Agenda

• Overview of PCI DSS

• Compliance Levels and Requirements

• PCI DSS in More Detail

• Discussion, Questions and Clarifications
Overview of PCI-DSS

• Topics in this section
  – PCI-DSS Defined
  – Brief History
  – Responsibilities
  – Terminology for Who’s Who
  – Confusion: PCI vs. AIS, CISP, SDP…
  – PCI Assessments
  – PCI Enforcement
PCI-DSS Defined

- Payment Card Industry Digital Security Standards
  A collaborative effort to achieve a common set of security standards for use by entities that process, store or transport payment card data.

- Multiple Credit Card organisations participating in PCI efforts
  Members include Visa, MasterCard, American Express (Amex), Diner’s Club, Discover Card, and JCB
Brief History

- **Companies developed and managed own standards independently**
  - Visa – (AIS) Account Information Security
  - MasterCard – (SDP) Site Data Protection
  - American Express – (DSS) Data Security Standards
  - Discover Card – (DISC) Discover Card Information Security and Compliance
Responsibilities

- **MasterCard** is responsible for certifying products and companies capable of fulfilling the Scanning requirements. These are often referred to (somewhat erroneously) as SDP Certified products and/or companies.

- **Visa** is responsible for training and certifying companies and individuals capable of fulfilling the Onsite Audit requirements. Such companies are called QSAs (Qualified Security Assessors) and the individuals are called QSAPs (Qualified Security Assessor Personnel).

- **The other PCI organisations** are contributors to the standards.
Terminology for Who’s Who

- Visa and MasterCard are made up of Member organisations who can be either Acquirers or Issuers (or both)
- Acquirers are the Members of the Visa or MasterCard organisations which handle Merchants
- Issuers are the Members of the Visa or MasterCard organisations that issue the cards to Cardholders
- Merchants are those entities who “accept” card transactions
- Cardholders are, well, card holders…
- Service Providers are the entities that provide any service requiring the processing, storing or transport of card information on behalf of any of the above
Diagrammatically...

Acquirer

is a member of

Issuer

and/or

MasterCard

VISA

may or may not
be the same as

Merchant

provides processing services to

issues cards to

Cardholder

uses card to buy from

Copyright Security-Assessment.com 2007
Confusion: PCI vs. AIS, CISP, SDP…

- PCI is the collaborative effort
- The AIS Program is the Visa management of compliance to PCI for Acquirers, Merchants and Service Providers for most regions (compliance is managed regionally)
- CISP is Visa USA’s Card Information Security Program; basically equivalent to the AIS Program (not used in Asia-Pacific)
- SDP is MasterCard’s (global) program for management of compliance to PCI for Acquirers, Merchants and Service Providers
PCI Assessments

- Scanning is only acceptable from MasterCard certified products and providers
- Audits are to be performed by Visa certified assessors
- Merchants and Service Providers submit Reports on Compliance to their Acquirers
- Visa requires its Acquirers to provide an annual “Certificate of Compliance” on Merchants and Service Providers
- MasterCard requires its Acquirers to complete a similar “Acquirer Submission and Status Compliance” form
- Acquirers are responsible for ensuring that their Merchants use Service Providers that are PCI DSS compliant
PCI Enforcement

- Visa and MasterCard require their Acquirers to ensure the compliance of their Merchants and Service Providers.

- Visa and MasterCard are able to penalise their Acquirers for having Merchants or Service Providers that are non-compliant.

- Acquirers can pass on penalties to their Merchants and Service Providers through their contractual relationships.

