

» What is the Payment Card Industry Data Security Standard? «

A white paper by Gary Dawkin
Siemens Insight Consulting



The Payment Card Industry Data Security Standard (PCI) is the amalgamation of VISA's Cardholder Information Security Program (CISP) and Site Data Protection (SDP) created by MasterCard International. The PCI Standard was developed to provide a 'minimum security standard' with regards to cardholders' account and transaction information.

While card issuers introduce new security measures to make the use of a card more secure for an individual, identity theft around the globe is becoming an ever increasing problem. Measures such as this are often not enough to cater for organised crime, often more interested in the financial gains available from obtaining large quantities of customer details from one source than the lower volumes associated with physical card theft.

External threats are the most common consideration when data losses are first explored, yet reports show that at least seventy percent of information theft is by insider breach.

Who does it concern?

All parties involved in accepting credit or debit card payment, process, collect or store credit card transaction information. Regardless of the value of the transaction, these parties are required to meet the PCI Standard. Failure to meet the requirements set in the PCI Security Standard may result in substantial fines and/or the revoking of card processing privileges. The level of the fines will be proportional to the extent of data lost. While fines and loss of privileges are potentially tangible, the damage caused by bad publicity around the event is not. Bad publicity can be far more damaging than the penalties.

What if your data is compromised?

One high-profile case in America during mid 2005 led to 40 million accounts being compromised including 800,000 across Europe. Both VISA and American Express ceased dealing with the company and instructed acquiring banks to cease trading as well. As a result of the compromise and the publicity, the business ceased to be viable and began wind down proceedings.

On a smaller scale, towards the end of 2005, fraud losses of £600,000 from over 25,000 card details were traced back to merchants in Sweden. Although the case was not covered by the media, it caused severe disruption for both the third party processors and merchants involved. Forensic studies showed the cards were used in online gambling events, with many high value transactions, including one transaction for more than £23,000.

What are the penalties?

Both VISA and MasterCard have published fine schedules for PCI. Under VISA operating regulations, members may be assessed fines for data compromise or non-compliance with PCI requirements. First violation will receive fines up to \$50,000 for a rolling 12 month period or until the merchant demonstrates that all track data has been removed. A second violation will incur \$100,000 for a 12 month rolling period. Third violation details are at management's discretion. The MasterCard fine structure is slightly different, but merchants should expect initial fines of up to \$100,000 and \$10,000 per day after 60 days, not to exceed \$500,000 annually. At present, fines are shown in US Dollars. Please be aware that fines are levied across the globe.

What does the PCI Standard offer?

The PCI Standard has been designed to protect the handling of customer details throughout the payment cycle. It is broken into twelve main categories which, in turn, break down into around two hundred sub requirements. Compliance to PCI can be achieved in a number of ways. By far the simplest is to reduce the amount of data held. Many companies store card data because that is what they have always done or do not purge data after it is no longer needed. Often the data may be kept in the belief it is needed for transaction tracking, fraud detection, regulatory, legal or other business processing. While business needs do exist, the requirement is actually the card's transaction history, rather than the card's physical data.

The PCI elements are designed to complement each other. Achieving compliance in one section, but scoring badly in another will lead to a PCI failure.

The overall message in PCI is to store less data, but factors such as understanding the data flow, encryption, network and application vulnerabilities, improving security awareness and training, monitoring and network segmentation all play their part. Storage of card validation value (CVV) and personal identification numbers (PIN) are strictly forbidden, but other data can be kept. The MINIMUM account information that needs to be rendered unreadable is the payment card account number.

All elements of an infrastructure could be a potential source of data leak. Encryption of card data should take place at the source of entry. If encryption is only adopted when data is at rest then data compromise attempts may take place on its transition from application to database. PCI does not make any distinction between the use of hardware or software encryption methods, although it references options such as one way hashing, truncation, Index tokens with PADs or strong cryptography such as Triple DES (128 Bit) or AES (256 Bit) with secure key management.

The flow of data during day-to-day activities could leave unencrypted details in the database (strictly prohibited under PCI) or on devices and media that can be prone to loss or theft. Strict controls around identity management will ensure that only authorised users gain the necessary access to systems. Users must not be able to view card data, obfuscation methods must be used. The first six and the last four digits are the maximum allowed to be displayed. Regular database cleansing must take place to remove unnecessary details. Segmentation of the database server from the general network can further assist access controls.

