

PCI DSS Lessons Learned

Educause Security Conference 2008

Mike Leach, Project Manager

Jenn Stewart, Project Technical Coordinator

Copyright Penn State, 2008. This work is the intellectual property of the author. Permission is granted for this material to be shared for non-commercial, educational purposes, provided that this copyright statement appears on the reproduced materials and notice is given that the copying is by permission of the author. To disseminate otherwise or to republish requires written permission from the author.

Overview

1. The Penn State Community
2. IPAS Project Overview
3. Compliance Approach
4. Misconceptions
5. Lessons Learned

Who is Penn State?

1. 24 Campus Locations

- Distributed across Commonwealth
- Why we take cards

2. 52 Merchant Areas

- Swipe terminals (dial-up, IP-based)
- In-house eCommerce
- Third-party applications

Project Overview

Information Privacy and Security (IPAS)

Multi-year, multi-phase effort with
University-wide scope

- Phase I: Evaluate PCI-DSS systems and networks
- Phase II: Focus on privacy and security practices

Project Team

- Designated Staff
 - Project Manager
 - Sr. Network Analyst
 - Technical Coordinator
- Administration
 - Security Operations and Services Sr. Director
 - Chief Privacy Officer

IPAS Sponsorship & Leadership

- Sponsorship
 - Executive VP and Provost
 - Sr. VP for Finance and Business
- Oversight
 - Vice Provost for Information Technology Services
 - University Controller



PCI DSS

Optional? No way!

History of PCI DSS

- Five major card brands joined forces
- 12 strict security requirements
 - 2005, PCI DSS v1.0
 - 2006, PCI DSS v1.1
 - 2008, SAQ A, B, C, D, E
- Ongoing efforts
 - Annual SAQ
 - Compliance can be broken in 1 minute



Audience Assessment

**Who has already gone through
PCI DSS validation?**



IPAS Approach

Challenges, Misconceptions
and Lessons Learned

Education for IPAS Team

- Educate Yourself First
 - Treasury Institute's PCI DSS Conference
 - EDUCAUSE Security Conference
 - Joined PCI SSC
 - VISA and MasterCard training
 - Benchmark with other institutions

Understanding of PCI DSS

- Navigating PCI DSS, *Understanding the Intent of the Requirement*
- Qualified Security Assessor (QSA)
- Working Group and Subcommittees
 - University-wide Participation
- Help others Understand

Card Processing Assessment

- Controller Office
 - Merchant IDs
- Search for Payment Applications
 - Clubs, associations
 - Seasonal sales
 - Non-credit courses & seminars
- Word of Mouth

Qualified Security Assessor

1. Provides guidance and interpretation of the DSS
2. Online Portal
3. External Scans
4. Policies
5. Compliance Validation

Check the Source

- QSA Challenges
 - Verify with the DSS & SAP
 - PCI FAQ
- Acquiring Bank Miscommunication
 - Merchant level
 - Sales vs. Technical reps
- Card Brands - always correct

Raising Awareness

- Deans, Chancellors, VPs
- Designated IT, Admin, Financial Staff
- Training Offerings
 - Classroom (mandatory)
 - Online
 - On-demand
 - Document attendance
 - Enable information dispersion
- Funding Strategies

Misconceptions

- Scope
 - PCI DSS applies to Cardholder Data Environment (CDE)
- Use of dial-up swipe terminals
- Need for software updates and sanitization of older versions
- Network segmentation
- Truncated card numbers

Centralized Services

- Benefits
 - Limits scope
 - Smaller administrative cost
- eCommerce solutions in-house
- Firewall services
- Future centralized services

IPAS Consulting Services

- Remediation Plans
- Network Diagrams
- Reference Architecture
 - Segmentation outline
- Online Portal (QSA)

Policies

1. QSA Provided
 - Comprehensive
 - Adapted to local practices
2. Specific to department/area
 - General best practices
 - Integrate with network security policies

Compliance Validation

- Validation Timeline
 - Firm dates
 - Extension requests
- Online Portal
 - IP addressing schemes
 - External scans
 - Self Assessment Questionnaire (SAQ)
 - v1.1

Lessons Learned Summary

1. Obtain high level institutional support
2. Engage QSA if necessary
3. Train everyone involved in PCI
4. Be available for consulting
 - Scope creep
5. Consider centralized services
6. Share the knowledge

Question & Answer Session

Questions?

Information Privacy and Security

814.867.1340

ipas@psu.edu

<http://ipas.psu.edu>