

PCI "Straight Talk" 3

Diana Kelley and Ed Moyle

Agenda

- **Requirements 7 through 12**
- **Wrap-up**

Agenda

- **Requirements 7 through 12**
 - Requirements "At a Glance"
 - Requirements Walkthrough
- **Wrap-up**

Compliance: Improve Your Processes, Leverage Technologies and Reduce Costs

The PCI Requirements “at a Glance”

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

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure systems and applications

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

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

Requirement 12: Maintain a policy that addresses information security

Compliance: Improve Your Processes, Leverage Technologies and Reduce Costs

Requirement 7: Restrict Access

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

● What it means

- You have a policy and documented processes to limit who can get to cardholder data
- You have systems that enforce the policy

● Questions

- Do we need an automated access control system?
- Access control system? You mean like Windows™?

● Gotchas

- Lack of access control policy (documentation)



Fact: Many firms have the tech, but lack the policy

Impact and Quick Hits: Restrict Access

1.2 Impact

- Minimal (explanations/clarifications only)

Quick Hits

- **“Oceans” of policy**
 - Policy stating principle of least privilege
 - Alignment of access to job function
 - Signoff by management of employee roles
- **A documented access control system**
 - Covering all systems in scope
- **A “default deny” posture for the access control system**

Compliance: Improve Your Processes, Leverage Technologies and Reduce Costs

“Assign a unique ID to each person with computer access”

Requirement 8: Unique IDs

● What it means

- You give everyone with access to cardholder data a unique ID
- You authenticate use of that ID using a strong password or (for remote access) two factors

● Questions

- What about shared IDs?
- Is entering two passwords two-factor? What about a PIN and a password?

● Gotchas

- Two-factor authentication

Impact and Quick Hits: Unique IDs

1.2 Impact

- Auditors now specifically required to test secure password storage both in transmission and storage

Quick Hits

- Procedures
 - For adding/removing users
 - For password reset
 - For password issuance
- Two-factor authentication for remote access
- A method for encrypting password during transmission and storage
- Password lockout
- Authenticated access to databases
- Password strength requirements
 - Length, Age, Uniqueness, Complexity

Compliance: Improve Your Processes, Leverage Technologies and Reduce Costs

Requirement 9: Physical Access

“Restrict physical access to cardholder data”

● What it means

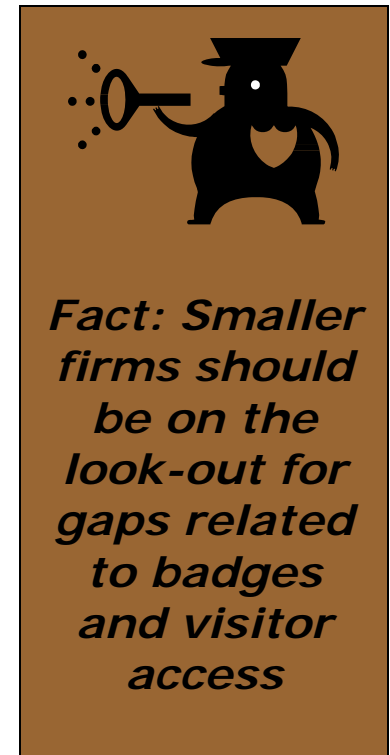
- You protect the physical facilities used for processing of cardholder data

● Questions

- Do we need cameras?
- Our culture is resistant to badges ...

● Gotchas

- Badges in the SMB
- Network jacks



Impact and Quick Hits: Physical Access

1.2 Impact

- Adds wiggle room for camera requirements
- Excludes POS from camera requirement (whew!)
- Now requires annual review of backup storage
- Annual media inventory

Quick Hits

- A policy governing how media is used and stored
- Badges or other identification method (even for visitors)
- A visitor log
- Secure storage for media (and annual review)
- A way to label, track, and dispose of media
- Protection for network jacks

Compliance: Improve Your Processes, Leverage Technologies and Reduce Costs

Requirement 10: Auditing

● What it means

- You maintain system logs and have procedures to monitor, correlate, and retain them

● Questions

- Daily log review?!?!?
- Can we use a log aggregator or correlation engine?

● Gotchas

- Manual log review procedures that don't get followed

“Track and monitor all access to network resources and cardholder data”



Log correlation and harvesting could be cheaper long-term than manual review

Impact and Quick Hits: Auditing

1.2 Impact

- Requirement to copy “write logs” for “external-facing devices” to log server (changed from wireless logs). Much more is covered now (firewalls, routers, gateway hosts, VPN concentrators, etc.)

Quick Hits

- Link events to individual users
- Restrict access to logs
- Retain audit data for at least one year
- Back up the logs
- Use file integrity monitoring (on logs)
- Follow your policy for log review

Compliance: Improve Your Processes, Leverage Technologies and Reduce Costs

Requirement 11: Testing

“Regularly test security systems and processes”

● What it means

- You conduct required quarterly tests (wireless, external, and internal)
- You conduct required annual tests (network and app penetration test)

● Questions

- File integrity monitoring? Like Tripwire?
- What do they mean by penetration test?
- Do we have to use an ASV for the test?

● Gotchas

- If you miss a required test...
- Testing after network changes



Impact and Quick Hits: Testing

1.2 Impact

- Tightened requirements for validating external scanning (after year 1, you must have four passing scans to be compliant)

Quick Hits

- Intrusion detection
- File integrity monitoring
- Four passing ASV tests
- Annual penetration testing
- Internal scanning

Compliance: Improve Your Processes, Leverage Technologies and Reduce Costs

Requirement 12: Policy

“Maintain a policy that addresses information security”

● What it means

- You author and maintain a body of policy documentation stating how you will address DSS requirements

● Questions

- What should I screen new hires for? Criminal history? Credit scores? References?

● Gotchas

- There’s a lot of documentation – chances are, you don’t have all you need

Impact and Quick Hits: Policy

1.2 Impact (lots of changes here)

- Disconnect and vendor-approval now required for all remote technologies (not just modems)
- Remote-access download prohibition (of cardholder data) clarified to include all media
- Vendor vetting and governance

Quick Hits

- Have policy addressing all of the PCI requirements as well as the additional items under requirement 12
- Publish policy to impacted personnel (usually, all employees)
- Have an awareness program that addresses PCI
- Screen employees
- Have incident response processes in place (and test them annually)
- Make your vendors/partners comply with PCI
- Annual risk assessment!

Questions?

- **Any questions about specific requirements?**

Compliance: Improve Your Processes, Leverage Technologies and Reduce Costs

Agenda

- Requirements Overview
- **Wrap up**

Wrap-up: Requirements

- **Understand the requirements**
 - The audit procedures *are* the assessment - take a half hour and read them
- **Know your shortcomings**
 - Self-assess before calling in a QSA
- **Address what you can before you pull the trigger**
 - It's easier (and cheaper) to fix problems without a QSA "armchair quarterbacking" – fix or minimize problem areas before you make the call

Questions? Comments

Thank you!