Insider Threat Risk Management

Bheshaj Krishnappa
Program Manager, Resilience and Risk

RELIABILITY FIRST
Texas Reliability Entity, Inc. (Texas RE) strictly prohibits persons participating in Texas RE activities from using their participation as a forum for engaging in practices or communications that violate antitrust laws. Texas RE has approved antitrust guidelines available on its web site. If you believe that antitrust laws have been violated at a Texas RE meeting, or if you have any questions about the antitrust guidelines, please contact the Texas RE General Counsel.
Insider Threat Risk Management

Bheshaj Krishnappa
Program Manager, Resilience & Risk
Certified Insider Threat Program Evaluator
October 29, 2020
Insider Threat Risk Management – Building a culture of preparedness through awareness and best practices

- Industry of 3,200 utilities, employs over 400,000 employees, 7,677 Power Plants, 55,000 Sub-stations, 450,000 miles of transmission. (Scott Wilson, DOE)
A malicious insider is a current or former employee, contractor, or other business partner who:

- has or had **authorized access** to an organization’s network, system or data [or facilities] and,

- intentionally **exceeded or misused** that access in a manner that…

- **negatively affected** the confidentiality, integrity, or availability of the organization’s information or information systems [and facilities].
The chart represents 929 total cases of fraud, sabotage, and theft of IP. Source: SEI CERT/CMU (2018)

Unintentional Insider Threat as a threat vector?
Insider Threat Incident Types in Utilities

Source: Insider Threat Trends in Utilities Sector. CERT SEI CMU, 2020
Actor Motivations within Insider Privilege and Misuse Breaches (2014-2018)

Source: https://enterprise.verizon.com/resources/reports/insider-threat-report.pdf
Unmet Expectations Observed in Cases

➢ Salary/bonus/promotion
➢ Freedom of online actions
➢ Work ethic
➢ Overestimated abilities
➢ Access to information following termination
➢ Use of company resources
➢ Job dissatisfaction
➢ Supervisor demands
➢ Coworker relations
➢ Responsibilities

Source: SEI CERT/CMU
Insider Threat Focus for Utilities

➢ Insider Sabotage
  • An insider’s use of IT or facilities to direct specific harm at an organization or individual by:
    – deletion of information
    – bringing down systems/facilities

➢ Unintentional Insider Threat (UIT)
  • A current or former employee, contractor, or other business partner who:
    – has or had authorized access to an organization’s network, system, data [or facilities] and,
    – who through their action/inaction without malicious intent causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization’s information or information systems [or facilities]

Source: SEI CERT/CMU
A subcontractor at an energy management facility breaks the glass enclosing the emergency power button, and then shuts down computers that regulate the exchange of electricity between power grids. This happened despite the fact that his own employer had disabled his access to their own facility following a dispute.

- **Potential Impact**: Internal power outage; Shutdown of electricity between the power grids in the US

Source: SEI CERT/CMU
Insider Threat Sabotage

- Usually involves the most technical or sophisticated types of attacks
- Is usually committed by more technical staff, such as systems and network/database administrators, or similar types of staff
- Is usually done for revenge or in response to perceived wrongs or unmet expectations
- Is often performed by employees who have had previously observed events where they were clearly disgruntled
- Can potentially be identified and mitigated by noticing the technical and behavioral precursors and acting on it
- Can also be prevented by ensuring good information assurance practices are in place along with good human resource and physical security policies and practices

Source: SEI CERT/CMU
1 in 5 jobs in America are held by a worker under contract.  

NPR/Marist poll, 2018

NPR Poll - Key Findings:

• **20%** of all American workers are contract workers (hired to work on a specific project or for a fixed period of time)

• **51%** of contract workers do not receive benefits from their jobs

• **49%** of contract workers have income that varies greatly from month-to-month or seasonally

• **65%** of contract workers are male and **62%** are under 45 years of age
Source: 2020 Verizon Data Breach Investigations Report
Top Enablers for Insider Attacks

This is the first year that the Privilege Misuse pattern is not in the top three overall. In the 2019 report, Privilege Misuse at 23% of attacks, while in 2020, it has dropped to just 8.7%. (DBIR 2020)
Access Misuse

➢ Analysis of information from work-issued endpoints and 300,000 employee and contractor accounts reveal exposing confidential and sensitive information online and in the cloud (Dropbox, Google, and Microsoft SharePoint) in some 98% of organizations.

➢ Assessments detected an increase of 10% over 2018 of employees and contractors transferring confidential and sensitive data via unencrypted USB drives, personal email accounts, and cloud applications.

