Risk Mitigation & Incident Response
Week 12
Gartner’s Security Processes You Must Get Right

IT’s Responsibility
1. Change Management
2. Disaster Recovery & Business Continuity
3. Project Life Cycle Management
4. Vendor Management

Security’s Responsibility
1. Security Governance
2. Policy Management
3. Awareness & Education
4. Identity & Access Management
5. Vulnerability Management
6. Incident Response

IT Governance
Rich Flanagan
# Gartner’s Security Processes You Must Get Right

<table>
<thead>
<tr>
<th>Security’s Responsibility</th>
<th>IT’s Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Policy Management</td>
<td>2. Disaster Recovery &amp; Business Continuity</td>
</tr>
<tr>
<td>5. Vulnerability Management</td>
<td></td>
</tr>
<tr>
<td>6. Incident Response</td>
<td></td>
</tr>
</tbody>
</table>
Incident Response

1. Preparation
2. Detect and Expose
3. Triage
4. Classify and Contain
5. Remediate
6. Report and Post-Mortem
Incident Response

1. Preparation
2. Detect and Expose
3. Triage
4. Classify and Contain
5. Remediate
6. Report and Post-Mortem
The iPremier Case

• Take 30 minutes
• How well did the iPremier Company perform during the seventy-five minute attack? If you were Bob Turley, what might you have done differently during the attack?
• The iPremier Company CEO, Jack Samuelson, had already expressed to Bob Turley his concern that the company might eventually suffer from a “deficit in operating procedures.” Were the company’s operating procedures deficient in responding to this attack? What additional procedures might have been in place to better handle the attack?
• Now that the attack has ended, what can the iPremier Company do to prepare for another such attack?
• In the aftermath of the attack, what would you be worried about? What actions would you recommend?