Three Critical Success Factors for PCI Assessment

Seth Peter

NetSPI

April 21, 2010

RISK COMPLIANCE SECURITY

Introduction

- Seth Peter
  - NetSPI Chief Technology Officer and Founder
  - 15 year history of application, system, and network assessment
  - PCI QSA, PA-QSA
- About NetSPI
  - Founded in 2001
  - Exclusive focus: information security consulting
    - Security & compliance assessments, security program development
    - No hidden agenda, no product to sell, no influenced opinion
  - PCI QSA, ASV, and PA-QSA certifications
  - Firm believers that compliance does not equal security

Agenda

- PCI DSS, an evolving standard
- Interpreting requirements
- Three critical success factors
  - Pre-assessment preparation
    - Common audit mistakes
  - Remediation
  - Payment applications

Evolving Standard

- The PCI SSC has adopted a two-year lifecycle process for PCI DSS
- Changes based upon input from 5 brands & participating organizations
- Incorporates lessons learned from recent breaches
- Addresses some technology changes
- Relatively new audit program

Room for Interpretation?

- While some PCI DSS requirements are crystal clear, others leave some…
  - **1.1.3** Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone

VS

  - **1.1.5** Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure

Room for Interpretation?

- Another example
  - **2.1** Always change vendor-supplied defaults **before** installing a system on the network…

VS

  - **2.2.1** Implement only one primary function per server

– OR

  - **2.2.3** Configure system security parameters to prevent misuse

Pre-assessment Preparation

- Compliance is ongoing, not an annual event
- While the DSS is somewhat risk based…

  DSS audits are pass/fail
- Auditors are required to collect three types of evidence
  - Documentation
  - Interviews
  - Observation (configurations, process, state, action, and network traffic)

Common Audit Mistakes

- Firewall rulesets
- System hardening
- Application development practices
- Penetration testing
- Third-party service providers
- Auditing & logging
- General advice

- **1.1.5** Documentation and business justification for use of all services, protocols, and ports allowed…
- **1.2.1** Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment
- **1.3.1** Implement a DMZ to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment
- **1.3.5** Restrict outbound traffic from the cardholder data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ

Common Audit Mistakes

- Firewall rulesets
- System hardening
- Application development practices
- Penetration testing
- Third-party service providers
- Auditing & logging
- General advice

- **1.1.5** Every firewall rule should be itemized down to the src/dest IP address, dest protocol/port, include a documented reason, and call out if the protocol is encrypted or not.
- **1.2.1, 1.3.1** If you've done your homework for 1.1.5, you should be well along your way. Be sure to avoid:
  - Overly permissive outbound rules
  - Overlapping rules
  - IP-based rules w/o port restrictions
  - Use of protocol ranges
- **1.3.5** Bottom line, don't allow your back-end systems to access the Internet. If they process over the Internet, whitelist your processor IPs and ports; document all controls

Common Audit Mistakes

- Firewall rulesets
- System hardening
- Application development practices
- Penetration testing
- Third-party service providers
- Auditing & logging
- General advice

- **2.2** Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards
- **2.2.1** Implement only one primary function per server
- **2.2.2** Disable all unnecessary and insecure services and protocols
- **2.2.3** Configure system security parameters to prevent misuse
- **2.2.4** Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers

Common Audit Mistakes

- Firewall rulesets
- System hardening
- Application development practices
- Penetration testing
- Third-party service providers
- Auditing & logging
- General advice

- **2.2** Configuration standards should be mapped to an external standard; document variations. Itemize all 3rd party components and include within your standard. Be prepared to demonstrate how you've implemented the standard
- **2.2.1** Can you describe the function in two words or less? Ensure the services required to run are all related to that function. Avoid the examples sited within the audit procedures
- **2.2.2, 2.2.4** Inventory the running services, remove anything unrelated or auxiliary. Avoid unencrypted protocols and applications with known vulnerabilities
- **2.2.3** Document and understand all configurable application or service parameters

Common Audit Mistakes

- Firewall rulesets
- System hardening
- Application development practices
- Penetration testing
- Third-party service providers
- Auditing & logging
- General advice

- **6.3** Develop software applications in accordance with PCI DSS… and based on industry best practices, and incorporate information security throughout the software development life cycle
- **6.3.7** Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability
- **6.5** Develop all web applications… based on secure coding guidelines such as the *Open Web Application Security Project Guide.*
- **6.6** For public-facing web applications… either:
  - Do an application vulnerability security assessment
  - Place application behind a web-application firewall

Common Audit Mistakes

- Firewall rulesets
- System hardening
- Application development practices
- Penetration testing
- Third-party service providers
- Auditing & logging
- General advice

