PCI DSS 101:
The Background You Need for Understanding the PCI DSS

A New Net Technologies Whitepaper

Mark Kedgley

CTO - New Net Technologies

www.newnettechnologies.com

Abstract

Any organization storing, processing, or transmitting Primary Account Numbers (PAN) must comply with the Payment Card Industry Data Security Standard or PCI DSS.

Understanding the background, the objectives, and the detailed requirements of the standard is still proving to be a challenge for thousands of organizations around the world. This whitepaper aims to give a basic backgrounder in traditional '101' style.

> *"The PCI Security Standards Council... launched in 2004. The Council's five founding global payment brands -- American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa Inc. -- have agreed to incorporate the PCI DSS as the technical requirements of each of their data security compliance programs"*
>
> https://www.pcisecuritystandards.org/

What is it, and Why is it Important?

The Payment Card Industry Data Security Standard was designed as a comprehensive list of best practice measures and processes for handling, processing, storing, and transmitting payment card data.

The PCI DSS was formulated by the payment card companies such as Visa and Mastercard in response to the growing number of instances of theft and misuse of payment card details. The first version of the PCI DSS was released in December 2004 and mandates a wide range of measures required to ensure the protection of payment card data.

The measures are summarized in the 12 section PCI DSS, but a high-level overview can be broken down into 3 main areas

- **Active Technological Security Measures** (firewalls, intrusion detection systems, anti-virus, file-integrity monitoring, data encryption)
- **IT Security Best Practices** (masking of card data within applications, configuration 'hardening', regular updates to password and security keys, regular vulnerability scans and penetration tests, review of all security and audit logs)
- **General Security Best Practices** (such as physical building security measures and personnel awareness of IT Security measures)

Today, the PCI Security Standards Council has been established by the major payment card brands and is the body "responsible for the development, management, education, and awareness of the PCI Security Standards".

The 12 Point PCI DSS

The latest version of the PCI DSS is Version 3.2. It retains the same 12 Core requirements as previous versions of the standard, which in turn branch into more than 250 controls – the full standard can be accessed at https://www.pcisecuritystandards.org/security_standards/documents.php but the following is a summarized 'plain English' version.

1. *Use a Firewall – typically the core 'Card Data Processing' systems are segregated from the Corporate Network using an internal firewall in addition to any external internet-facing firewall*

2. *Secure system access through Configuration Hardening - use non-default passwords, SSL/TLS and SSH for any system access, disable unnecessary services and protocols to minimize accessibility*

3. *Use Masking and Encryption of Cardholder Data to ensure that data is unreadable if stolen, but only ever store as little data as possible*

4. *Use Encryption for any cardholder data when being transferred over public networks*

5. *Use Anti-Virus Software, regularly updated*

6. *Increase the inherent security of all systems through Configuration Hardening i.e. remove known vulnerabilities through patching and configuration settings*

7. *Use Identity and Access Management controls to minimize access to cardholder data system on a strict 'need to know' basis*

8. *Assign a unique ID to each user and enforce strong authentication*

9. *Lock your Doors – utilize physical security measures to restrict access to systems such as door locks, badge readers and video cameras*

10. *Track and Monitor all access to all network resources and cardholder data – centrally backup event and audit log trails, especially for logons*

11. *Get a Vulnerability Scan and Penetration Test by an Approved Scanning Vendor performed every 3 months and after nay significant network change. Use file-integrity monitoring to protect critical system and configuration files*

12. *Adopt an Information Security Policy to ensure there is an appreciation of the PCI DSS objectives by all employees and contractors*

As you can see, even in this greatly summarized format, there is a huge array of both technological requirements and procedural/organizational requirements needed.

So Who Exactly is Subject to the PCI DSS?

Regardless of what the tangible cost of payment card fraud actually is, there is no alternative for any card merchant but to comply with the PCI DSS. However, the burden of proving your compliance with the standard does vary according to the volume of transactions being processed.

Any merchant storing, processing or transmitting Primary Account Numbers (PAN) must comply with the PCI DSS.

Processing is often one of the key qualifiers in that, a PC used to access a secure on-line payment portal can still be defined as 'within scope' of the PCI DSS which means even small organizations are still subject to the PCI DSS. For instance, card 'skimming' techniques are widespread, generally targeting the card reader or PIN entry device, or via software installed on the PC making the transaction.

> *"6.4 Follow change control procedures for all changes to system components"*
>
> *https://www.pcisecuritystandards.org/*

The PAN must be rendered unreadable while the Cardholder Name, Service Code, and Expiration date can be stored in readable format.

Card data that absolutely must not be stored comprises:

- ***The Track 1 and Track 2 data*** (all the cardholder and card data is stored within two tracks on the card magnetic stripe and chip embedded on chip and pin cards)
- ***The Card Verification Value*** (CVV – typically the three digits printed onto the card signature strip)
- ***The PIN data*** (the card PIN number used to authorize a transaction on a Chip and PIN card)

All card transactions represent a risk, including ecommerce transactions. For Visa Merchants:

- ***Level 1 -*** Merchants processing more than 6 million transactions annually are required to have an on-site PCI Data Security Assessment and quarterly network scans. On-site assessments may be completed internally or by an outside Qualified Security Assessor or QSA.
- ***Level 2 -*** Merchants processing 1 million to 5,999,999 transactions annually are required to complete a Self-Assessment and perform quarterly network scans.
- ***Level 3 -*** Merchants processing 20,000 to 1,000,000 e-commerce transactions annually are required to complete a Self-Assessment and perform quarterly network scans.
- ***Level 4 -*** Merchants process less than 20,000 e-commerce transactions annually and all merchants across channel up to 1,000,000 VISA transactions annually and are required to complete an annual self assessment and annual security scans.

