2015 PCI DSS Meeting

OSU Business Affairs
Projects, Improvement, and Technology (PIT)
Robin Whitlock
Today’s Presentation

- What do you need to do?
- What is PCI DSS?
- Why PCI DSS?
- Who Needs to Comply with PCI DSS?
- What does PCI DSS Compliance Mean?
- Penalties for Non-Compliance
- Compliance Life Cycle
- Goals & Requirements
- New PCI DSS v3.1
- Cardholder Data/Storage
- What do you have to do?
- SAQs
- Resources
- Questions
Your to do list by December 11:

1. Verify credit card merchant information on the PCI DSS Status Report and provide updates to Business Affairs
2. Merchant managers complete and sign the Cover Page & SAQ
   - Annual PCI DSS Assessment must be completed for all Merchants
3. Obtain 3rd Party PCI DSS Certificate of Compliance (if applicable).
   - This is required if your merchant uses an OST approved 3rd party vendor other than TouchNet.
4. Business Center Manager or FAM must review and sign
5. Send to Robin Whitlock
What is PCI DSS?

- Payment Card Industry Data Security Standards
  - Continuously evolving security best practices for credit card merchants and cardholder data
  - Common set of industry tools and measurements to help ensure the safe handling of sensitive information
  - Provides an actionable framework for developing a robust account data security process – including preventing, detecting and reacting to security incidents (https://www.pcisecuritystandards.org/merchants/index.php)

- Administered by the PCI Security Standards Council, which was founded by the major credit card companies (VISA, MC, Discover…)
Why PCI DSS?

- 154 breaches of sensitive information to date in 2015 (affecting >153 million records)¹

- Notable retail breaches since November 2013²

  - Target
  - Albertsons
  - PF Changs
  - Supervalu
  - Home Depot
  - Michaels
  - UPS Stores
  - Dairy Queen
  - Staples
  - Neiman Marcus
  - Aaron Brothers
  - CVS
  - Kmart
  - eBay
  - Goodwill

¹ Privacy Rights Clearinghouse: [https://www.privacyrights.org](https://www.privacyrights.org), 10/26/15
Who Needs to Comply with PCI DSS?

- Applies to all entities that store, process or transmit cardholder data (merchants, payment card issuing banks, processors, developers…)
  - That means you!

- Compliance is mandatory
  (eCommerce Policy, Oregon State Treasury, PCI DSS).

- Merchant Managers are responsible for merchant compliance:
  - Attestation
    “I understand that each merchant has fiscal and data security responsibility for proper use of the Merchant ID. I further understand that failure by the merchant to abide by PCI standards could result in fines to the University and/or loss of Merchant ID. To the best of my knowledge, this cover sheet and the information in the attached PCI SAQ (if applicable) accurately represents the operations, procedures, and practices of the Merchant ID's listed above.”
  (Payment Card Industry Data Security Standards Annual Assessment Cover Page).
What does PCI DSS Compliance Mean?

- In security terms, it means that your business adheres to the PCI DSS requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

- In operational terms, it means that you are playing your role to make sure your customers' payment card data is being kept safe throughout every transaction, and that they – and you – can have confidence that they're protected against the pain and cost of data breaches.

(https://www.pcisecuritystandards.org/merchants/index.php)
Penalties for Non-Compliance

- Fines of $50-$90 per cardholder data compromised
  - Non-compliant merchants are penalized by acquiring banks
- Revocation of merchant credit card acceptance
- Loss of customers
- Loss of reputation
- Possible civil litigation from breached customers

Compliance Life Cycle

Pre-Assessment / Gap Analysis

Implement / Remediate

PCI:DSS Validation

Ongoing Compliance Monitoring

On-going process, not a one-time event
## PCI DSS Goals & Requirements

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

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>A-EP</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>B</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>B-IP</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>C</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>D</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

- SAQs A-EP and B-IP are new 3.0/3.1 SAQs
- Requirement 10 is new to SAQ C with 3.0
What’s New: PCI DSS v3.1

- PCI DSS was updated from v2.0 to v3.1
- Focus is on incorporating PCI DSS requirements into day-to-day activities, not just a once-a-year assessment.
- More requirements across the board
- Changes to SAQs
  - Incorporation of new/changed requirements
  - Expected testing added
  - Format updates
  - New SAQs: A-EP, B-IP
  - Updated eligibility criteria for existing SAQs
What is Cardholder Data?

- Primary Account Number (PAN)
- Expiration Date
- Cardholder Name
- Chip/Magnetic Strip Data
- CAV2/CVC2/CVV2
1. **BEST PRACTICE:** DO NOT STORE CARDHOLDER DATA.
2. **NEVER** store using electronic media, for example database or spreadsheet.
3. These data elements must be protected if stored in conjunction with the PAN.
4. Sensitive authentication data must not be stored after authorization (even if encrypted).
5. Magnetic stripe or chip.

### PCI Data Storage

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Storage Permitted</th>
<th>Protection Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cardholder Data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary Account Number (PAN)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cardholder Name[3]</td>
<td>Yes</td>
<td>Yes[3]</td>
</tr>
<tr>
<td>Expiration Date[3]</td>
<td>Yes</td>
<td>Yes[3]</td>
</tr>
<tr>
<td>Sensitive Authentication Data[4]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Magnetic Strip Data[5]</td>
<td>No</td>
<td>N/A</td>
</tr>
<tr>
<td>CAV2/CVC2/CVV2</td>
<td>No</td>
<td>N/A</td>
</tr>
</tbody>
</table>

---

[1] - Magnetic stripe or chip.
[2] - Database or spreadsheet.
[3] - These data elements must be protected if stored in conjunction with the PAN.
[4] - Sensitive authentication data must not be stored after authorization (even if encrypted).
What do we have to do?

