Bursar’s Round Table
PCI Compliance

Spring FOCUS 2009
Stonewall Jackson Hotel
Staunton Va.

Session Contacts

Ken Sinarski - Associate Comptroller (UVA) – (kes7h@virginia.edu)

J. Devin Herod – Training & Project Specialist (UVA) – (jdh5w@virginia.edu)

Linda Combs – Director of University Business Office (JMU) – (combslc@jmu.edu)

B. C. Worsley – Banking Coordinator (UVA) – (bsw5w@virginia.edu)

The 2-Second Brief

1) You are always one click away from non-compliance. PCI is an on-going effort, not an annual certification. Compliance will become a larger & more costly process.

2) Limit your scope wherever possible – Remove cardholder data wherever possible!

3) Outsourcing is not a panacea – if one of your merchants enters data at their station into a hosted website, that station and all it is connected to is now in scope – welcome to SAQ C or D! How do you know when a third party is compliant?

4) Most acquirers are deciding that an institution will file one composite SAQ for their institution, regardless of the number of merchants you have.

5) ANYTHING that stores transmits, or processes cardholder data is in scope – you do not have to be a merchant!

6) With requirement 12.8 in version 1.2, operational & I.T. policies are greater emphasized and the lack of adequate policies results in audit findings.

7) Prepare for PA-DSS and Wireless WEP encryption deadlines (2010). Check your systems to make sure they are not storing or archiving cardholder data!

8) Payment Cards expected us to be in PCI compliance in 2006 – Prioritize your risks!
A Quick PCI DSS Recap/Reference

<table>
<thead>
<tr>
<th>Control Objectives</th>
<th>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</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</td>
</tr>
</tbody>
</table>

The Payment Card Industry Data Security Standards

Self-Assessment Questionnaire for PCI Compliance

The self-assessment questionnaire is a tool used by merchants to self-validate their PCI compliance. There are four versions of the self-assessment questionnaire. Which one is right for you depends on how you process payment cards.

<table>
<thead>
<tr>
<th>Self-Assessment Questionnaire Type</th>
<th>Description</th>
<th># of Questions to be Answered</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Card not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. This would never apply to face-to-face merchants.</td>
<td>11</td>
</tr>
<tr>
<td>B</td>
<td>Imprint-only merchants with no electronic cardholder data storage, and stand-alone terminal merchants, no electronic cardholder data storage</td>
<td>24</td>
</tr>
<tr>
<td>C</td>
<td>Merchants with point-of-sale systems connected to the Internet, no electronic cardholder data storage</td>
<td>32</td>
</tr>
<tr>
<td>D</td>
<td>All other merchants</td>
<td>226 (Full DSS)</td>
</tr>
</tbody>
</table>

Merchants not storing cardholder data electronically are eligible for Self-Assessment Questionnaire Types A, B, and C, which are shorter and easier to complete than Type D. So your choice is either don’t keep cardholder data or expect to spend a lot of time answering questions.
Is it Card Holder Data?

<table>
<thead>
<tr>
<th>Data Element</th>
<th>Storage Permitted</th>
<th>Protection Required</th>
<th>PCI DSS Req. 3.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cardholder Data</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Primary Account Number (PAN)</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Cardholder Name*</td>
<td>YES</td>
<td>YES*</td>
<td>NO</td>
</tr>
<tr>
<td>Service Code*</td>
<td>YES</td>
<td>YES*</td>
<td>NO</td>
</tr>
<tr>
<td>Expiration Date*</td>
<td>YES</td>
<td>YES*</td>
<td>NO</td>
</tr>
<tr>
<td>Sensitive Authentication Data**</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Full Magnetic Stripe</td>
<td>NO</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>CVC2/CVV/CID</td>
<td>NO</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>PIN / PIN Block</td>
<td>NO</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Source: PCI SSC

Truncated PANs are defined as a maximum of the first 6 and the last 4 digits.

