Insider Threats in the Software Development Lifecycle

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.

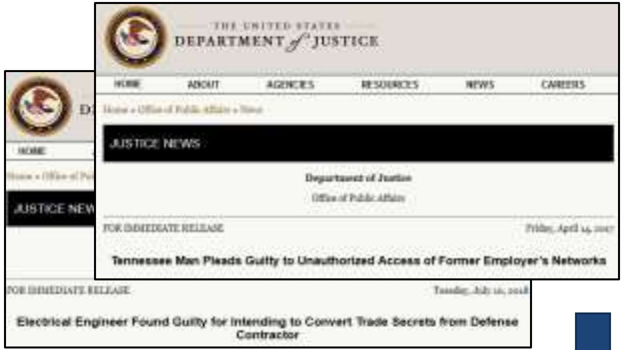
The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

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.

DM22-0899

Insider Threat Research at the SEI



THE UNITED STATES DEPARTMENT of JUSTICE

HOME ABOUT AGENCIES RESOURCES NEWS CAREERS

Home » Office of Public Affairs » News

JUSTICE NEWS

Department of Justice

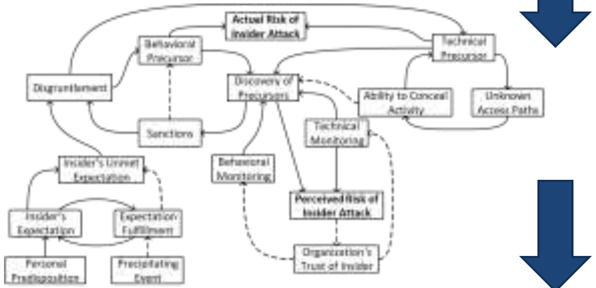
Office of Public Affairs

FOR IMMEDIATE RELEASE Friday, April 14, 2017

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

FOR IMMEDIATE RELEASE Tuesday, July 10, 2018

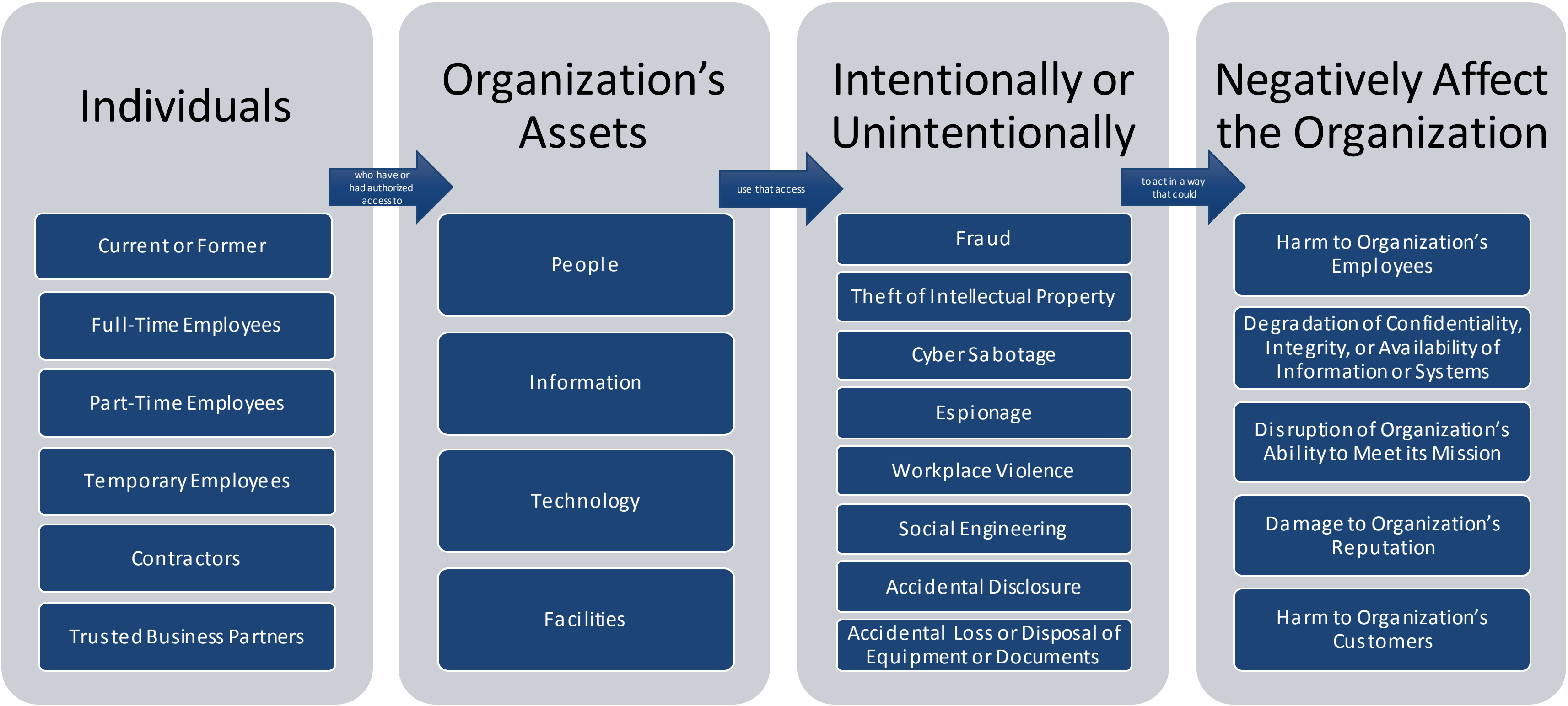
Electrical Engineer Found Guilty for Intending to Convert Trade Secrets from Defense Contractor