<table>
<thead>
<tr>
<th>Level/Tier</th>
<th>Merchant Criteria</th>
<th>Validation Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Merchants processing over 6 million Visa transactions annually (all channels)</td>
<td>• Annual Report on Compliance by Qualified Security Assessor (“QSA”)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Quarterly network scan by Approved Scan Vendor (“ASV”)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Attestation of Compliance Form</td>
</tr>
<tr>
<td>2</td>
<td>Merchants processing 1 million to 6 million Visa transactions annually (all channels)</td>
<td>• Annual Self-Assessment Questionnaire</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Quarterly network scan by ASV</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Attestation of Compliance Form</td>
</tr>
<tr>
<td>3</td>
<td>Merchants processing 20,000 to 1 million Visa e-commerce transactions annually</td>
<td>• Annual SAQ</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Quarterly network scan by ASV</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Attestation of Compliance Form</td>
</tr>
<tr>
<td>4</td>
<td>Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually</td>
<td>• Annual SAQ</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Quarterly network scan by ASV if applicable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Requirements set by acquirer</td>
</tr>
</tbody>
</table>
Annual PCI DSS Assessment Documents

Documents due by December 11, 2015:

1. OSU Cover Page
2. Self Assessment Questionnaire (SAQ A-D Appropriate to merchant)
3. 3rd Party PCI DSS Certificate of Compliance (if applicable)
Self Assessment Questionnaire (SAQ)

- Completed by the merchant manager
- Subset of full requirements
- Broken down by Goals & Requirements
- Made up of Yes / No / Not Applicable responses
  - NA or “Compensating Control”- must be explained
  - No- Must have Remediation Date and Actions
- Attestation Section
  - Fill out the Merchant Version
  - Do not complete the Service Provider Version
- Details will be covered in break-out sessions
### Which SAQ?

See PCI DSS Status Report for your merchant

<table>
<thead>
<tr>
<th>SAQ</th>
<th># Questions</th>
<th>ASV Scan?</th>
<th>Pen Test?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A</strong></td>
<td>14</td>
<td>No</td>
<td>No</td>
<td>Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. Not applicable to face-to-face merchants.</td>
</tr>
<tr>
<td><strong>A-EP</strong></td>
<td>139</td>
<td>Yes</td>
<td>Yes</td>
<td>E-commerce merchants who outsource all payment processing and have a website that does not directly receive cardholder data but can impact security of the payment transaction. Not applicable to face-to-face merchants.</td>
</tr>
<tr>
<td><strong>B</strong></td>
<td>41</td>
<td>No</td>
<td>No</td>
<td>Imprint-only merchants with no electronic cardholder data storage, or standalone, dial-out terminal merchants with no electronic cardholder data storage. Terminals not IP-connected.</td>
</tr>
<tr>
<td><strong>B-IP</strong></td>
<td>83</td>
<td>Yes</td>
<td>No</td>
<td>Merchants with standalone, IP-connected point of sale terminals.</td>
</tr>
<tr>
<td><strong>C</strong></td>
<td>139</td>
<td>Yes</td>
<td>Yes</td>
<td>Merchants with payment application systems connected to the Internet, no electronic cardholder data storage.</td>
</tr>
<tr>
<td><strong>D</strong></td>
<td>326</td>
<td>Yes</td>
<td>Yes</td>
<td>All other merchants not included in descriptions for SAQ types A through C above, and all service providers defined by a payment brand as eligible to complete an SAQ.</td>
</tr>
</tbody>
</table>

Multiple Merchant Consolidation

Multiple merchants can be combined into a single submittal if:

1. The merchant IDs (MIDs) are of the same type (i.e. all POS, Web...)
2. All merchants are managed by same merchant manager
3. The same policies and procedures apply to all merchants
4. Strictest SAQ will apply (the one with the most questions)
5. List all merchants on cover page
Misconceptions

- Self assessment means you’re compliant
- Compliance means you won’t suffer a breach
- Outsourcing takes away your need for compliance
- PCI:DSS is just about IT
- A single product can make you compliant
- Compliance can be automated
SAQ Review Sessions

- Line-by-line review of PCI DSS 3.1 SAQs
  - OSU-specific information
  - Changes from version 2.0 to 3.1

- Schedule:
  - SAQ A: 11/4/15 10:00AM
  - SAQ B: 11/4/15 11:00AM
  - SAQ B-IP: 11/9/15 9:00AM
  - SAQ C: 11/9/15 11:00AM
Your to do list by December 11:

1. Verify credit card merchant information on the PCI DSS Status Report and provide updates to Business Affairs
2. Merchant managers complete and sign the Cover Page & SAQ
   - Annual PCI DSS Assessment must be completed for all Merchants
3. Obtain 3rd Party PCI DSS Certificate of Compliance (if applicable)
   - This is required if your merchant uses an OST approved 3rd party vendor other than TouchNet.
4. Business Center Manager or FAM must review and sign.
5. Send to Robin Whitlock
   - Electronic submission is preferred.
Resources

- Copies of your last assessment can be emailed to you on request
  - Status Report by Business Center
  - Forms: Cover Page and SAQ
  - OSU-specific SAQ instructions
  - Other supporting documents
Thank You

Business Affairs Contact

- Robin Whitlock
  - Robin.Whitlock@OregonState.edu, 541-737-0622