Insider Threats: Your Questions. Our Answers

Randy Trzeciak
Dan Costa
Conducting research, modeling, analysis, and outreach to develop socio-technical solutions to combat insider threats.
The Insider Threat Defined

The potential for an individual who has or had authorized access to an organization’s assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.
Scope of the Insider Threat

Individuals
- Current or Former
- Full-Time Employees
- Part-Time Employees
- Temporary Employees
- Contractors
- Trusted Business Partners

Organization’s Assets
- People
- Information
- Technology
- Facilities

Intentionally or Unintentionally
- Fraud
- Theft of Intellectual Property
- Cyber Sabotage
- Espionage
- Workplace Violence
- Social Engineering
- Accidental Disclosure
- Accidental Loss or Disposal of Equipment or Documents

Negatively Affect the Organization
- Harm to Organization’s Employees
- Degradation of Confidentiality, Integrity, or Availability of Information or Systems
- Disruption of Organization’s Ability to Meet its Mission
- Damage to Organization’s Reputation
- Harm to Organization’s Customers

who have or had authorized access to
use that access
to act in a way that could
Insider Threat Mitigation

Insider Incident
- Prevent / Detect
- if detected
- Respond / Recover

Insider Threat
- Identify / Deter
- if detected
- Consistent Response

Insiders
- Not Alienate

Insider Threat Program
Goal for an Insider Threat Program

Opportunities for prevention, detection, and response for an insider attack
Key Components of an Insider Threat Program

- Organization-wide Participation
- Formalized and Defined Program
- Integration with Enterprise Risk Management
- Insider Threat Practices Related to Trusted Business Partners
- Prevention, Detection, and Response Infrastructure
- Insider Threat Training and Awareness
- Data Collection and Analysis Tools, Techniques, and Practices
- Confidential Reporting Procedures and Mechanisms
- Oversight of Program Compliance and Effectiveness
- Insider Threat Incident Response Plan
- Communication of Insider Threat Events
- Protection of Employee Civil Liberties and Privacy Rights
- Policies, Procedures and Practices to Support the InTP
<table>
<thead>
<tr>
<th></th>
<th>Recommended Best Practices for Insider Threat Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Know and protect your critical assets.</td>
</tr>
<tr>
<td>2</td>
<td>Develop a formalized insider threat program.</td>
</tr>
<tr>
<td>3</td>
<td>Clearly document and consistently enforce policies and</td>
</tr>
<tr>
<td></td>
<td>controls.</td>
</tr>
<tr>
<td>4</td>
<td>Beginning with the hiring process, monitor and respond</td>
</tr>
<tr>
<td></td>
<td>to suspicious or disruptive behavior.</td>
</tr>
<tr>
<td>5</td>
<td>Anticipate and manage negative issues in the work</td>
</tr>
<tr>
<td></td>
<td>environment.</td>
</tr>
<tr>
<td>6</td>
<td>Consider threats from insiders and business partners in</td>
</tr>
<tr>
<td></td>
<td>enterprise-wide risk assessments.</td>
</tr>
<tr>
<td>7</td>
<td>Be especially vigilant regarding social media.</td>
</tr>
<tr>
<td>8</td>
<td>Structure management and tasks to minimize unintentional</td>
</tr>
<tr>
<td></td>
<td>insider stress and mistakes.</td>
</tr>
<tr>
<td>9</td>
<td>Incorporate malicious and unintentional insider threat</td>
</tr>
<tr>
<td></td>
<td>awareness into periodic security training for all</td>
</tr>
<tr>
<td></td>
<td>employees.</td>
</tr>
<tr>
<td>10</td>
<td>Implement strict password and account management</td>
</tr>
<tr>
<td></td>
<td>policies and practices.</td>
</tr>
<tr>
<td>11</td>
<td>Institute stringent access controls and monitoring</td>
</tr>
<tr>
<td></td>
<td>policies on privileged users.</td>
</tr>
<tr>
<td>12</td>
<td>Deploy solutions for monitoring employee actions and</td>
</tr>
<tr>
<td></td>
<td>correlating information from multiple data sources.</td>
</tr>
<tr>
<td>13</td>
<td>Monitor and control remote access from all endpoints,</td>
</tr>
<tr>
<td></td>
<td>including mobile devices.</td>
</tr>
<tr>
<td>14</td>
<td>Establish a baseline of normal behavior for both</td>
</tr>
<tr>
<td></td>
<td>networks and employees.</td>
</tr>
<tr>
<td>15</td>
<td>Enforce separation of duties and least privilege.</td>
</tr>
<tr>
<td>16</td>
<td>Define explicit security agreements for any cloud</td>
</tr>
<tr>
<td></td>
<td>services, especially access restrictions and monitoring</td>
</tr>
<tr>
<td></td>
<td>capabilities.</td>
</tr>
<tr>
<td>17</td>
<td>Institutionalize system change controls.</td>
</tr>
<tr>
<td>18</td>
<td>Implement secure backup and recovery processes.</td>
</tr>
<tr>
<td>19</td>
<td>Close the doors to unauthorized data exfiltration.</td>
</tr>
<tr>
<td>20</td>
<td>Develop a comprehensive employee termination procedure.</td>
</tr>
<tr>
<td>21</td>
<td>Adopt positive incentives to align the workforce with</td>
</tr>
<tr>
<td></td>
<td>the organization.</td>
</tr>
</tbody>
</table>

http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=540644 or search "cert common sense guide insider threat"
CERT Insider Threat Portfolio

Awareness
- Common Sense Guide to Mitigating Insider Threats
- Insider Threat Blog
- Insider Threat Awareness Training
- Industry-Specific Studies
- Threat Applicability Studies

Evaluation
- Insider Threat Vulnerability Assessment
- Insider Threat Program Evaluation
- Insider Threat Self-Assessment

Assistance
- Insider Threat Program Building
  - Planning
  - Stakeholder Identification
  - Achieving Executive Support
  - Risk Management Integration
  - Governance and Policy Development
  - Communication Plan Development

Support
- Control Development and Measurement
- Indicator Development and Measurement
- Hub Architecture and Design
- Sentiment and Linguistic Analysis
- Insider Incident Management
- Insider Threat Tool Evaluation
- Metrics Development

Transition
- Executive Workshop
- Team Workshop
- Program Building Facilitated Workshop
- Insider Threat Program Manager Certificate
- Insider Threat Vulnerability Assessor Certificate
- Insider Threat Program Evaluator Certificate
- Insider Threat Analyst Training

Insider Threat Stewardship

- Insider Incident Collection and Analysis
- Ontology Development and Maintenance
- Modeling and Simulation
- Customized Research
- Mitigation Pattern Language
- Exploration
Agenda