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

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

Scale of the Insider Threat

1 in 3 cybercrimes are perpetrated by insiders

Insider incidents have increased by 47% since 2018 (Source: Ponemon [2022 Cost of Insider Threat Global Report])

1 in 4 insider incidents are perpetrated by trusted external entities

1 in 3 insider incidents are committed with malicious intent

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

Insider Threats in the SDLC – Observed Vulnerabilities

Requirements Definition

- Neglecting to define **authentication** and **role-based access control** requirements simplified insider attacks.
- Neglecting to define **security requirements/separation of duties** for **automated business processes** provided an easy method for insider attack.
- Neglecting to define requirements for **automated data integrity checks** gave insiders the security of knowing their actions would not be detected.

Design

- Insufficient attention to security details in **automated workflow processes** enabled insiders to commit malicious activity.
- Insufficient **separation of duties** facilitated insider crimes.
  - not designed at all
  - no one to “check the checker”
- Neglecting to consider security vulnerabilities posed by “**authorized system overrides**” resulted in an easy method for insiders to ”get around the rules”.

Implementation

- Lack of **code reviews** allowed insertion of backdoors into source code.
- Inability to **attribute actions** to a single user enabled a project leader to sabotage team’s development project.

Deployment

- Lack of enforcement of **documentation practices** and **backup procedures** prohibited recovery efforts when an insider deleted the only copy of source code for a production system.
- Use of the same **password file** for development and the operational system enabled insiders to access and steal sensitive data from the operational system.
- **Unrestricted access** to all customers’ systems enabled a computer technician to plant a virus directly on customer networks.
- Lack of **configuration control** and well-defined **business processes** enabled libelous material to be published to organization’s website.

