GET THE PCI DSS COMPLIANCE PROGRAM YOU NEED

Carolann G Lazarus, CISA, CCEP
IT Audit Manager
State University of New York, University at Buffalo
PCI Compliance Initiative Co-Lead

Higher Education Compliance Conference - SCCE
Tuesday June 11, 2019

UB is a research-intensive public university founded in 1846.
We are the largest and most comprehensive campus in the 64-campus SUNY system.
We have three campuses that encompass nearly 1,250 acres and 200 buildings.
We offer over 125 undergraduate degrees and over 320 graduate, professional and certificate programs.
Our student body consists of over 21,000 undergraduates and almost 10,000 graduate and professional students.
We employee just over 6,000 full-time equivalent employees.
About Me

- Co-Lead of the PCI Compliance Initiative, which has recently morphed into the PCI Compliance Committee
- Significant audit experience with compliance in higher education
- CCEP
Our PCI Compliance Initiative

PCI DSS OVERVIEW

Payment Card Industry Data Security Standard
PCI DSS Overview

Payment Card Industry (PCI) Data Security Standards (DSS)

Started with VISA in 2001. Incorporated into the PCI DSS in 2004 with the 6 major card brands.

Not a government regulation or law.

PCI DSS Overview

Payment Card Industry (PCI) Security Standards Council

https://www.pcisecuritystandards.org/

- Overview
- Guidelines
- SAQs
- Documents
- Training
PCI DSS Overview

Developed to increase control of card holder data in order to reduce credit card fraud and exposure

Applies to all merchants and service providers that store, process or transmit cardholder account data, regardless of volume

Updated annually, major update every three years – last major in April 2016

All merchants must annually self-assess compliance – SAQ’s

Consequences include fines, penalties and ineligibility to process credit cards in addition to brand and reputation damage

6 Goals and 12 Requirements of the PCI DSS

<table>
<thead>
<tr>
<th>Goals</th>
<th>PCI DSS Requirements</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 employees and contractors</td>
</tr>
</tbody>
</table>

Depending on the method used to accept credit card payments, some of these requirements may not be applicable. For example, only a few apply to a department that uses a credit card terminal connected to an analog or cellular phone line to process credit card payments.
Why Do We Need a PCI Compliance Program?

- Protect the institutions customers. Students, Parents, Faculty, Staff
- Protect the institutions reputation and resources
- Reduce risk of penalties

University of Connecticut Hack Exposed Students' Credit Cards, SSNs

CYBERATTACK 101: WHY HACKERS ARE GOING AFTER UNIVERSITIES

“Data Breaches Put a Dent in Colleges’ Finances as Well as Reputations”

The costs of a breach can run into the millions of dollars, according to data-security professionals who work in higher education.
RECOGNITION

How do you know your program needs improvement?

Recognizing the Need

Historic Actions 10+ yrs
- Committee
- Define category and level
- Identify merchants
- IT Networks
- Scanning
- SAQs
- Policies and Procedures

Wayback Machine
Recognizing the Need

Status 3 yrs Ago
- No Committee
- Missing Documentation
- Old Risk Assessment
- Decentralized w/o Oversight
- No Policy
- No Ownership
- Little Awareness

Recognizing the Need

Coherent Program:
- Committee
- Roles
- Training
- SAQ coordination
- Swipe terminals ownership
- Scanning
- Liaison with Acquiring Bank
Recognizing the Need

Independent Affiliates
- Training
- SAQ coordination
- Swipe terminals
- Scanning
- Liaison with Acquiring Bank

Improvement Drivers
- Compliance Cycle
- Management Changes
- Oversight (or lack of)
- Audits
KEY COMPONENTS

• Can you Pass an Audit?
• What Don’t you Know?
• PCI Committee

Key Components

Can you pass an audit?

- Risk Assessment
- Defined Roles
- SAQ’s
- Policy & Procedures
- Training
- IT Security
- Data Flow Diagram
Key Components

What Don’t You Know?
- What’s your transaction level
- How many merchants do you have?
- How much do you process $$?
- Who’s your acquiring bank?
- Which SAQ(s) do you need to complete?
- How many staff require training and what percentage have?
- Are your policy and procedures up-to-date?
- Who’s your QSA?

