Data Driven Security

Policy & Compliance

Steve Nyman
CISO, Dartmouth College
Who Really Cares?

• This is a college, not a corporation or the government. No one is targeting us.
  – Yes they are!
    • Economic Espionage....Russian Spy ring
      – Included a Microsoft employee
      – One spy targeted college prof
    • Thieves: financial info  (Russian mob: cleaned out account)
    • Data thieves: from China, accessing Library technical subscription svcs, using stolen accounts
  – Target of opportunity...stumble on a gold mine
    • For the challenge, fun, bragging rights, ??
    • Argentina....where no law exists against computer hacking
      – Took two years to prosecute following arrest
Surveillance on the streets of Argentina Pizza arrives, but where’s the Red Bull?
Inside the mind of a hacker

• Traced to subject from UK to Argentina within a few days
• A search warrant for subject’s apartment obtained within one week on grounds of theft of telephone service.
• All computers in entire apartment building seized. Neighbors not happy!!!
• Forensic review provided irrefutable evidence of attack
• Argentine courts dragged for over a year.
• Case resolved via a mediation settlement in lieu of prosecution
• Hacker interview
What went wrong?

• Attack occurred in 2003 during 2 yr transition to policy control environment. Compliance deadline was Jan 1, 2004.
• Merger brought in business units which were way out of compliance (password policy)
• Poorly organized and inadequate security patch management (especially for high risk data). Critical patch time- 5 weeks.
• After Jan 1, 2004, no major network intrusion, but virus problems due to patch delays.
• By end 2006, critical patch policy- 5 days.
Lucked Out

- Argentina attack could have been worse!
- Not very sophisticated, but smart enough
  - Hacker could have
    - taken down, defaced, altered, the web server
    - jumped to the backend database
    - stolen intellectual property
    - destroyed or tampered with data...FDA!!
    - transited the network for more targets
- A dedicated adversary would have done it all
Dartmouth Strategy to Mitigate Risk

• Formed DISC, March 2009
• DISC Develops
  – Policy and controls
  – Audit & compliance mechanism
  – Awareness campaigns
• Risk assessment: Information Management Modeling by each dept
  – Identify/protect the high risk info
Assessing Risk

• Impact of unauthorized:
  – Disclosure
  – Modification
  – Loss of availability

• Likelihood of a breach **attempt**
  ▪ 1: low (data not known or value is low)
  ▪ 2: medium (some aware of value and damage that could result from an attack)
  ▪ 3: high (widely known, obvious value/damage)
<table>
<thead>
<tr>
<th>Info Object</th>
<th>Owner</th>
<th>System</th>
<th>Risk Impact</th>
<th>Likelihood</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>D L M</td>
<td>D L M</td>
<td>C I A</td>
</tr>
<tr>
<td>Compensation</td>
<td>Nordberg</td>
<td>Oracle HRMS</td>
<td>2 3 2</td>
<td>3 3 3</td>
<td>2 3 2</td>
</tr>
<tr>
<td>Investment</td>
<td>Russ</td>
<td>EFS</td>
<td>3 2 2</td>
<td>3 1 1</td>
<td>3 1 1</td>
</tr>
<tr>
<td>Budget</td>
<td>Weinman</td>
<td>Oracle/ Hyperion</td>
<td>2 2 1</td>
<td>1 1 1</td>
<td>1 1 1</td>
</tr>
<tr>
<td>Actual</td>
<td>Goodness</td>
<td>Oracle GL/OGA</td>
<td>2 2 2</td>
<td>1 1 1</td>
<td>1 1 1</td>
</tr>
</tbody>
</table>

**Example of an Info Management Model**

**RISK SCALE (for illustrative purposes only)**

0- no impact

1- minimal impact, less than $1 M, little impact on reputation

2 - moderate impact, between $1M and $5M, may tarnish reputation

3- severe and potentially irreversible damage, over $5M, long lasting damage to reputation

Dartmouth College 2010
Join **Info Security Policy Objectives** with **IMM Info Objects** based on matching **Protection Levels**

<table>
<thead>
<tr>
<th>Dartmouth Control #</th>
<th>DARTMOUTH INFORMATION SECURITY CONTROL OBJECTIVES</th>
<th>Protection LEVEL</th>
<th>Type</th>
<th>ISO</th>
<th>HIPAA</th>
<th>PCI</th>
<th>MA 201 CMR 17</th>
<th>GLBA/FERPA</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Section 1</strong></td>
<td>SECURITY POLICY</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>Information Security policy must be approved by the Dartmouth Information Security Council (DISC), and published to the Dartmouth community, and relevant third parties. Policy must be reviewed at least annually.</td>
<td>1 1 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.3</td>
<td>Contracts with third parties which process Dartmouth information, must specify the information security requirements where appropriate, and these requirements will vary depending on the nature of the contract and the business conducted on behalf of Dartmouth by the third party.</td>
<td>1 1 1</td>
<td></td>
<td></td>
<td>164.308(a)(2)</td>
<td>12.1</td>
<td>17.03(1)</td>
<td>314.4(e)</td>
</tr>
<tr>
<td><strong>Section 7</strong></td>
<td>CORRECT PROCESSING IN APPLICATIONS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7.6</td>
<td>Application Developers must verify that changes to a system or application comply with regulatory requirements.</td>
<td>3 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Dartmouth College 2010
Immediate Risk Mitigation

• PGP full disk encryption
  – Windows and Mac
  – Operational pilot underway

• Identity Finder
  – Finds PII
  – Enterprise reporting of results
  – Operational pilot underway
Final Step

• Information Protection Plan
  – IMM + applicable controls
    • Many requirements will already be met by virtue of systems managed by Computing Services
  – Plan to implement utilizing IT services & manual process changes
  – Waivers for exceptions for specified period, typically no longer than 6 - 12 months.

• The IPP is reviewed annually and updated
• Waivers may be renewed after a review
• Audit for compliance
• Awareness/training to reinforce security with the community

Dartmouth College 2010