 Requirements*

- Annual On-Site Security Audit and Quarterly Network Scans must be performed by an Independent Security Assessor, Qualified Independent Scan Vendor or Internal Audit if signed by an Officer of the Company

## *Level 2 Merchant*

- 150,000 to 6 million transactions a year

## *Level 2 Requirements*

- Annual self assessment questionnaire
- Quarterly scan by a PCI Approved Scanning Vendor

## *Level 3 Merchant*

- 20,000 to 150,000 transactions a year

## *Level 3 Requirements*

- Annual self assessment questionnaire
- Quarterly scan by a PCI Approved Scanning Vendor

## *Level 4 Merchant*

- Less than 20,000 transactions a year

## *Level 4 Requirements*

- No need to report compliance but must maintain compliance

To help organisations achieve compliance a number of firms have been accredited by PCICo to be either a Qualified Security Assessor (QSA) or an Approved Scanning Vendor (ASV). The QSA is authorised to complete the onsite security audit required for Level 1 merchants; the ASV will complete the quarterly scans required by Level 1, 2 & 3 merchants. Lists of authorised suppliers are maintained on the PCI DSS website



# PCI Data Security Standard

---

## The Problem:

So why does the payment card industry feel that there is a need to impose this standard on merchants and processors? The answer is the increasing number of security breaches that are being reported.

The most infamous example is that of CardSystems Solutions. MasterCard investigated a security breach at the Atlanta-based company in 2005, where hackers stole 263,000 credit card numbers, exposed 40 million more and several million dollars of fraudulent credit and debit card purchases were made with counterfeit cards. As a result of the breach, CardSystems was very nearly forced out of business and was eventually purchased by PayByTouch. The CardSystems hack is considered by IT security experts to be the most severe publicised information security breach ever. It caused company shareholders, financial institutions and card holder's damage estimated in the millions of dollars.

The PCI DSS is the direct response to incidents such as this. However, the biggest problem facing all organisations that potentially have to achieve PCI DSS compliance is that the requirements are very broad and subject to interpretation. PCICo, set up to manage the PCI DSS, has also been accused of not providing enough information or assistance to merchants.

Compliance to the PCI DSS is NOT optional. The card schemes have stated that they can and will impose fines on those organisations that do not seek compliance by 30<sup>th</sup> June 2007. In some cases these fines could run into hundreds of thousands of pounds. Other punishments will include the merchant being permanently excluded from the card acceptance programme. It is likely that there will be several high profile 'examples' to illustrate that the card schemes will use the punishments on those organisations that have chosen not to be compliant.

The combination of a lack of information and help and the compulsory nature of the standard has naturally left many senior executives feeling uneasy about their responsibilities and the steps they should be taking to avoid the fines and the negative publicity that will inevitably follow.



# PCI Data Security Standard

---

Despite the efforts of the payment card industry, there will inevitably be some organisations that will not be compliant by June 2007. Whether this is through ignorance, the (perceived) lack of information and help from PCI Co or a deliberate decision to ignore the Standard, the outcome for those companies will be at best, a loss of revenue. In the worst cases, some companies will cease trading.

The problems faced by non-compliant firms will include:

- Financial penalties
- Withdrawal of point-of-sale equipment
- Revocation of card scheme membership
- Negative publicity
- Loss of consumer and supplier confidence
- Reduction in sales revenue

The business world is littered with stories of how poor publicity can damage an organisation. The Coca Cola Company operate one of the strongest and most well known brands in the world. Yet even they managed to create a spectacular global PR disaster in 2004, by trying to pass off tap water as 'pure' bottled water. The 'Dasani' brand was irreparably damaged, destroying a £7 million marketing campaign in the process and causing a massive drop in the Coca Cola share price.

The Coca Cola Company was able to survive this problem because of its vast resources and powerful marketing department. Most firms are not so lucky. Adopting an 'ostrich approach' and hoping that the issue of PCI DSS compliance will go away is not going to work.



# PCI Data Security Standard

---

## The Implication:

### Company Director Responsibilities

To help explain what work will need to be completed, we will use the example of a successful, medium sized business with a thriving Internet-based shop that is processing an estimated 40,000 customer payment card transactions a year.

At a board meeting, the question of compliance with the PCI DSS has been raised. The Managing Director has asked the board members (Finance Director, Chief Information Officer, Operations Director and Human Resources Director) to report on the current state of compliance and to identify those areas that will need to be improved or upgraded to achieve compliance.