48% vs. 15%
The number of employees that are required to seek permission for external USB use… and the number that actually ask for permission.

Up 91%
Employees using personal, web-based email on company endpoints - up from 91% last year.

Source: Dtex Systems 2019 Insider Threat Intelligence Report
Remote Working Challenges

56%

**HIDE & SEEK**
Companies with remote workers intentionally circumventing security controls to mask online activity

450% increase from previous years

Over 70% of escalated incidents also included at least one attempt to circumvent another security control in order to exfiltrate data without detection

72%

**GIVE AND TAKE**
Companies with data theft by a leaving or joining employee

230% increase over previous years

Over 40% of incidents detected included a combination of flight risk and abnormal reconnaissance and/or data aggregation behaviors

Source: https://www2.dtexsystems.com/2020-Insider-Threat-Report
Often, an elicitee has some of these characteristics:

- Desire to appear well-informed
- Tendency to gossip
- Desire to be appreciated and show they have something to contribute
- Tendency to correct others
- Believes others are honest
- Is prone to showing off

On the other side of the equation, an elicitor tends to have these characteristics:

- Pretends to know of associations in common with the elicitee
- Feigns ignorance of a topic
- Exploits the elicitee’s instinct to complain or brag
- Uses flattery and appreciation as psychological tools
- Obliquely introduces topics in order to gain insight
- Deliberately says something wrong, hoping the elicitee will offer a correction

Source: Verizon Insider Threat Report
Organizations need to consider the many potential issues involving working conditions in creating an environment that is supportive to employees/contractors (such as adequate reward and recognition).

Improving workplace resiliency

Just as training employees helps to build confidence, so does recognition of performance. Thus, one of the most direct ways to increase resiliency is to build people up by recognizing them for their work. The act of thanking employees and acknowledging quality work helps create a positive and productive environment - in effect, the opposite of a hostile workplace. (Building a Hostility-Free Workplace, Raquella Solon)


- A comprehensive report containing assessment summary analysis, areas for improvement, resources to improve the program, benchmarking, etc.

Entity/User data is protected to maintain confidentiality and integrity.

Tool security
- Securely hosted in RF at https://insiderthreat.rfirst.org
- Data is encrypted at storage and transit
- Multifactor authentication and stringent password policy

Available to all entities in the RF footprint for free!
<table>
<thead>
<tr>
<th>Practice Area</th>
<th>Maturity Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Know and protect your critical assets</td>
<td>1 2 1 4 2,75</td>
</tr>
<tr>
<td>Develop a formalized insider threat program</td>
<td>1 4 2 1</td>
</tr>
<tr>
<td>Clearly document and consistently enforce policies and controls</td>
<td>1 2 2 2 5</td>
</tr>
<tr>
<td>Hiring process, monitor and respond to suspicious or disruptive behavior</td>
<td>2 21.8 1 5</td>
</tr>
<tr>
<td>Anticipate and manage negative issues in the work environment</td>
<td>2 1.8 1 5</td>
</tr>
<tr>
<td>Consider threats from insiders and business partners in enterprise wide risk assessments</td>
<td>3 1.75 1 9 12</td>
</tr>
<tr>
<td>Be especially vigilant regarding social media</td>
<td>2 1.67 4</td>
</tr>
<tr>
<td>Structure management and tasks to minimize insider stress and mistakes</td>
<td>2 1.67 4 5</td>
</tr>
<tr>
<td>Incorporate malicious and UIT awareness into periodic security training</td>
<td>2 1.67 5</td>
</tr>
<tr>
<td>Implement strict password and account management policies and Ps</td>
<td>1 4 2 14 2 7</td>
</tr>
<tr>
<td>Institute stringent access controls and monitoring policies on privileged users</td>
<td>1 2 1.67</td>
</tr>
<tr>
<td>Solutions for monitoring employee actions and correlating information from multiple sources</td>
<td>1 2 1.67</td>
</tr>
<tr>
<td>Monitor and control remote access from all end points, including mobile devices</td>
<td>2 1.674 6</td>
</tr>
<tr>
<td>Establish a baseline of normal behavior for both networks and employees</td>
<td>2 1.66 1 7</td>
</tr>
<tr>
<td>Enforce separation of duties and least privilege</td>
<td>2 1.6 4</td>
</tr>
<tr>
<td>Define explicit security agreements for any cloud services</td>
<td>4 2 2 4</td>
</tr>
<tr>
<td>Institutionalize system change controls</td>
<td>1 2 1.67</td>
</tr>
<tr>
<td>Implement secure backup and recovery processes</td>
<td>1 3 1.75 4</td>
</tr>
<tr>
<td>Close the doors to unauthorized data exfiltration</td>
<td>1 2 2 1 5 7</td>
</tr>
<tr>
<td>Develop a comprehensive employee termination procedure</td>
<td>1 2 2.55 4</td>
</tr>
<tr>
<td>Adopt positive incentives to align the workforce with the organization</td>
<td>1 3 1.75 4</td>
</tr>
</tbody>
</table>

