Information Security Advisory Council (ISAC)

August 4, 2009

Welcome!
Agenda

• Welcome & Introductions
• History Lesson
• Old Business
  • Personal Information Risk Group (PIRG) Wrap-Up
• New Business
  • ISAC Objectives
  • Program Overview
  • Timing & Expectations
• Next Meeting/Logistics
Welcome and Introductions

Information Security Team

Jim Sibenaller
Director, Enterprise Architecture and PMO

- Overall vision and direction for security

Leilani Lauger
Information Security Officer

- Security program management

Erik Decker
Security Administrator
- General security administration
  - Incident response
  - Investigations

Open
Enterprise ERP Security Administrator
- LOCUS security administration
# ISAC Members

**Chair:** Leilani Lauger, *University Information Security Office*

<table>
<thead>
<tr>
<th>Department/Area</th>
<th>Primary</th>
<th>Alternate</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Academic Affairs</strong></td>
<td>John Connolly</td>
<td>Francesca Pirovano</td>
</tr>
<tr>
<td><strong>Advancement</strong></td>
<td>Ron Iwanski</td>
<td></td>
</tr>
<tr>
<td><strong>Finance</strong></td>
<td>Cory O’Brien</td>
<td></td>
</tr>
<tr>
<td><strong>Financial Assistance</strong></td>
<td>Tad Verdun</td>
<td>Eric Weems</td>
</tr>
<tr>
<td><strong>Human Resources</strong></td>
<td>Carol Mc Cormack</td>
<td>Mike Capulong</td>
</tr>
<tr>
<td><strong>ITS - Infrastructure</strong></td>
<td>Dave Wieczorek</td>
<td>Jeff Apa</td>
</tr>
<tr>
<td><strong>ITS - Applications</strong></td>
<td>Cheryl Heckel</td>
<td>Charlotte Pullen</td>
</tr>
<tr>
<td><strong>Registration &amp; Records</strong></td>
<td>Diane Hullinger</td>
<td>Eric Pittenger</td>
</tr>
<tr>
<td><strong>Risk Management</strong></td>
<td>Stephen Ham</td>
<td>Sue Bodin</td>
</tr>
<tr>
<td><strong>Student/Judicial Affairs</strong></td>
<td>Jeremy Inabinet</td>
<td>Tim Love</td>
</tr>
<tr>
<td><strong>Ex-Officio</strong></td>
<td>Jim Sibenaller</td>
<td></td>
</tr>
</tbody>
</table>
A Little History

• ISAC is a “reincarnation” of PIRG
  » PIRG established to address a single security concern – protecting personally identifiable information (PII)
  » ISAC created to provide a broader focus on information security and corresponding risks

• Subcommittee of the IT Executive Steering Committee
  » Part of IT Governance
  » Report to the ITESC 3-4 times a year
    • Recommendations for change
    • Project Updates
    • Capital Requests
ITESC Structure

- ITESC Charter
  - The Information Technology Executive Steering Committee (ITESC) leads a set of processes for IT governance and investment prioritization for Loyola University Chicago. These processes should be timely, transparent, and clearly aligned with the university's goals and strategies.

- ITESC Members - Key senior management

- Subcommittees
  - The ITESC Subcommittees allow for senior level staff members within Loyola to provide recommendations regarding technology needs, value and corresponding business priority.

- Details at http://www.luc.edu/its/governance/gov_itesc.shtml
IT Executive Steering Committee

Academic Technology Committee
Chair: Carol Scheidenhelm
Charter
The Academic Technology Subcommittee is charged with advising on technology directions, strategies, policies, plans, and priorities important to Loyola’s goals in teaching, learning, research, and other academic objectives.

Project Review Board
Chair: Kevin Smith
Charter
The Project Review Board is charged with the responsibility of reviewing and prioritizing all work requests that are presented to ITS for application review, installation, development, enhancement or customization.

Architecture Review Board
Chair: Jim Sibenaller
Charter
The Architecture Review Board will build the technology roadmap that enables Loyola University Chicago to fulfill its mission and vision effectively while adapting to a changing higher education environment.

Personal Information Risk Group
Chair: Joe Bazeley
Charter
Identify and safeguard using necessary policies, processes, procedures, and technologies all areas within Loyola that use personally identifiable information (PII) or other information protected by Local, State, or Federal regulations.

University Coordinating Committee

Recommended Initiatives

*External Request

Chair: Susan Malisch
Charter
The ITESC leads a set of processes for IT governance and investment prioritization for Loyola University Chicago.
The Academic Technology Subcommittee is charged with advising on technology directions, strategies, policies, plans, and priorities important to Loyola's goals in teaching, learning, research, and other academic objectives.

The Project Review Board is charged with the responsibility of reviewing and prioritizing all work requests that are presented to ITS for application review, installation, development, enhancement or customization.

The Architecture Review Board will build the technology roadmap that enables Loyola University Chicago to fulfill its mission and vision effectively while adapting to a changing higher education environment.

