Security Liaison Meeting

March 22, 2012

Agenda

- Welcome
- Review of Role of the Security Liaison
- Updates from Mason's CIO
- Updates from the IT Security Office
- Guest Speaker: Brian J. Tillet, Chief Security Strategist for Symantec Public Sector
- Security Liaison Questions and Concerns

The Security Liaison

- Appointed by Vice Presidents, Deans and Directors
- Understands responsibility for two way communications, to the department and to the ITU
- Understands the balance between security and business needs
- Pursues clarity in policy development and revisions
- Understands the impact of policy on departmental business process and communicates areas of concern

The Role of the Security Liaison

- Point of contact in their unit for security recommendations and requests coming from the VPIT. Responsible for disseminating this information to the unit's leadership and their offices.

- Point of contact in their unit for security incidents, suspected and real. Act as a conduit to the Computer Security Incident Response Team (CSIRT).

- Initiate Security Risk Assessments by contacting the IT Security Office.

- Inform the VPIT and the President's Chief of Staff of possible gaps in training and support programs necessary to carry out requirements set forth in Policies and Directives.

- Review proposed Security Policies. Provide guidance on how to put a new or revised policy into practice.

CIO’s Update

Security Assessments

- Role of the BOV
- How Areas of Potential Risk Were Identified
- Assessments to be Conducted by Third party Vendors:

  - vulnerability assessments and penetration testing on departmental servers
  - assessing business processes in selected departments handling highly sensitive data

Purpose of 3rd Party Vendor Security Assessments

- Identify existing security risks
- Match up with "best practices"
- Recommend changes and mitigating controls
- Document the findings
- Department moves forward with remediation and/or formally accepts the identified risks

IT Security Office Update

Current Threats

Responding to Phishing emails

“Drive by” Malware downloads

Inappropriate storage of highly sensitive data

Departmental servers not properly administered

Busy Email System

From February 20 through March 21, 2012

- 130,624,911 attempted messages
- 9,579,462 messages were “clean” (7.3%)

New Policy

Approved March 19, 2012

Policy 1314

Physical Access to Sensitive IT Facilities:

"All university departments must establish procedures to protect Information Technology (IT) resources that process or store highly sensitive data from unauthorized physical access, tampering, and theft. Access to facilities that house IT systems and highly sensitive data must be restricted to individuals who have a legitimate business need for such access."

Welcome

Brian J. Tillet

Chief Security Strategist for Symantec Public Sector

Security Liaisons

- Questions and Concerns