The following pages are designed to highlight the relevant areas of the PCI DSS for each of the executives identified above. It should be noted that this paper is concerned with compliance to the PCI DSS only and not country-specific government regulatory requirements that, in many cases, will exceed those of the PCI DSS.

Each of the requirements of the PCI DSS should not be seen as being mutually exclusive. The PCI DSS has two main purposes: the protection of information and the protection of customer identities. In most cases to achieve this there will be an overlap in the areas of responsibility for each of the directors.

It is essential that a senior manager (normally the Chief Security Officer) is appointed to oversee the compliance procedure. He or she should be the single point of contact and liaison for QSAs and ASVs and should also be responsible for ensuring that staff and management are kept informed of the progress made in gaining PCI DSS compliance.



# PCI Data Security Standard

---

## Managing Director Responsibilities

The Managing Director (MD) is responsible for the whole company. It will be the responsibility of the MD to ensure that all board directors are aware of the requirements of the PCI DSS and that they will be able to handle its implementation.

You are concerned with all of the requirements for the PCI DSS, as this will have a direct impact on general consumer confidence and ultimately, your customers. The ability to demonstrate adherence to the Standard will show that your organisation has adopted best practice methods to maintain the security and integrity of the personal data that you hold.

Adherence to the PCI DSS should be seen as a very positive step, rather than an additional burden. In many cases, it will prepare your organisation for compliance with other regulations.

### *Primary Actions*

The MD should ensure the following are undertaken:

- Request a timetable for the implementation of the PCI DSS
- Promote the benefits of the PCI Standard throughout the organisation



# PCI Data Security Standard

---

## Finance Director Responsibilities

The Finance Director (FD) is primarily responsible for ensuring that the financial integrity of the company is maintained at all times. For the PCI DSS, the FD will be mostly concerned with the following areas:

### *Protect Cardholder Data*

- 3: Protect stored cardholder data
- 4: Encrypt transmission of cardholder data across open, public networks

### *Implement Strong Access Controls Measures*

- 7: Restrict access to cardholder data by business need-to-know
- 8: Assign a unique ID to each person with computer access
- 9: Restrict physical access to cardholder data

The protection of stored cardholder data will be of the greatest concern because this will be the data most at risk from hackers and unauthorised access. It also represents the greatest threat to the organisation in terms of fraud and brand, often the company's biggest asset. .

Subsection 3.1 states that 'cardholder data storage is kept to a minimum'. It will also be necessary to develop a 'data retention and disposal policy'.

Subsection 3.4 is also of particular importance as it specifies how the company should handle and store the Primary Account Number (PAN). The treatment of the PAN is fundamental to the application of the PCI DSS. If your company stores, processes or transmits information relating to the PAN, then you WILL be required to comply with the PCI DSS. There are no exceptions to this rule.

The most common elements of cardholder and sensitive authentication data are shown in figure 1. The table is not exhaustive, but does serve to illustrate how different security requirements must be applied to the various data elements.



# PCI Data Security Standard

Figure 1: Common elements of cardholder and sensitive authentication data

	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4
Cardholder Data	PAN	YES	YES	YES
	Cardholder Name*	YES	YES	NO
	Service Code*	YES	YES	NO
	Expiration Date*	YES	YES	NO
Sensitive Authentication Data**	Full Magnetic Stripe	NO	N/A	N/A
	CVC2 / CVV2 / CID	NO	N/A	N/A
	PIN / PIN Block	NO	N/A	N/A

\* These elements must be protected if stored in conjunction with the PAN

\*\* Sensitive authentication data must not be stored after authorisation

To ensure that an audit trail exists and that it is possible to detect whether card data has been tampered with, it will be necessary to ensure that the organisation implements a layered approach to data security. A reliance on a single perimeter security device, such as a firewall, will not be sufficient to achieve PCI DSS compliance.

It is a requirement of the PCI DSS that controls are in place to prevent unauthorised access to card data from both external and internal sources. It is no longer acceptable to automatically treat an internal resource as trusted.

## *Primary Actions*

The FD should check to ensure that the following policies and practices are in place:

- All payment card data is stored on encrypted hard drives
- Appropriate controls are in place for the storage of the encryption keys



# PCI Data Security Standard

---

- An acceptable usage policy for all IT systems, with definitions for the use and storage of passwords, should be documented and distributed to all members of staff

## Chief Information Officer Responsibilities

The Chief Information Officer (CIO) is the person responsible for the security of the company's communications and other business systems, especially those exposed to intrusion from external hackers.

