Relating Insider Cyber Sabotage and Workplace Violence

Dan Costa, Technical Manager, Enterprise Threat and Vulnerability Management | CERT Division
dlcosta@sei.cmu.edu
Insider Threat Research at the SEI

Conducting data collection, modeling, analysis, and outreach to develop socio-technical solutions to combat insider threats.

Splunk Query Name: Last 30 Days - Possible Theft of IP
Terms: 'host=HECTOR' [search host="zeus.corp.merit.lab" Message="A user account was disabled. " | eval Account_Name=mvindex(Account_Name, -1) | fields Account_Name | strcat Account_Name "@corp.merit.lab" sender_address | fields - Account_Name total_bytes > 50000 AND recipient_address="*" | fields client_ip, sender_address, recipient_address, message_subject, total_bytes]
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
The Critical Path to Insider Risk

Insider IT Sabotage Overview

**Background**

*Insider IT sabotage:* insider incidents in which the insider uses information technology to direct specific harm at an organization or individual.

**Motivations:** revenge, primarily in response to a negative work-related event such as a demotion, transfer, dispute with a co-worker, or termination.

**Incident progression:** an insider’s unmet expectations (pay, promotion, workload, etc.), combined with personal predispositions (history of rule violations, coworker conflicts, etc.), may lead to disgruntlement. Disgruntled insiders may begin to exhibit behavioral precursors (decline in work performance / attendance, etc.), which may be discovered by the organization, who in turn imposes sanctions. Sanctions can lead to increased disgruntlement, pushing an insider down the path to an incident. Technical precursors follow, including setting up unknown access paths to conceal activity. Without sufficient technical and behavioral monitoring, the organization’s perceived risk of an insider attack may be lower than the actual risk. This can lead to an organization over-trusting an insider, which in combination with decreased monitoring, can impair the organization’s ability to detect an attack.

**Associated Potential Risk Indicators**

<table>
<thead>
<tr>
<th>Personal Predispositions</th>
<th>Stressors</th>
<th>Concerning Behaviors</th>
<th>Harmful Act</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Co-worker conflicts</td>
<td>Sudden decline in job performance or work attendance</td>
<td>Unauthorized modification or deletion of critical system configurations</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Unauthorized modification or deletion of logs or backups</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Creating and using backdoor, shared, non-attributable, and unauthorized accounts</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Downloading and installing malicious code and / or hacking tools</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tampering with, disabling, or attempting to disable security controls</td>
</tr>
</tbody>
</table>

**Risk Model**

**Applicable Data Sources**

<table>
<thead>
<tr>
<th>Account creation logs</th>
<th>Identity management systems</th>
<th>Change and configuration management systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intrusion detection / prevention systems</td>
<td>User activity monitoring</td>
<td>Backup system access logs</td>
</tr>
<tr>
<td>Confidential / anonymous reporting systems</td>
<td>Human resource management systems</td>
<td>Employee performance management systems</td>
</tr>
</tbody>
</table>
Workplace Violence and Insider Cyber Sabotage: Two Sides of the Same Coin?

- Hostile Act
  - Active shooter
- Problematic Organizational Responses
  - Loss/Suspension of Rights and Privileges
  - Verbal threats to cause physical harm
- Concerning Behaviors
  - Perceived harassment by coworkers
- Stressors
  - Resolving conflict by physical means
- Personal Predispositions
  - Hacker
  - Lack of resources to do job well
  - Visiting internet underground
  - Demotion without changing access
  - Execution of malicious code
Hypothesis: Common Path Before Divergence
If Correct, So What?

- Cost savings in controls
- Better risk models
- Increased value for cross-organization collaboration
Insider Harm to Others Overview
Stressors by ICS and WPV
Findings
## Best Practices for Insider Threat Mitigation

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>Know and protect your critical assets.</td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>Develop a formalized insider threat program.</td>
</tr>
<tr>
<td><strong>3</strong></td>
<td>Clearly document and consistently enforce policies and controls.</td>
</tr>
<tr>
<td><strong>4</strong></td>
<td>Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.</td>
</tr>
<tr>
<td><strong>5</strong></td>
<td>Anticipate and manage negative issues in the work environment.</td>
</tr>
<tr>
<td><strong>6</strong></td>
<td>Consider threats from insiders and business partners in enterprise-wide risk assessments.</td>
</tr>
<tr>
<td><strong>7</strong></td>
<td>Be especially vigilant regarding social media.</td>
</tr>
<tr>
<td><strong>8</strong></td>
<td>Structure management and tasks to minimize unintentional insider stress and mistakes.</td>
</tr>
<tr>
<td><strong>9</strong></td>
<td>Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.</td>
</tr>
<tr>
<td><strong>10</strong></td>
<td>Implement strict password and account management policies and practices.</td>
</tr>
<tr>
<td><strong>11</strong></td>
<td>Institute stringent access controls and monitoring policies on privileged users.</td>
</tr>
<tr>
<td><strong>12</strong></td>
<td>Deploy solutions for monitoring employee actions and correlating information from multiple data sources.</td>
</tr>
<tr>
<td><strong>13</strong></td>
<td>Monitor and control remote access from all endpoints, including mobile devices.</td>
</tr>
<tr>
<td><strong>14</strong></td>
<td>Establish a baseline of normal behavior for both networks and employees.</td>
</tr>
<tr>
<td><strong>15</strong></td>
<td>Enforce separation of duties and least privilege.</td>
</tr>
<tr>
<td><strong>16</strong></td>
<td>Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.</td>
</tr>
<tr>
<td><strong>17</strong></td>
<td>Institutionalize system change controls.</td>
</tr>
<tr>
<td><strong>18</strong></td>
<td>Implement secure backup and recovery processes.</td>
</tr>
<tr>
<td><strong>19</strong></td>
<td>Close the doors to unauthorized data exfiltration.</td>
</tr>
<tr>
<td><strong>20</strong></td>
<td>Develop a comprehensive employee termination procedure.</td>
</tr>
<tr>
<td><strong>21</strong></td>
<td>Adopt positive incentives to align the workforce with the organization.</td>
</tr>
</tbody>
</table>

---

**URL:** [http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=540644](http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=540644)
A Holistic Approach to Insider Risk Management

- Formalized and Defined Insider Risk Management Program (IRMP)
- Organization-Wide Participation
- Oversight of Program Compliance and Effectiveness
- Confidential Reporting Procedures and Mechanisms
- Insider Threat Incident Response Plan
- Communication of Insider Threat Events
- Protection of Workforce Member Civil Liberties and Privacy Rights
- Integration with Enterprise Risk Management
- Practices Related to Managing Trusted External Entities (TEEs)
- Prevention, Detection, and Response Infrastructure
- Insider Threat Training and Awareness
- Data Collection and Analysis Tools, Techniques, and Practices
- IRMP Policies, Procedures, and Practices
- Positive Incentives
For More Information

- *The Common Sense Guide to Mitigating Insider Threats, Sixth Edition*
- *Balancing Organizational Incentives to Counter Insider Threat*
- *Navigating the Insider Threat Tool Landscape: Low-Cost Technical Solutions to Jump-Start an Insider Threat Program*
- *Insider Threats Across Industry Sectors*
- *Insider Threat Program Manager Certificate*
- *Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls*
- *Analytic Approaches to Detect Insider Threats*
- *Workplace Violence & IT Sabotage: Two Sides of the Same Coin?*
Questions / Discussion