Carnegie Mellon University
Software Engineering Institute

Insider Threats: Your Questions. Our Answers

Randy Trzeciak

Dan Costa

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

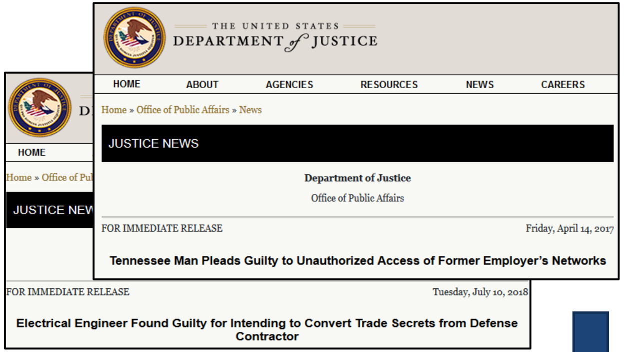
This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

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.

DM19-0940

The CERT National Insider Threat Center



THE UNITED STATES DEPARTMENT of JUSTICE

HOME ABOUT AGENCIES RESOURCES NEWS CAREERS

Home » Office of Public Affairs » News

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE Friday, April 14, 2017

Tennessee Man Pleads Guilty to Unauthorized Access of Former Employer's Networks

D

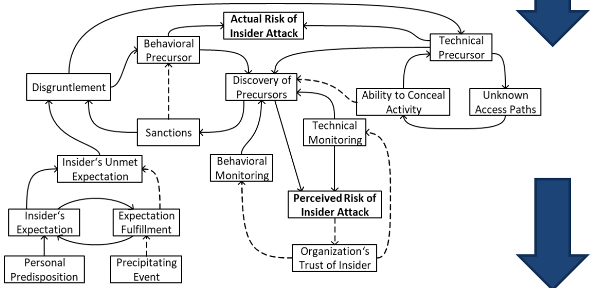
HOME

Home » Office of Pu

JUSTICE NEV

FOR IMMEDIATE RELEASE Tuesday, July 10, 2018

Electrical Engineer Found Guilty for Intending to Convert Trade Secrets from Defense Contractor