The process of PCI DSS compliance is likely to have the most impact on the CIO. Although any organisation that has already implemented best practice procedures (such as properly maintained firewalls, staff usage policies etc) may find that they have already completed many of the requirements for PCI DSS compliance.

For the PCI DSS, the CIO will be primarily concerned with the following areas:

### *Build and Maintain a Secure Network*

- 1: Install and maintain a firewall configuration to protect cardholder data
- 2: Do not use vendor-supplied defaults for system passwords and other security parameters

### *Maintain a Vulnerability Management Program*

- 5: Use and regularly update anti virus software
- 6: Develop and maintain secure systems and applications

### *Regularly Monitor and Test Networks*

- 10: Track and monitor all access to network resources and cardholder data
- 11: Regularly test security systems and processes

### *Maintain an Information Security Policy*

- 12: Maintain a policy that addresses information security

The construction of a secure network infrastructure is the goal of all CIOs. The nature of this type of network construction will inevitably mean that applications such as anti virus programs are routinely



# PCI Data Security Standard

---

deployed across the entire network infrastructure. It is important to understand however, that the PCI DSS requirements apply to all system components.

The PCI DSS defines system components as any network component (firewall, switch, router, wireless access point etc.), server or application that is included or connected to the cardholder data environment. The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data (see Figure 1).

In this instance, the first job of the CIO should therefore be to ensure that a complete network audit is undertaken to identify all devices that may have to be certified as compliant.

In addition, Requirement 6 specifies the need for secure systems and applications. This may mean that you will need to implement a secure application development lifecycle, which could require a significant investment both in time and money to achieve.

As the CIO of an organisation that is processing approximately 40,000 payment card transactions a year, this makes you a Level 3 merchant. The organisation will be required to submit an annual self assessment questionnaire and have a quarterly external scan completed by a PCI ASV.

## *Primary Actions*

The CIO should initially complete the following:

- Appoint a senior manager (normally the Chief Security Officer) to oversee the PCI DSS compliance project
- Request that a thorough network and application audit be completed
- Appoint an ASV to carry out the quarterly scans
- Review the need for a secure application development life cycle



# PCI Data Security Standard

---

## Operations Director Responsibilities

The Operations Director (OD) is tasked with ensuring that the organisation continues to function day-to-day in the most efficient manner possible. Although the impact of the PCI DSS is less obvious, it is possible that it will mean that new procedures and work practices need to be introduced.

For the PCI DSS, the OD will be primarily concerned with the following area:

### *Implement Strong Access Controls Measures*

- 7: Restrict access to cardholder data by business need-to-know
- 8: Assign a unique ID to each person with computer access
- 9: Restrict physical access to cardholder data

As the organisation has grown rapidly, in response to customer demands, you are aware that devices and server access controls have been relaxed to allow staff to 'multi-task'.

The PCI DSS puts in place a strong requirement to design systems to allow for audit trails to be established. If this is to be achieved, it is essential that all staff are allocated a unique identification number and that access to all systems concerned with the processing of payment card details, can be tracked and logged.

The OD will be required to liaise with the CSO and CIO to establish which systems will require auditing and then ensure that this is implemented correctly.

### *Primary Actions*

The OD should check the following:

- Identify those systems and staff who process payment card details
- Develop revised procedures to ensure that user access can be logged
- Promote awareness of the PCI DSS requirements through staff workshops and training



# PCI Data Security Standard

---

## Human Resources Director Responsibilities

Dependent on the size of the company, the Human Resources Director (HRD) may be responsible for employment, compensation, benefits, training and development and employee relations.

The impact of the PCI DSS is most likely to affect the HRD with regards to policy and procedure. The HRD will be primarily concerned with the following area:

### *Regularly Monitor and Test Networks*

10: Track and monitor all access to network resources and cardholder data

### *Maintain an Information Security Policy*

12: Maintain a policy that addresses information security

The HRD would be expected to have a considerable amount of input to both the staff usage policies and the management of staff relations through regular updates and bulletins. The requirements of the PCI DSS mean companies will be forced to track staff usage of critical payment systems.

