# Common Missteps in PCI Audit

**Ed Moyle**

**Compliance Workshop**

**Friday, June 20 2008**

# Agenda

- **Level-set: PCI Validation Overview**
- **Issues From the Field**
- **Problems and Solutions**
- **Wrap up**

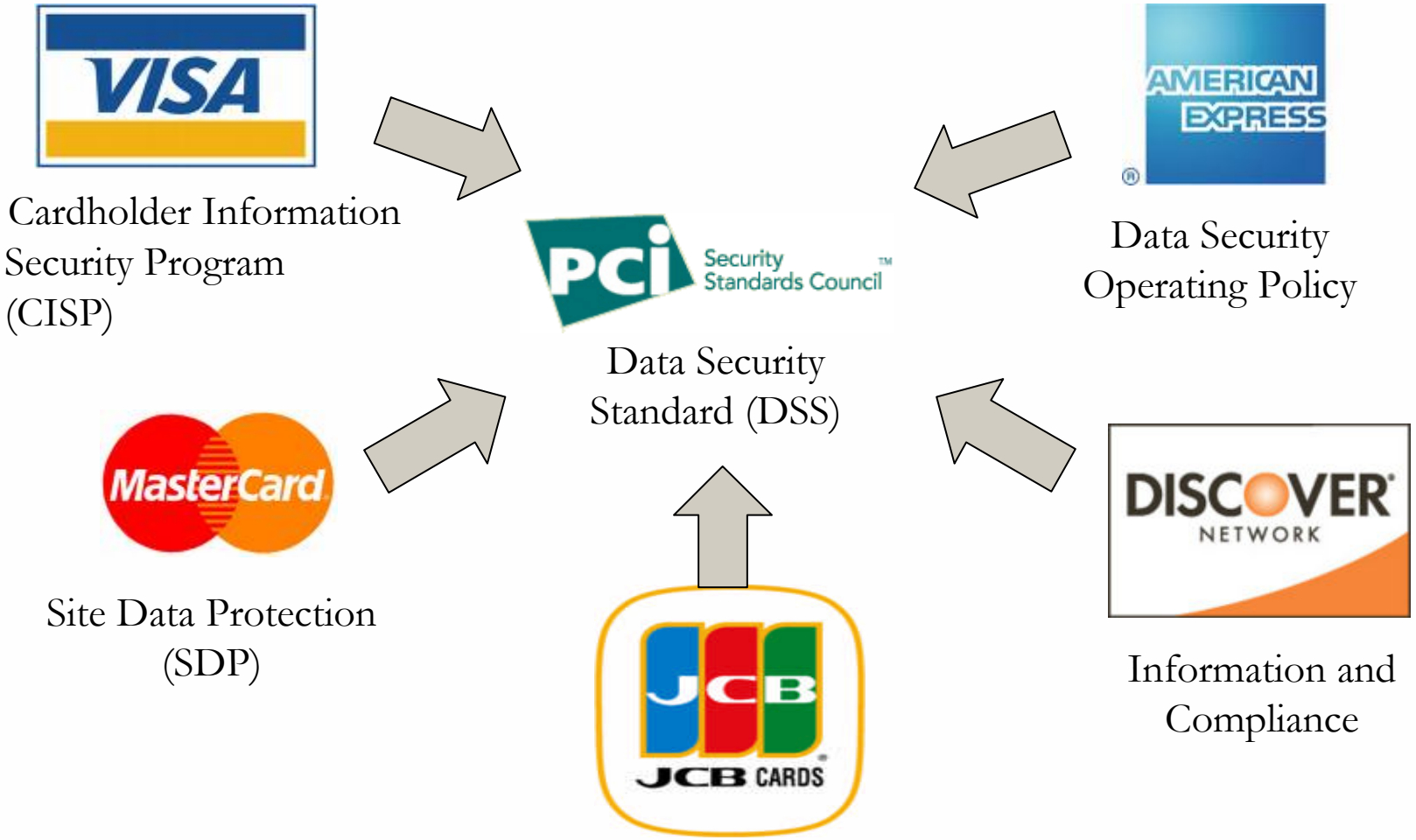
**"The PCI Data Security Standard represents a common set of industry tools and measurements to help ensure the safe handling of sensitive information… the standard provides an actionable framework for developing a robust account data security process - including preventing, detecting and reacting to security incidents." – PCI Standards Council**

