

# PCI COMPLIANCE

ISOAG MEETING  
JULY 11<sup>TH</sup>, 2012





WHERE DOES IT COME FROM?



**AMERICAN  
EXPRESS**

**DISCOVER<sup>®</sup>**  
NETWORK

**VISA**

# WHAT'S IT FOR?



# WHO NEEDS IT?

- All merchants, small or large, that accept credit cards, need to be PCI compliant.
- Sell a product?
  - Liquor
  - License
  - Gifts
- Charge for events?
  - Classes
  - Registrations
  - Events
- Fees/Penalties

# WHO NEEDS IT?

Level	Merchant Criteria
1	Process over 6,000,000 transactions annually <u>or has suffered a breach</u>
2	Process between 1,000,000 and 6,000,000 transactions annually
3	Process between 20,000 - 1,000,000 transactions annually
4	Process under 20,000 transaction annually

# HOW IS IT CHECKED?



# HOW IS IT CHECKED?

<b>Level</b>	<b>Merchant Criteria</b>
1	3rd party PCI approved Qualified Security Assessor(QSA) to perform a yearly onsite assessment, yearly penetration tests and quarterly security scans by an approved PCI scanning vendor
2 and 3	complete a yearly self assessment questionnaire(SAQ) and quarterly security scans by an approved PCI scanning vendor
4	Recommended to perform level 2 and 3 requirements but not enforced

# WHAT ARE THE COMPONENTS?

1. Install and maintain a firewall
2. Do not use vendor default passwords
3. Protect stored data
4. Encrypt transmissions of cardholder data

# WHAT ARE THE COMPONENTS?

5. Use and update antivirus software
6. Develop and maintain secure systems and applications
7. Restrict access by need-to-know
8. Assign unique IDs to all users

# WHAT ARE THE COMPONENTS?

9. Restrict physical access to cardholder data
10. Track and monitor access to cardholder data
11. Regularly test security systems and processes
12. Maintain an information security policy

# IMPLEMENTATION DETAILS...

We use Trustwave for

- SAQ
- QSA
- Quarterly vulnerability scans
- Internal and External Penetration testing



Powered By **SpiderLabs**®

# WHAT IF I DON'T?

- Starts with fines
- Removal credit card acceptance privileges
- Reporting requirements
  - COV reputation at stake
- If found non-compliant and a breach occurs, additional charges levied per account compromised

# A PROGRAM FOR PCI COMPLIANCE

# GETTING TO COMPLIANCE



**1. ORGANIZE**



**2. ASSESS**



**3. PLAN &  
REMEDiate**



**4. EDUCATE**



**5. VERIFY**

# STEP 1: ORGANIZE

Determine Who Leads



# STEP 1: ORGANIZE

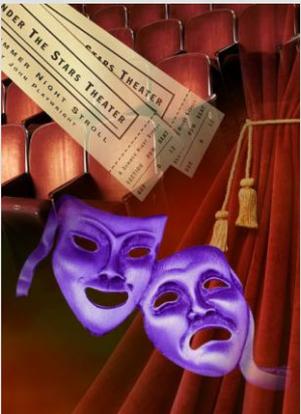
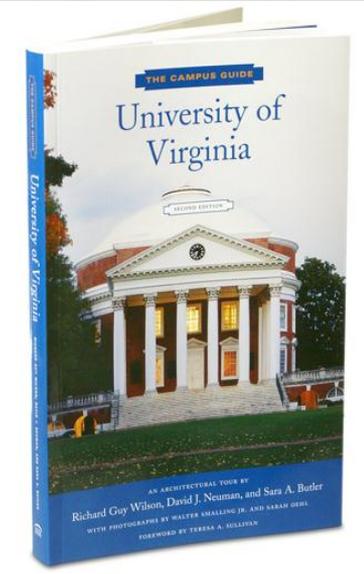
Involve All Appropriate Parties



# STEP 2: ASSESS

- Determine Scope
  - Merchant level (based on card transaction volume)
  - Processes where CHD stored, processed, or transmitted
  - PCI regulations applicable to each process

# LOTS TO CONSIDER IN HIGHER ED ENVIRONMENT



# STEP 2: ASSESS

- Determine Scope
  - Merchant level (based on card transaction volume)
  - Processes where CHD stored, processed, or transmitted
  - PCI regulations applicable to each process
- Conduct Gap Analysis

# STEP 2: ASSESS

- Determine Scope
  - Merchant level (based on card transaction volume)
  - Processes where CHD stored, processed, or transmitted
  - PCI regulations applicable to each process
- Conduct Gap Analysis
- Investigate Scope Reduction Options

# STEP 3: PLAN & REMEDIATE

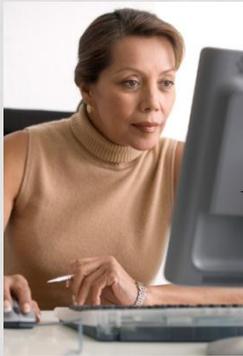
Top five vulnerabilities according to VISA:

1. Storing prohibited data, e.g. card verification values
2. Unpatched systems
3. Use of vendor default settings and passwords
4. Poorly coded web applications
5. Unnecessary and vulnerable services on servers

# STEP 3: PLAN & REMEDIATE



**Ensure sensitive data collected only when essential**



**Ensure sensitive data access authorized to least # of people**



**Business Processes & Supporting Technology**



**Ensure sensitive data stored or transmitted only when essential**



**Ensure sensitive data handled only by highly secured devices and networks**

**Enhance data protection policies/procedures as needed**  
**Strengthen data protection provisions in 3<sup>rd</sup> party contracts**

# REDUCE SCOPE

- Eliminate storage of data
  - If you don't need to keep the card data for
    1. Returns
    2. Affinity Programs
    3. Return purchases
  - Don't!
- Outsource payment processing
- Segment network

# STEP 4: EDUCATE

- Training program for managers and staff covering:
  - PCI compliance overview
  - Applicable policies and procedures
  - Incident reporting guidance
  - Consequences of non-compliance
- Central repository of resources
- Periodic updates to executives

# EDUCATE TO ERADICATE



False front (Skimmer) placed over the face of an ATM in Texas.



