Incidents and Breaches: The Executive Management Decision-Making Process In Higher Education

Overview

Sam Segran
Chief Information Officer
Texas Tech University

© TTU 2016
Factors influencing data breach management in higher education:

- Nature of the breach
- Type of data involved
- Scale of the breach
- Type of higher education institution
- How the institution is organized to respond to a breach (or not!)
Data typically found in higher education

- Student educational data (FERPA)
- PII (Texas Business & Commerce Code §521)
- Financial aid information (Red Flag Rules)
- Payment card information (PCIDSS)
- PHI (HIPAA)
- Research data – sensitive, economic, defense, energy, etc. (various state/federal requirements)
- Other sensitive data (e.g., network security logs, police security, etc.)
- Other operational data
- Public

Higher Education – Data Types
Carnegie Classification Of Institutions of Higher Education (IHE)

- Doctoral Universities
- Master’s Colleges & Universities
- Baccalaureate Colleges
- Baccalaureate/Associate’s Colleges
- Associate’s Colleges
- Special Focus Institutions (e.g., faith-related, medical schools, law schools, etc.)
- Tribal Colleges
Governance

- Public v. Private Institutions
- System (multi-campus system) v. Single institution
- Governor and Legislators (for Public Institutions)
- Board of Regents/Trustees
- CEO – Chancellor/President
- Senior Administration
- IT reporting structure
  - Centralized < --- > Decentralized
- Institutional Culture
Incidents and Breaches: The Executive Management Decision-Making Process In Higher Education

General Incident Response Process For Higher Education

Sam Segran
Chief Information Officer
Texas Tech University

© TTU 2016
**Identification**

- Is it a breach? Who decides?
  - Example: Texas Business & Commerce Code §521.053(a) – “unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data.”
  - If No: Follow normal Incident Response Plan (IRP)
  - If Yes: Follow breach notification process and IRP
Incident management process

- After identifying incident type:
  - Analyze incident/breach
  - Determine next steps
- Small/isolated incidents generally worked out between central IT and departmental IT
- Major incidents/actual breach response coordinated by CIO Office, working with other executives

General Incident Response Process
For Higher Education
Incident management process

- Major incidents/actual breach response coordinated by CIO Office at 2 levels:
  - Tactical
    - Operational steps to contain/remedy situation
    - Typically managed by Security Officer and technical team(s)
  - Executive
    - Coordination with other senior administrators
    - Breach notification requirements
    - State/Federal reporting requirements
    - Communications Plan
Notification process:

- Coordination at CIO Office level
  - Executives to be notified
  - Internal notifications
    - FYI only, no action needed
    - Legal: what information to release, timing of announcement(s)
    - How high?
    - Functional area(s): incident containment/remediation
  - External Notification
    - Regulatory agencies – Legal/other
    - Media - Public Relations
    - Political – Government Relations
### Areas that are generally involved with process:

<table>
<thead>
<tr>
<th>Senior University Administration</th>
<th>Other University Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>President</td>
<td>Deans &amp; Department Chairs</td>
</tr>
<tr>
<td>Provost</td>
<td>Registrar</td>
</tr>
<tr>
<td>VPR</td>
<td>Human Resources</td>
</tr>
<tr>
<td>CFO</td>
<td>Audit</td>
</tr>
<tr>
<td>VP Student Affairs</td>
<td>Public Relations</td>
</tr>
<tr>
<td>GC/Legal</td>
<td>Risk Management</td>
</tr>
<tr>
<td>Government Relations</td>
<td>Compliance</td>
</tr>
<tr>
<td>CIO</td>
<td>Office of International Affairs</td>
</tr>
<tr>
<td></td>
<td>Student Media</td>
</tr>
</tbody>
</table>

**External**

<table>
<thead>
<tr>
<th>State/federal agencies (FBI, HHS, DoE, DoD, etc.)</th>
<th>Law enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Media</td>
</tr>
</tbody>
</table>
Incidents and Breaches: The Executive Management Decision-Making Process In Higher Education

Planning Ahead

Sam Segran
Chief Information Officer
Texas Tech University

© TTU 2016
Proactive incident response – planning ahead

• Stakeholders
  – Identify key contacts
    o Establish communication processes ahead of time
    o Establish relationships ahead of time

• Incident response processes

• Communications templates

• Integration with DRP/BCP/institutional emergency management plan

• Cyber liability insurance (Risk Management)

• Training and awareness

• Periodic review
“Of course this website is safe. As an extra measure of security, they make you sign in with your Social Security number, mother’s name, your bank account, home address, phone number, and date of birth.”