# DSS in a nutshell

**The PCI (Payment Card Industry) DSS (Data Security Standard) is:**

- **A set of *minimum baseline* controls for securing payments**
- **Required (everyone in the payment lifecycle must comply)**
- **A unified standard agreed to by all card brands**

# A unified standard



# Everyone must comply (resistance is futile)

- **Everyone must <u>be</u> compliant with the standard**

Merchants (Accepting Cards)

Acquirers (Merchant Banks)

Issuers (Cardholder Banks)

Service Providers (Everybody Else)

- **Some firms must also <u>validate</u> compliance**
  - Large-volume merchants (thresholds set by card brands)
  - Certain service providers
  - Smaller merchants subject to acquirer requirements

# PCI "Audit" (Compliance Validation)

- **While everyone must *be* compliant, some firms must also *validate* compliance via assessment**
- **Firms must validate if:**
  - **They meet specific volume-related criteria defined by individual card brands (careful, these differ from brand to brand)**
  - **Are required to by their acquiring bank**
- **Compliance validation happens when a signed RoC (Report on Compliance) is submitted**
- **PCI assessors recognized by the Standards council are called "QSA's" (Qualified Security Assessors)**

# Can I assess myself?

- **Short answer: maybe** **(but you probably don't want to)**
- **Long answer: despite popular myth, you *can* assess yourself, provided:**
  - You follow the audit procedures
  - Your acquirer agrees
  - You're a *level 1* merchant (e.g. "Amazon.com")
  - You're not a service provider
  - An approved officer (think CEO or CFO) signs on the "dotted line" (attests to the veracity of the results)
  - You're absolutely sure you're going to do it right
- **Typical assessment scenarios:**
  - A QSA assessing a merchant
  - A QSA assessing a service provider

# Agenda

- Level-set: PCI Validation Overview
- **Issues From the Field**
- Problems and Solutions
- Wrap up

# Report from the trenches…

- **Generally speaking, most firms don't do well the first time through**
  - Costs money
  - Wastes time
- **It's an opportunity for improvement:**
  - By learning from the mistakes of others, you can be better prepared
- **Most often, the issues are one of a few preventable issues that could have been fixed before the assessment**
  - By hearing what the issues are, you go into the process with an eye to the most common "problem areas"

# The good news…

- **The most common issues are preventable with a bit of planning and "elbow grease"**
- **You can fix all the issues yourself**
- **Advancing your PCI compliance can help you comply with other regulations as well**

# The most common issues…

- **90 something percent of the time, it's one or more of the "deadly half-dozen":**
  1. Inappropriate scope
  2. Insufficient documentation
  3. Application issues (particularly legacy applications)
  4. Unnecessary (or inappropriate) data storage
  5. Compensating controls (that don't compensate)
  6. Bad timing
- **If you can get past these, you're in pretty good shape**

# Agenda

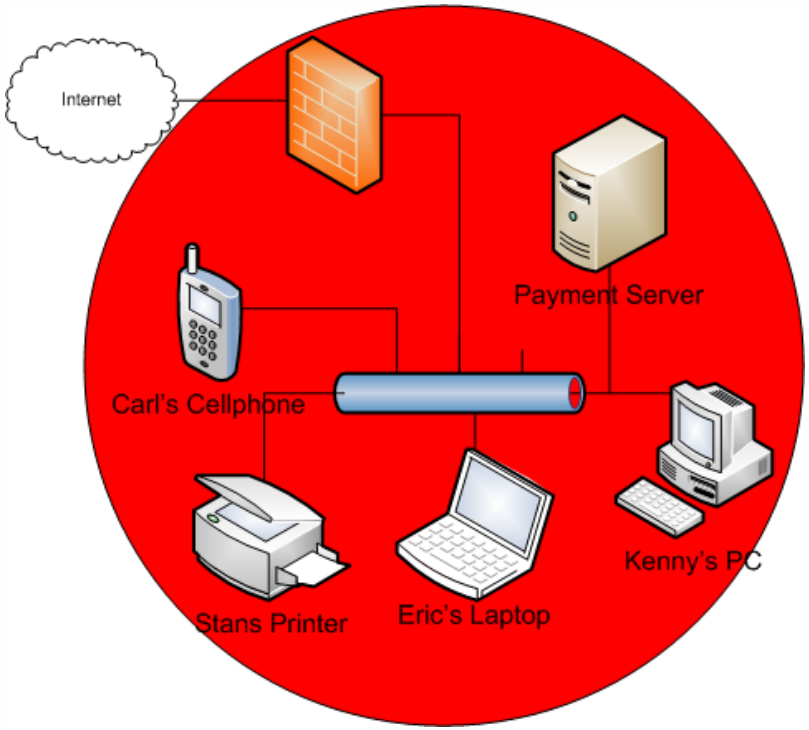
- Level-set: PCI Validation Overview
- Issues From the Field
- **Problems and Solutions**
- Wrap up

