Georgia Tech Information Security Informational Update – Fall 2009
• GT Information Security Goals
• Information Security Architecture
• Information Security Guidelines
• Information Security Monitoring Facts
• Specific Incident Response (Collaborative Model)
• Security Program Impact
GT Information Security Goals

• Support the Institute’s academic and research goals

• Ensure seamless and secure access to teaching and administrative resources

• Protect Institute users, IT resources, and data

• Enhance the Education and Awareness Program

• Ensure compliance with various regulatory and legal bodies
GT Information Security Architecture

A Road Map - Assuring information confidentiality, data integrity and systems availability.

**Deterrent Mechanisms**
- Secured Services
- Campus Border Filters
- Unit Level Firewalls
- Virtual Private Networks
- Host Based Security
- Intrusion Prevention

Reduce chance of

**Detective Methods**
- Self Assessment
- Vulnerability Scans
- Process Review
- Intrusion Detection Systems
- Network Monitoring
- System Audit

Disclose & generate statistics of

Create input for

**Prevention**
- Computer and Network Usage Policy
- Unit Level Information Security Policy
- Incurred Residual Risk
- Education and Awareness Programs
- Sharing Incident Information
- Systems Administrator Skill Sets
- Process Improvement

Reduces

<table>
<thead>
<tr>
<th>Threat</th>
<th>Catalyst</th>
<th>Attack</th>
<th>Exploits</th>
<th>Vulnerability</th>
<th>Results in IMPACT TO OUR MISSION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Natural</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Business Continuity</td>
</tr>
<tr>
<td>Manmade</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Financial</td>
</tr>
<tr>
<td>Internal</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Regulatory</td>
</tr>
<tr>
<td>External</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Legal</td>
</tr>
<tr>
<td>Ease of Use tools</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Reputation</td>
</tr>
<tr>
<td>Knowledge Base</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Prompts

**Reactive Measures**
- Incident Response Procedures
- Computer Forensics
- Service Restoration
- Legal Action
- System Modification

Reduce
**Security Program Impact**

- **Intrusion Detection**
- **2001:** Nimda
- **2002:** Klez
- **2003:** Blaster
- **2004:** Mydoom
- **2005:** Bagel
- **2006:** Sasser
- **2007:** Botnets
- **2008:** Worms

- **Started unit-level Firewall program**
- **GT InfoSec Guidelines**
- **Network Admission**
- **Executive risk management seminar**
- **Anti-Spam/Virus E-mail Gateway**
- **Campus-wide Data Cleanup**
- **Student Information Exposure Laptops / Unit Repositories**
- **T4/Sakia – facility to house student info**

- **Average attacks per week**
  - 2001: 5500
  - 2002: 2875
  - 2003: 2463
  - 2004: 1662
  - 2005: 556
  - 2006: 81
  - 2007: 172
  - 2008: 118

- **Incidents per Year**
  - 2001: 2 million
  - 2002: 2.5 million
  - 2003: 3.75 Million
  - 2004: 5.5 million
  - 2005: 6+ million
  - 2006: +110 million
  - 2007: 10+ million
  - 2008: 150+ million

Office of Information Technology
http://www.oit.gatech.edu
## GT Information Security Guidelines

(Short version)

http://www.oit.gatech.edu/it-policies/policy/unit-level-information-security-guidelines

<table>
<thead>
<tr>
<th>Chairs, Directors &amp; Managers</th>
<th>College/Unit Technical Lead/CSR</th>
<th>Computers Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsibilities</td>
<td>Responsibilities</td>
<td>Responsibilities</td>
</tr>
<tr>
<td>➢ Clearly assign technology roles within the unit.</td>
<td>➢ Coordinate all technology and information security issues within the unit.</td>
<td>➢ Become familiar with applicable computing and security policies.</td>
</tr>
<tr>
<td>➢ Verify that every system has a qualified system administrator with the appropriate skills to maintain the system.</td>
<td>➢ Develop security guidelines and procedures.</td>
<td>➢ Choose “strong” passwords, change them frequently and do not share them with others. A strong password has at least eight characters, a combination of numbers, upper and lowercase letters, and has at least one special character such as !@#$%^&amp;*.</td>
</tr>
<tr>
<td>➢ Develop unit-level security guidelines and procedures that support unit-level policy.</td>
<td>➢ Develop software &amp; hardware standards and use centrally supported and funded applications when applicable.</td>
<td>➢ Contact your CSR before installing new software on your system.</td>
</tr>
<tr>
<td>➢ Ensure the implementation of the data access policy within the unit to include training of authorized users.</td>
<td>➢ Work with unit leadership to generate a list of mission critical services and sensitive information servers.</td>
<td>➢ Do not transmit sensitive information such as social security or credit card numbers via email.</td>
</tr>
<tr>
<td>➢ Approve a list of mission critical services and servers containing sensitive information and provide the list to OIT Information Security.</td>
<td>➢ Audit unit systems under the control of approved system administrators, report systems with poor controls and maintenance to the Security Lead or management.</td>
<td>➢ Log off or lock your keyboard when stepping away from your work area and use a password activated screensavers.</td>
</tr>
<tr>
<td>➢ Coordinate software &amp; hardware standards for approval by the Dean or AVP.</td>
<td>➢ When possible use GT Active Directory or Kerberos for managing department passwords.</td>
<td>➢ Report security problems, issues, or misuse to your CSR as soon as possible for remediation.</td>
</tr>
<tr>
<td>➢ Coordinate all major technology and information security issues with the Security and/or Technical Lead.</td>
<td>➢ Review system access logs and service offerings, report any issues to management.</td>
<td>➢ Shred documents with sensitive information before discarding.</td>
</tr>
<tr>
<td>➢ Review monthly vulnerability scans and report outstanding issues to OIT-Information Security for assistance with resolution.</td>
<td>➢ Perform monthly vulnerability scans on all systems, resolve issues and generate reports for leadership to review.</td>
<td>➢ When traveling, do not carry a laptop or other mobile devices that contain sensitive information.</td>
</tr>
<tr>
<td>➢ Conduct an annual security self assessment and develop a plan to remediate issues.</td>
<td>➢ Implement a patch management system for the unit.</td>
<td>➢ Complete the online information security tutorial.</td>
</tr>
</tbody>
</table>
• Incidents are typically classified as Level 1 (malware) or Level 2 (affecting desktops/servers). If the incident is something beyond a normal malware infection, OIT is engaged to perform a deeper analysis.

• OIT does NOT monitor email & files, or inspect faculty/staff computers unless there is an incident, complaint, or subpoena that would trigger OIT to perform a review.

• Before investigating faculty/staff computers, email, or files, senior leadership will review the request, and if warranted, approve a specific set of review actions.
• Event or Incident Requiring Collaboration

• Ad-Hoc Group Convenes

• Other resources to be considered on a situational basis

• Is this incident likely to result in criminal or civil legal action

• Is this incident likely to result in an administrative action that is localized within the Institute

• Assign Oversight Role, Conduct Investigation, Follow Up & Reporting

http://www.audit.gatech.edu/IAcollabratrative2.pdf