PC-DSS Compliance Strategies

2011 NDUS CIO Retreat
July 27, 2011
Theresa Semmens, CISA
True or False

• Now that my institution has outsourced credit card processing, I don’t have to worry about compliance?
A bank robber’s new target

• Sony Playstation – 100 M accounts compromised (included CC data)
  • Sony stated they “couldn’t be hacked.”
  • LulzSec (ninja hackers) have claimed to be the group behind the recent attack on Sony, and has also upset Nintendo and FBI affiliate Infragard.
Key Takeaways

General concepts related to PCI-DSS
Reducing the PCI compliance scope
Minimizing impact of security breach
Importance of removing financial data from the IT environment
Issues for Higher Education
Three Levels of Standards

• PIN Transaction Security Standard
  – Payment cards, scanning terminals, point of sale devices. Only use those approved by acquiring bank (Bank of North Dakota)

• PA-DSS
  – Payment Application Data Security Standard – requires development of secure applications that are sold, distributed and licensed to third party vendors

• PCI-DSS
  – Includes all merchants that accept credit cards for payment of services and goods
## PCI Overview 101

<table>
<thead>
<tr>
<th>What is PCI?</th>
<th>What is DSS?</th>
<th>What is the latest PCI DSS 2.0 update?</th>
<th>What are the PCI business drivers?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global credit card security standards council led by a policy-setting committee from VISA, MC, AMEX, etc.</td>
<td>A framework for developing a robust payment card data security process</td>
<td>Provides clarification and additional guidance Standard updated every 3 years</td>
<td>Protection of assets Mandatory compliance Security against breaches Brand integrity</td>
</tr>
</tbody>
</table>
PCI compliance is a continuous process

Assess

NDUS

Report

Remediate
Assess

Identify card holder data

Inventory IT assets, business processes for CC payment processing

Analyze for vulnerabilities
1. **Inventory** your campus merchants and their payment systems

   1. Determine if system is listed on PCI Council’s website of certified payment applications
   2. System not listed? Request letter of explanation on position for PA-DSS
Analyze vulnerabilities

- Assess which departments and colleges may be using and storing CC data
- Do they have a process in place? Do they use a Hosted application for payments?
Remediate

First step: Policy and Procedure

- Develop and implement a policy specific to electronic payment transactions
- “Plug the holes” Fix issues found in assessment
Report

Compile and submit required remediation validation records (if applicable), and submit compliance reports to the acquiring bank and card brands you do business with.
## PCI-DSS – 6 goals, 12 requirements

<table>
<thead>
<tr>
<th>Goals</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 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 card holder data</td>
<td>3. Protect stored data</td>
</tr>
<tr>
<td></td>
<td>4. Encrypt transmission of cc data and sensitive data</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 systems and applications</td>
</tr>
<tr>
<td>Implement strong access control measures</td>
<td>7. Restrict access on a need-to-know basis</td>
</tr>
<tr>
<td></td>
<td>8. Unique ID and password required for access</td>
</tr>
<tr>
<td></td>
<td>9. Restrict physical access to cardholder data</td>
</tr>
<tr>
<td>Monitor and test networks</td>
<td>10. Track and monitor all access to network resources and cc 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>
# Card Holder Data

<table>
<thead>
<tr>
<th>Card Holder Data</th>
<th>Sensitive Authentication Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Account Number (PAN)</td>
<td>Full magnetic stripe data or equivalent on a chip</td>
</tr>
<tr>
<td>Cardholder Name</td>
<td>CAV2/CVC2/CVV2/CID</td>
</tr>
<tr>
<td>Expiration Date</td>
<td>PINs/PIN blocks</td>
</tr>
<tr>
<td>Service Code</td>
<td></td>
</tr>
</tbody>
</table>

![Image of credit card with elements labeled (PAN, CAV2/CVC2/CVV2/CID, CID)]
Primary Account Number

• The Primary Account Number (PAN) is the defining factor in the applicability of the PCI DSS requirements.
• PCI-DSS requirements are applicable if a PAN is stored, processed, or transmitted.
• PAN not stored or transmitted – PCI-DSS does not apply.
Merchant

For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services. Note that a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers.