# Enemy #1: Inappropriate Scope

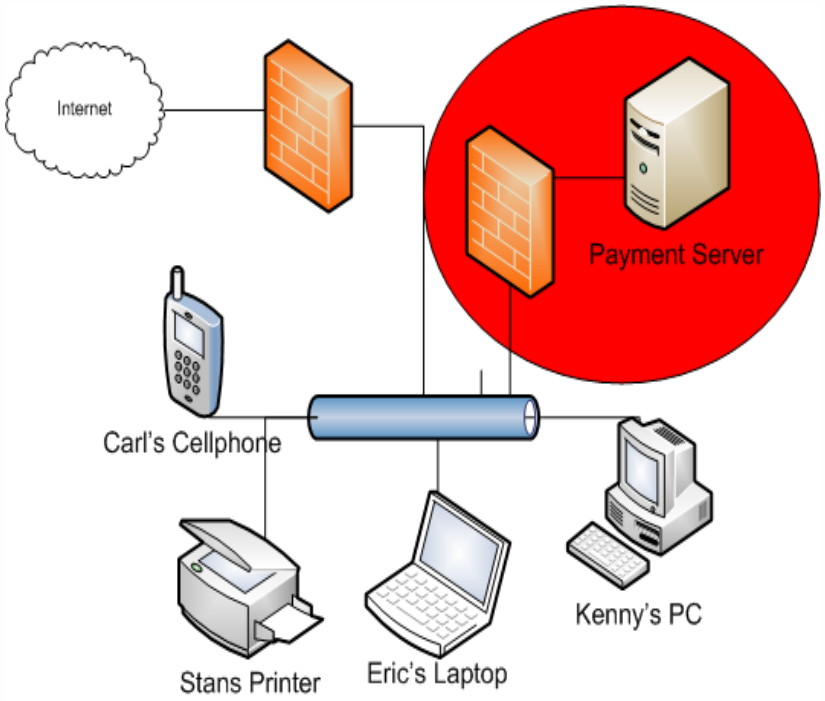
- **#1 most common assessment issue**
- **Remember, the assessment scope applies only to the cardholder data environment (CDE)**
  - Cardholder environment: systems that **store, process, or transmit** cardholder data
- **The assessor must include everything in scope that is not segmented from the CDE**
- **No segmentation? Then the assessor *must* include *everything* in scope**
  - This is where most firms start
  - This approach rarely (never?) leads to a clean ROC

# Scoping Example

**Red area denotes scope of PCI assessment**




**Unzoned (everything in scope)**




**Zoned (strategic scope)**

# The Solution: Zones (Enforcement of Scope)

- **Once you have defined the scope of the CDE, you need to enforce it; usually with:**
  - Firewalls
  - Physical separation ("air gap")
- **If you don't enforce the scope, again the assessor must evaluate the entire environment**
- **Document it**
  - Document how your zoning approach enforces the scope
  - Document why you've chosen the approach you have
    Document who is responsible for maintaining the boundary