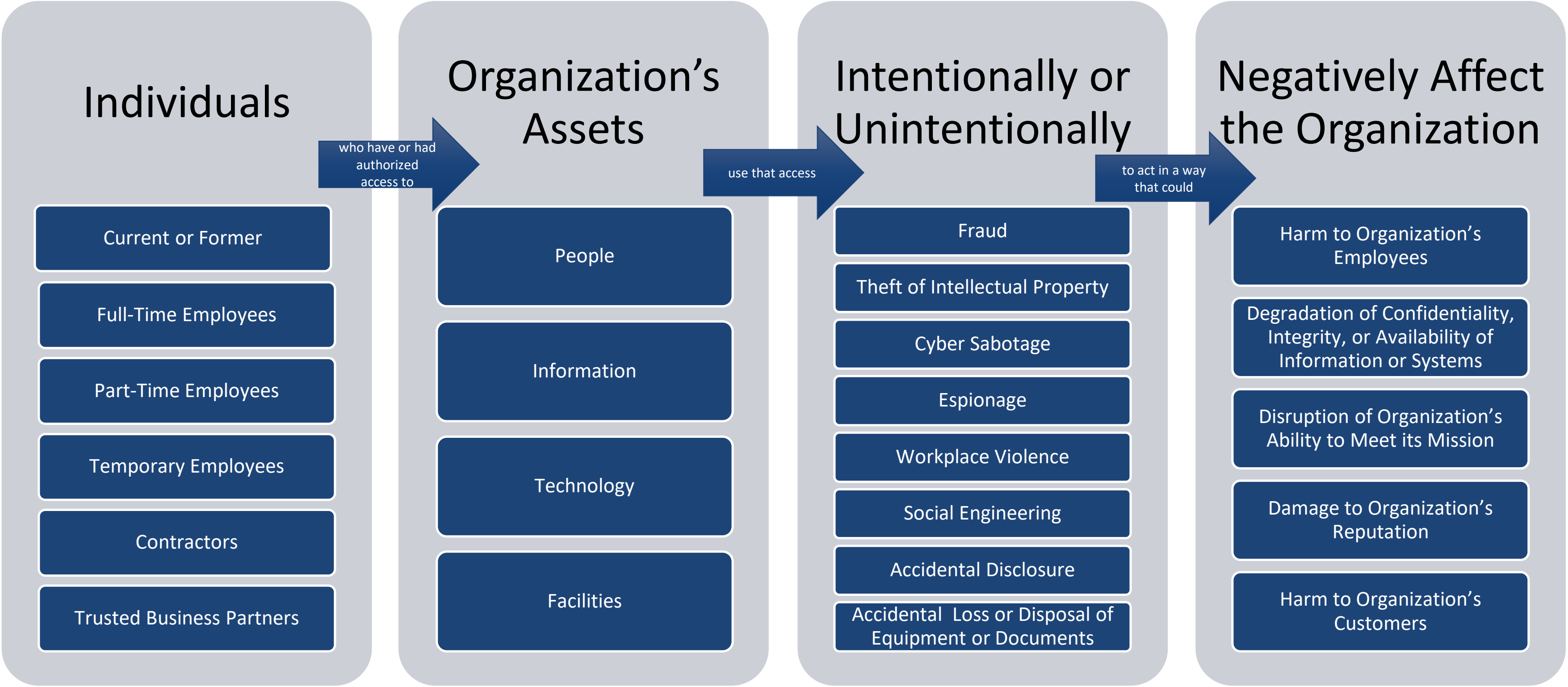
```
Splunk Query Name: Last 30 Days - Possible Theft of IP
Terms: 'host=HECTOR [search host="zeus.corp.merit.lab" Message="A user account was  disabled. *" |
eval Account_Name=mvindex(Account_Name, -1) | fields Account_Name | strcat Account_Name
"@corp.merit.lab" sender_address | fields - Account_Name]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

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

who have or had authorized access to

Organization’s Assets

- People
- Information
- Technology
- Facilities

use that access

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

to act in a way that could