PCI Committee
- Standing
- Representative
- Accountable
- Acts as a Steering Committee
- Takes Action
- Performs Oversight
- Compliance Program
HURDLES & SOLUTIONS

Hurdles & Solutions

The Wrong People
- Sponsors
- Committee Members
- Subject Matter Experts
**Hurdles & Solutions**

**The Right People**
- Make it easy
- What’s the benefit to them
- Not the obvious choice
- Take advantage of change
- Don’t ignore users

**Ineffective Committee**
- Meet infrequently/ad hoc
- No worker bees
- Missing deliverables
- High turnover
Hurdles & Solutions

Functional Committee
- Ownership / Leadership
- Rules
- Training
- Planned turnover
- Scheduled, sufficient meetings
- Accountability
- Valued

Hurdles & Solutions

Lack of Knowledge
- Ultimate arbiter
- Awareness
- Direction
Hurdles & Solutions

Understanding
- QSA
- Training
- Awareness Activities
- Surveys
- Documentation

TOOLS & RESOURCES
Tools & Resources

✓ Treasury Institute for Higher Education
Has taken a leading role in supporting PCI compliance. They hold an annual PCI DSS workshop in the spring. It's a very good value.
http://www.treasuryinstitute.org/pci-dss-description/

✓ Higher Ed PCI listserv
To subscribe or unsubscribe via the World Wide Web, visit
http://lists.gonzaga.edu/mailman/listinfo/pci-compliance-l
or, via email, send a message with subject or body 'help' to
pci-compliance-l-request@lists.gonzaga.edu
You can reach the person managing the list at
pci-compliance-l-owner@lists.gonzaga.edu

Tools & Resources

✓ Shared space – box
✓ Tracking
  ▪ Spreadsheets
  ▪ LMS – Learning Management System
✓ Project Management App
  ▪ Planning
  ▪ Tracking
  ▪ Documenting
✓ QSA – Qualified Security Assessor
  ▪ Phone calls
  ▪ On-sight assessments
Questions

Carolann G Lazarus, CISA, CCEP
IT Audit Manager,
University at Buffalo, SUNY
716-829-6947
lazarus@buffalo.edu

Higher Education Compliance Conference - SCCE
Bonus 1 — (These slides are from a previous presentation that was focused more on using audit methodology to evaluate our compliance program)

**Five Audit Objectives**
1. Compliance Program
2. Monitoring/Oversight
3. Training
4. Policies, Procedures, Guidelines
5. Enforcement

**Bonus 1**

1. **Compliance Program**
   - Is there a program / plan in place?
   - Who’s assigned?
   - Was a risk assessment performed?
   - Have the requirements been identified?
Bonus 1

2. Monitoring/Oversight
   • Is appropriate management responsible?
   • Planned checks and reviews are performed?
   • Evidence is retained?
   • Results are communicated?
   • Program is updated as needed?

Bonus 1

3. Training
   • A training program is in place?
   • Covers targeted personnel?
   • Evidenced?
   • Updated?
**Bonus 1**

### 4. Policies, Procedures, Guidelines
- Is the appropriate owner identified?
- Are they approved and updated?
- How are they communicated?

### 5. Enforcement
- Requirements are promoted?
- Compliance is enforced?
**Bonus 2** — (The next slides are from the previous presentation and show some of the actual planning process documents for our PCI Compliance Initiative)

<table>
<thead>
<tr>
<th>PHASE 1 – PLANNING</th>
<th>-defined the Phases</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Actions/Deliverables</strong></td>
<td><strong>Tasks</strong></td>
</tr>
<tr>
<td><strong>Problem Statement</strong></td>
<td>Define and Approval</td>
</tr>
<tr>
<td><strong>Project Charter</strong></td>
<td>Determine</td>
</tr>
<tr>
<td></td>
<td>• Goals</td>
</tr>
<tr>
<td></td>
<td>• critical success factors</td>
</tr>
<tr>
<td></td>
<td>• Scope</td>
</tr>
<tr>
<td></td>
<td>• Constraints</td>
</tr>
<tr>
<td></td>
<td>• Risks</td>
</tr>
<tr>
<td></td>
<td>• Benefits</td>
</tr>
<tr>
<td><strong>Roles and Responsibilities</strong></td>
<td>Define</td>
</tr>
<tr>
<td></td>
<td>Project Team Members</td>
</tr>
<tr>
<td></td>
<td>Project Needs</td>
</tr>
<tr>
<td><strong>Discovery and Gap Analysis</strong></td>
<td>Inventory -</td>
</tr>
<tr>
<td></td>
<td>• Merchants/Departments</td>
</tr>
<tr>
<td></td>
<td>• Data Flow Diagram</td>
</tr>
<tr>
<td></td>
<td>• Business Process</td>
</tr>
<tr>
<td></td>
<td>• Network(s)</td>
</tr>
<tr>
<td></td>
<td>• Devices</td>
</tr>
<tr>
<td></td>
<td>• Data - what is stored, transmitted, etc.</td>
</tr>
<tr>
<td><strong>Data Warehousing</strong></td>
<td>Where physically</td>
</tr>
<tr>
<td></td>
<td>Responsibility</td>
</tr>
</tbody>
</table>