The ITESC leads a set of processes for IT governance and investment prioritization for Loyola University Chicago.
Old Business - PIRG

- PII Status
- Future of PII Protection Program
PII Status

- Project is very late
  - 10/31 ➔ 12/31 ➔ 3/31 ➔ 8/31?
- High level of follow-up was required
- 2 Departments Remaining – aiming for completion in August
**PII Status**

**Loyola PC's To Be Scanned (Non-Lab)**

- Remaining: 25 (.3%)
- Completed: 2320 (99.7%)

**PC Counts**

<table>
<thead>
<tr>
<th>PC Counts</th>
<th>Count</th>
<th>Pct</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total to be Scanned</td>
<td>2328</td>
<td></td>
</tr>
<tr>
<td>Completed</td>
<td>2320</td>
<td>99.7%</td>
</tr>
<tr>
<td>Remaining</td>
<td>8</td>
<td>.3%</td>
</tr>
</tbody>
</table>

**PII Identification**

- PII Found: 582 (25%)
- PII Not Found: 1738 (75%)

**PC Counts**

<table>
<thead>
<tr>
<th>PC Counts</th>
<th>Count</th>
<th>Pct</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Scanned</td>
<td>2320</td>
<td></td>
</tr>
<tr>
<td>PII Found</td>
<td>582</td>
<td>25%</td>
</tr>
<tr>
<td>PII Not Found</td>
<td>1738</td>
<td>75%</td>
</tr>
</tbody>
</table>
Future of PII Protection Program

• The ITESC approved moving forward with encrypting all University-owned computers.
  » Software licenses have been purchased
  » Testing is in progress and the rollout is scheduled to begin in September

• What will the new Data Steward role be?
  » Potential Roles:
    • Steward of Loyola Protected Data
    • Liaison between ITS and individual departments
    • Responsibilities could include:
      – Education of departments on PII policies
      – Participation in other compliance efforts such as annual PCI Survey

  » Based on decisions, new training will be developed and provided to Data Stewards
Future of PII Protection Program

• Should the University continue to manage PII scanning on desktops?
  » Option I:
    • Continue with current approach of having Data Stewards perform PII scans using the latest version of Spider, Spider 2008.
    • Conduct scans annually instead of semi-annually?
    • Requires approximately 1/3 FTE to manage follow-up with Data Stewards

  » Option II:
    • Implement centrally managed software to replace current application
    • How frequently to scan?
      – Will still require action on the part of Data Stewards and end users to remove PII
    • Requires additional effort from ITS staff to manage application
      – Estimate .02 FTE for ongoing maintenance and .1 FTE for communication with Data Stewards
New Business

- ISAC Objectives
- Draft Information Security Program
  » Business Drivers
  » Goals and Objectives
  » Role of Information Security
  » Approach
  » Program Elements
  » Risk Assessment
  » Roadmap
ISAC Objectives

• Information Security Advisory Council (ISAC)
  » Broad focus on Information Security and Risk Management
  » Provide guidance and oversight of Information Security program with emphasis on:
    • Risk assessment process and risk prioritization
    • Strategy
    • Policy
  » Ensure policies and program are sufficient to meet legal, regulatory and contractual requirements
  » Monitor and evaluate the effectiveness of the University Information Security Program
  » Serve as an advocate for the Information Security program
Business Drivers

Targets – Our Assets
- 311,000+ SSNs
- 15,000+ Credit Card numbers
- Student/Parent Financial Data
  - Also, information on high-profile students or parents

External Threats
- Identity Theft
  - Hackers and Organized Crime
- Spammers / Phishers
  - 70% of spam is generated by compromised computers
- Human Error
- Physical Theft (of electronic devices/data)
- Regulations and Laws
- Acts of God

Internal Threats
- Students
  - Unauthorized grade changes
  - Harassment of another student or faculty member
- Faculty and staff
  - Disgruntled employees
  - Negligent employees

The threats are not just theoretical

1 http://searchcio.techtarget.com/news/article/0,289142,sid182_gci1096215,00.html
## Goals and Objectives

<table>
<thead>
<tr>
<th>Maintain confidentiality, integrity, and availability of information systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Prevent compromise of Loyola Protected and Sensitive Data</td>
</tr>
<tr>
<td>• Protect the integrity of critical systems</td>
</tr>
<tr>
<td>• Monitor for intrusion and misuse of systems</td>
</tr>
<tr>
<td>• Maintain the availability of systems required by students, faculty and staff</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protect Loyola’s reputation</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Maintain compliance with regulations (PCI, FERPA, HIPPA, PIPA), laws, and contractual agreements</td>
</tr>
<tr>
<td>• Protect the confidentiality of student, parent, faculty and staff personal information</td>
</tr>
<tr>
<td>• Limit liability</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Enable Loyola to provide a safe computing environment for students, faculty and staff</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Inform the Loyola community of protective measures to take against existing and upcoming security threats</td>
</tr>
<tr>
<td>• Provide technology that mitigates the risks of security threats</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Identify and provide guidance on risk management and information security issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Provide assistance and consultation on information security and risk management issues</td>
</tr>
<tr>
<td>• Facilitate and coordinate security audits and assessments of information technology infrastructure</td>
</tr>
<tr>
<td>• Provide reasonable assurance that security objectives are being achieved</td>
</tr>
</tbody>
</table>
Role of Information Security

• Manage risk related to Information and Information Technology

• Manage and facilitate the creation of appropriate Information Security policies

• Ensure a safe computing environment for students, faculty and staff

• Manage compliance with laws and regulations related to Information Technology

  » Future discussion question: What is Information Security’s role in Compliance?