# Enemy #2: Inadequate Documentation

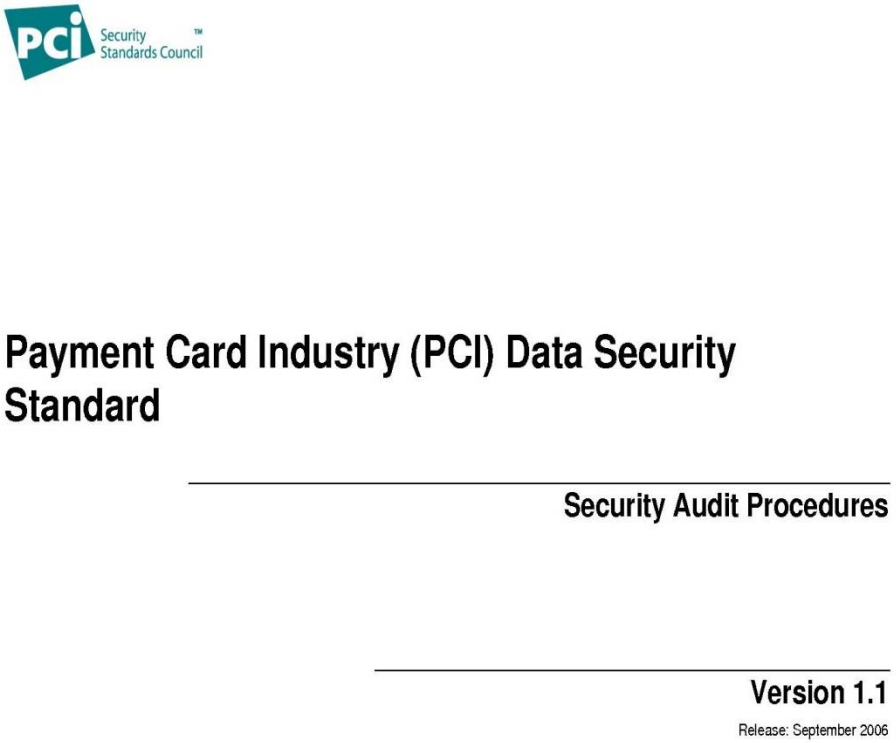
- **Remember, the requirements aren't "rocket science"**
  - Chances are good you're already (mostly) compliant
- **But "if there's no document, it doesn't exist"**
  - Your QSA must disregard ad-hoc or informal processes
  - Which means you need to have documented policy and defined procedures
- **Don't forget to document – even if you're pretty confident that your process meets the requirement**

# The Solution: They have to document as well…

**"Forewarned is forearmed"**

**QSA's *must* follow the defined assessment procedures. This means *everything* they are going to do, look for, evaluate, request, or sample is written down and can be found online.***

**If you had the answers to a test ahead of time, wouldn't you at least glance at it while studying**




*https://www.pcisecuritystandards.org/docs/pci_audit_procedures_v1-1.doc

# Enemy #3: Apps

- **Apps are hard, no matter how you slice it**
  - In the large organization, there are hundreds (thousands?) of them
  - In the SMB, might not be a "core competency"
  - No matter who you are, probably prioritized lower on the list
- **The requirements for apps are pretty tough**
  - OWASP "Top Ten"
  - Lifecycle requirements
  - New requirements for code review and/or "application-level firewall" (this means "a web application firewall (WAF)"*) effective as of now (June 2008)
- **Many organizations have so many apps – and may not have a solid strategy for application security in place**

***Information Supplement: Requirement 6.6 Code Reviews and Application Firewalls Clarified**

# A note about legacy environments

- **For a long time, the retail vertical was (comparatively) unregulated**
  - Much of what our IT shops deployed were put in place before PCI was a requirement
  - As such, they did not address the PCI requirements
- **Many firms have legacy applications in place that do not meet the requirements**
  - How often do IT shops re-evaluate legacy apps?
  - Many firms just don't know that these systems are out there
  - Old POS systems are **notorious** for causing problems