- Any NDUS institution that accepts credit cards for payment
## Merchant Classification

- **Four levels of classification**

<table>
<thead>
<tr>
<th>Level</th>
<th>Merchant Classification Criteria</th>
</tr>
</thead>
</table>
| 3     |                                      | Visa: any merchant processing 20,000-1 M e-commerce transactions  
        |        | MasterCard: any merchant processing 20,000-150,000 e-commerce transactions  
        |        | AMEX: any merchant regardless of transaction channel that processes less than 50,000 transactions |
| 4     |                                      | Visa: any merchant that processes fewer than 20,000 Visa e-commerce transactions or processes fewer than 1 M Visa transactions  
        |        | MasterCard: Any merchant that processes fewer than 20,000 MasterCard e-commerce transactions and less than 6 MasterCard transactions |
# Merchant Validation

<table>
<thead>
<tr>
<th>Merchant Level</th>
<th>Validation Actions</th>
<th>Validated By</th>
<th>Deadline</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Annual PCI Self-Assessment Questionnaire and Quarterly Network Scan</td>
<td>Merchant Qualified Independent Scan Vendor</td>
<td>AMEX recommended 10/31/06</td>
</tr>
<tr>
<td>4</td>
<td>Annual PCI Self-Assessment Questionnaire and Quarterly Network Scan</td>
<td>Merchant Qualified Independent Scan Vendor</td>
<td>Validation requirements and dates are determined by the merchant’s acquirer</td>
</tr>
</tbody>
</table>
Merchant Responsibilities

• Meeting the requirements of PCI-DSS
• Requiring by contract that engaged third parties meet all PCI security standards
  – Understanding what processors those third parties use
• Completing the PCI Self-Assessment Questionnaire, if required
• Hiring a qualified independent scan vendor, if required
• Engaging a qualified outside assessor, if necessary
• Protecting other confidential/sensitive information
Acquirer

Also referred to as “acquiring bank” or “acquiring financial institution.”

Entity that initiates and maintains relationships with merchants for the acceptance of payment cards.

• Bank of North Dakota
SAQ

Self Assessment Questionnaire (SAQ) is a validation tool for organizations that are not required to undergo an on-site assessment for PCI DSS compliance. Different SAQs are specified for various business functions. The organization’s acquiring bank/financial organization can also determine if a SAQ needs to be completed.
Hosted Payment Acceptance Vendors

• Entities that transmit and process e-commerce transactions and remove the scope of payment process from the Merchant’s systems and network. Vendor examples include TouchNet, CyberSource, and Heartland.
True or False

• Athletics uses a third party processor to process credit cards. The Athletics department processes seat and ticket reservation requests when customers call in. The person responsible for making the reservations and obtaining payments uses the payment gateway from the third party processor to submit credit card payment. My institution is compliant for PCI-DSS.
PCI Compliance Scope Issues

• If CC payment information touches your systems and network, it is within scope of PCI
  – What to look for....

• IPv6 does not lend well to the requirements of PCI

• Wireless POS/swipe machines/terminals

• Access to CC information

• Solutions: Some good, some not so good
  – Virtual machines, separate, dedicated machines, NAT, internal subnets, etc.
Ten Step Approach to Compliance

1. Create a work group to develop policy and procedure related to PCI
   1. Form a “coalition” group compromised of key stakeholders to write, develop, implement, disseminate policy and procedure.
2. Inventory campus merchants and payment systems
3. Determine if each payment system is listed on the PCI Council’s Web site of certified payment applications
4. Contact those vendors whose systems are not listed and request a letter explaining their position on PA-DSS
5. Require all Hosted payment vendors to be PA-DSS compliant
Ten Step Approach to Compliance

6. Centralize payment environment, require all campus merchants to adhere to PCI policy, standards, and procedures
7. Review new and contracts up for renewal to ensure the contract meets or exceeds PCI standards
8. Require education and training for all who have access to CC data
9. Do background checks for all employees who handle CC data
10. Assume guardianship and management of IT related resources for CC data
PC-DSS Compliance Strategies

Theresa Semmens, CISA
Theresa.Semmens@ndsu.edu