- Penalties can presently be financial against the Acquirer and restrict a Merchant’s / Service Provider’s ability to accept transactions.
Compliance Levels and Requirements

• Topics in this section
  – Merchant Levels
  – Service Provider Levels
  – Merchant Requirements
  – Service Provider Requirements
  – Network Security Scanning
  – Self Assessment Questionnaire
  – QSA Onsite Review
**Merchant Levels**

- MasterCard and Visa declare to their Acquirers which of their Merchants are at what Level, but the breakdown is approximately (similar across Visa AP and MasterCard):

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>Any Merchant processing over 6,000,000 transactions per year, compromised in the last year, or identified by another payment card brand as Level 1</td>
</tr>
<tr>
<td>Level 2</td>
<td>Any Merchant processing between 150,000 and 6,000,000 e-commerce transactions per year, or identified by another payment card brand as Level 2</td>
</tr>
<tr>
<td>Level 3</td>
<td>Any Merchant processing between 20,000 and 150,000 e-commerce transactions per year, or identified by another payment card brand as Level 3</td>
</tr>
<tr>
<td>Level 4</td>
<td>Any Merchant processing less than 20,000 e-commerce transactions per year, and all other Merchants processing up to 6,000,000 transactions per year</td>
</tr>
</tbody>
</table>
Service Provider Levels

- MasterCard and Visa declare to their Acquirers which of their Service Providers are at what Level, but the breakdown is approximately:

<table>
<thead>
<tr>
<th>Level 1</th>
<th>All Service Providers that process, store or transmit over 600,000 transactions or accounts annually (or that store card data for Level 1 or 2 Merchants for MasterCard)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 2</td>
<td>Any Service Provider that is not in Level 1 and stores, processes or transmits more than 120,000 accounts or transactions annually (and that store card data for Level 3 Merchants for MasterCard)</td>
</tr>
<tr>
<td>Level 3</td>
<td>Any Service Provider that stores, processes or transmits less than 120,000 accounts or transactions annually (and all other Storage Entities not in Levels 1 or 2 for MasterCard)</td>
</tr>
</tbody>
</table>
# Merchant Requirements

<table>
<thead>
<tr>
<th>Level</th>
<th>QSA Onsite Review</th>
<th>Self Assessment</th>
<th>Network Security Scan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>REQUIRED (annually)</td>
<td>Not Required</td>
<td>REQUIRED (quarterly)</td>
</tr>
<tr>
<td>Level 2</td>
<td>Not Required</td>
<td>REQUIRED (annually)</td>
<td>REQUIRED (quarterly)</td>
</tr>
<tr>
<td>Level 3</td>
<td>Not Required</td>
<td>REQUIRED (annually)</td>
<td>REQUIRED (quarterly)</td>
</tr>
<tr>
<td>Level 4</td>
<td>Not Required</td>
<td>Recommended (annually)</td>
<td>Recommended (annually)</td>
</tr>
</tbody>
</table>
## Service Provider Requirements

<table>
<thead>
<tr>
<th>Level</th>
<th>QSA Onsite Review</th>
<th>Self Assessment</th>
<th>Network Security Scan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>REQUIRED (annually)</td>
<td>Not Required</td>
<td>REQUIRED (quarterly)</td>
</tr>
<tr>
<td>Level 2</td>
<td>REQUIRED (annually)</td>
<td>REQUIRED (annually)</td>
<td>REQUIRED (quarterly)</td>
</tr>
<tr>
<td></td>
<td>for MasterCard for Visa</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 3</td>
<td>Not Required</td>
<td>REQUIRED (annually)</td>
<td>REQUIRED (quarterly)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Network Security Scanning

- Targets Internet facing devices, systems and applications including
  - routers and firewalls
  - servers and hosts (including virtual!)
  - applications
- **Must be performed using an offering from a MasterCard certified provider:** [https://sdp.mastercardintl.com/vendors/vendor_list.shtml](https://sdp.mastercardintl.com/vendors/vendor_list.shtml)
- **May not have any Severity 3 or greater issues:**
  - 5 (Urgent): Trojan Horses, file read and write exploits, remote command execution
  - 4 (Critical): Potential Trojan Horses, file read exploit
  - 3 (High): Limited exploit of read, directory browsing and denial of service
Self Assessment Questionnaire

