LEADING THE WAY TO PCI COMPLIANCE:
IT'S ALL ABOUT PLANNING AND COLLABORATION

Tammy Clark, Chief Information Security Officer
Georgia State University
Kelley Bogart, Senior Information Security Analyst
University of Arizona
**Some Stops along the Way...**

- Why (Me) PCI?!
- Do I Have to Do This?!
- Can it be Quick and Painless??
- How Do I Get Started?
- University of Arizona’s Approach to PCI Compliance (It’s Working!)
- Lessons Learned
- New Developments (i.e. More Stuff to Do!)
- Very Helpful Resources!
- Questions?
The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that **ALL** organizations that *process, store or transmit* credit card information ensure that cardholder data is protected.
Who Does PCI DSS Apply To?

- PCI applies to ALL organizations or merchants, regardless of size or number of transactions, that accept, transmit or store any cardholder data.
- Using a third-party company does not exclude you from PCI compliance. It may cut down on your risk exposure and consequently reduce the effort to validate compliance. However, it does not mean you can ignore PCI.
THE IMPORTANCE OF ‘MERCHANT LEVELS’

- Merchants fall under four categories of PCI compliance, depending on the number of transactions they process each year.
- Each payment card brand (Visa, MasterCard, etc.) has their own requirements and definitions of PCI compliance levels.

<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) or Global merchants identified as Level 1 by any Visa region ²</td>
<td>Annual Report on Compliance (“ROC”) by Qualified Security Assessor (“QSA”) or internal auditor if signed by officer of the company. Quarterly network scan by Approved Scan Vendor (“ASV”). 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 (“SAQ”). Quarterly network scan by ASV. 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. Quarterly network scan by ASV. 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 recommended. Quarterly network scan by ASV if applicable. Compliance validation requirements set by acquirer.</td>
</tr>
</tbody>
</table>

¹ - Compromised entities may be escalated at regional discretion

² – Merchant meeting Level 1 criteria in any Visa country/region that operates in more than one country/region is considered a global Level 1 merchant. Exception may apply to global merchants if no common infrastructure and if Visa data is not aggregated across borders; in such cases merchant validates according to regional levels.
The payment brands may, at their discretion, fine an acquiring bank $5,000 to $100,000 per month for PCI compliance violations, normally the result of a credit card data breach. The banks will most likely pass this fine on downstream till it eventually hits you (the) merchant.

In the event of a cardholder data breach, your organization will be designated a Level One merchant and have to pay for multiple assessments and compliance audits from then on....

Add to that the costs of providing credit protection to ‘victims’ of ID theft, reputational damages, etc...
PCI Standards

‘Slurped’ from the PCI Security Council Standards Council Website:

PCI SSC – Independent Industry Standards Body providing oversight of the development and management of Payment Card Industry Security Standards on a Global Basis

- **PCI DSS – Data Security Standards**
  Entities that store, process and/or transmit cardholder data

- **PCI PTS – PIN Transaction Security**
  Manufacturers who specify and implement device characteristics and management of personal identification number (PIN) entry terminals used for payment card financial transactions

- **PCI PA-DSS – Payment Application Data Security Standards**
  Software developers and integrators of payment applications that store, process or transmit cardholder data as part of the authorization or settlement when these applications are sold, distributed, or licensed to third parties.
Each card brand develops and maintains its own PCI DSS compliance programs and handle compliance tracking, enforcement, definition of merchants, service provider levels, penalties or fees assigned.

--American Express: www.americanexpress.com/Datasecurity
--Discover Financial Services: www.discovernetwork.com/fraudsecurity/disc.html
--MasterCard Worldwide: www.mastercard.com/sdp
--Visa Inc.: www.visa.com/Cisp
**Cardholder Data**

- Information printed on the physical credit card
  - PAN – Primary Account Number
  - Cardholder Name
  - Service Code, Expiration Date
- Sensitive Authentication Data:
  - Mag strip, track data
  - Track data on a chip
  - CAV2/CVC2/CVV2/CID, Pin/Pin Block

Where is the Card Identification Data (CID) and the Card Verification Value (CVV)?