Maintenance

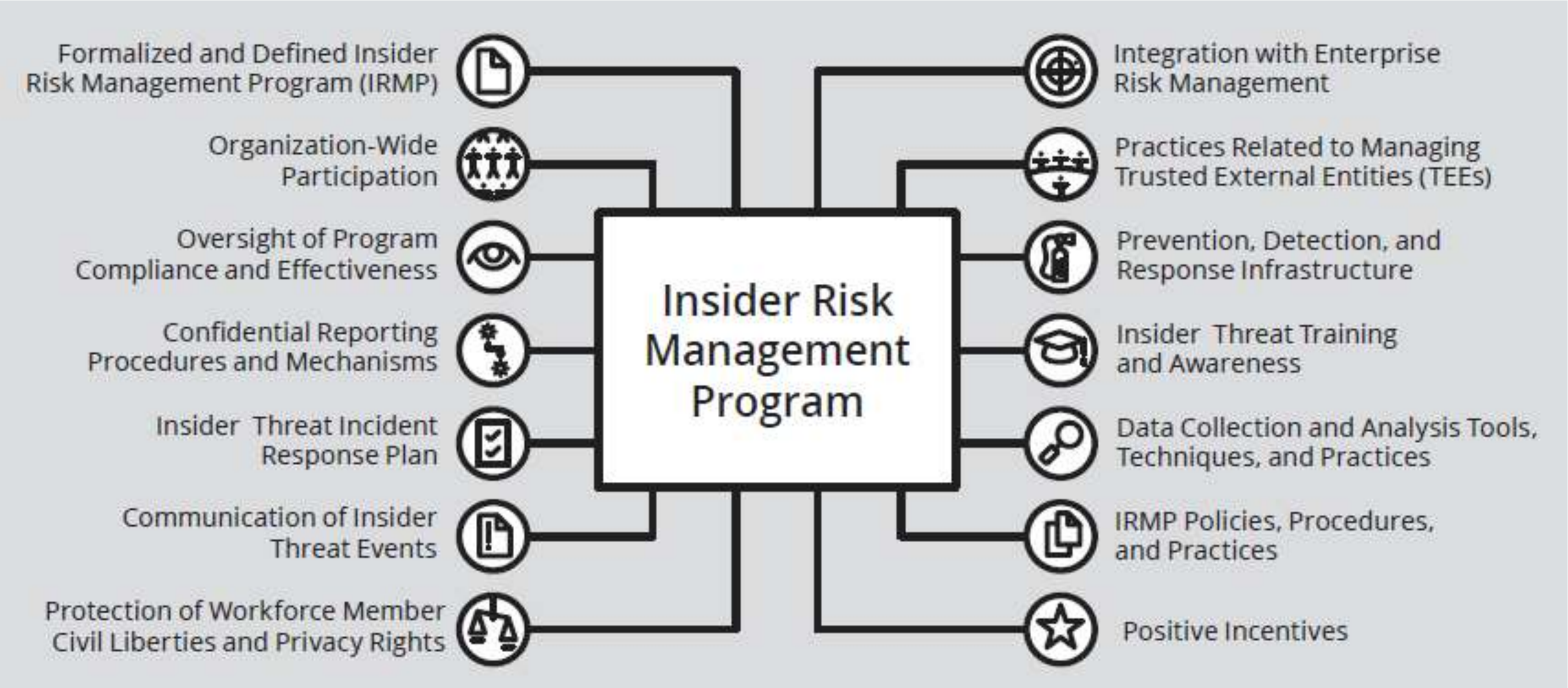
- Lack of **code reviews** facilitated insertion of malicious code.
- Ineffective **configuration control** practices enabled release of unauthorized code into production.
- Ineffective or lack of **backup processes** amplified the impact of mass deletion of data.
- **End-user access** to source code for systems they used enabled modification of security measures built into the source code.
- Ignoring known **system vulnerabilities** provided an easy exploit method.

Best Practices for Insider Threat Mitigation

1. Know and protect your critical assets	2. Develop a formalized insider risk management program
3. Clearly document and consistently enforce administrative controls	4. Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior
5. Anticipate and manage negative issues in the work environment	6. Consider threats from insider and trusted external entities in enterprise-wide risk assessments
7. Be especially vigilant regarding social media	8. Structure management tasks to minimize insider stress and mistakes
9. Incorporate insider threat awareness into periodic security training for all workforce members	10. Implement strict password and account management policies and practices
11. Institute stringent access controls and monitoring policies on privileged users	12. Deploy solutions for monitoring workforce member actions and correlating information from multiple sources
13. Monitor and control access from all end points, including mobile devices	14. Establish a baseline of normal behavior for both networks and workforce members
15. Enforce separation of duties and least privilege	16. Define explicit security agreements for clous services, especially access restrictions and monitoring capabilities
17. Institutionalize system change controls	18. Implement secure backup and recovery processes
19. Mitigate Unauthorized data exfiltration	20. Develop a comprehensive workforce member termination procedure
21. Adopt positive incentives to align the workforce and the organization	22. Learn from past insider incidents

https://resources.sei.cmu.edu/asset_files/WhitePaper/2022_019_001_886876.pdf

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
Insider Risk Management Program
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

Insider Threats in the Software Development Life Cycle

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

Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls

Analytic Approaches to Detect Insider Threats

Spotlight On: Insider Theft of Intellectual Property Inside the United States Involving Foreign Governments

Workplace Violence & IT Sabotage: Two Sides of the Same Coin?

An Insider Threat Indicator Ontology

Questions / Discussion