Camera hidden inside pamphlet holder next to ATM at the University of Texas campus

# NEED TO IDENTIFY...



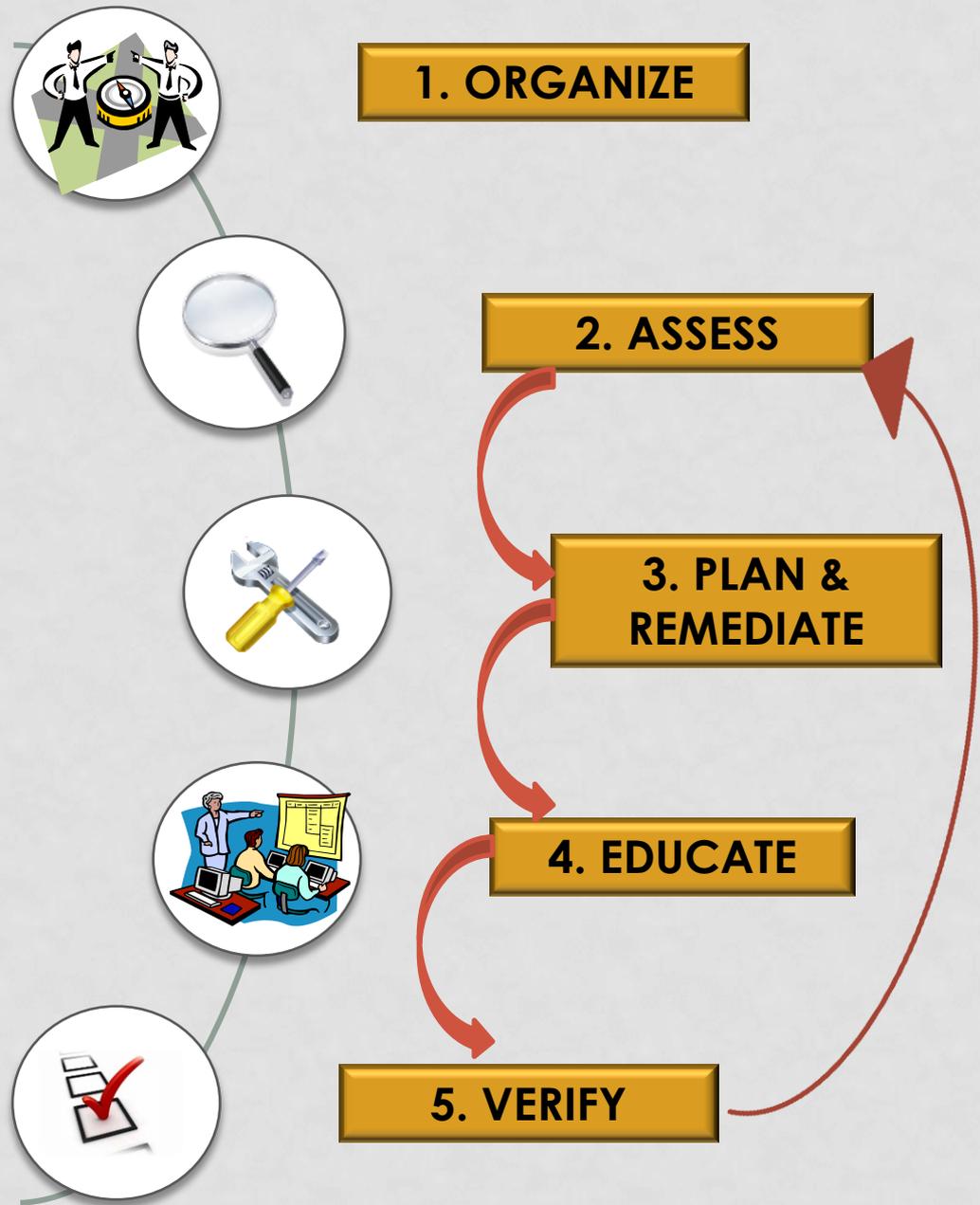
- Pwn Plug Elite
- \$800, available to the public
- Has everything needed to sniff/steal/send pre-installed

# STEP 5: VERIFY

- Annual self-assessment questionnaire
- Quarterly\* vulnerability scans of Internet-facing, in-scope IP addresses
- Annual\* penetration tests
- Attestation of compliance form

\* and after significant change occurs

# COMPLIANCE IS AN ONGOING PROCESS



# SOME PCI MYTHS

- Outsourcing card processing makes us compliant
- PCI compliance is an IT project
- PCI will make us secure
- PCI requires us to hire a QSA
- PCI requirements are unreasonable
- We don't take enough credit cards
- We completed a SAQ so we're compliant

# MORE INFO

- <https://www.pcisecuritystandards.org/>
- Andy Hallberg
  - [Andrew.Hallberg@abc.virginia.gov](mailto:Andrew.Hallberg@abc.virginia.gov)
- Shirley Payne
  - [scp8b@virginia.edu](mailto:scp8b@virginia.edu)