PCI DSS in Higher Education
About Sikich LLP

- Sikich LLP is a leading accounting, advisory, investment banking, technology and managed services firm
  - One of the country’s top 35 largest CPA firms
  - Ranked 3,829 on Inc. magazine's list of the 5,000 fastest-growing companies in the world
  - More than 650 employees in 11 locations
About 403 Labs

- 403 Labs, a division of Sikich LLP, is a full-service information security and compliance consultancy
  - Qualified Security Assessor (QSA)
  - Payment Application Qualified Security Assessor (PA-QSA)
  - Approved Scanning Vendor (ASV)
  - PCI Forensic Investigator (PFI)
  - QSA for Point-to-Point Encryption (QSA (P2PE))
  - PA-QSA for Point-to-Point Encryption (PA-QSA (P2PE))
About the Presenter

- B.A., English, from the University of California, Irvine
- M.Ed., Higher Education Leadership, from the University of Arkansas
- 20 years experience in higher education:
  - IT Director for Financial Affairs/Treasurer
  - Director of commerce compliance/security
- Previous PCI Internal Security Assessor (ISA)
- Current PCI Qualified Security Assessor (QSA)
Agenda

• Payment Card Industry (PCI) Overview
• Ongoing and New Challenges with the PCI DSS v3.0
• Higher Education and PCI: Complexity Collides
• Why Worry?
• Compliance and Security
• Building a PCI Program
• Executive Role
Agenda

• Payment Card Industry (PCI) Overview
  • Ongoing and New Challenges with the PCI DSS v3.0
  • Higher Education and PCI: Complexity Collides
  • Why Worry?
• Compliance and Security
• Building a PCI Program
• Executive Role
PCI Overview: Ecosystem

- Five payment brands enforce the PCI Data Security Standard (PCI DSS)
  - Track compliance and enforce standards (fines, sanctions)
  - Determine event response (forensics)
  - Define merchant levels
PCI Overview: Ecosystem

- PCI Security Standards Council (PCI SSC or “the Council”) develops the PCI DSS (and other standards) with input from the card brands and the Participating Organization (PO) community
  - New standards introduced on a three-year cycle
PCI Overview: Ecosystem

• Issuer role
  • Provide payment cards to cardholders (customers)
  • Pay the acquiring bank
  • Bill the cardholder

• Acquirer (merchant bank) role
  • Set merchant level
  • Determine compliance
  • Approve compensating controls
PCI Overview: Ecosystem

• Merchant role
  • Sell goods and services to cardholders
  • Pay discount fees to acquiring bank
  • Responsible for validating compliance and security to acquiring bank
PCI Overview: Ecosystem

- Service Provider role
  - “Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the security of cardholder data.”

1 Payment Card Industry Data Security Standard Glossary, Abbreviations and Acronyms
PCI Overview: Ecosystem

- Colleges and universities are comprised of one to many merchants
- Most will self-assess to their acquirers (banks)
- Nearly all will work with service providers
  - Due diligence, contracts, monitoring
- Schools can become unwitting service providers
  - Need to validate to partners and card brands
PCI Overview: Scope

- PCI Data Security Standard (PCI DSS)
  - Applies to all people, processes and systems that:
    - Store, process or transmit cardholder data (aka cardholder data environment or CDE)
  - Also applies to networks and systems that connect to the CDE OR affect the security of the CDE
PCI Overview: The PCI DSS

- Six goals
- 12 major requirements
- 300+ individual requirements
- 500+ individual controls
- 100% must be in place 24/7/365 for compliance (must be business as usual)
- Maintaining PCI compliance can be a challenge
## PCI Overview: The PCI DSS

### PCI Data Security Standard – High Level Overview

<table>
<thead>
<tr>
<th>Category</th>
<th>Sub-Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build and Maintain a Secure Network</td>
<td>1. Install and maintain a firewall configuration to protect cardholder data</td>
</tr>
<tr>
<td></td>
<td>2. Do not use vendor-supplied defaults for system passwords and other security parameters</td>
</tr>
<tr>
<td>Protect Cardholder Data</td>
<td>3. Protect stored cardholder data</td>
</tr>
<tr>
<td></td>
<td>4. Encrypt transmission of cardholder data across open, public networks</td>
</tr>
<tr>
<td>Maintain a Vulnerability Management Program</td>
<td>5. Use and regularly update anti-virus software or programs</td>
</tr>
<tr>
<td></td>
<td>6. Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td>Implement Strong Access Control Measures</td>
<td>7. Restrict access to cardholder data by business need to know</td>
</tr>
<tr>
<td></td>
<td>8. Assign a unique ID to each person with computer access</td>
</tr>
<tr>
<td></td>
<td>9. Restrict physical access to cardholder data</td>
</tr>
<tr>
<td>Regularly Monitor and Test Networks</td>
<td>10. Track and monitor all access to network resources and cardholder data</td>
</tr>
<tr>
<td></td>
<td>11. Regularly test security systems and processes.</td>
</tr>
<tr>
<td>Maintain an Information Security Policy</td>
<td>12. Maintain a policy that addresses information security for all personnel.</td>
</tr>
</tbody>
</table>
Agenda

