Information Security Advisory Council (ISAC)

March 9, 2017
Agenda

» Approval of minutes from last meeting
» Updates
  • 2017 PCI-DSS
  • 2017 Assessments
  • PII
» Committee Updates
  • Policy Committee
  • HIPAA Committee
  • DLP TAC
» New business
  • Phishing Testing
  • Discussion
  • Next Meeting
» Adjournment
Updates

» PCI
  • RFP out for bid
  • Survey Sent
  • Program to begin April 2017

» Assessments
Updates 2017 Security Assessments

» FY17 Recommended Application List (Based on Risk)

- Penetration Testing for High Security Network – Mandatory
- PCI Segmentation Testing for High Security Network - Mandatory
- Full External Penetration Test, last done in 2013, medium risk.
- Lawson, v9 assessed in FY14, v10 live in FY16, medium risk.
- CBORD, last assessed in FY12, medium risk.
- Maxxess, assessed in FY12, recently upgraded, low risk.
- Kronos, v7 assessed in FY14, v8 live in FY17, never been assessed, low risk.
- Academic Works, never been assessed, low risk.

- Above plan was approved in the Directors meeting on 1/25/17
Updates 2017 PII Program

» Survey Action Items

• The Data Steward training materials will be updated and improved so that “re-training” sessions can occur.
• The program will undergo a “reboot” which will include communication to all faculty & staff and a reemphasis of the importance of the program by Senior Leadership. – Data Steward delivered or Mass Email
• Develop and distribute new communication tools and helpful instructions for remediation and troubleshooting.
• The Identity Finder software has being upgraded to a new version which includes improvements to email scanning and speed of execution.
• Improvements to the Reporting to make it more self-service.
• Management reporting will be created to keep Senior Leadership informed regarding the status of the program, progress and achievements, and impediments hampering completion. This was asked for by the ITESC members so that they could be more supportive of Data Steward needs.
• A Data Steward “Think Tank” will be created. This will be a voluntary group of yourselves that will be involved in identifying self-correction and process improvement opportunities within the program. We will be sending out additional information on how to volunteer/be involved.
• The inventory and asset management technology at Loyola is being reviewed and changes will be implemented to simplify the PC inventory process.
Committee Reports

- Policy Committee
  - Cheryl Heckel
- HIPAA Committee
  - Jim Sibenaller
- DLP Technical Advisory Committee
  - Jim Pardonek
PHISHING TEST RESULTS

February, 2017
Select 500 random faculty & staff
Perform 2 phish tests over 45 day period with training in-between

- Phish test 1 – Voice Mail (10 days)
- Training (3 weeks)
  - 250 took Wombat training
  - 250 took LUC training
- Phish test 2 – Password Change (10 days)
Demographics

Employee Type
- Staff, 207, 41%
- Faculty, 293, 59%

Campuses
- Lake Shore, 225, 45%
- Health Sciences, 54, 11%
- Retreat & Ecology, 2, 0%
- Water Tower, 219, 44%

500 Total
Results Summary

![Phishing Test Results - Total](image)
Click Through Results

Dual Clickers

- Staff, 38%
- Faculty, 63%
Device Info

Operating Systems
- Windows, 65%
- iPhone, 21%
- Macintosh, 9%
- Android, 3%
- iPad, 2%

Browsers
- Chrome, 35%
- Safari, 29%
- Internet Explorer, 25%
- Firefox, 11%

Browser Type
- Desktop, 74%
- Mobile, 26%
Vulnerable Plug-Ins

Vulnerable Plugins (171 Devices)

- Flash: 70% (119)
- PDF: 46% (79)
- Java: 29% (50)
- Quicktime: 24% (41)
- Silverlight: 18% (30)
- Other: 2% (6)
Password

PW Phishing Test Results - Total

PW Phishing Test Results - Faculty

PW Phishing Test Results - Staff
New Business

» Discuss Recommendations from Phishing Test
» Additional Discussion
Next meeting (May)

- Agenda Items?