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

Insider Threat Mitigation

Insider Incident

Prevent / Detect

if detected

Respond/Recover

Insider Threat

Identify / Deter

if detected

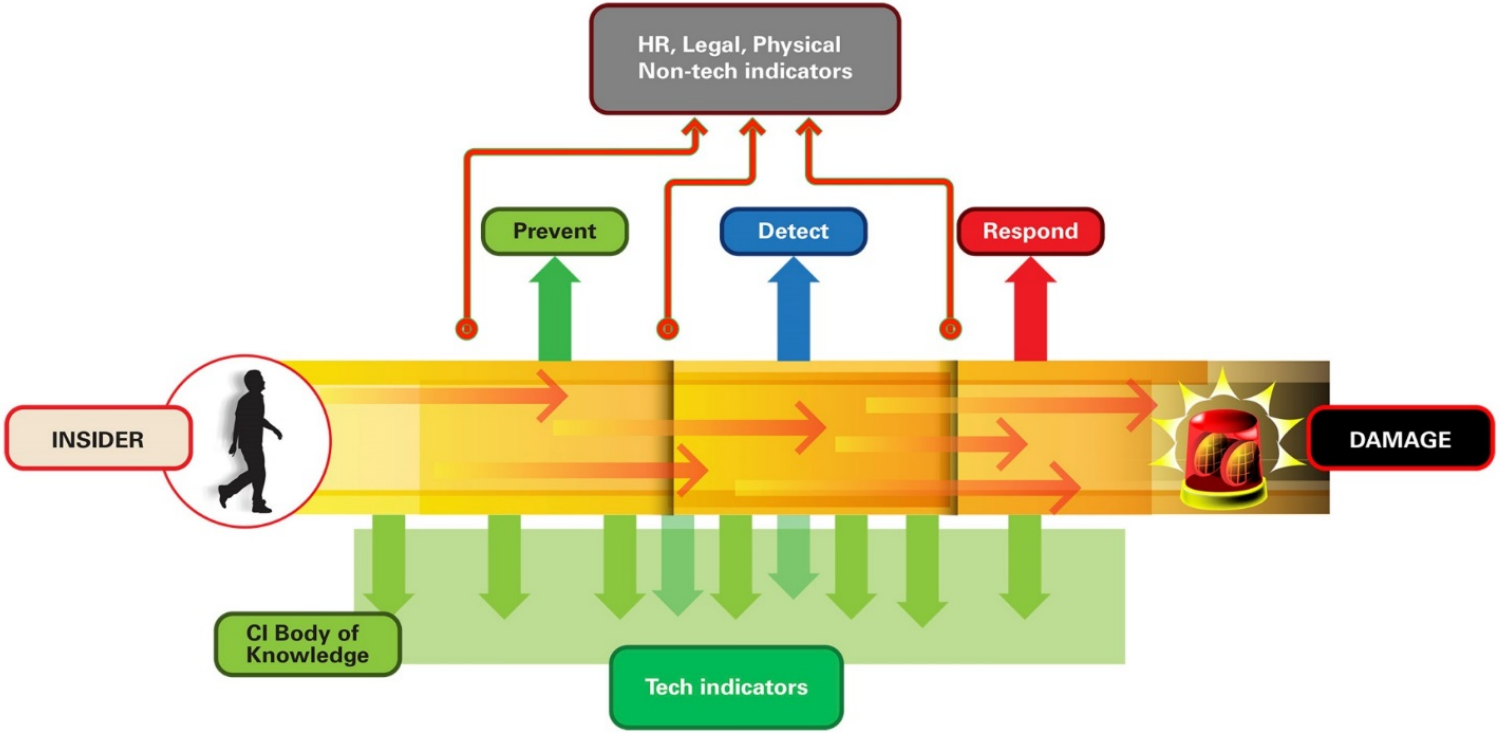
Consistent Response

Insiders

Not Alienate

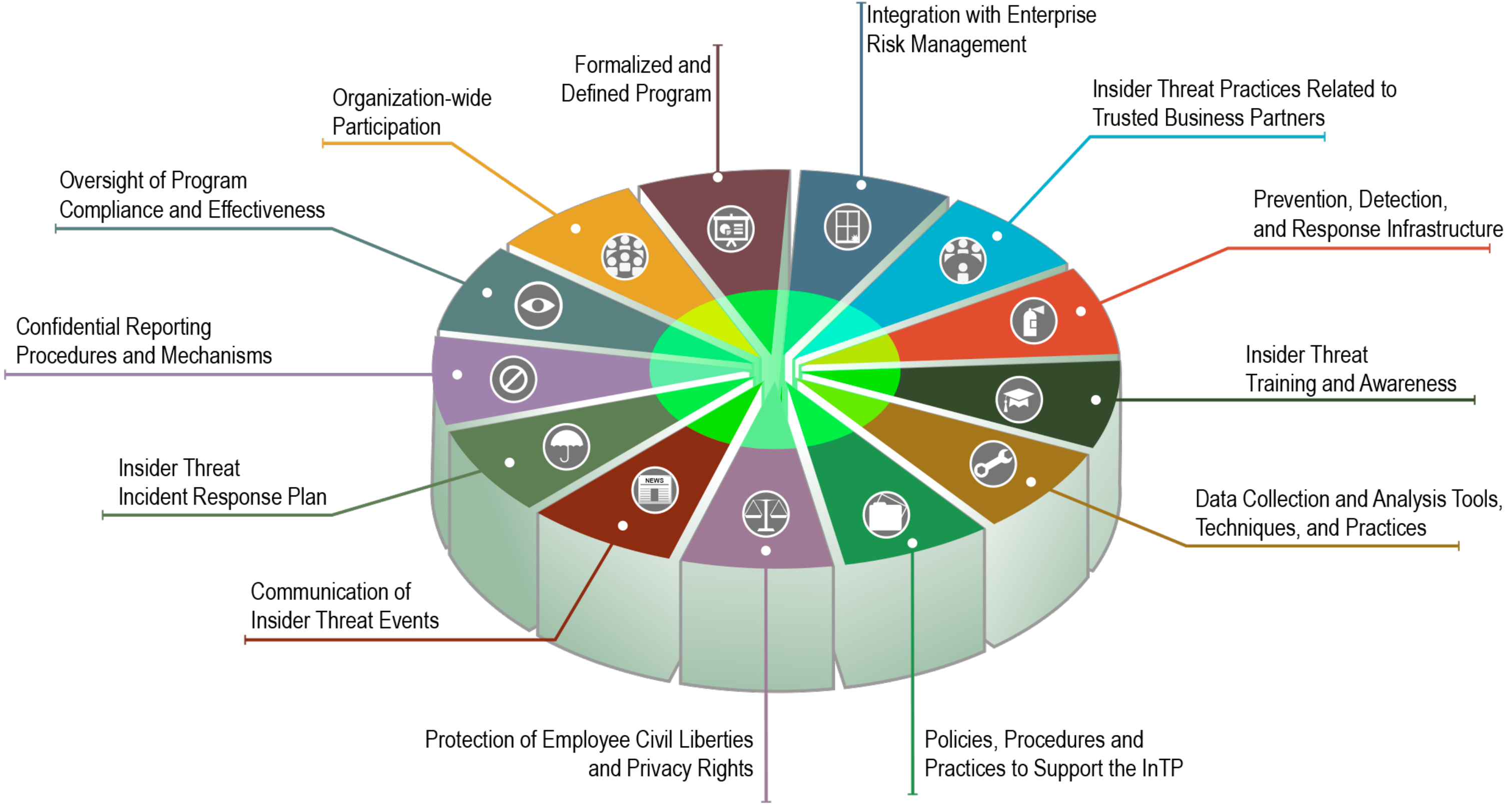
Insider Threat Program

Goal for an Insider Threat Program



Opportunities for prevention, detection, and response for an insider attack

Key Components of an Insider Threat Program

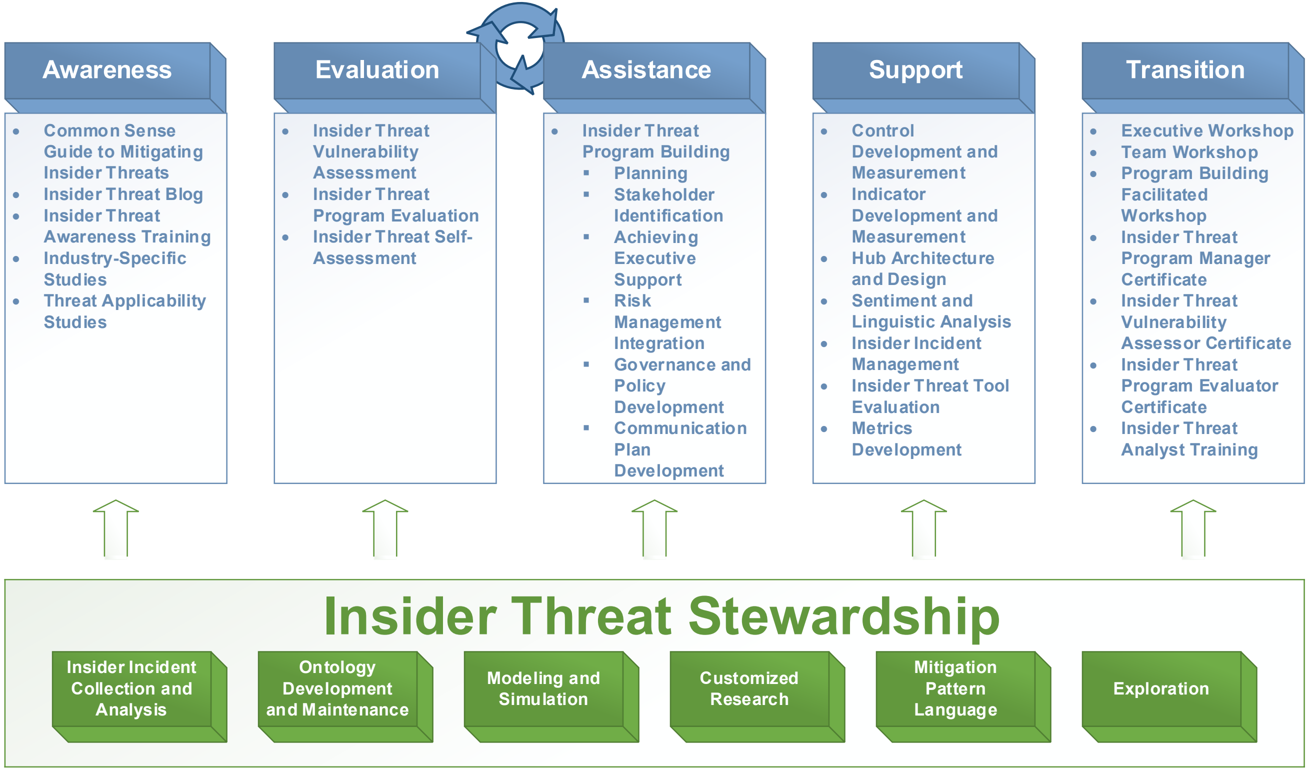

Integration with Enterprise Risk Management
Formalized and Defined Program
Organization-wide Participation
Insider Threat Practices Related to Trusted Business Partners
Oversight of Program Compliance and Effectiveness
Prevention, Detection, and Response Infrastructure
Confidential Reporting Procedures and Mechanisms
Insider Threat Training and Awareness
Insider Threat Incident Response Plan
Data Collection and Analysis Tools, Techniques, and Practices
Communication of Insider Threat Events
NEWS
Protection of Employee Civil Liberties and Privacy Rights
Policies, Procedures and Practices to Support the InTP

Recommended Best Practices for Insider Threat Mitigation

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

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