Information Security Advisory Council (ISAC)

January 27, 2014
Agenda

» Welcome
» Review of 2013 activities and accomplishments
» Update on VPN TAC
» Update on Password Management TAC
» Update on Web Application Firewall TAC
» Discussion / Approval of new guideline regarding responsibilities for protected data when moving
» Discussion of Mobile Device Security enforcement / policy
» Discussion of Employee Receipt of Equipment form
2013 Activities and Accomplishments

» 2013 PCI-DSS
  • Program completed, October 2013
  • New requirements for 2014

» 2013 PII Program
  • Single scan in 2013
    o Time Constraints
    o Staff turnover
  • All departments completed by January 15, 2014
  • Uptick in PII found as result of PDF scanning

» Awareness
  • Program started with Twitter, Facebook and Blogs
  • Survey being developed along with Institutional Research

» Draft Policy Review
  • All draft policies approved by President’s Cabinet
TAC Activities and Updates

» Web Application Firewall
  • Kick Off January 1024
  • What does it do?
  • Requirements for 2014 PCI-DSS

» VPN Replacement
  • F5 Phased Out EOL
  • New Functionality
  • Better user experience
  • RFP Due from vendors 1/31/2014

» Mobile Payment Processing
  • Based on need specified by Treasury
  • RFP – Received and under review

» Password Management
  • Replacement of PAM
  • Need to lower Helpdesk Ticket Load (over 8500 calls in 2013)
  • Easier self-serve functionality
New Guidelines and Policies

» Handling of Protected and Sensitive Data During an Office Move
  • Why do we need this?
  • Discussion on Revisions
  • Approve / Table

» Mobile Device Security Enforcement Policy
  • Outlines requirements for personal devices containing Loyola Data
  • Currently no University Policy
  • Applies to portable devices

» Employee Receipt of Equipment Form / Policy
  • Outlines ownership requirements for portable devices issued to employees by the university
  • Currently no University Policy
  • Applies to Issued portable devices
  • May serve as an inventory process during termination
## 2013 PCI-DSS Compliance Program

<table>
<thead>
<tr>
<th>PCI DSS Requirements</th>
<th>Total # of Applicable Requirements</th>
<th># of Requirements Currently Met</th>
<th># of Requirements Partially Met</th>
<th># of Requirements Not Met</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>1: Firewall</td>
<td>21</td>
<td>21</td>
<td>0</td>
<td>0</td>
<td>100%</td>
</tr>
<tr>
<td>2: No Vendor Defaults</td>
<td>7</td>
<td>7</td>
<td>0</td>
<td>0</td>
<td>100%</td>
</tr>
<tr>
<td>3: Protect Stored Data</td>
<td>19</td>
<td>19</td>
<td>0</td>
<td>0</td>
<td>100%</td>
</tr>
<tr>
<td>4: Encryption Over Public Networks</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>100%</td>
</tr>
<tr>
<td>5: Anti-Virus</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>100%</td>
</tr>
<tr>
<td>6: Secure Systems and Apps</td>
<td>8</td>
<td>8</td>
<td>0</td>
<td>0</td>
<td>100%</td>
</tr>
<tr>
<td>7: Restrict by Need-to-Know</td>
<td>9</td>
<td>9</td>
<td>0</td>
<td>0</td>
<td>100%</td>
</tr>
<tr>
<td>8: Unique ID's for Access</td>
<td>21</td>
<td>21</td>
<td>0</td>
<td>0</td>
<td>100%</td>
</tr>
<tr>
<td>9: Restrict Physical Access</td>
<td>17</td>
<td>17</td>
<td>0</td>
<td>0</td>
<td>100%</td>
</tr>
<tr>
<td>10: Track &amp; Monitor</td>
<td>28</td>
<td>28</td>
<td>0</td>
<td>0</td>
<td>100%</td>
</tr>
<tr>
<td>11: Regular Testing</td>
<td>10</td>
<td>10</td>
<td>0</td>
<td>0</td>
<td>100%</td>
</tr>
<tr>
<td>12: Maintain Policies</td>
<td>39</td>
<td>39</td>
<td>0</td>
<td>0</td>
<td>100%</td>
</tr>
<tr>
<td>Appendix: A</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>184</strong></td>
<td><strong>184</strong></td>
<td><strong>0</strong></td>
<td><strong>0</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>
2013 PCI-DSS Compliance Program

Overall Compliance Rating by Requirement

PCI DSS Requirement

- 1: Firewall
- 2: No Vendor Defaults
- 3: Protect Stored Data
- 4: Encryption Over Public Networks
- 5: Anti-Virus
- 6: Secure Systems and Apps
- 7: Restrict by Need-to-Know
- 8: Unique ID's for Access
- 9: Restrict Physical Access
- 10: Track & Monitor
- 11: Regular Testing
- 12: Maintain Policies
- Appendix: A

Overall Compliance Rating by Requirement

- # Not OK

PCI DSS Requirement
PII Program Update

<table>
<thead>
<tr>
<th>2013 PII Compliance Status</th>
<th>Pending</th>
<th>Active</th>
<th>Remediation Complete</th>
<th>Complete</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Departments</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>64</td>
<td>64</td>
</tr>
<tr>
<td></td>
<td>0%</td>
<td>0%</td>
<td>0%</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

PII Complete Information

<table>
<thead>
<tr>
<th></th>
<th>2013 Scan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Computers in Scope</td>
<td>2939</td>
</tr>
<tr>
<td>Computers in Data Steward Inventory</td>
<td>2939 (100.00%)</td>
</tr>
<tr>
<td>Total Endpoints Scanned</td>
<td>2939 (100.00%)</td>
</tr>
<tr>
<td>Remediation Completed</td>
<td>2939 (100.00%)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Primary Data Stewards</td>
<td>64</td>
<td>62</td>
<td>64</td>
<td>67</td>
<td></td>
</tr>
<tr>
<td>Data Stewards Reporting</td>
<td>64</td>
<td>100.0%</td>
<td>62</td>
<td>100.0%</td>
<td>64</td>
</tr>
<tr>
<td>Computers</td>
<td>2939</td>
<td>3210</td>
<td>2690</td>
<td>2483</td>
<td>2322</td>
</tr>
<tr>
<td>PII Found</td>
<td>547</td>
<td>18.61%</td>
<td>397</td>
<td>12.37%</td>
<td>614</td>
</tr>
<tr>
<td>PII Left on Device</td>
<td>0</td>
<td>0.00%</td>
<td>31</td>
<td>0.97%</td>
<td>89</td>
</tr>
</tbody>
</table>
2013 Changes
- Identity Finder scans launched remotely via console
- Data Steward able to choose time for remote scan
- OCR (PDF) scanning enabled to improve compliance
- Data Steward was only required to review the results of computers where potential PII is identified

2014 Changes
- Return to twice a year scanning
- Outlook email scanning enabled
- Identity Finder upgraded to latest version
  - New Features? (brief)
2013 Security Awareness Program
Approved Policies

- Access Control Policy
- Antivirus Policy
- Computer Security Standard
- Incident Response Plan
- Incident Response Plan – Appendix
- Log Management Standard
- Network Firewall Policy
- Network Firewall Standard
- Password Standards
- Router and Switch Standard
- Security Awareness Policy
- Security Policy
- Server Security Standard
- Vulnerability Assessment Policy
Next Steps

Next meeting

• March 2014
• Location – WTC
• Agenda Items?