---

Note: The content above is a transcription of the text and table from the image. It may contain slight variations from the original due to the nature of transcribing visual text into a readable format.
### Bonus 2

#### Define the Phases

**PHASE 2 - Define**

<table>
<thead>
<tr>
<th>Actions/Deliverables</th>
<th>Tasks</th>
<th>Misc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies</td>
<td>Develop Approve Disseminate</td>
<td>Include: enforcement monitoring consequences</td>
</tr>
<tr>
<td>Standards/Procedures/Guidelines</td>
<td>Develop Approve Disseminate</td>
<td>- Business Processes - Software Purchases - Annual SAQ's - PCI Implementation Each Site PCI Data Security Standard Approved Solutions</td>
</tr>
</tbody>
</table>

**PHASE 3 - Monitor**

<table>
<thead>
<tr>
<th>Actions/Deliverables</th>
<th>Tasks</th>
<th>Misc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Committee(s)</td>
<td>Initiate PCI Steering Cmte</td>
<td></td>
</tr>
<tr>
<td>Training</td>
<td>Identify population</td>
<td></td>
</tr>
<tr>
<td>Monitor/Validate/Enforce</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Develop Merchant ID Tracking</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Incident Response (concurrent with phase 1)**

<table>
<thead>
<tr>
<th>Actions/Deliverables</th>
<th>Tasks</th>
<th>Misc.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident Response</td>
<td>Templates Draft process</td>
<td>leverage existing processes</td>
</tr>
</tbody>
</table>
Bonus 2

Meetings

✓ Frequency
✓ Documented Agendas
✓ Written Minutes
✓ Action Items Spreadsheet
✓ Decision List
✓ Parking Lot

PCI Compliance Initiative

Date: April 21, 2017
Time: 10:30
Location: S67 Hall
Attendees: Jane Doe, Janet Doe - Sponsors
          Carolann Lazarus and Han Doe - Project Leads
          John Doe, Jim Doe, Julie Doe, John Doe, Jeff Doe - Executive Team

Agenda:
1. Review - Previous Meeting Notes, Action Items, Decision List
2. Project Team meeting - reschedule
3. Gantt Timelines - Review - Overall and Phase 1
4. Rules and Responsibilities
5. Incident Response
6. Discovery - Begin inventory of merchants, network/system components and
devices. Also 3rd Party contracts
7. Other - New requests to accept credit cards
8. PCI Conference Sessions/Handouts

Attachments - Gantt Timelines
Meeting Documents - Agenda, Meeting Notes, Action Items, Decisions, Compliance Project
Phase, Role, Inventory List

Problem Statement: The current state of PCI awareness and compliance across UB’s business
processes needs improvement to raise the level of assurance that UB’s PCI compliant environment
effectively reduces the risk of reputational damage, monetary penalties, compromised cardholder
data and/or loss of ability to accept cards

Expectations for Meeting Participation
1. These discussions will require listening to each other with an open mind. Participants should be sensitive
   and understanding of the views of others and the tasks that are being discussed.
2. These discussions also require that all who are present contribute to the conversation. All opinions add
   value, and should be put forth and balanced against the opportunity to do so. Remember that we all have our
   own expectations and approaches, and that value within that diversity.
3. Each participant should take responsibility for maintaining the meeting’s agenda.
   The facilitator will begin by reviewing the agenda and encouraging discussion of issues.
   Participants should stay focused on the topics at hand.
4. Keep your comments brief and to the point (see “parking lot” for those issues that are important to discuss outside
   of a particular meeting). Do not let discussions go over the scheduled time.
5. Take ownership and responsibility for your engagement in the project. Participants, take notes that are
   important to you, and keep them and follow up on actions items that are assigned.
6. Meet the project group regularly as a team obligation. All in attendance should ensure that these expectations
   are being met.