**CVV**
Encoded into the magnetic stripe.
*Also Called:*
- Visa = CVV1
- MC = CVV1
- AmEx = CID

**CID**
The three digit number following the account number in the signature panel.
*Also Called:*
- Visa = CVV2, 3-digits, back of card
- MC = CVC2, 3-digits, back of card
- AmEx = Manual CID, 4-digits, front of card
PCI DSS Goals/Requirements

Find out more at:  https://www.pcisecuritystandards.org/security_standards/index.php
CONDUCTING PCI COMPLIANCE REVIEWS

1. Find all credit card merchant accounts
2. Find out from the Acquirer what level your transaction counts, and merchant level(s)
3. Obtain information on merchants’ credit card processing methods, service providers used
4. Find out where card holder data is processed, transmitted and stored—paper and electronic form
5. Scope the PCI review based on the above
6. Evaluate Cardholder Data Environments
7. Evaluate Service Providers
8. Ensure PCI Reporting of Compliance or Non Compliance
9. Assist Non compliant merchants adhere to PCI and University requirements, policies and standards
“Clean house” and get rid of data you don’t need:

- Find CHD (Card Holder Data) and Sensitive Authentication data
  - Protecting the above is the focus of the PCI DSS 2.0 requirements
  - The major goal at many universities is to reduce the scope by eliminating data storage and transmission...
STEP TWO—HIGH LEVEL APPROACH TO PCI COMPLIANCE

If You Need The Data (store, process, transmit) Secure It!

- **Ensure Data Protection Across Your Networks and Endpoints**
  - C.I.A.--This is an objective of an effective information security program and not specific to PCI, but is also a part of the DSS requirements

- **Use PCI Certified Payment Applications**

- **Deploy Access Controls**

- **Encrypt stored card holder data**
STEP THREE—HIGH LEVEL APPROACH TO PCI COMPLIANCE

**LEAD, PLAN and COLLABORATE**

- Get ‘Executive Level’ Support
- Form Cross-Campus Teams/Alliances between Finance, IT, and Information Security to develop PCI policies, procedures and training for campus merchants
- Agree on preferred credit card processing methods
- Oversee all of your service providers—ensure their contracts have PCI and breach notification language
- Assist merchants with compliance
THE UNIVERSITY OF ARIZONA’S APPROACH TO PCI COMPLIANCE
ABOUT THE UNIVERSITY OF ARIZONA

- 39,000 students
- >$217 million annual sales
- >2.1 Million annual transactions
- Level II merchant
- Accept MC/Visa, AMEX, Discover
- 228 merchants

- 72 Merchant Groups
- No SAQ D’s
- Decentralized IT
- 18 Colleges
- 329 Academic Programs
- Student Services- Student Union, Bookstore, Parking and Transportation Services, Athletics, UA Presents, Residence Halls, Campus Health
IF YOU BUILD IT THEY WILL COME....... 

- Bottom up Building  
  - Building brick by brick  
- Team Approach  
  - We are all in this together!  
- Support  
  - We are right there beside you.  
- Education  
  - Mandatory merchant meetings  
  - Site visits - Cussing, discussing and discovery
COLLABORATION – IT’S A TEAM EFFORT

- Compliance Officer – Bursar office
- Internal Audit
- Information Security Office
- UA Security Operations
- Campus Merchants
  - Business manager
  - IT representative
- Qualified Security Assessor – Security Metrics
Responsibility and Accountability

- Campus Policy and Merchant Agreement
  - Business Manager ownership (merchant responsible person) is key to departments taking compliance seriously.
- Documentation, documentation, documentation
  - Creating policy templates
  - Document process flow
- Third party compliance certification
UNIT LEVEL UNDERSTANDING

- PCI-DSS is security awareness training “ah-ha” moments.
  - Why do we need to do that for?!
  - Make sure everyone is on the same page and meet with all parts of the department
- It’s **not** just IT
- Simplifying Compliance
  - Think of it as cash...
- Creating Eyes and Ears
Why is Financial Services doing this to us?!  
You talkin’ to me?  
Legacy systems  
  Old out - new in.  
New staff  
What Now?  
  Peeling back the layers  
Fax Machines  
What other areas in the department affects PCI-DSS?  
  What is in scope?  
Who are the players?  
Aargh….I don’t know enough!  
Time and $$$$  
What is next? Never completes - it is a process-eternal vigilance
WHERE WE LEAD THEY WILL FOLLOW......

- Realize it will take a lot longer than you think and sometimes it feels like herding cats
- Program Management
  - Organizing Merchants
    - Grouping
  - Merchant Oversight
    - SAQ console/ reporting
SCOPING AND SEGMENTATION

- PCI VLAN separate from other department business systems and processes
  - Data flows of all credit card processes
    - Understand the flow of information
  - Systems diagrams
    - To tie the technology to the processes
- NO USE OF UNIVERSITY WIRELESS
  - Handhelds checked out from our merchant back for remote cc processing activities
- NO USE OF LAPTOPS
  - With a couple well thought out exceptions
- Policy templates
Move to the Left Campaign

- Shift CC processing to be more inline with needs and IT support structure
  - From virtual terminal to dial pay
  - From silent order pages where CC nbrs are entered on a University website to hosted order page with Cybersource.
- NO STORAGE of Credit Cards (i.e. NO SAQ D’s)
- SAQ C’s have to be approved, quarterly meetings to keep on track
MANAGEMENT OF COMPLIANCE