This raises questions about the invasion of staff privacy. In many countries, the monitoring of user activity is heavily regulated by government legislation. Policies may need to be rewritten to expressly allow the monitoring of staff activity. In some countries, companies would be required to obtain individual staff consent.

Whilst the intention of the PCI DSS is to protect and secure data, it may be seen by some as an overly invasive policy and this will require careful management by the HRD to ensure that the reasons for implementing the Standard are clearly explained.

### *Primary Actions*

The HRD should check the following:

- Review staff policies relating to computer usage
- Review country-specific privacy regulations
- Liaise with the CIO to ensure that new policies and procedures are correctly implemented



# PCI Data Security Standard

---

## Conclusion

### The Benefits of the PCI DSS

The PCI DSS is simply the latest initiative by the payment card industry to try and improve data security and therefore increase consumer confidence in the use of payment cards. The card schemes are obviously keen to promote the benefits of the PCI DSS and these include:

- Improved consumer confidence
- Increased spending on payment cards
- To demonstrate and uphold best practice
- Protect brand and company reputation
- Potentially reduce the loss of revenue and legal costs associated with a security breach
- Promote good customer and public relations

In a perfect world, there would be no need to have a data security standard, such as the one devised by the PCI. All organisations would treat customer data with the up most importance and ensure that it was properly stored and encrypted at all times.

However, the reality is sadly very different. The PCI DSS has been developed out of necessity to maintain consumer confidence in the various payment card schemes. The payment card schemes are all too aware of the detrimental effect on their brands from the continuous stream of reported security breaches that have exposed customer payment card data.

There will now be a scramble for scarce security consultancy resources to help the many thousands of organisations who will need to be compliant with the new standard before June of this year. It is likely that many will find themselves in an almost impossible position, with a lack of resource and a large amount of remedial work to complete in a short space of time.

It is possible to complete the audit process without the use of a QSA. However, this will require that the necessary resources and expertise available in house to complete the project. Any organisation that has not considered the impact that PCI DSS will have on their business should do so now and seek the help of an appropriately experienced security consultancy as a matter of urgency.



## PCI Data Security Standard

---

The positive side to the PCI DSS is that it should dramatically improve the standard of data security for many organisations. This will have benefits beyond the payment card industry because there is no reason why the requirements of the Standard cannot be applied to other data stored within the corporate network.

Corsaire's principal security consultants have vast commercial and technical expertise. They understand that PCI DSS compliance is about more than just implementing the correct technical processes and procedures; it requires an understanding of how an organisation functions and where necessary, a realignment of its business practices.

Organisations must realise that the PCI DSS is not a one-off compliance requirement; it is an ongoing commitment to best practice data security. It will require continued vigilance and improvement as necessary to maintain data integrity. Organisations that embrace the Standard will reap the benefits for many years to come.



# PCI Data Security Standard

---

## References

The Payment Card Industry Security Standards Council ([www.pcisecuritystandards.org](http://www.pcisecuritystandards.org))

The Payment Card Industry Data Security Standard version 1.1 (September 2006)

MasterCard Site Data Protection Program ([www.mastercard.com/sdp/](http://www.mastercard.com/sdp/))

Visa Account Information Security Programme (<http://www.visaeurope.com/aboutvisa/security/>)

## Acknowledgements

This white paper was written by Chris Leppard MBCS CISSP, Technical Account Manager at Corsaire.

## About The Author

Chris has more than 15 years experience in IT and IT security, working in both technical and sales capacities. His career has taken him from the banking industry to major Telco's and specialist security consultancies. In recent years he has concentrated on technical sales, providing complex IT security solutions to a number of FTSE 250 clients.

## About Corsaire

Corsaire is a market leader in information security consultancy and vulnerability research. Privately founded in 1997, we provide a range of consulting, assessment and research services to help organisations measure their security posture and build a thorough compliant security program to support their business strategy.

We operate on an international basis with a presence across Europe and the Asia-Pacific rim. Our clients include some of the world's best known blue-chip multinationals, many of whom are listed on the FTSE, DAX and Fortune 500 stock indices although we also have a selection of UK government authorities and mid-range organisations.

Most of our clients have been drawn from the e-banking, finance, telecommunications, insurance, legal, IT and retail sectors. They are all mature buyers, operate at the highest end of security and understand the differences between the ranges of suppliers in the current market place. For more information contact us at [info@corsaire.com](mailto:info@corsaire.com) or visit our website at <http://www.corsaire.com>