EHMA 2009 - SEVILLE

Responsible Information Technology Security Strategy

Ian Millar CHTP

The six steps to security

WHAT IS PCI COMPLIANCE

- **PCI DSS** stands for **Payment Card Industry Data Security Standard**.
- It was developed by the major credit card companies as a guideline to help organizations that process card payments prevent credit card fraud, hacking and various other security vulnerabilities and threats.
- A company processing, storing, or transmitting payment card data must be PCI DSS compliant

PCI COMPLIANCE

- Non-compliant companies who maintain a relationship with one or more of the card brands, either directly or through an acquirer risk losing their ability to process credit card payments and being audited and/or fined.
- All in-scope companies must validate their compliance annually. This validation can be conducted by auditors - i.e. persons who are PCI DSS Qualified Security Assessors (QSAs)

Build and Maintain a Secure Network

Requirement 1:

Install and maintain a firewall configuration to protect cardholder data

Requirement 2:

Do not use vendor-supplied defaults for system passwords and other security parameters

Protect cardholder data

Requirement 3:

Protect stored cardholder data

Requirement 4:

Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

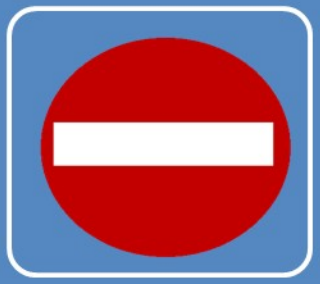
Requirement 5:

Use and regularly update anti-virus software

Requirement 6:

Develop and maintain secure systems and applications

Implement Strong Access Control Measures



Requirement 7:

Restrict access to cardholder data by business need-to-know

Requirement 8:

Assign a unique ID to each person with computer access

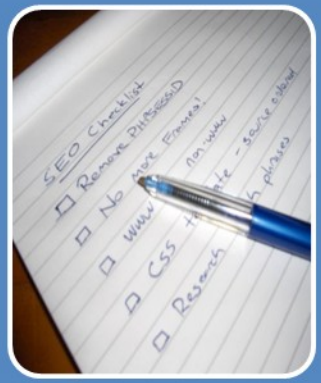
Requirement 9:

Restrict physical access to cardholder data

Regularly Monitor and Test Networks

Requirement 10:

Track and monitor all access to network resources and cardholder data



Requirement 11:

Regularly test security systems and processes

Maintain an Information Security Policy