Alex Woda
Security and Audit Solutions

Achieving Compliance with the PCI Data Security Standard

Alex Woda

Alex Woda
Security and Audit Solutions

Agenda

- PCI Security Compliance Background
- Security Breaches - How do they happen?
- Overview of the Security Standards
- 10 Best Practices for Achieving Compliance
- Questions

Alex Woda
Security and Audit Solutions

Payment Card Industry Overview: Terminology

"Card Association"
- Licensor of brand, e.g. VISA

"Issuer"
- Financial Institution that issues cards, e.g. TD Bank

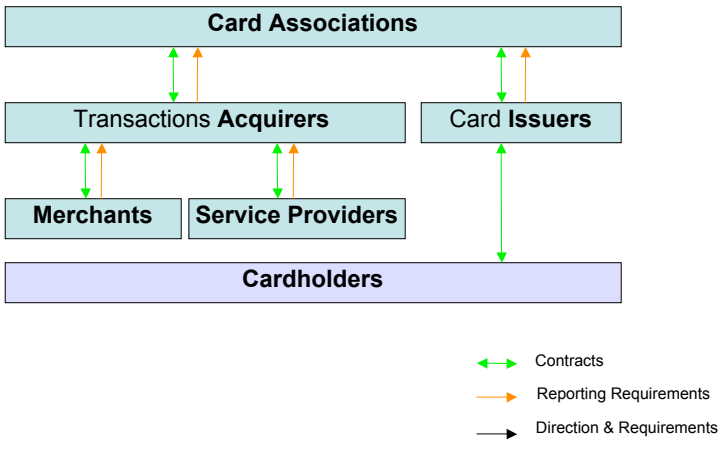
"Acquirer"
- Accepts card transactions for association, e.g. TD Bank, Global Payments, Moneris, etc.

"Service Provider"
- Merchant Services (e.g. storefront host)
- "IPSP" Internet Payment Service Provider

"Merchant"
- Takes cards as payment
- "MOTO" Mail Order / Telephone Operator

Alex Woda
Security and Audit Solutions

Payment Card Industry Overview



Alex Woda
Security and Audit Solutions

Before Payment Compliance (2000)

- **Increase in Risks to Acquirers and Consumers**
  - Card Not Present Fraud (Identity Theft)
  - Web Server Certificates not adequate for e-commerce Security
  - Public disclosure of losses and breaches are rare
  - Erosion of Industry and Brand confidence
  - "Zero liability" for cardholders announced in 2000
- **First Major Security Breach made public**
  - Public disclosure of a possible compromise of 3.7M cards @ Egghead.com – December 22, 2000
  - Industry damage control cost estimated at $20M with millions of cards cancelled days before Christmas
- **Industry wide security improvements needed**
  - Public disclosure laws such as California Bill-1386
  - Payment Card Industry Data Security Standards

Alex Woda
Security and Audit Solutions

Major Card Security Breaches

- **Card Systems International hacked in 2005**
  - **Approx. 40 Million Cards compromised**
  - **Service Provider Network Gateway was hacked**
  - **Modifications made to Web Server Software**
- **TJX Stores hacked in 2007**
  - **Approx. 60 Million Cards compromised**
  - **Stores were not PCI compliant**
  - **Hackers gained access to non-protected Wi-Fi Networks**
  - **Drive-By Hacking**
- **Royal Bank of Scotland Worldpay (US 2008)**
  - **Customer information and payroll cards (2 Million)**
  - **Included open loop gift cards**

Alex Woda
Security and Audit Solutions

Major Card Security Breaches

- **Geeks.com (Dec. 2007 but reported in 2008)**
  - Stored client info and CVV / CVC
  - E-commerce site hacked
- **Hannaford Brothers - 2008**
  - More than 5 Million Cards compromised
  - Stores were PCI compliant
  - Hackers targeted servers that transmit card data to processor
  - Not addressed in PCI DSS (new vulnerability)
- **Heartland Payment Systems Jan. 2009**
  - Investigation is still in progress
  - Service provider for retailers and e-commerce
  - Processes more than 100 Million transactions per month
  - Malicious code found on servers
  - Extent of cardholder data loss not documented

Alex Woda
Security and Audit Solutions

Who Gets Hacked?