Sounds like a Lot of Work and Expense – What is the Cost Justification for the PCI DSS?

Trying to understand the actual cost of payment card fraud is not straightforward – by their very nature, fraudulent transactions are hidden.

Visa Europe report a level of fraud around 6 cents for every €100 spent. It is important to realize that this is the cost of fraud for Visa Europe itself (as opposed to the total cost associated with card fraud which would include lawsuit costs between merchants, acquirers and issuers). All the same, in 2009, those cards were used to make purchases and cash withdrawals to the value of more than €1.3 trillion. Doing the math, this would place an estimate on the cost of fraud to be €780M – just for Europe, and just for Visa.

In order to extrapolate these numbers, based on Visa Inc. Q1 FY 2010 earnings statement, Visa's global network processed payments totalling $4.4 trillion. Assuming Visa held a 38.3% market share of the credit card marketplace and 60.7% of the debit card market, the total value of payment card transactions for the world would be around $8.5 trillion. If Visa's notional 6 cents for every dollar formula was applied, this would give an estimated value of fraud for the global payment card market of $5 billion – although again, this is purely for the card companies themselves.

> *"Estimated Global Fraud - $78B*
>
> *Estimated Payment Card Fraud worldwide $5B"*

Compare this figure with other sources that suggest the overall cost of UK Plastic card fraud was nearly £610m in 2008, an increase of more 14% over 2007 (figures published by APACS, the UK Payment Industry). Extrapolating this number at the same 14% per annum increase would give a 2010 figure of over £730M(approx. $1.2 Billion) just for the UK.

Figures from the UK Card Association claim card fraud reduced by 20% in their most recent figures, based on January to June 2010 so these figures may be lower than estimated. Global estimates for the cost of Online fraud – including identity theft and all payment-card abuse and organized crime – reached around $78bn last year (according to research house Global Uncertainties)

If you are reading this as a Card Merchant though, the figures that will be more interesting for you are what the potential costs for you are. For Visa members, failure to report any suspected or confirmed loss of transaction data the member will be subject to a penalty of $100,000 per incident, rising to $500,000 depending on the scale and seriousness of the breach. Regarding remediation costs, most estimates cost this at between $90 and $302 per record.

The cost of compliance may also increase by way of making a compromised Tier 2,3 or 4 merchant subject to Tier 1 merchant PCI DSS requirements, with the more stringent auditing process being required.

The absolute penalty for a payment brand is to disqualify a merchant from being able to process card transactions.

It is worth mentioning that in one of the few publicized breaches, Heartland Payment Systems (*http://corporate.visa.com/media-center/press-releases/press974.jsp*) are agreeing to pay $60M in compensation to card issuers that have suffered losses as a result of the criminal breach of Heartland's systems. The loss of customer trust and the corporate shame of being exposed as an organization that has compromised their customers' personal data could ultimately be far more expensive.

What Happens in the Event of us Being Breached?

Visa provides the following steps for 'compromised entities':

- *Immediately contain and limit the exposure. Prevent further loss of data by conducting a thorough investigation of the suspected or confirmed compromise of information.*
- *Alert all necessary parties immediately. Including:*
  - ***Your internal information security group and incident response team***
  - ***Your merchant bank***
  - ***Visa Fraud Investigations and Incident Management group***
  - ***Your local office of the United States Secret Service***
- *Provide all compromised Visa, Interlink, and Plus accounts to your merchant bank within 10 business days.*
- *Within 3 business days of the reported compromise, provide an Incident Report document to your merchant bank.*

Is PCI DSS Compliance Required by Law?

The Minnesota Plastic Card Security law doesn't make PCI a legal requirement, but it does mandate that companies storing credit card information that subsequently suffer a breach will need to reimburse the card issuer for any costs associated with the breach. In other words, it reinforces a key PCI requirement rather than legislating it.

https://www.revisor.mn.gov/bin/getpub.php?type=law&year=2007&sn=0&num=108a

Similarly, the Nevada 'Security of Personal Information' law, and Nevada Senate Bill 227 specifically states a requirement to comply with the PCI DSS.

http://www.leg.state.nv.us/75th2009/Bills/SB/SB227_EN.pdf

Also, The Washington House Bill 1149 (Effective Jul 01, 2010) "recognizes that data breaches of credit and debit card information contribute to identity theft and fraud and can be costly to consumers".

http://apps.leg.wa.gov/documents/billdocs/2009-10/Pdf/ Bills/Session%20Law%202010/1149-S2.SL.pdf

Massachusetts is introducing 201 CMR 17.00 which seemingly borrows from the PCI DSS.

http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf

Several other states are making attempts to enforce PCI DSS-aligned legislation such as Texas, California, Illinois, and Connecticut. The overwhelming majority of the US, Puerto Rico & the Virgin Islands have legislation that requires disclosure of breaches.