AISA Sydney

15th April 2009

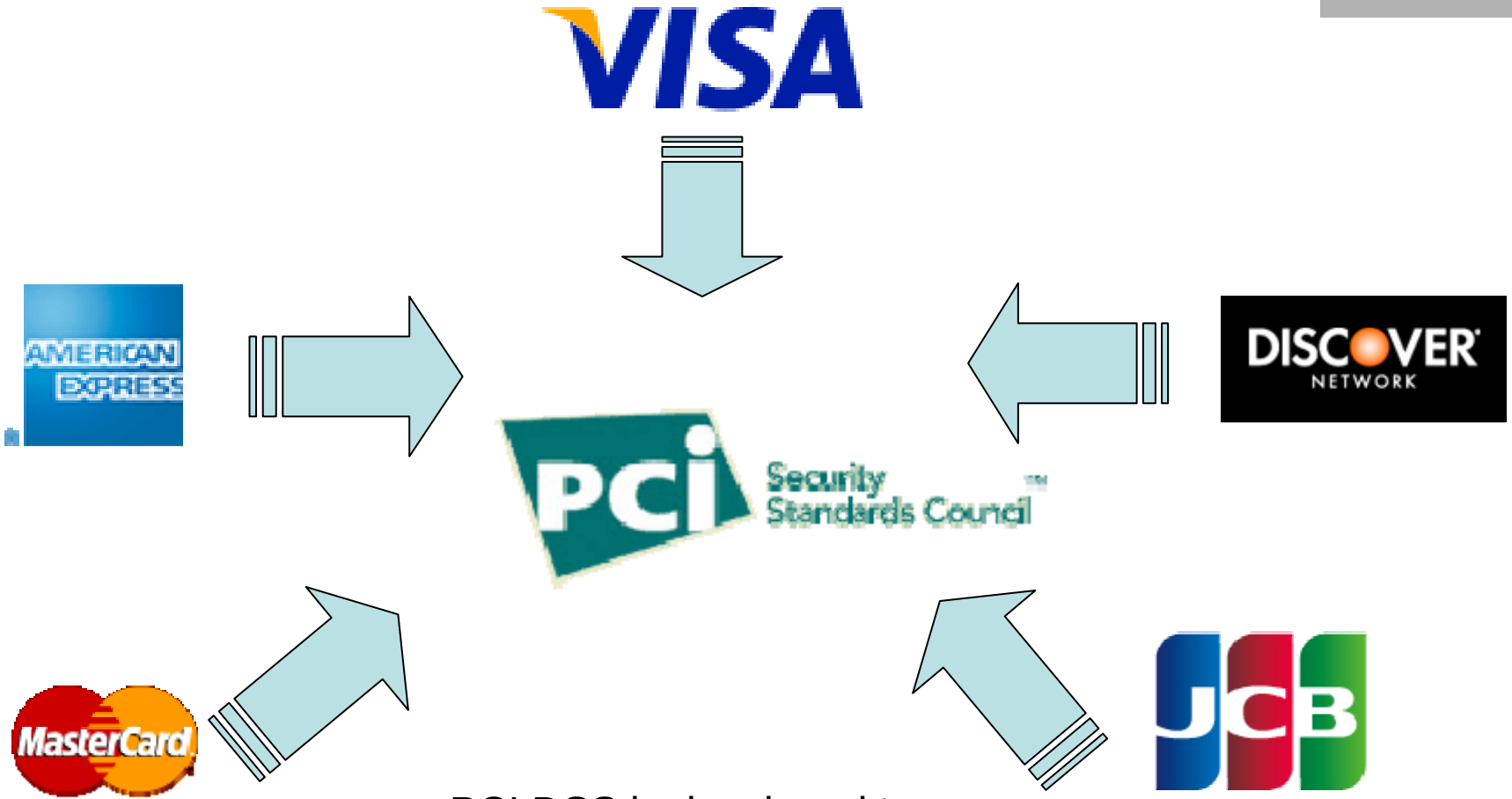
Where PCI stands today: Who needs to do What, by When

Presented by: David Light
Sense of Security Pty Ltd
www.senseofsecurity.com.au

Agenda

- Overview of PCI DSS
- Compliance requirements – What & When
- Risks & consequences of non-compliance
- Lessons learned & prioritising remediation
- Approach for PCI compliance