**MASKED PANS are still in scope!!

<table>
<thead>
<tr>
<th>Rating Average</th>
<th>Response Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.92</td>
<td>12</td>
</tr>
<tr>
<td>3.33</td>
<td>12</td>
</tr>
<tr>
<td>3.17</td>
<td>12</td>
</tr>
<tr>
<td>2.08</td>
<td>12</td>
</tr>
<tr>
<td>3.36</td>
<td>12</td>
</tr>
<tr>
<td>2.42</td>
<td>12</td>
</tr>
<tr>
<td>2.67</td>
<td>12</td>
</tr>
<tr>
<td>2.98</td>
<td>12</td>
</tr>
<tr>
<td>3.25</td>
<td>12</td>
</tr>
<tr>
<td>2.07</td>
<td>12</td>
</tr>
<tr>
<td>3.73</td>
<td>11</td>
</tr>
<tr>
<td>3.08</td>
<td>12</td>
</tr>
<tr>
<td>3.55</td>
<td>11</td>
</tr>
<tr>
<td>3.00</td>
<td>11</td>
</tr>
</tbody>
</table>

Spring 2009 FOCUS PCI Survey Results
Keeping a Weather Eye Out – Deadlines & Changes

First, keep in mind that the Payment Cards have expected us all to be in compliance with PCI-DSS since its issuance in 2006!

“Last year Visa gave its acquirers until July 31, 2007 to submit plans to get their Level 4 merchants compliant.”
(http://www.treasuryinstitute.org/blog/index.php?itemid=177)

There are a number of deadlines and changes coming up in the next year or two. Here is a high level alert to some of what is coming:

**PA-DSS- (Payment Application Data Security Standard)** - On April 15, 2008, the Payment Card Industry Security Standards Council (PCI SSC) launched the PA-DSS program (Payment Application Data Security Standard). This program was formerly under the supervision of Visa Inc. and known as the Payment Application Best Practices (PABP).  [https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml)

- **January 2008** – Acquirers could no longer sign on new merchants using a payment application with a known vulnerability
- **October 1, 2008** – Acquirers were restricted to only adopting level 3 & 4 merchants that had proven PCI compliance and PA-DSS compliant (and verified) applications.
- **JULY 2010** – ALL merchants will be required to certify that applications are PA-DSS compliant! This means that if you are considering a new payment application (ticket sales, development systems, parking lots, etc.), you should insure they are on the list (or verify that they are compliant and waiting to be added) BEFORE you sign the contract, or you may be replacing it again in a year.

**Wireless Payments** - The Payment Card Industry Data Security Standards have tightened rules for processing credit cards over wireless LANs. As of March 31st 2009, the use of WEP encryption was prohibited from new implementations in systems transmitting or connected to card holder data. WEP encryption has been broken by on-line criminals since the mid-2000’s and was the primary method for the TJ Maxx data loss in January 2007. **By JUNE 30 2010**, all wireless systems must have been revised to stronger wireless encoding (WEP-free). WPA & WPA2 are currently front-running codes.

**PCI DSS Revisions** - now have 2-year life cycle. “The lifecycle ensures a gradual, phased use of new versions of the standard without invalidating current implementations of PCI DSS or putting any organization out of compliance the moment changes are published. The Council is committed to following this process to ensure transparency and continuity of compliance.”
[https://www.pcisecuritystandards.org/pdfs/OS_PCI_Lifecycle.pdf](https://www.pcisecuritystandards.org/pdfs/OS_PCI_Lifecycle.pdf)
Deadlines & Changes (cont.)

“The Council will publish similar lifecycles for the Payment Application Data Security Standard (PA-DSS) and the PIN Entry Device (PED) Security Requirements.”

New Standards Coming for:

- **Unattended Payment Terminals** – These standards will address new requirements for PCI-related issues dealing with kiosks, gas pumps, and HSMs (Hardware/host security modules (non-cardholder interfaces or embedded devices)).

- **Point of Interaction (PCI-POI) Standards**-

- **PED-DSS (Pin Entry Devices) becoming Pin Transaction Systems (PTS-DSS)** – with broader scope for all parts of the PIN entry systems.

**Translation:**

Compliance initiatives will continue to increase in the near future, and there will be an increase in the costs associated with maintaining compliance.
Topics in Training

Formal training in PCI by THE PCI Standards Council

PCI Standards Training Program 2009

A comprehensive PCI Standards Training program offered directly by PCI SSC.

2009 Training Schedule
How to Register
Fees
General Information
Contact Us

This is a 2-day training course based directly on the PCI SSC Qualified Security Assessor (QSA) training program. Attendees will learn what the QSAs learn so they can better prepare for an on-site PCI DSS assessment or perform the assessment internally. This is not a certification course.

