Insider Threat Overview

Dan Costa

Bob Ditmore

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.

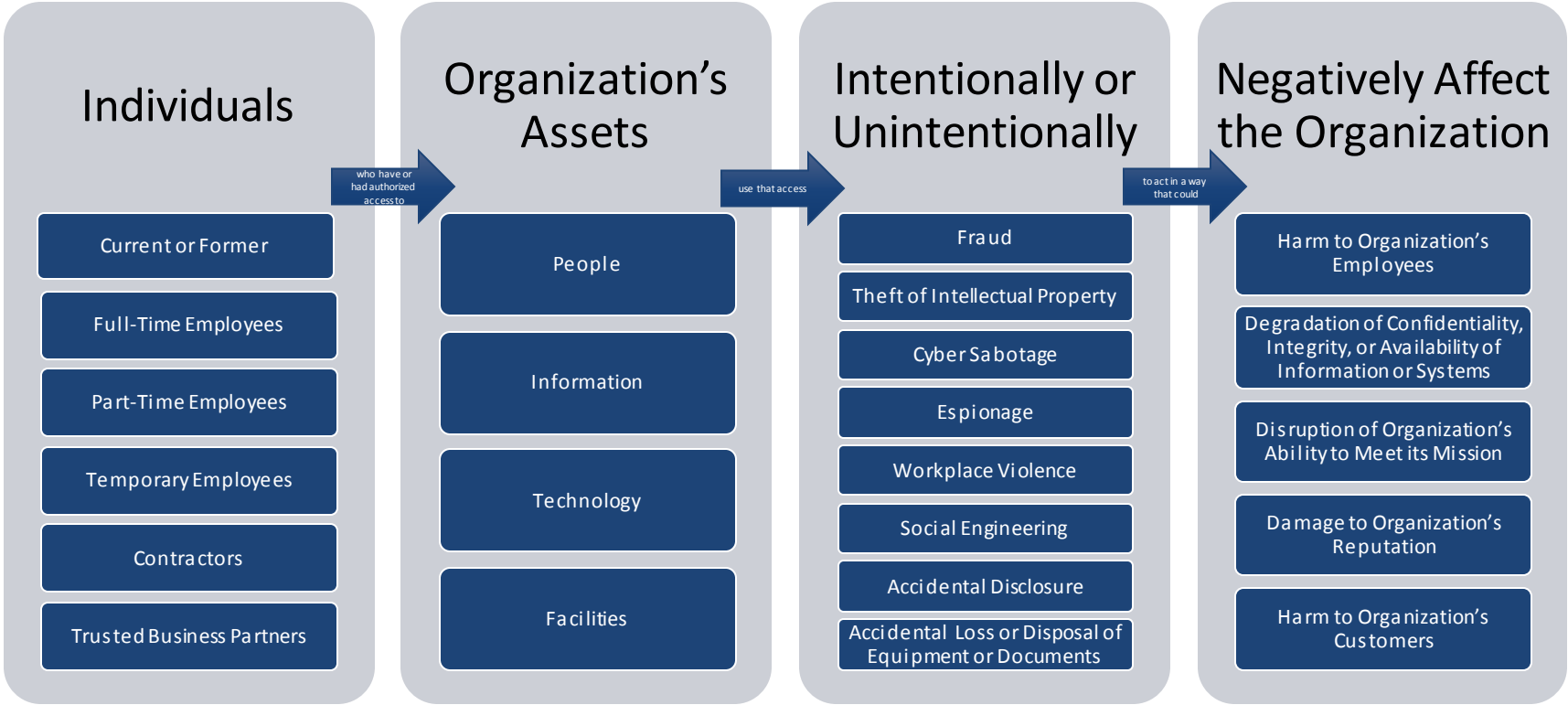
DM22-0151

Insider Threat Research at the SEI


```
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



Insider IT Sabotage Overview

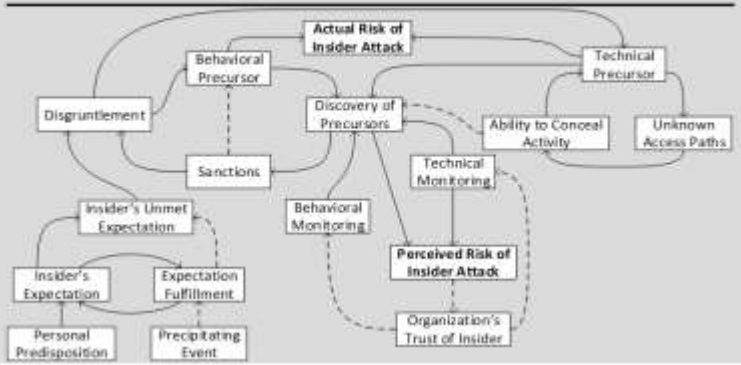
Background

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.

Risk Model



Associated Potential Risk Indicators

Personal Predispositions	• Repeated violation of organizational policies and procedures
Stressors	• Co-worker conflicts
Concerning Behaviors	• Sudden decline in job performance or work attendance • Aggressive or violent behavior
Harmful Act	• Unauthorized modification or deletion of critical system configurations • Unauthorized modification or deletion of logs or backups • Creating and using backdoor, shared, non-attributable, and unauthorized accounts • Downloading and installing malicious code and / or hacking tools • Tampering with, disabling, or attempting to disable security controls

Applicable Data Sources

Account creation logs	Identity management systems	Change and configuration management systems
Intrusion detection / prevention systems	User activity monitoring	Backup system access logs
Confidential / anonymous reporting systems	Human resource management systems	Employee performance management systems

Insider Threats in the SDLC – Observed Vulnerabilities

Requirements Definition	Design	Implementation	Deployment	Maintenance

• 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.
	• 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".
		• 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.
			• 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.
				• 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.	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

A Holistic Approach to Insider Risk Management

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 Threats in the Software Development Life Cycle

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