Information Security Advisory Council (ISAC)

May 8, 2015
Agenda

- **Updates**
  - UIISO Staff - Updates
  - Password Management
  - PCI 2015 - Update
  - Information Security Risk Assessment Status/Results
  - Bradford Ownership
  - VPN Replacement - Update

- **New Initiatives**
  - Public Directory – HSD Info & email image
  - Removing Links From Email
  - Awareness/Securing the Human

- **Demos (Time Permitting)**
  - VPN
  - Securing the Human Training
Updates

» UISO Staff - Updates
  • Departure of Brett Weston
  • Cai Wang Replacement
    o Starting July 1

» Password Management
  • New System from ASPG/ReAct
  • Web-Based with Multiple Reset Options
    o Challenge Questions
    o Previous Password
    o SMS – Text Message
    o Email
  • No password changes from Helpdesk

» PCI 2015 - Update
  • Program started 4/30
  • New requirements
  • Version 3.1
Updates

» Information Security Risk Assessment Status/Results
  • Jim Sibenaller

» Bradford Ownership
  • Jim Pardonek / Chris Campbell

» VPN Replacement – Update
  • Jim Pardonek
### Risk Assessment – Review

#### Likelihood

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>2. One occurrence within 5 years</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>10</td>
</tr>
<tr>
<td>3. Multiple occurrences within 5 years</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>12</td>
<td>15</td>
</tr>
<tr>
<td>4. Foreseeable within the year</td>
<td>4</td>
<td>8</td>
<td>12</td>
<td>16</td>
<td>20</td>
</tr>
<tr>
<td>5. Multiple times this year</td>
<td>5</td>
<td>10</td>
<td>15</td>
<td>20</td>
<td>25</td>
</tr>
</tbody>
</table>

#### Impact

- **Negligible**: Risk is minor and unlikely to have significant impact. Strategic Plan: Monitor. Budget: Review. Performance: Review.
- **Moderate**: Risk is significant and requires attention. Strategic Plan: Mitigate. Budget: Review. Performance: Monitor.
- **High**: Risk is significant and requires immediate action. Strategic Plan: Mitigate. Budget: Review. Performance: Monitor.

#### Risk

- **Risk Assessment**: Likelihood x Impact = Risk

#### Notes

- **Likelihood**: The likelihood of occurrence is assessed on a scale of 1 to 5, with 1 being negligible and 5 being catastrophic.
- **Impact**: The impact of the risk is assessed on a scale of 1 to 5, with 1 being negligible and 5 being catastrophic.
- **Risk**: The overall risk is calculated by multiplying the likelihood by the impact. The risk can range from low to high.

---

Prepared by: [Your Name]
Date: [Date]

*Note: This table and diagram are meant for educational purposes and should be adapted to fit specific organizational needs.*

---

Images and diagrams are not included in the plain text representation.
## Risk Assessment – Results

<table>
<thead>
<tr>
<th>Risks</th>
<th>Assessed</th>
<th>Unique</th>
<th>Treatments</th>
<th>Themes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Projects</td>
<td>Programs</td>
</tr>
<tr>
<td>High</td>
<td>24</td>
<td>19</td>
<td>11</td>
<td>4</td>
</tr>
<tr>
<td>Medium</td>
<td>76</td>
<td>49</td>
<td>16</td>
<td>7</td>
</tr>
<tr>
<td>Accept</td>
<td>13</td>
<td>13</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th>Total</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>113</td>
<td>81</td>
<td>20*</td>
<td>8*</td>
<td>28*</td>
</tr>
</tbody>
</table>

* denotes unique items
Risk Assessment – High Risk Themes

T01. A shortage of skilled information security specialists.

T02. Change management processes are not consistently applied throughout the university in a manner that ensures changes are made and approved based on risk and security best practices.

T03. End-user systems may not have security controls enforced on them, but only required by policy.

T04. Information systems are not uniformly inventoried, nor are their configurations or states of vulnerability known.

T05. Internet-provided services are used to share data, but are not under the control or policies of the University.

T06. Network cables / connections are not secured against accidents or intentional sabotage.

T07. Passwords for user accounts are inherently vulnerable to guessing, oversharing, or exposing to unauthorized parties.

T08. The security audit and effectiveness measurement functions that are applied to the most sensitive systems are not applied to all at-risk systems.

T09. Security incident and event management does not yet cover all systems that create a risk to protected information.

T10. The vulnerability management program does not yet include a scheduled process for regularly scanning and resolving systems against known vulnerabilities, or established hardening standards.

T11. University community members may not have appropriately detailed instructions for handling information in a secure or legally compliant manner.

T12. Wireless routers are not yet secured against foreseeable attacks by hackers who are in the vicinity of Loyola campuses.
Risk Assessment – Next Steps

» Assess dependencies of treatments to risks
» Size the treatments
» Assign Owners & Participants to treatments
» Evaluate the value/impact of completing a treatment
» Assess dependencies of treatments to other ITS projects
» Prioritize treatments
» Create a master schedule of work (multiple years)
» Begin remediation
» Report progress continually
Bradford NAC Support

» Support assumed by UISO in February
Loyola Secure Access

» Don’t say VPN
» New solution from Juniper
» More robust OS support
» Replacement of the Certificates
» Single Sign-on Options
New Initiatives

» Public Directory – HSD Info & email image
» Removing Links From Email
» Awareness/Securing the Human
Public Directory

1. Adding of HSD Faculty to LUC Directory

2. Replacing email text with image
Several universities have had funds redirected by stolen credentials.

Loyola dedicates time and dollar resources to educate Faculty and Staff about what a phishing email may look like.

One item frequently mentioned is to ignore requests for account or login information in an email.

Regular emails with links to logon pages are sent by various departments as a means to add convenience for staff.

Logon pages can be easily spoofed to appear authentic.
Phishing and Links in Email Proposal

» Create or amend a policy that prohibits the use of links in email messages that lead to a login page.

» Communicate to staff that links will no longer be used.

» Instruct to use www.luc.edu and the links dropdown to deliberately access systems.
Securing the Human

» Purchased from SANs
  • 2 year subscription

» Hosted on Sakai
  • 43 modules averaging 3 minutes in length

» Mandatory Modules
  • PCI Compliance

» Includes tracking and quizzes

» Additional Campaign Materials
  • Screen Savers
  • Newsletters
  • Posters
Demos

» VPN
  • https://lsa.luc.edu

» Securing the Human Training
  • https://www.securingthehuman.org/enduser/
Next meeting (June/July)

• Tentative Agenda
  • Privacy Policy
  • Cloud Policy Updates
  • Multi Factor Authorization Expansion
  • Bradford Improvements
  • Location – LSC
  • Agenda Items?