**Maturity Level:**
- **Not Implemented**
- **Partially Implemented**
- **Largely Implemented**
- **Fully Implemented**
- **Maturity Level**
## Practice Area Heatmap

### Assessment - Entity A

#### Insider Threat Program Checklists of Quick Wins and High-Impact Solutions

<table>
<thead>
<tr>
<th>Practice Area</th>
<th>Recommendation</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Know and protect your critical assets</td>
<td>Incorporate malicious and UIT awareness into periodic security training</td>
<td>1.60 (Partially Implemented)</td>
</tr>
<tr>
<td>2.75 (Largely Implemented)</td>
<td>1.00 (Not Implemented)</td>
<td></td>
</tr>
<tr>
<td>Develop a formalized insider threat program</td>
<td>Monitor and control remote access from all end points, including mobile devices</td>
<td>1.67 (Partially Implemented)</td>
</tr>
<tr>
<td>2.00 (Partially Implemented)</td>
<td>Establish a baseline of normal behavior for both networks and employees</td>
<td>1.86 (Partially Implemented)</td>
</tr>
<tr>
<td>Clearly document and consistently enforce policies and controls</td>
<td>Enforce separation of duties and least privilege</td>
<td>1.50 (Partially Implemented)</td>
</tr>
<tr>
<td>2.20 (Partially Implemented)</td>
<td>Close the doors to unauthorized data exfiltration</td>
<td></td>
</tr>
<tr>
<td>Be especially vigilant regarding social media</td>
<td>Define explicit security agreements for any cloud services</td>
<td></td>
</tr>
<tr>
<td>1.50 (Partially Implemented)</td>
<td>Implement secure backup and recovery processes</td>
<td>1.75 (Partially Implemented)</td>
</tr>
<tr>
<td>Institute stringent access controls and monitoring policies on privileged users</td>
<td>2.00 (Partially Implemented)</td>
<td></td>
</tr>
<tr>
<td>1.67 (Partially Implemented)</td>
<td>Institutionalize system change controls</td>
<td></td>
</tr>
<tr>
<td>Structure management and tasks to minimize insider stress and mistakes</td>
<td>Develop a comprehensive employee termination procedure</td>
<td>2.50 (Largely Implemented)</td>
</tr>
<tr>
<td>1.80 (Partially Implemented)</td>
<td>Adopt positive incentives to align the workforce with the organization</td>
<td>1.75 (Partially Implemented)</td>
</tr>
<tr>
<td>1.60 (Partially Implemented)</td>
<td>Solutions for monitoring employee actions and correlating information from multiple sources</td>
<td>1.67 (Partially Implemented)</td>
</tr>
<tr>
<td>1.67 (Partially Implemented)</td>
<td>Consider threats from insiders and business partners in enterprise wide risk assessments</td>
<td>1.75 (Partially Implemented)</td>
</tr>
<tr>
<td>2.14 (Partially Implemented)</td>
<td>Implement strict password and account management policies and Ps</td>
<td></td>
</tr>
<tr>
<td>2.00 (Partially Implemented)</td>
<td>Institute stringent access controls and monitoring policies on privileged users</td>
<td>1.67 (Partially Implemented)</td>
</tr>
<tr>
<td>1.60 (Partially Implemented)</td>
<td>Incorporate malicious and UIT awareness into periodic security training</td>
<td>1.60 (Partially Implemented)</td>
</tr>
<tr>
<td>1.00 (Not Implemented)</td>
<td>Monitor and control remote access from all end points, including mobile devices</td>
<td>1.67 (Partially Implemented)</td>
</tr>
<tr>
<td>1.86 (Partially Implemented)</td>
<td>Establish a baseline of normal behavior for both networks and employees</td>
<td>1.86 (Partially Implemented)</td>
</tr>
<tr>
<td>1.50 (Partially Implemented)</td>
<td>Enforce separation of duties and least privilege</td>
<td>1.50 (Partially Implemented)</td>
</tr>
<tr>
<td>Close the doors to unauthorized data exfiltration</td>
<td>Define explicit security agreements for any cloud services</td>
<td></td>
</tr>
<tr>
<td>2.00 (Partially Implemented)</td>
<td>Implement secure backup and recovery processes</td>
<td>1.75 (Partially Implemented)</td>
</tr>
<tr>
<td>1.75 (Partially Implemented)</td>
<td>Institutionalize system change controls</td>
<td></td>
</tr>
<tr>
<td>2.00 (Partially Implemented)</td>
<td>Develop a comprehensive employee termination procedure</td>
<td>2.50 (Largely Implemented)</td>
</tr>
<tr>
<td>1.75 (Partially Implemented)</td>
<td>Adopt positive incentives to align the workforce with the organization</td>
<td>1.75 (Partially Implemented)</td>
</tr>
</tbody>
</table>
Areas of Improvement