- **6.3** Map your development standards to both PCI and an Industry Best Practice. Ensure your SDLC includes: security requirements, risk/threat modeling, code review, security testing (vulnerability and business logic)
- **6.3.7** Either use a third party for code review or document your code review checks and processes, and train your developers
- **6.5** Don’t just list the OWASP Top 10 in your coding standards, but refer or include in-depth OWASP information
- **6.6** For application assessments, ensure you are testing all application functionality as an authenticated user, and include manual authorization and authentication checks

Common Audit Mistakes

- Firewall rulesets
- System hardening
- Application development practices
- Penetration testing
- Third-party service providers
- Auditing & logging
- General advice

- **11.3** Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following:
- **11.3.1** Network-layer penetration tests
- **11.3.2** Application-layer penetration tests

Common Audit Mistakes

- Firewall rulesets
- System hardening
- Application development practices
- Penetration testing
- Third-party service providers
- Auditing & logging
- General advice

- **11.3** Penetration testing is often misunderstood
  - A penetration test is not a vulnerability assessment; tests should attempt to exploit vulnerabilities and weaknesses at the network and application level
  - An internal penetration test means from within your cardholder environment
  - Start with the threat discussion, model your tests accordingly
  - Use a third party or ensure your tester is adequately trained
  - Goal is to determine if unauthorized access can be achieved

Common Audit Mistakes

- Firewall rulesets
- System hardening
- Application development practices
- Penetration testing
- Third-party service providers
- Auditing & logging
- General advice

- **12.8** If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following:
- **12.8.3** Ensure there is an established process for engaging service providers including proper due diligence prior to engagement
- **12.8.4** Maintain a program to monitor service providers' PCI DSS compliance status

Common Audit Mistakes

- Firewall rulesets
- System hardening
- Application development practices
- Penetration testing
- Third-party service providers
- Auditing & logging
- General advice

- **12.8.3** Consider creating a third-party risk assessment program, similar to BITS or ISO:27002. It should include:
  - Assessment questionnaire
  - Interview questions
  - Consider onsite review if the risk or relationship warrants it
  - Establish risk decision criteria
  - If you are provided a third-party audit report or ROC, ensure the scope includes your specific solution
- **12.8.4** Conduct this activity on an annual basis, and be prepared to terminate the contract if requirements are not being maintained

Common Audit Mistakes

- Firewall rulesets
- System hardening
- Application development practices
- Penetration testing
- Third-party service providers
- Auditing & logging
- General advice

- **5.2** Ensure that all anti-virus mechanisms are … capable of generating audit logs
- **10.1** Establish a process for linking all access to system components to each individual user
- **10.5.4** Write logs for external-facing technologies onto an internal log server
- **10.5.5** Use file-integrity monitoring or change-detection software on logs
- **10.6** Review logs for all system components at least daily
- **11.5** Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files

Common Audit Mistakes

- Firewall rulesets
- System hardening
- Application development practices
- Penetration testing
- Third-party service providers
- Auditing & logging
- General advice

- **5.2** Consider sending your AV logs to the centralized log server
- **10.1** Yes, activity logging should include, network, system, application, database, and anything you else you can think of
- **10.5.4** Include all external systems logs within your log server
- **10.5.5** Your FIM must be installed, monitoring log files, and configured to alert
- **10.6** In order to satisfy daily log review, you must implement a rules engine
- **11.5** Your FIM deployment must monitor system files, application files, and other areas where cardholder data is stored (databases, transaction logs, etc.)

Common Audit Mistakes

- Firewall rulesets
- System hardening
- Application development practices
- Penetration testing
- Third-party service providers
- Auditing & logging
- General advice

- Get to know all locations of cardholder data
  - Historical data
  - Debug files
  - Backup media
  - Offsite storage
- Review retail environments
  - POS - log, history, flat files
  - Back office
  - Reports, paperwork, receipts
  - Archival/storage
  - Avoid over-focus on corporate/IT environments

Pre-assessment Preparation

- Engage your auditor early
  - Obtain detailed project plans, evidence requirements, and interview topics
  - Validate your assumptions prior to an onsite
- Consider a gap analysis with new DSS versions
- Organize your artifacts and be prepared to:
  - Document
  - Discuss
  - Demonstrate

Remediation

- Unfortunately, gaps happen. To avoid missing audit deadlines:
  - Inquire about any identified gaps frequently
  - Discuss options with your auditor, and try to find the common ground between compliant and business-justifiable
  - Work off of one common gap report that contains your remediation plan
- Engage your Acquirer/Processor

PA-DSS

- Applications that are not compliant with DSS requirements may require compensating controls
- PA-DSS applies to software vendors and their customers
- Using compliant apps doesn’t mean you’re compliant
- PCI standard, Visa mandate

For More Information…

- This presentation is further outlined in a free whitepaper at www.netspi.com
- Ongoing PCI dialog at: www.netspi.com/blog
- Email the QSA: seth.peter@netspi.com

netspi

RISK COMPLIANCE SECURITY