- Is a selected subset of the full Onsite Audit criteria
- Is completed by the Merchant or Service Provider
- Is submitted to Acquirer(s)
- Is made up mainly of Yes/No/Not Applicable responses
- Is broken into five of the six sections from PCI DSS:
  - Build and Maintain a Secure Network
  - Protect Cardholder Data
  - Implement Strong Control Measures
  - Regularly Monitor and Test Networks
  - Maintain an Information Security Policy
QSA Onsite Review

- Is a detailed audit against the PCI Data Security Standard
- Potentially targets all systems and networks that store, process and/or transmit cardholder information
- Includes review of contractual relationships, but not assessment of the Third Parties themselves
- Biggest difficulties in having onsite reviews are the initial scoping and the subsequent cost of correction to compliant levels
- QSA provides a Report on Compliance *when compliant* for submission to the Acquirer. Interim reports may be asked for by the Acquirer
PCI DSS in More Detail

• Topics in this section
  – Authoritative Documentation
  – PCI DSS Structure
  – PCI DSS Control Evaluation
  – Onsite Review Practicalities
Authoritative Documentation

• Visa and MasterCard maintain equivalent copies at:
  – http://www.visa-asia.com/secured or
  – http://sdp.mastercardintl.com
  – https://www.pcisecuritystandards.org/

• Specifically, copies of the PCI Data Security Standard can be downloaded from

• …and copies of the PCI Audit Procedures can be downloaded from
  – https://sdp.mastercardintl.com/doc/pci_audit_procedures.doc or
PCI DSS Structure

• Is made up of six key sections:
  – Build and Maintain a Secure Network
  – Protect Cardholder Data
  – Maintain a Vulnerability Management Program
  – Implement Strong Control Measures
  – Regularly Monitor and Test Networks
  – Maintain an Information Security Policy

• Each section has a set of Requirements, for example:
  – Build and Maintain a Secure Network
    • Requirement 1: Install and maintain a firewall configuration to protect data.
    • Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.
PCI DSS Structure, Continued

• Each Requirement has a rationale and a set of sub-requirements specified for review, for example:
  – Requirement 1: Install and maintain a firewall configuration to protect data.
    – Firewalls are computer devices that control computer traffic allowed into a company’s network from outside, as well as traffic into more sensitive areas within a company’s internal network. All systems need to be protected from unauthorized access from the Internet, whether for e-commerce, employees’ Internet-based access via desktop browsers, or employees’ email access. Often, seemingly insignificant paths to and from the Internet can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

• 1.1 Establish firewall configuration standards that include:
  – 1.1.1 A formal process for approving and testing all external network connections and changes to the firewall configuration
  – 1.1.2 A current network diagram with all connections to cardholder data, including any wireless networks
  – 1.1.3 Requirements for a firewall at each Internet connection and between any DMZ and the Intranet
There are presently twelve Requirements, each having about five or six sub-requirements (many having sub-sub-requirements of their own…)

In short, it isn’t a small amount of analysis!
The PCI Security Audit Procedures give some guidance on what will be checked for. An example of this can be seen by:

6.3.7 Review of custom code prior to release to production or customers, to identify any potential coding vulnerability.

TESTING PROCEDURE

- 6.3.7.a Obtain and review written policies to confirm they dictate that code reviews are required, and must be performed by individuals other than the originating author of the code.
- 6.3.7.b Confirm that code reviews are occurring for new code as well as after code changes.
Onsite Review Practicalities

• **Make sure you scope correctly**
  – The appropriate placement of a stateful firewall can reduce the scope dramatically

• **If not compliant, it will be necessary to submit planning information on how compliance will be achieved**
  – This will be monitored and policed both by your QSA and Acquirer

• **It may be possible to use compensating controls to meet a requirement**
  – Must be controls over and above what is already specified, and
  – Must meet the intent of the Requirement
  – At the discretion of the QSA and must be agreed to by Acquirer
Discussion and Questions?

http://www.security-assessment.com

Drazen.Drazic@security-assessment.com