PCI requires companies to track all access to card data and maintain a record of that. This section is all encompassing as it ties together other parts of the Standard. Without logging, it will be impossible to detect or determine the areas that may have suffered attack or an actual breach.

The benefits for your business

Around the world, there is a general expectation – and often legal requirement - that every business should protect its customers and specifically all data relating to them.

When adhering to PCI, not only will you achieve good security practices, you will also satisfy other guidelines - such as Principles defined by the Data Protection Act (DPA), such as:

- Identify if risks exist in the way your systems and processes store or transmit any card-holder data
- If risks are highlighted, you will be clearly able to define necessary solutions to resolve them
- Ensure that your service providers do not put your business at risk
- Demonstrate that you are serious about security.

Full compliance to PCI will protect against:

- Financial liabilities
- The risk of legal and investigative costs associated with compromise
- Unwanted public relations issues arising from compromise.

Common reasons given to keep card data

During PCI readiness investigations, many different areas of the business will express their need to see all card data. While some existing business processes may need some changes, most cases can be resolved with a well designed encryption solution, without the need to see the full card number again.

In my department all my staff need to see the card number for their job!

While the department may currently work in this way, all that you actually require is a unique number to identify each transaction throughout its lifecycle. Replacing the sixteen digit card number across the centre of each card, with a unique string of hashes will achieve this.

We don't perform e-commerce transactions, so how can we be hacked?

Around 70% of computer-based crime begins with company employees. They could be the most long-standing employees or the contractor that started on Monday.

Making card data unusable to unauthorised parties will remove temptation and protect your business. Generally, companies that do not offer e-commerce solutions have in-house systems better designed for workflow; where security is not a major consideration.

How can we track fraud without the card number?

You probably already have a fraud detection system in place with algorithms to spot activity. Now you will need to look for common hashed or encrypted numbers that link all transactions together. Upon finding a fraudulent transaction, you will be able to contact your acquiring bank to retrieve the original

We won't be able to offer refunds or chargebacks without the card number

You will know the date and time of the transaction and name of the customer and have probably created a number of other identifiers shared with the bank. Your acquirer will be able to send back card details matching those criteria. Run it through the encryption and match it to your records. You can then identify any transaction in question.

Removing card details is just too difficult

No one said it would be easy! Tasks required in order to purge card details from your system include removing legacy data and training staff on new ways to handle data. Your organisation faces many risks if this is not done. You may well consider accepting the risks, but unfortunately, the introduction of PCI means that the fine structure passes directly to the merchant. It also means that banks and acquirers with merchants that do not want to comply will begin to retract services because *they* will not want to accept the risk.

How do we comply with the PCI Standard?

The requirements to achieve PCI compliance are slightly different between the four different merchant's levels defined by VISA and MasterCard.

However, an annual assessment of system design and processes, plus quarterly external vulnerability scanning are common across them all.

Siemens Insight Consulting has significant experience in undertaking infrastructure reviews, secure network design, security awareness training and identity management solutions in order to deliver the requirements for PCI readiness.



Author's biography

Gary Dawkin is a Consultant at Insight Consulting. He has over 15 years Information Technology experience in both Lloyds Insurance Market and Financial sector environments.

Gary's specialist areas include secure network design, implementation, development and compliance, these include.

- Secure infrastructure builds for compliance to regulations. i.e. Payment Card Industry (PCI) and Sarbanes-Oxley (SOX)
- Networking perimeter security solutions including firewalls, email and web content checking, anti-virus solutions and reporting
- Undertaking and managing IT health checks, internal and external vulnerabilities
- Finding technical solutions to police internal policies in order to reduce time and overheads
- Working with IT Security Teams and project managers to meet the needs of the customer, while offering affordable levels of effective security without impacting performance.

Insight Consulting is the specialist Security, Compliance, Continuity and Identity Management unit of Siemens Communications and offers a complete, end-to-end portfolio encompassing:

- Security
- Continuity
- Managed Services
- Compliance
- Identity Management
- Training

Siemens Insight Consulting subscribes to the CESG Listed Advisor Scheme (CLAS) and CHECK services. We're also certified against BS 7799 and are a preferred supplier of services to the UK Government and are an accredited Catalyst supplier.

If you'd like to find out more about how we can help you manage risk in your organisation, visit our web site at www.siemens.co.uk/insight
Siemens Insight Consulting
Tel: +44 (0)1932 241000
Fax: +44 (0)1932 236868

www.siemens.co.uk/insight