PCI Compliance 3.1

University of Hawaii

About Us

• Helping organizations comply with mandates, recover from security breaches, and prevent data theft since 2000.
• Certified to conduct all major PCI compliance validations
Today’s Agenda

• Why the need for PCI compliance
• Increase in SAQ types
• Determining your SAQ type
• Changes from PCI 2.0 to 3.0/3.1
• External vulnerability scans
• VOIP requirements and risks

Presenter: David Page
QSA, CISSP

Why Comply with PCI?

securityMETRICS®
Increase In Fraud Activity

• It’s not just retail
• Universities are targets
  – Large amounts of data
  – Many systems to access
• University of Maryland
  – 300,000 data records (including SSN)
• UCLA Health System
  – 4.5 Million patients affected

Change to PCI 3.0/3.1

“It’s about making PCI compliance part of your business, not a once-a-year, study-for-the-test kind of thing.”

- Bob Russo, General Manager of PCI SSC

• Clarification
• Additional guidance
• Evolving requirements
SAQ A

- Card-not-present transactions
  - Ecommerce
  - Mail/telephone-order
- Outsource all cardholder data functions

14 requirements
Key points to comply
- Policies and procedures
- Training
- No scans required
SAQ A-EP

• Ecommerce merchants who outsource all payment processing
• Merchants’ website(s) doesn’t directly receive cardholder data but can impact the security of the payment transaction

• 139 requirements
• Key points to comply
  • External vulnerability scan
  • Penetration Test
  • Policies and procedures
  • Training

SAQ B

• Dial-out terminal (analog phone line)
• Imprint-only
• No electronic cardholder data storage

• 37 requirements
• Key points to comply
  • Policies and procedures
  • Training
• No scans required
### SAQ B-IP

- PTS-approved payment terminals with an IP connection
- Terminal not connected to other networks or devices
- No electronic cardholder data storage

- 83 requirements
- Key points to comply
  - External vulnerability scan
  - Policies and procedures
  - Training

### SAQ C-VT

- Merchants using only web-based virtual terminals
- Machine is dedicated to only processing cards
- No electronic cardholder data storage

- 73 requirements
- Key points to comply
  - Policies and procedures
  - Training
  - No scans or penetration test required
SAQ C

• Merchants with payment application systems connected to the Internet
• No electronic cardholder data storage

SAQ P2PE-HW

• Using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solution
• No electronic cardholder data storage
SAQ D

• Store payment cards electronically
  – Point of sale system
  – E-mail, E-FAX
  – Voice recordings
• Merchants not included in any other SAQ type

• 335 requirements
• Key points to comply
  • External/Internal vulnerability scan
  • Penetration Test
  • Policies and procedures
  • Training

Key Changes from PCI 2.0 to 3.0/3.1
Change in Scope

- In-scope system components:
  - Systems providing security services
  - Facilitate segmentation
  - Impact security of the CDE
- Web redirection servers

PCI Requirement 1

- Clarified what network diagram must include (1.1.2)
  - All connections between cardholder data environment, including any wireless networks
- Current diagram showing all cardholder data flows (1.1.3)
PCI Requirement 1

Card Flow Diagram Example

1. Swipe
2. Data encrypted
3. Send to processor for approval
4. Approval returned
5. Transaction data stored

Network Diagram Example

PCI Requirement 2

- Maintain inventory of system components in scope for PCI DSS (2.4)
  - Maintain list of hardware & software components with function descriptions
  - Interview personnel to verify list is current
PCI Requirement 4

- Use strong cryptography & security protocols to safeguard transit data (4.1)
- Interception of unencrypted data over public network easy & common
- Updated to include satellite communications
- SSL and TLSv1 no longer considered strong encryption.

PCI Requirement 5

- Evaluate evolving malware threats for systems not commonly affected by malware (5.1.2)
- Ensure anti-virus solutions actively run & cannot be altered/disabled without managerial approval (5.3)
PCI Requirement 6

• Secure development of internal & external software applications (6.3)
• Requirement for coding practices to protect against broken authentication & session management (6.5.10)
  – Examine development policies & procedures
  – Interview responsible personnel

PCI Requirement 7

• Define access needs for each job role (7.1.1)
  – System components & data resources
  – Level of privilege required for accessing resources
PCI Requirement 8

• Education and training on password policy implementation (8.4)
• Service providers with remote access must use unique login credentials for each customer (8.5.1)
• Physical/logical controls required to uniquely ID users of alternate authentication mechanisms (8.6)
  – e.g. PIN, biometric data, password

PCI Requirement 9

• Control physical access to sensitive areas for onsite personnel (9.3)
• Protect direct contact payment devices from tampering and substitution (9.9)
  – Maintain up-to-date list of devices (9.9.1)
  – Periodically inspect device (9.9.2)
  – Provide staff awareness training (9.9.3)
PCI Requirement 10

• Log use of and changes to identification and authentication mechanisms (10.2.5)
• Record all pauses, stops, and initializations of audit logs (10.2.6)
• Review logs of all system components based on policies & risk management strategy (10.6.2)

PCI Requirement 11

• Maintain an inventory of authorized wireless access points (11.1.1)
• Implement methodology for penetration testing (11.3)
• Implement process to respond to change-detection system alerts (11.5.1)
PCI Requirement 12

- Document which requirements are managed by service provider & entity (12.8.5)
- Service provider written acknowledgement of data responsibility (12.9)
VOIP Risks

- Same risks as any internet connection
  - Merchants don’t think of phones as point of attack
  - Searchable online
- VOIP traffic may contain card holder data
  - Call center taking cards for payment
  - Voice recordings for QA
- Attacker can use VOIP as point of entry

The Pivot Attack
PCI Requirements for VOIP Lines

• Complete SAQ B-IP*
• External vulnerability scan on public IP address
  – Looks for vulnerabilities on external network
  – Produces a pass or fail status
  – For failing items there will be remediation tips

Take Aways
Take Aways

- Correctly identify scope and SAQ requirement
- Increased documentation on processes
- Focus on monitoring (physical inspection, logs)
- Implementing layers of security
- Security of individual systems
- Focus on detecting rather than reacting
- **We can help**

Questions?

consulting@securitymetrics.com

If you have any questions, please call SecurityMetrics at (801) 705-5700. Let them know that you are processing with Bank of Hawaii.