Meetings should be brief and on-topic.
## Bonus 2

### Meetings - Action List

<table>
<thead>
<tr>
<th>Date Listed</th>
<th>#</th>
<th>Action Item</th>
<th>Phase</th>
<th>Responsibility</th>
<th>Due Date</th>
<th>Status</th>
<th>Completion Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/9/2017</td>
<td>2</td>
<td>UBBox setup and sharing</td>
<td>Administration</td>
<td>Doe</td>
<td>ASAP</td>
<td>Complete</td>
<td>3/14/2017</td>
<td>Discussed at 3/9/17 meeting. Doe/Eoe will develop a Santity show and update the project status.</td>
</tr>
<tr>
<td>3/9/2017</td>
<td>3</td>
<td>Share PCI listserv information</td>
<td>Administration</td>
<td>Doe</td>
<td>ASAP</td>
<td>Complete</td>
<td>3/16/2017</td>
<td>Discussed at 3/9/17 meeting. Doe/Eoe will develop a Santity show and update the project status.</td>
</tr>
<tr>
<td>3/9/2017</td>
<td>4</td>
<td>Schedule Executive Team meetings every two weeks</td>
<td>Administration</td>
<td>Doe/Johnson</td>
<td>ASAP/Ongoing</td>
<td>Complete</td>
<td>3/15/2017</td>
<td>Discussed at 3/9/17 meeting. Doe/Eoe will develop a Santity show and update the project status.</td>
</tr>
<tr>
<td>3/9/2017</td>
<td>5</td>
<td>Define project phases</td>
<td>Planning</td>
<td>Doe</td>
<td>ASAP</td>
<td>Complete</td>
<td>3/31/2017</td>
<td>Discussed at 3/9/17 meeting. Doe/Eoe will develop a Santity show and update the project status.</td>
</tr>
<tr>
<td>3/9/2017</td>
<td>6</td>
<td>Begin to define roles &amp; responsibilities</td>
<td>Planning</td>
<td>Doe</td>
<td>ASAP</td>
<td>Complete</td>
<td>3/31/2017</td>
<td>Discussed at 3/9/17 meeting. Doe/Eoe will develop a Santity show and update the project status.</td>
</tr>
<tr>
<td>3/9/2017</td>
<td>7</td>
<td>Gantt Chart - Phase 1</td>
<td>Planning</td>
<td>Doe and J. Doe</td>
<td>ASAP</td>
<td>Complete</td>
<td>4/21/2017</td>
<td>Discussed at 3/9/17 meeting. Doe/Eoe will develop a Santity show and update the project status.</td>
</tr>
</tbody>
</table>

### Meetings - Decision List

<table>
<thead>
<tr>
<th>#</th>
<th>Decisions</th>
<th>Date</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Asst. VP Financial Management, will be added to the Executive Team</td>
<td>3/9/2017</td>
<td>Sponsors</td>
</tr>
<tr>
<td>2</td>
<td>Incident Response was given a high priority and turned into a separate action item, and not part of the defined phases. This should be worked on concurrently with the rest of the project. The existing incident response process will be leveraged.</td>
<td>3/9/2017</td>
<td>Sponsors and Exec.</td>
</tr>
<tr>
<td>3</td>
<td>Executive Team Members are expected to be working members</td>
<td>3/21/2017</td>
<td>Sponsors</td>
</tr>
<tr>
<td>4</td>
<td>Gantt Timeline for the overall project and Phase 1 was presented to the Sponsors and Exec Team and approved as written. (this is a living document and may change as needed)</td>
<td>4/21/2017</td>
<td>Sponsors and Exec team</td>
</tr>
<tr>
<td>5</td>
<td>Device Inventory will only include physical terminals</td>
<td>5/12/2017</td>
<td>Sponsors and Exec team</td>
</tr>
<tr>
<td>6</td>
<td>Storage of Initiatives documents will be on Ubbox. Ownership of the individual documents will be decided as needed.</td>
<td>6/9/2017</td>
<td>Sponsors and Exec team</td>
</tr>
<tr>
<td>7</td>
<td>Any non-UB entity using UB facilities and/or infrastructure who processes credit card transactions will be required to attest to PCI compliance.</td>
<td>6/9/2017</td>
<td>Sponsors and Exec team</td>
</tr>
<tr>
<td>8</td>
<td>We will continue meetings through January</td>
<td>9/20/2017</td>
<td>Exec Team</td>
</tr>
</tbody>
</table>
**Bonus 2**

**How do we Maintain Success?**

- PCI Policy
- Official Committee – responsibility and accountability documented in the policy
- Oversight of PCI – annual reviews of compliance.
- Periodically identify units accepting credit cards
- Refresh annual training
- Awareness activities

**THE END**