PCI FOR HIGHER EDUCATION

John Musgrove, MS, CISA
Deputy Director, Technology Audit
Mandate

“Everyone involved in the payment process has a duty to consumers to protect their data to the highest standard.”

--Bob Russo, PCI Security Standards Council
John Musgrove, Atypical Auditor

• Meandering Career Path
  – Corpsman/Paramedic, USN-R for USMC
  – Diener, Cancer Statistician

• Information Systems: Bachelors, Masters, @VCU
  • Programmer, Reports Specialist, Systems Analyst, DBA, Architect

• Graduate Certificates @VCU
  • Instructional Technology, 2012
  • Nonprofit Management, 2014
  • Geospatial Information Systems, 2015

• Voracious Traveler – 35 countries and counting
Credit Card Fraud

• Is Big Business!
  – $1.5B in 2000

• Grows exponentially each year

• Stolen CC sells for $1 each on black market
Credit Card Breaches

• December 2006: TJ Max
  – 45M customers affected
  – $40M in fines
  – Biannual 3rd party security audit for 20 years

• January 2009: Heartland Payment Systems
  – 130M payment records
Even More CC Breaches

• November 2013: Target
  – 40M Credit and Debit Cards
  – Revised to 110M in January
  – Supplier Portal identified as Point of Entry

• September 2014: Home Depot
  – 56M Debit and Credit Cards
Consumer Risks

• Breached system for trusted retail partner
• ATM, self POS “skimmers” for harvesting
• Separation of customer and card for purchase
• Storage / use of card with smart phone
• Debit cards less safe than credit for fraud
PCI Definition

- Payment Card Industry
- Five Major Brands: MC, V, AE, D, DC
- DSS – Data Security Standard
Breach Ramifications

- Loss of banking relationship
- Mandated external security reviews
- Reputation damage
- Increased fees from financial partners
DSS History

- 1999: Visa’s Cardholder Information Security Program (CISP)
- 2004: PCI DSS 1.0
- 2006: PCI Security Standards Council formed
- 2009: PCI DSS Wireless Guideline
- 2011: PCI DSS 2.0
- 2013: PCI DSS 3.0
Formal Audit Approach

• QSA vs SAQ

• QSA: Qualified Security Assessor
  – Certified annually by PCI SSC
  – External auditing of merchants

• SAQ: Self-Assessment Questionnaire
  – Environment-specific requirements
  – Attestation of compliance
Audit Program: Full Review

• Self-managed, hosted or stored POS systems

• Six Objectives

• Objectives supported by 12 Requirements

• Certified QSA to complete
Full Review Objectives

• Secure Systems and Network
• Protection of Cardholder Data
• Vulnerability Management
• Strong Access Controls
• Monitoring and Testing
• Information Security Policies and Procedures
Audit Program: Third Party

• One Objective
  – Third Party Service Provider assessment
    • Annual assessment, or
    • Multiple, on-demand assessments
  • And

• Use of a PA-DSS Application
• In a PCI DSS compliant environment
Self Assessment Guidelines

• Never store sensitive Authentication Data
• Point of Sale security
• Cardholder Data
  – Don’t store what isn’t needed
  – Consolidate and isolate what is stored
• Ensure compensating controls
• Enlist professional assistance and training
Readiness, the Practical Approach

• Review treasury procedures for completeness
• Catalog each payment site in organization
• Survey entire population
• Interview non-respondents
• Visit high volume areas
• Round-out sample with judgmental additions
Review Treasury Procedures

- Inspect processes for standardization
- Verify centralized management commitment
- Review policy lifecycle
  - Definition, Implementation, Compliance, Review
Catalog Payment Site Participants

- Brainstorm possible payment collectors
- Retrieve active merchant IDs from Treasury
- Verify last activity and volume for each
Survey Entire Population

• Standardized questionnaire

• Determine contact/responsible individual

• Provide adequate lead time, clear deadlines
Interview Non-Respondents

- May have incorrect data for merchant ID
- Personnel changes impact continuity
Visit High Volume Areas

- Typically have stable processes
- Highest risk for breach or fraud
Judgmental Sample

• Complete remaining gap with selected areas

• Compare processes for high and low volumes

• Every payment collection site has risk
Typical Findings

• Policy, procedures missing or incomplete
• Self-review not completed annually
• Outdated equipment
• Shared logins or inability to assign unique ID
• Retained data, analog and/or digital
• Gaps in proactive education
Best Practices

• Limited collection/storage of data

• Restrictions on refunds

• Readiness review or SAQ for Benchmark
Word of Caution

• “The world has enough for everyone's need, but not enough for everyone's greed.”

--Mahatma Gandhi
References


• https://www.pcisecuritystandards.org/