Insider Threat Mitigation Strategies that Protect Privacy and Civil Liberties

Randy Trzeciak
Document Markings

Copyright 2019 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

DM19-0940
Randall (Randy) Trzeciak

Software Engineering Institute; CERT Division; Cyber Risk and Resilience Directorate
Director National Insider Threat Center

Heinz College; School of Information Systems & Management
Program Director: MS Information Security Policy & Management
CERT Faculty
What is the National Insider Threat Center?
TheCERTNationalInsiderThreatCenter-1

Center of insider threat expertise

Began working in this area in 2001 with the U.S. Secret Service

Mission: enable effective insider threat mitigation, incident management practices, and develop capabilities for deterring, detecting, and responding to evolving cyber and physical threats

Action and Value: conduct research, modeling, analysis, and outreach to develop & transition socio-technical solutions to combat insider threats
SEI/CERT/NITC: Leader in Insider Threat Research

We possess a unique combination of

• empirical evidence
• modeling and simulation expertise
• software engineering expertise
• cybersecurity expertise
• DoD mission space knowledge
• data science expertise
• collaborative research relationships with a cadre of multidisciplinary experts in social and behavioral sciences

Our focus on developing repeatable, verifiable, and context-aware processes and preventative controls is a key differentiator between our applied research and system integrators.
Operational Research Capabilities

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=indexOf(Account_Name, "-t") | fields Account_Name | strsub(Account_Name, "+corp.merit.lab" sender_address | fields - Account_Name) total_bytes > 50000 AND recipient_address=""|"corp.merit.lab" startDayago=30 | fields client_ip, sender_address, recipient_address, message_subject, total_bytes"
CERT’s Critical Path to Insider Risk

**Personal Predispositions**
- Medical / Psychiatric Conditions
- Personal or Social Skills
- Previous Rule Violations
- Social Network Risks

**Stressors**
- Personal
- Professional
- Financial

**Concerning Behaviors**
- Interpersonal
- Technical
- Security
- Financial

**Problematic Organization Responses**
- Inattention
- No risk assessment process
- Inadequate investigation
- Summary dismissal or other actions that escalate risk

Source: Shaw, Sellers (2015); Carnegie Mellon University (2006 - Present)
Insider Incident Types (not exhaustive)

National Security Espionage

IT System Sabotage

Theft of IP – Entitled Independent

Espionage / Sabotage

Fraud

Theft of IP – Ambitious Leader
Recent Publications
Recent Publications

• Insider Threat Blog
  Patterns and Trends in Insider Threat Across Sectors (9 part series)
  Improving Insider Threat Detection Methods Through Software Engineering Principles
  High-Level Technique for Insider Threat Program's Data Source Selection
  Windows Event Logging for Insider Threat Detection

• Common Sense Guide to Mitigating Insider Threats, Sixth Edition

• Navigating the Insider Threat Tool Landscape: Low-Cost Technical Solutions to Jump-Start an Insider Threat Program

• The Critical Role of Positive Incentives for Reducing Insider Threats

• Analytic Approaches to Detect Insider Threats

• Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls
Best Practices for Mitigation of Insider Threats
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
- Communication of Insider Threat Events
- Confidential Reporting Procedures and Mechanisms
- Insider Threat Incident Response Plan
- Protection of Employee Civil Liberties and Privacy Rights
- Policies, Procedures and Practices to Support the InTP
## Recommended Best Practices for Insider Threat Mitigation

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></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 controls.</td>
</tr>
<tr>
<td>4</td>
<td>Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.</td>
</tr>
<tr>
<td>5</td>
<td>Anticipate and manage negative issues in the work environment.</td>
</tr>
<tr>
<td>6</td>
<td>Consider threats from insiders and business partners in 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 insider stress and mistakes.</td>
</tr>
<tr>
<td>9</td>
<td>Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.</td>
</tr>
<tr>
<td>10</td>
<td>Implement strict password and account management policies and practices.</td>
</tr>
<tr>
<td>11</td>
<td>Institute stringent access controls and monitoring policies on privileged users.</td>
</tr>
<tr>
<td>12</td>
<td>Deploy solutions for monitoring employee actions and correlating information from multiple data sources.</td>
</tr>
<tr>
<td>13</td>
<td>Monitor and control remote access from all endpoints, including mobile devices.</td>
</tr>
<tr>
<td>14</td>
<td>Establish a baseline of normal behavior for both 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 services, especially access restrictions and monitoring 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 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"](http://resources.sei.cmu.edu/library/asset-view.cfm?assetId=540644)
Open Source Insider Threat (OSIT) Information Sharing Group
Open Source Insider Threat (OSIT) Information Sharing Group

Community of Interest for insider threat program practitioners across industry organizations

Over 400 members from ~155 organizations

Special Interest Groups
- Banking / Finance
- Data Analytics
- Privacy

Monthly Telecons
- Tool Vendor Demos

Bi-annual In-Person Meetings
- Hosted by various members of the group

To join, contact: rft@cert.org
For More Information

National Insider Threat Center website
http://www.cert.org/insider-threat/

National Insider Threat Blog
https://insights.sei.cmu.edu/insider-threat/

Randall F. Trzeciak
Director – National Insider Threat Center
CERT Division / Software Engineering Institute
412.268.7040
rft@cert.org