Recent Data Breaches

Food Service	54%
Retail	25%
Entertainment	5%
Travel	4%
Universities	4%
Telecommunications	3%
Non-Profit	2%
Media	1%
Petroleum	1%
Government	1%

Alex Woda
Security and Audit Solutions

How Was it Done?

Recent Data Breaches

• Compromise POS Software	71%
• Internet Shopping Carts	22%
• Back End Processing System	6%
• Hardware Terminals	1%

Source: PCI Assessor Trustwave

Alex Woda
Security and Audit Solutions

Payment Compliance Origins (2001)

- **Origins of Compliance Programs**
  - MasterCard International – Site Data Protection Program (SDP) announced May 2001
  - VISA US – Cardholder Information Security Program (CISP) announced June 2001
  - VISA International – Account Information Security (AIS) Standard and regional programs announced November 2001
- **Some Confusion in the Beginning**
  - Acquirers and Merchants unsure of requirements
  - Lack of awareness and training
  - 3 different standards and 3+ different compliance programs world wide
  - Different requirements
  - Different compliance dates
  - Little enforcement

Alex Woda
Security and Audit Solutions

Payment Compliance Today (2008+)

- **Security Programs Align on new standard**
  - VISA, MasterCard align standards and programs on "Payment Card Industry (PCI) Security Standard" December, 2004
  - Focus on e-commerce and large volume merchants in 2005
  - All merchants need to comply
- **PCI Security Programs**
  - VISA US and VISA Canada use one standard - Release 1.2
  - VISA approves Qualified Independent Security Assessors
  - MasterCard International sets standard for Internet facing systems, evaluates and approves Qualified Scanning Vendors
- **Acquirers and merchants need to be in compliance**
- **Penalties for companies not in compliance**
- **Independent forensic investigations mandated for all breaches**
- **www.pcisecuritystandards.org for more information**

Alex Woda
Security and Audit Solutions

Benefits of PCI Compliance

- **Reduced liability for merchant and acquirer in the event of a breach**
  - **$500k plus $25 per card if duty of care not demonstrated by Merchant**
- **Improve and monitor protection of critical systems**
- **Increased security over personal/confidential data**
- **Reduces likelihood of a breach**
- **Supports Sarbanes-Oxley and Bill 198 compliance**
- **Evidence of system access in logs**

Alex Woda
Security and Audit Solutions

PCI Data Security Standard

- 6 major areas, 12 categories, and more than 200 specific requirements
- Requirements added after security breaches detected
  - eg. cannot store cardholder data in non-encrypted format
  - secure wireless networks
  - monitor for malicious code and unusual activity
- Version 1.2 released October 2008
- Clarification of compensating controls

Alex Woda
Security and Audit Solutions

Merchant Compliance Requirements

	Annual Visa Transaction Volume	Merchant Type	Self-Assessment Questionnaire	Vulnerability Scan	On-site Review
1	over 6,000,000	All Brick&Mortar MOTO E-commerce		✓ Quarterly	✓ Annual
2 3	20,000 to 6,000,000	E-comm	✓ Annual	✓ Quarterly	
4 A	1,000,000 to 6,000,000	Brick&Mortar MOTO	✓ Annual	✓ Quarterly	
4 B	B/M and MOTO < 1,000,000 E-comm < 20,000	All other merchants	✓ Annual	✓ Annual	

© Visa Canada

- Level 1, 2, & 3 are standard in all VISA regions world-wide
- Level 4 is specific to VISA Canada
- All levels are based upon risk and include:
  - -Transaction volumes
  - -Card not present
  - -Previous account compromise
- Additional requirements for Merchant Service Providers

Alex Woda
Security and Audit Solutions

PCI Data Security Requirements

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other non-secure parameters

Protect Cardholder Data

3. Protect stored data
4. Encrypt transmission of cardholder data and sensitive information across public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Alex Woda
Security and Audit Solutions

PCI Assessment Requirements

(cont.)