- Security Metrics
  - Management of SAQ’s for all merchants
  - Quarterly external scans for in scope internet connected devices c’s
  - New this year annual scans of servers with hosted order pages (this is not currently a requirement for SAQ A’s but we see it as a huge gap)

- Annual Onsite assessment
GAP ANALYSIS
LESSONS LEARNED

▪ Last Minute-itis
  ▪ Nothing would get done it wasn’t for the last minute.
    ▪ Semiannual merchant meetings - pre and post annual third party assessments
    ▪ New this year PCI 101 for all management and IT reps
  ▪ Merchants need quarterly timelines
  ▪ SCOPING is crucial
    ▪ NO LAPTOPS or UAWIFI use in cc process
▪ Beware!
  ▪ New applications, change in process, ideas or new projects that may jeopardize compliance
CONTINUED LESSONS

- Trust but verify - Quarterly reviews
- Documentation Distress.
- Differing expertise/knowledge mix
- Utilize different campus compliance regulations to work together
- The same solution does not always work for same problem.
- Organize, organize, organize
FUTURE BUILDING

- Quarterly Scans SAQ A’s
  - Possibly contracting for hosted e-commerce
- Quarterly Meetings with SAQ C’s
- More Awareness Trainings (PCI 101 and IT)
- Encrypted at Read Head Readers/Swipes.
- Limit, Limit, Limit Scope
- Ongoing QSA Consulting
Simplifying Your Compliance Efforts

Same approach for any compliance program

1. Identify Program Team – Compliance Officer
2. Scoping
3. Unit Responsible persons (Department Head, Business manager, IT)
4. Education (Management, End-User and IT)
5. Assessments – Gap Analysis
   - Risk Assessments (unit self assessment questionnaires, Data Flows, System Diagrams, interviews to gather missing details)
   - Scanning (devices and applications)
6. Action Planning for non-compliance
NEW REPORTING REQUIREMENTS

- June 30, 2012 Cutover for Requirements 6.2 and 6.5.6
  - Change in PCI reporting that will require organizations to assign risk rankings to newly detected vulns affecting the card holder environment
  - Risk rankings should be based on industry standards/practices (NIST, ISO, etc)
  - Should classify risk in a manner which facilitates prioritization for remediation (high, medium, low)
  - Ongoing testing of applications in scope, ‘high’ results on vuln scans
WHAT’S ON THE HORIZON?

- Effective 1 October 2012, Visa will expand the Technology Innovation Program (TIP) to the U.S. TIP will eliminate the requirement that eligible merchants annually validate their compliance with PCI DSS for any year in which at least 75% of the merchant’s Visa transactions originate from ‘dual-interface’ EMV chip-enabled terminals, in addition to other qualifying criteria.

- Read about it: [VISA Expands TIP to U.S.A.](#)
UNIVERSITY-CENTRIC RESOURCES/POLICIES

- EDUCAUSE Information Security Guide
- EDUCAUSE PCI DSS Resources
- Baylor University Payment Card Policy
- The Ohio State University Credit Card Merchant Policy Credit Card Handling Responsibilities and Procedures
- Auburn University and Affiliated Organizations Policies for Credit Card Processing and Security
- University of Arizona PCI Resource Page
- Indiana University PCI Checklist
- Clark University PCI Policy
- University of Cincinnati Credit Card Processing Procedure
- Tufts University PCI Presentation
- Notre Dame Credit Card Support Program

Georgia State University
RESOURCES TO ASSIST WITH COMPLIANCE

- PCI Security Standards Council Resources For Merchants
- PCI DSS Glossary
- PCI DSS Self Assessment Questionnaire
- PCI Rocks Video
- Visa's Data Security Primer For Merchants
- Contracting PCI DSS Compliance
- Symantec Compliance Matrix Poster
- Gartner PCI Webcast
- OWASP Open Web Application Security Project
PCI ASSESSMENT TOOLS, CHECKLISTS, AND RESOURCES

- PCI Compliance checker
- Security Bytes PCI Compliance Checker Trial
- Security Metrics PanScan Tool
- Imperva Free PCI Compliance Checklist
- Better Business Bureau PCI Audit Checklist
- PCI Compliance Guide
- Qualys PCI Compliance for Dummies
- PCI: Dead Man(date) Walking? Article
- Compliance Fatigue: How to Stop Chasing Compliance... (Upcoming Webinar May 22nd @ 12pm EST
- Getting Started With PCI DSS - Trustwave Webinar
Resources

Presentation and related resources available at http://security.arizona.edu/educause2012

Georgia State University
http://www.gsu.edu/ist/security.html

University of Arizona Information Security Office
http://security.arizona.edu