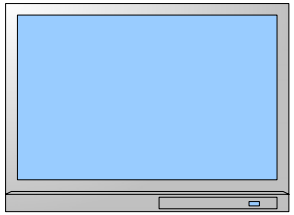
PCI Security Standards Council Members



PCI DSS is developed to encourage and enhance cardholder data security

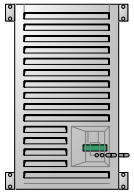
Terminology: Merchant, Acquirer, Issuer and Service Provider

Client



Customer requests purchase transaction on PC

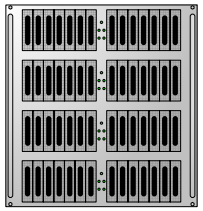
Merchant



OR

OR
Merchant swipes the card, enters the dollar amount.

Authorisation request is sent to acquiring merchant bank.



Service Providers

Merchant receives authorisation response and completes the transaction.

Merchant bank forwards authorisation response to merchant.

Customer bank sends funds to merchant bank.

Customer Bank:
Issuer

Customer bank verifies credit card and clears request.

Merchant bank sends transaction information to customer bank (Issuer) through Card Scheme Network

Merchant Bank:
Acquirer

Who must comply?

- **Everyone** who stores, processes or transmits cardholder data must comply with PCI DSS
  - PCI compliance is mandatory
  - PCI applies to all parties in the payment process
  - You cannot be partially compliant: **Compliance is PASS/FAIL**

Who must comply?

- If you **outsource** components of your PCI process to Service Providers, they must comply
  - Either they are included in your scope
  - Or they must provide evidence to demonstrate their compliance

Six Goals, Twelve Requirements

The Payment Card Industry Data Security Standard (PCI DSS)	
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 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**
Implement Strong Access Control 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**

PCI DSS Merchant Levels (Visa and Mastercard)

	Level 1	Level 2	Level 3	Level 4
	More than 6m Transactions or Cardholder data has been compromised	Between 1m and 6m transactions	Between 20k and 1m e-commerce transactions	All Others (Under 20k e-commerce and under 1m transactions)
Self Assessment *	**Not Required**	**Mandated**	**Mandated**	**Mandated**
Vulnerability Scan †	**Mandated**	**Mandated**	**Mandated**	**Mandated**
Onsite Review ‡	**Mandated**	**Not Required**	**Not Required**	**Not Required**

Example: Visa penalties of US$10k & US$5k / merchant / month from Sept 2009 for Merchant Levels 1 and 2 respectively. Acquirer is liable.

Westpac Merchant Levels (Visa/MasterCard/Bankcard)

	Level 3	Level 2	Level 1	Level 0
	Above A$800,000 or Cardholder data has been compromised	Between A$150,000 & A$800,000	Between A$30,000 & A$150,000	Under A$30,000
Self Assessment *	**Mandated**	**Mandated**	**Mandated**	**Not Required**
Vulnerability Scan †	**Mandated**	**Mandated**	**Not Required**	**Not Required**
Onsite Review ‡	**Mandated**	**Not Required**	**Not Required**	**Not Required**

Service Provider Obligations

Level	Visa	MasterCard	American Express	Requirement
1	VisaNet processors or any service provider that stores, processes and/or transmits over 300k transactions / year	All Third Party Processors (TPP) All Data Storage Entities (DSE) that store, transmit or process greater than 1m transactions	All Third Party Processors (TPP)	• **Annual onsite review & ROC by Qualified Security Assessor (QSA)** • **Quarterly network security scan by ASV (Approved Scanning Vendor)**
2	Any service provider that stores, processes and/or transmits less than 300k transactions / year	All DSEs that store, transmit or process less than 1m transactions	N/A	• **Annual completion of PCI DSS self assessment questionnaire** • **Quarterly network security scan by ASV**

Feb.1, 2009: Only Level 1 service providers will be listed on Visa's List of PCI DSS Compliant Service Providers

Who must comply and When?

- **Merchants, Acquirers, Issuers, Service Providers:**
  - **PCI Compliance is mandatory NOW.**
- **Merchants: VISA penalties will apply:**
  - September 30, 2009: Level 1& 2: Attest to not storing prohibited data (aligned with Acquirers)
  - September 30, 2010: Level 1: Full compliance
  - Fines are issued to the Acquiring Bank, who may pass it on to the Merchant

Who must comply and When?