- Payment Card Industry (PCI) Overview
- **Ongoing and New Challenges with the PCI DSS v3.0**
- Higher Education and PCI: Complexity Collides
- Why Worry?
- Compliance and Security
- Building a PCI Program
- Executive Role
Ongoing and New Challenges with the PCI DSS v3.0

- Scoping and segmentation
- New Self-Assessment Questionnaires (SAQs)
- Service provider oversight
- Penetration testing rigor
Ongoing and New Challenges with the PCI DSS v3.0

• Security monitoring for customer interaction devices
• EMV (Chip & PIN or Chip & Signature)
• Branded campus ID cards
• Mobile payments
Agenda

• Payment Card Industry (PCI) Overview
• Ongoing and New Challenges with the PCI DSS v3.0
• Higher Education and PCI: Complexity Collides
• Why Worry?
• Compliance and Security
• Building a PCI Program
• Executive Role
Higher Education and PCI: Complexity Collides

- Colleges and universities are like small cities
  - Retail, kiosks, ecommerce, telephone/call center, ticketing, parking, fundraising, dining, vending…
- Often multiples of each environment
- Decentralized IT and/or policy
  - Different teams might have differing goals and priorities
- Can never outsource your responsibility
Agenda

• Payment Card Industry (PCI) Overview
• Ongoing and New Challenges with the PCI DSS v3.0
• Higher Education and PCI: Complexity Collides
• Why Worry?
• Compliance and Security
• Building a PCI Program
• Executive Role
Universities, Lawmakers Targets of Security Breaches, ID Theft

Even security experts fall victim.

While public attention has been drawn to high-profile cyberattacks on private companies such as Target, other entities, such as universities, are not immune, as Government Technology reported last week. And this week, the list of public-sector targets continues to grow.

North Dakota University reported a server breach that exposed the names and Social Security numbers of about 300,000 students, former students and faculty. While the breach was spotted a month ago, the university delayed reporting it to those most likely to be affected while conducting an investigation to determine what exactly happened.
Why Worry?
Why Worry?

• The Ponemon Institute’s 2013 Cost of Data Breach Study estimated:
  • $111 per breached record (education sector)
  • $188 per breached record (overall U.S. average)
  • Average breach for 2012 involved 23,647 records
    • ~ $2.6M at the lowest rate listed above
    • Investigations, breach notifications, credit monitoring
  • Reputational risks difficult to quantify
Agenda

• Payment Card Industry (PCI) Overview
• Ongoing and New Challenges with the PCI DSS v3.0
• Higher Education and PCI: Complexity Collides
• Why Worry?
• **Compliance and Security**
• Building a PCI Program
• Executive Role
Compliance and Security

• The PCI DSS looks like a compliance challenge
• Temptation: focus on compliance
  • What do we need to do to tick this box?
  • How do we get a clean report?
Compliance and Security

• The PCI DSS looks like a compliance challenge
• Temptation: give it to business/treasury
  • “They’re used to working with banks”
  • Business people know compliance programs
  • Usually lack technical expertise needed to analyze many of the PCI DSS controls
Compliance and Security

• The PCI DSS looks like a security challenge
  • Breaches, breaches and more breaches…
• Temptation: give it to IT or Information Security (IS)
  • They understand technology and security
  • Look at all of those firewall, network and other IT requirements!
  • IT/IS may not be used to creating/implementing policy or managing complex business relationships
Compliance and Security

- The PCI DSS is both a security and compliance challenge
- In the end, it is a business challenge
  - Risk-based decision making
  - Consider business impact of choices
  - “Business as Usual”
- Consider security as the path to compliance
- PCI compliance is a program, not a project!
Agenda

- Payment Card Industry (PCI) Overview
- Ongoing and New Challenges with the PCI DSS v3.0
- Higher Education and PCI: Complexity Collides
- Why Worry?
- Compliance and Security
- Building a PCI Program
- Executive Role
Building a PCI Program

• Involve all stakeholders
• Many approaches: consider a committee
  • Business/Treasury/Procurement
  • Legal
  • Internal Audit
  • Information Technology
  • Information Security
• Someone must still be the overall program lead
Building a PCI Program

• Policies are a necessary step
  • Not the entire picture
• An assessment also measures how you adhere to and implement your policies
• Procedures
  • Drive “Business as Usual”
  • Help management be aware of commerce activities
Agenda

• Payment Card Industry (PCI) Overview
• Ongoing and New Challenges with the PCI DSS v3.0
• Higher Education and PCI: Complexity Collides
• Why Worry?
• Compliance and Security
• Building a PCI Program
• Executive Role
Executive Role

• Assemble your team
• See that policies and procedures are created
• Make sure those procedures are implemented and become “Business as Usual”
• Provide necessary resources
• Delegate necessary authority
• Create the culture of buy in through visible executive support
403 Labs
Security, Simplified.

A division of Sikich LLP

Thank You!

pcampbell@sikich.com
www.403labs.com
877.403.LABS