The course will cover: PCI Program, Scoping a PCI DSS Assessment, PCI DSS v1.2 Requirements and Compensating Controls

In addition to the QSA training materials, the Standards training course will also cover how to develop an internal PCI DSS compliance program to sustain PCI compliance after the on-site assessment is complete. The PCI DSS Compliance module will discuss how to develop an internal compliance program, sustain PCI DSS compliance and discuss security best practices outside of PCI DSS to improve the merchants overall security program.

2009 PCI SSC Standards Training Schedule

<table>
<thead>
<tr>
<th>Session</th>
<th>Date</th>
<th>Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>28, 29 May</td>
<td>08:00-18:00</td>
<td>Sydney Harbour Marriott Hotel, Sydney, Australia</td>
</tr>
<tr>
<td>2</td>
<td>17, 18 June</td>
<td>08:00-18:00</td>
<td>Westin Peachtree Plaza Hotel, Atlanta, GA, USA</td>
</tr>
<tr>
<td>3</td>
<td>1, 2, 3 July</td>
<td>08:30-17:30</td>
<td>08:30-12:30 Day 1 &amp; 2 Day 3 Hilton Heathrow London Airport Hotel</td>
</tr>
</tbody>
</table>

Additional 2009 Standards Training

The PCI SSC will be hosting additional Standards Training throughout 2009. The following are tentative locations and dates. Please note these are not officially scheduled. Please check back periodically for more information and how to register for training:

Tentative Locations and Dates:

- Toronto, Canada - July 22-24, 2009
- Prague, Czech Republic - October 22-23, 2009 (Prior to the European PCI SSC Community Meeting)
- San Francisco, US - December 8-10, 2009

https://www.pcisecuritystandards.org/education/training.shtml

Just the FAQs – PCI Council is maintaining a searchable FAQ site with a wealth of information:  
https://www.pcisecuritystandards.org/FAQ

Click on the Icon in the menu bar at the site
**External Training in PCI:**

- **Payment Card Training (MasterCard):**

- **Security Partner Training (e.g.: Trustwave)**

- **Other?**
Internal (Institutional) Training in PCI:

- **University of Virginia model (work in progress)**
  - Face-to-face merchant communications: Sitting down for the SAQs
  - Internal Collab PCI Site: Allows for coordination of documents, notices, and resources for University Merchants
  - Formal Training: PCI as a topic in a Business Professional program Cash Handling Course.

- **Outreach to the Interested**: Use of brochure to provide both warnings (Golden Rules) and information on expectations/guidelines.

- **Future Goals**:
  - Develop annual merchant training
  - Develop specific first-time training (on-line) for employees handling cardholder data
  - Providing specific guidance/recommendations for personnel looking to acquire a third-party payment card partner
  - Preparing a PCI awareness seminar for affiliated organizations (Foundations, contracted vendors, etc.)
  - Developing a training session for student organization officers related to cash handling & PCI best practices.
  - Increasing central level professional development with regard to PCI

**Peers to Examine:**
- Indiana University - [http://www.indiana.edu/~iutrea/forms/pcidsstrainingreg.html](http://www.indiana.edu/~iutrea/forms/pcidsstrainingreg.html)
- Others?
- Care to share your training? Visit the **FOCUS PCI Collab**! [https://collab.itc.virginia.edu/](https://collab.itc.virginia.edu/) - not a member yet? Contact Devin Herod (jdh5w@virginia.edu).
Some Lessons from the 2009 Treasury Institute’s PCI Workshop

- SAQ A & B qualified merchants do not require scanning!

- If you have a hosted website, but you allow someone to enter cardholder data for a customer through your terminals, your terminal has just placed you out of SAQ A and into SAQ C – it is being used as an application.

- If your systems store purchase card PANs in any form, those systems are in scope for PCI!

- Macs are not free from anti-virus requirements. The rule for systems (Linux, etc.) should be: If there is a risk and reasonable anti-virus software is available, it SHOULD be used.

- Make sure that data transmissions are NOT on VOIP (voice over internet) – these are web-based applications and more dangerous than analog phone lines.

