<table>
<thead>
<tr>
<th>System</th>
<th>Confidentiality</th>
<th>Integrity</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPSI Hospital Information System</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Exchange Server MV5000-1</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>EXT Old Hospital System with Records</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>NF3400-1 User Files, Accounting, and Encoder Software</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Pyxis Systems Pharmacy and Inventory</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Dictaphone Transcription System</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>E500 Appliance Virus Detection System</td>
<td>M</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>E800II Blood Gas system and Per se’ Billing System</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Chart Link System Physician Access thru SSL</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Linux System Undecided of use for now, still testing</td>
<td>L</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>JJJH2 Used for OWA and new helpdesk</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Panasonic Video Security System</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Rembrandt Sleep Lab System</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>
OCTAVE™

- Operationally Critical, Threat, Asset and Vulnerability Evaluation
  - Sort through complex organizational and technological issues
  - Defines an approach to information security risk evaluations
    - Comprehensive
    - Systematic
    - Context driven
    - Self-directed
- Self directed
  - Business and IT part of the team
- Three Phases
  - Build asset-based threat profiles
  - Identify infrastructure vulnerabilities
  - Develop security strategy and plans
<table>
<thead>
<tr>
<th>Threat Profile: System Problems</th>
<th>Patient Records System</th>
</tr>
</thead>
</table>

### Threats

- **Software defects**
  - Disclosure
  - Modification
  - Loss, Destruction
  - Interruption

- **Malicious Code**
  - Disclosure
  - Modification
  - Loss, Destruction
  - Interruption

- **System crashes**
  - Disclosure
  - Modification
  - Loss, Destruction
  - Interruption

- **Hardware defects**
  - Disclosure
  - Modification
  - Loss, Destruction
  - Interruption

### Threat Profile:

**Reputation**
- M M L M L

**Financial**
- M M M M H

**Productivity**
- M M L M L

**Fines**
- M M H M H

**Safety**
- M M H M H

**Other**
- M M H M H

### OCTAVE SM

Carnegie Mellon – Software Engineering Institute
### Human Actors Using Network Access

#### Basic Risk Profile

**Security Practice Areas**

<table>
<thead>
<tr>
<th>Probability</th>
<th>Sec Training</th>
<th>Sec Strategy</th>
<th>Sec Policy &amp; Reg</th>
<th>Coll Sec Mgmt</th>
<th>Cont Planning</th>
<th>Phys Acc Ctrl</th>
<th>Monitor Phys Sec</th>
<th>Sys &amp; Net Mgmt</th>
<th>Monitor IT Sec</th>
<th>Auth &amp; Author</th>
<th>Vul Mgmt</th>
<th>Encryption</th>
<th>Sec Arch &amp; Design</th>
<th>Incident Mgmt</th>
<th>Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very Much</td>
<td>R</td>
<td>R</td>
<td>Y</td>
<td>R</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>Accept</td>
</tr>
<tr>
<td>Somewhat</td>
<td>R</td>
<td>R</td>
<td>Y</td>
<td>R</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>x</td>
</tr>
<tr>
<td>Not At All</td>
<td>R</td>
<td>R</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>x</td>
</tr>
</tbody>
</table>

- **Accept**: Acceptance of risk.
- **Defer**: Deferral of risk.
- **Mitigate**: Mitigation of risk.

---

**OCTAVE℠**
Carnegie Mellon – Software Engineering Institute