# The Solution: Two options here

- **For COTS: For applications you don't develop, it's about to get much easier**
  - The standards council now "owns" the PA-DSS (Payment Application Data Security Standard)
  - Commercial tools will now undergo certification for compliance
- **For in-house applications: Read OWASP**
  - *The application requirements are verbatim from the OWASP top-ten*:
    - OWASP "Top Ten" (1 of 10): "Unvalidated Input"
    - Requirement clause 6.5.1: "[continued from 6.5] Cover prevention of common coding vulnerabilities… to include… [6.5.1] Unvalidated input"
    - Testing Procedure 6.5.1: "[continued from 6.5] …verify that processes are in place to confirm that web applications are not vulnerable to… [6.5.1] Unvalidated input"
  - Your assessor will be looking for a **documented** SDLC (software development lifecycle) that incorporates specific application security testing (using OWASP)
  - Assessors will usually look at the process first, and only a sample of specific apps

# Enemy #4: Data Storage

- **You can't store authorization data past authorization**
  - Don't ever store track (mag-stripe) data or CVV/CVC. No matter who says to. Seriously. Even if it's your acquirer.
- **There are good business reasons to store the PAN**
  - "One click"
- **If you're going to store it, you need to protect it**
  - If you store the PAN, you'll need to encrypt, truncate, or hash
  - Encrypting the PAN is the only approved way to store it so you can use it later, BUT that introduces key management (which is hard)

# The Solution: Limit what you keep

- **If there's any way you can get away with it, try not to store the PAN**
  - In many cases, there are other ways to solve the problem
  - Take time to validate assumptions and decide if cardholder data really does need to be stored
- **Consider a "data deletion" policy to govern storage of cardholder data**
- **Can you make it someone else's problem?**
  - Outsourcing some aspects of this can help limit your scope (for example, outsourced processing)

# Enemy #5: Poor Compensating Controls

- Many firms can't meet particular controls, so they attempt to apply compensating controls
- However, there are specific rules for compensating controls that need to be followed
- Not following the rules means your assessor can't accept it

# Solution: Toe the line

- **Compensating controls need to meet the intent and the rigor of the original requirement**
  - Adding key management doesn't help you meet an authentication requirement
- **Compensating controls must be documented**
  - Compensating controls are subjective, document fully to build your case
  - Even if you can't meet a control, document *why you can't* and *what else you're doing* to address the issue
  - Your assessor **wants** to agree with you. Thorough documentation makes it easy for the assessor to agree
- **Compensating controls have a shelf life**
  - They're a "stop-gap", not an "end state"

# Enemy #6: Bad Timing

- **"Alea iacta est" (the die has been cast)**
  - In many cases, firms can have a **fantastic** strategy for how to solve an issue, but the QSA can't use it because it's not what's in production
- **A QSA can't validate to what's not in production**
  - If it's not in production now, it can't be in or out of compliance – it's just not there

# The Solution: Pre-assess and pre-plan

- **Read the documentation your assessor will be using to evaluate you**
  - PCI Assessment Procedures available from the PCI Standards Council website (http://www.pcisecuritystandards.org)
  - PCI Standards Documentation
- **Pre-assess**
  - Do the pre-assessment questionnaire (even if you don't have to)
  - Go through a pre-assessment exercise (with or without a QSA) to make sure you have everything in place before the assessment starts
- **Deploy compensating controls before you use them for the "real deal"**

# Agenda

- Level-set: PCI Validation Overview
- Issues From the Field
- Problems and Solutions
- **Wrap up**

# Recap

- **Most issues are preventable**
  - Most of the issues come down to planning and preparedness
  - Planning you do in advance of the assessment translates directly into dollars for your organization
    - Less time-consuming for the assessment (which means it'll be cheaper)
    - A "clean" ROC means you don't need to pay for do-overs
    - Comprehensive documentation means less time your staff spends answering questions
- **Act before the assessment**
  - The time to find out that you have issues is before the assessment
  - Planning should be thorough – shoot for no surprises once the assessment is underway

# Remember

- **Documentation is key**
  - Document your strategy for compliance
  - Document the controls in place
  - Read and understand the documents your QSA's will be working from
- **It's a journey, not a destination**
  - Analyze where you think you are so you don't get blind-sided
  - Work with your assessor – you're both on the same team
- **Aggressively limit scope (!!) - you won't regret it**