- **Walt Conway’s Suggestions on Reducing PAN data on campus:**
  - Recurring payments – acquirer has alternatives
  - Chargebacks, refunds – let acquirer store PAN data
  - Legal requirements – these apply to banks, not you
  - Paper receipts – reprogram terminals or upgrade to truncate both copies
  - POS software stores PANs – reconfigure or replace

- **Who can you trust?**
  - How can you assure compliance from a Payment card partner?
    - Contractual Language – check the Collab site for UVA contract language and JMU merchant agreements
    - Require a copy of their signed “Attestation of Compliance”
  - How do you know if your application or wireless is safe to use? - Lists now hosted on the PCI site

    Get the List of Validated Payment Applications
    Get the List of PIN Entry Devices

- ASV Program Guide to be released next month – not only a guide for the Approved Scanning Vendors, but for merchants to use in preparation for dealing with an ASV ([https://www.pcisecuritystandards.org/](https://www.pcisecuritystandards.org/))
• How can you report issues with QSV or ASV companies?

Submit QSA Feedback Form
Submit ASV Feedback Form

• Current top PCI Violations:

Presentation at 2009 Treasury Institute PCI/DSS Workshop, Troy leach, PCI DSS Council Member.

• There is a solidification of ASV and QSV training that will limit the ability for many institutions to ‘employ’ their own internal resources in these areas

• New businesses are beginning to form that will deal specifically with Higher Education and compliance issues like PCI & Red Flags. Example: Campusguard.

• If you choose to engage a wireless system, look to see if they can use a licensed spectrum (like AT&T’s or others). The common unlicensed spectrum is shared by numerous other applications (bluetooths, cordless phones, microwave ovens, etc.) making them more vulnerable and prone to lower performance (interference). Licensed spectrum makes for better recourses if interfered with (already laws to defend in place).
Useful PCI DSS Resources

PCI Security Standards Council Website:

The site is managed by the PCI Security Standards Council founded by the five major credit card companies that lead the PCI DSS effort. You can find current copies of the PCI Standards, the SAQs, FAQs, Recent news releases and more.

https://www.pcisecuritystandards.org/

The Treasury Institute and NACUBO have collaborated on a PCI DSS News and Information Blog. In addition to a series of PCI primers, there are regular postings related specifically to Higher Ed. related topics:

- Treasury Institute Blog:
  - http://www.treasuryinstitute.org/blog/

The following are Walt Conaway’s picks for additional resources that you may find useful (http://www.treasuryinstitute.org/blog).

Educause is Higher Education’s dedicated source of IT and security information.
http://www.educause.edu/pcidss

This is the PCI Compliance Demystified blog. It is widely read by security experts and is a respected PCI blog.
http://www.pcianswers.com/

The Society of Payment Security Professional’s objective is to provide individuals and organizations involved in payment security with an online community to share information and access education and certification opportunities. Society members come from a variety of businesses including card brands, merchants, acquirers, issuers, ISOs, and more. Although their organizations may vary, they all share one purpose: To protect consumer data using the most current, viable technologies and processes.
http://www.paymentsecuritypros.com/

A good security and PCI blog with a bit of an international flavor: the editor is British working in Spain.
http://www.robnewby.blogspot.com/

As the title proclaims, this is “A Weblog for Risk Geeks.”
http://www.riskanalysis.riskmanagementinsight.com/

The Security Catalyst is a security site “helping to change the way people think.” The discussions are thoughtful and the participants are on a mission.
http://www.securitycatalyst.com/
Payment Card Industry (PCI) Data Security Standard Glossary, Abbreviations and Acronyms

We recommend the Payment Card Industry (PCI) Data Security Standard Glossary, Abbreviations and Acronyms

https://www.pcisecuritystandards.org/pdfs/pci_dss_glossary.pdf

Attached is the web address for an on-line video that we found particularly useful regarding a data loss at the N.Y.S. Dormitory Authority. It was a good example of a state agency’s experience with data loss. This will also be posted on the collab site.

http://downloads.feedroom.com/podcasts/t_assets/20081126/DataBreachFRr2_MP4_32VX.mp4?site=erepublic&cid=698d0d79d91748ef440129c0c45f1b2e98dfbaff&sid=e5c882ba99db9a619ddd7355b78ff50aae4931f2&pid=76288753ff922f2890909334cc35a6b784f92044

This document is to serve as a supplement for discussions about PCI and is provided by the University of Virginia’s Financial Administration Strategic Planning & Analysis (SP&A) group.

Courtesy SP&A