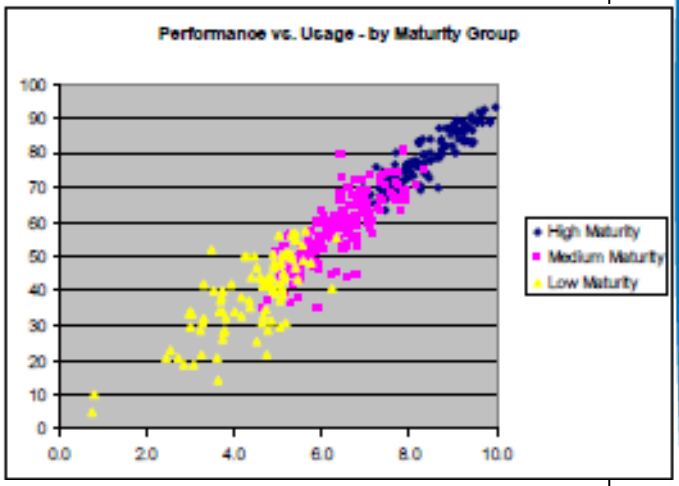
- **Acquirers (per VISA)**
  - September 30, 2009 - Attest to not storing prohibited data (aligned with level 1 merchants)
  - September 30, 2010 - Full PCI DSS compliance - (if not compliant provide ROC and remediation plan for evaluation)
- **Service Providers**
  - Need to provide evidence of compliance to align with their client's PCI compliance programs

3: Risks & consequences of non-compliance

- **Risks**
  - PCI DSS is mandatory
  - Breach impact can be massive (Forrester Research: US$90 to US$305 per lost record)
- **Consequences**
  - Card imposed fines up to US$500,000 per incident
  - Legal authorities need to be notified & free credit protection offered to those affected
  - Brand impacts (customer & shareholder level) & legal action by card holders

Performance gains expected from ongoing IT controls and compliance

- Loss from security events ↓
- Detection of security breaches via automated controls ↑
- Unplanned work ↓
- Success rate of changes ↑
- First fix rate ↑
- Servers per system administrator ↑



Lessons learned – Tips to avoid failure

Top 5 Failed Requirements	Relevant Compromise	Recommended Tactics
Requirement 3: Protect stored data	Unencrypted spreadsheet data; unsecured physical assets	Store less data; Understand the flow of data; Encrypt data
Requirement 11: Regularly test security systems and processes	POS/shopping cart application vulnerabilities; most data compromises can be attributed to a Web application vulnerability	Rigorously test applications; Scan quarterly
Requirement 8: Assign a unique ID to each person with computer access	Weak or easily guessed administrative account passwords	Improve security awareness
Requirement 10: Track & monitor all access to network resources & cardholder data	Lack of log monitoring and IDS data; Poor logging tools	Install intrusion detection or prevention devices; Improve log monitoring and retention
Requirement 1: Install & maintain a firewall configuration to protect data	Card numbers in the DMZ; Segmentation flaws	Segment credit card networks and control access to them

Source: Verisign

Lessons learned – Managing a PCI audit

- PCI is about people and business processes as well as systems
- Engage with experts
- Reduce scope where possible
- Set and manage expectations
- Have friends (internally) in high places
- Ensure governance for PCI audit is in place

Prioritising remediation effort

Prioritised Approach PCI SSC 2009

Six security milestones:

1. Remove sensitive authentication data and limit data retention
2. Protect the perimeter, internal, and wireless networks
3. Secure payment card applications
4. Monitor and control access to your systems
5. Protect stored cardholder data
6. The rest, and ensure all controls are in place

Start with a Scope Review

PCI DSS applies to any network component, server or application included or connected to the card-holder data environment

Start with a Scope Review, addressing:

- Network Segmentation
- Wireless
- Third Party / Outsourcing
- Sample Business Facilities & System Cmpnts
- Compensating Controls

PCI Assessment Approach

- Then commence the PCI Audit
  - Preparation
  - On-site Audit
  - Post-site Analysis and Reporting
  - Remediation
  - Final Audit and Lodgement
  - Maintenance
- Expect the PCI compliance program to take 6 to 12 months to complete

Thank you

David Light

Sense of Security Pty Ltd
Level 3, 66 King Street
Sydney NSW 2000

T: +61 (0)2 9290 4444
M: +61 (0)423 121 217
W: www.senseofsecurity.com.au
E: DavidL@senseofsecurity.com.au