• Provide Incident Response and Incident Handling services related to breaches of systems or information
**Approach**

- Balance academic and business needs with security imperatives

- Risk-based approach
  - Evaluate risk using a two-phased risk assessment
    - Phase I – High level risk assessment using ISO 27001/27002 Standards as a basis
    - Phase II – Broader and deeper risk assessment including interviews with staff and faculty who own and manage data
What is an Information Security Program?

– The policies, controls, services, and resources designed to achieve the Information Security goals of an organization

  • Provides guidance through policy and awareness
  
  • Details methods, processes, and controls to protect data

– Body of work will be documented and published to the UISO website
Program Elements

Plan and Roadmap

Governance (ISAC)

Policy
Controls
Services
Six Month Plan

Organize Information Security Advisory Council

Obtain approval for Plan and Program Framework

Complete Phase I Risk Assessment

Conduct Gap Analysis and make recommendations on priorities to ITESC

Project planning, scoping and funding
Governance

- Information Security Advisory Committee (ISAC)
  » Meets every 4-6 weeks initially, then every 2-3 months thereafter
  » Approves overall program and risk assessment approach
  » Provides guidance and University-wide perspective on risk evaluation
  » Approves final risk ranking and make recommendations on remediation projects to the ITESC
• Much policy work has already been done as a result of the PII and PCI projects

• The standards-based risk assessment will help identify where more work should be done and how efforts should be focused
Several policies are in draft and are going through the University governance process.

Policy review will be an annual process, changes will be approved first by the ISAC.

Policies:
- Acceptable Use Policy
- Access Control Policy
- Antivirus Policy
- DMCA (Digital Millennium Copyright Act) Policy
- Data Classification and Identification Policies
- Encryption Policy
- Information Security Policy
- Network Firewall Policy
- Ownership and Use of Data Policy
- Security Awareness Policy
- Vulnerability Assessment Policy

Standards:
- Computer Security Standard
- Log Management Standard
- Network Firewall Standard
- Password Standards
- Router and Switch Standard
- Server Security Standard

Processes:
- DMCA Process
- Incident Response Plan/Process
## Controls

Controls can be based on policy, technical measures or audit

<table>
<thead>
<tr>
<th>Policy / Process Controls</th>
<th>Technical Controls</th>
<th>Assessments and Internal Audits</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Change Management</td>
<td>• Firewalls</td>
<td>• Risk Assessments</td>
</tr>
<tr>
<td>• System and Network Configuration Standards</td>
<td>• Intrusion Prevention System</td>
<td>• Log Reviews</td>
</tr>
<tr>
<td>• Password Policies</td>
<td>• Security Information &amp; Event Management System</td>
<td>• User Account Reviews</td>
</tr>
<tr>
<td></td>
<td>• VPN</td>
<td>• Network Traffic Reviews</td>
</tr>
<tr>
<td></td>
<td>• Proxy Servers</td>
<td>• Vulnerability Scans</td>
</tr>
<tr>
<td></td>
<td>• Configuration Change Management</td>
<td>• Configuration Audits</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Access Audits</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Physical Access Audits</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Penetration Testing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PCI Assessments</td>
</tr>
</tbody>
</table>

### Footnote

Preventing people to lead extraordinary lives
Services

- Security Awareness
- Application Security Reviews
- Web Application Vulnerability Testing – tool based
- Network Vulnerability Scans – tool based
Risk Assessment

- The Risk Assessment will guide the next steps of the Information Security Program
  » Defines what needs to be done
  » Determines the priorities
  » Identifies the resources required
Proposed Timeline

<table>
<thead>
<tr>
<th>Jul</th>
<th>Aug</th>
<th>Sep</th>
<th>Oct</th>
<th>Nov</th>
<th>Dec</th>
<th>Jan</th>
<th>Feb</th>
<th>Mar</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISAC Formation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Program Approval</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Phase I Risk Assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Prioritization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITESC Approval</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Project Planning/Scoping</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Logistics

• Next meeting will be mid-September
  » Program Framework approval
  » PII scanning and the role of the Data Stewards
  » Draft a Charter
  » Discussion on Risk Assessment
Appendix - Glossary

Confidentiality
   Refers to the protection of information from unauthorized use or disclosure

Integrity
   Refers to the protection of information from unauthorized or accidental modification

Availability
   Refers to the accessibility of information and information systems