Anticipate and manage negative issues in the work environment

<table>
<thead>
<tr>
<th>Group Level 3</th>
<th>Description</th>
<th>Maturity Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Practice Area 5.1</td>
<td>My organization uses enhanced monitoring of employees with an impending or ongoing personnel issue, in accordance with organizational policy and laws. Enable additional auditing and monitoring controls outlined in policies and procedures. Regularly review audit logs to detect activities outside of the employee's normal scope of work. Limit access to these log files to those with a need to know.</td>
<td>1.00</td>
</tr>
<tr>
<td>Practice Area 5.2</td>
<td>My organization at all levels of management regularly communicates organizational changes to all employees. This allows for a more transparent organization, and employees can better plan for their future.</td>
<td>1.00</td>
</tr>
</tbody>
</table>
Benchmarking Performance

2020~Aggregated View  2019~Assessment
Resources

➢ Common Sense Guide to Mitigating Insider Threats, Sixth Edition – (free download)
   • https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=540644

➢ CERT Insider Threat Program Evaluator/Manager or Insider Threat Vulnerability Assessor Certificate
   • https://www.sei.cmu.edu/education-outreach/credentials/

➢ Center for Development of Security Excellence
   • https://securityawareness.usalearning.gov/itawareness/index.htm

➢ Vigilance Campaign Materials
   • https://www.cdse.edu/toolkits/insider/vigilance.html

➢ Insider Threat Toolkit
   • https://www.cdse.edu/toolkits/insider/index.php

➢ Insider Threat to Cyber Security – Kate Randall, FBI Insider Threat Analyst (example of using narcissism as a potential indicator among FBI special agents)

➢ Insider Threats: Your Questions. Our Answers
   • https://www.youtube.com/watch?v=w_LamZooELM

➢ Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls
   • https://resources.sei.cmu.edu/asset_files/WhitePaper/2015_019_001_446379.pdf

➢ RF Insider Threat Newsletter series
   https://rfirst.org/about/Newsroom/Newsroom%20Library/Issue%201%20Jan%2020Feb%202019.pdf
Not every organization has resources for a full fledged InTP.
• Awareness, training and posters can help.
How Can CIP Help?

➢ **CIP-003-6 R1 Cyber Security - Security Management Controls** requires entities to document and implement cyber security policies that collectively address physical and cyber security of critical assets, access controls, and information protection.

➢ **CIP-004-6 R3 Cyber Security - Personnel & Training** requires Personnel Risk Assessments (PRA) for all personnel requiring access to cyber or physical BES assets. This ensures personnel are properly vetted before they are granted access to facilities and data.

➢ **CIP-005-5 Table R1 P1.5 - Cyber Security - Electronic Security Perimeter(s)** requires entities to implement methods for detecting known or suspected malicious communications for both inbound and outbound communications.

➢ **CIP-006-5 Table R1 P 1.4 - Cyber Security - Physical Security of BES Cyber Systems** requires entities to implement a solution to monitor unauthorized physical access into a Physical Security Perimeter.

➢ **CIP-007-5 Table R4 Cyber Security - System Security Management** requires entities to log and generate alerts for successful or failed access attempts and failed login attempts along with detecting malicious code.
Other RF Projects

➢ **Cyber Resilience Assessment tool**: qualitative web-based self-assessment tool based on users’ understanding of resilience categories
  - Hosted in RF at [https://resilience.rfirst.org](https://resilience.rfirst.org)
  - Operational Resilience COP

➢ **RF IMPACT Tool**: qualitative web-based self-assessment tool based on 17 management practices tailored specifically to the electric utility industry
  - Hosted in RF at [https://camp.rfirst.org](https://camp.rfirst.org)

➢ **Exercise Master Planner Database**: Conduct incident response preparedness test whenever needed

➢ **ERO Insider Threat Task Force/COP**
Please visit the www.rfirst.org Contact Us page and choose Resilience from the list of Areas.
Questions & Answers