Implement Strong Access Control Measures

7. Restrict access to 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

Alex Woda
Security and Audit Solutions

Controversial Areas

- **PCI DSS is Prescriptive**
  - Detailed description of controls that must be in place
- **Storage of Cardholder data (Section 3)**
  - Remove complete track 2 data
  - Render primary account number (PAN) unreadable
  - PAN is used for database index, payment reconciliation
- **Application development**
  - Source code analysis and review
- **Audit Trails**
  - Log and monitor all access to cardholder data
- **Extent of security testing**
  - Penetration tests, security tests, vulnerability scans

Alex Woda
Security and Audit Solutions

Self-Assessment Compliance Questionnaire

- **Required annually for smaller merchants**
  - Self Assessment Completed by staff
  - Assistance often required for accurate completion
  - Should be completed by non-operations staff
- **Management formally acknowledge that they are in compliance**
- **Should be verified by a VISA approved assessor**
- **Filed with Acquirers and VISA**
- **Non-compliance must be addressed in action plans**

Alex Woda
Security and Audit Solutions

Compliance On-site

- **Required annually for large merchants**
  - Detailed security assessment
  - Performed by a VISA approved assessor
- **Scope of Review**
  - Any system or network which collects, processes, stores or transmits cardholder data
  - focus on malicious code protection and network security
- **Filed with Acquirers and VISA**
- **Non-compliance must be addressed in action plans**

Alex Woda
Security and Audit Solutions

Documentation Requirements

- **Information Security Policies and Standards**
- **Organization charts**
- **Up to date Network diagrams**
- **Payment application and infrastructure architecture**
- **Payment interfaces**
- **Firewalls rules**
- **Intrusion Detection / Prevention strategies**
- **Malicious code protection**
- **Security monitoring and assessments**
- **Control of User access to payment systems**
- **All 3rd party handling of transactions - contracts**

Alex Woda
Security and Audit Solutions

Compliance Vulnerability Scanning

- **Vulnerability Scans**
  - All Internet facing systems (not just e-commerce web servers)
  - Required on a quarterly basis
  - Should be assessed by a Security Specialist
- **Limitations of tests**
  - External security scanning of network ports
  - Tests are non-intrusive, however, disruptions may still occur
  - Tests are continuously being added to address new vulnerabilities
- **Vulnerabilities must be fixed**
  - Low risk findings are excluded
  - Potential vulnerabilities can be excluded if additional examination proves them not applicable

Alex Woda
Security and Audit Solutions

Best Practices for PCI Compliance

1. **Conduct an IT Risk Assessment**
   - Understand the environment and security risks
2. **Reduce the Scope**
   - Isolate, Compartmentalize and Secure
3. **Understand the Control Environment**
   - Document key controls - Are they working effectively?
4. **Buy Compliant Systems**
   - All vendors are required to be in compliance with certified software
   - Includes implementation guides that follow the PCI Standard
5. **Do not store Cardholder data**
   - Keep the data for as long as required to authorize the transaction
   - Mask or truncate the data when completed
   - Do not use card numbers for business intelligence or reporting

Alex Woda
Security and Audit Solutions

Best Practices for PCI Compliance

6. Update Policies and Standards
- Information security policies must be up to date and reference PCI

7. Detailed System Logging
- Logs must provide evidence of system access
- Logs must be secured
- Consider security event correlation tools

8. Secure the Network Perimeter
- Firewalls are not enough
- Need to use multiple devices and appliances for protection

9. Harden Servers
- Configuration standards and disciplined patch management

10. Control vendor and remote access
- Remote access for support and management access represents a severe security weakness

Alex Woda
Security and Audit Solutions

On the Road to PCI Compliance

- Conduct a Pre-assessment and risk analysis
- Investigate ways to reduce the risks
- Engage with a qualified security assessor to interpret PCI data security standard
- Create a detailed project plan for remediation
- Identify compensating controls
- Test the controls
- Implement a vulnerability management program