How to Sniff Out Insider Threats

Dan Costa

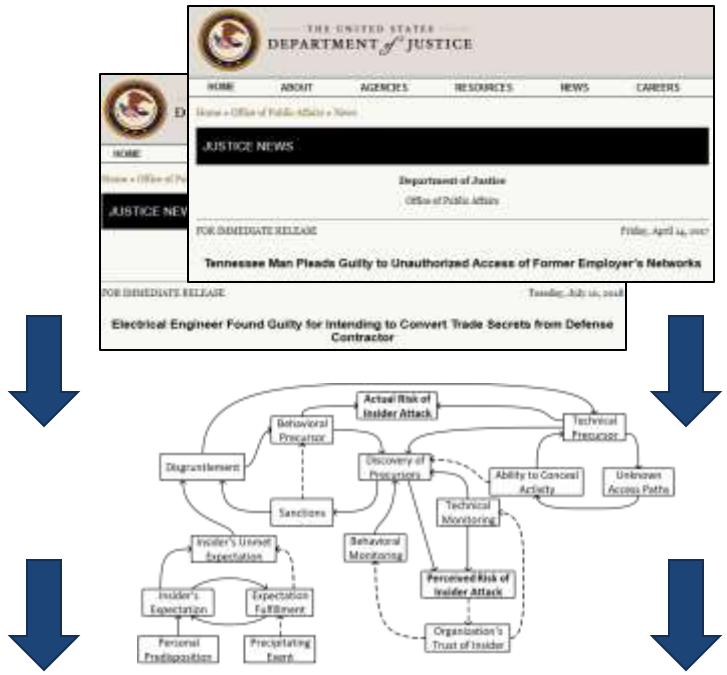
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

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.

DM22-0401

Insider Threat Research at the SEI



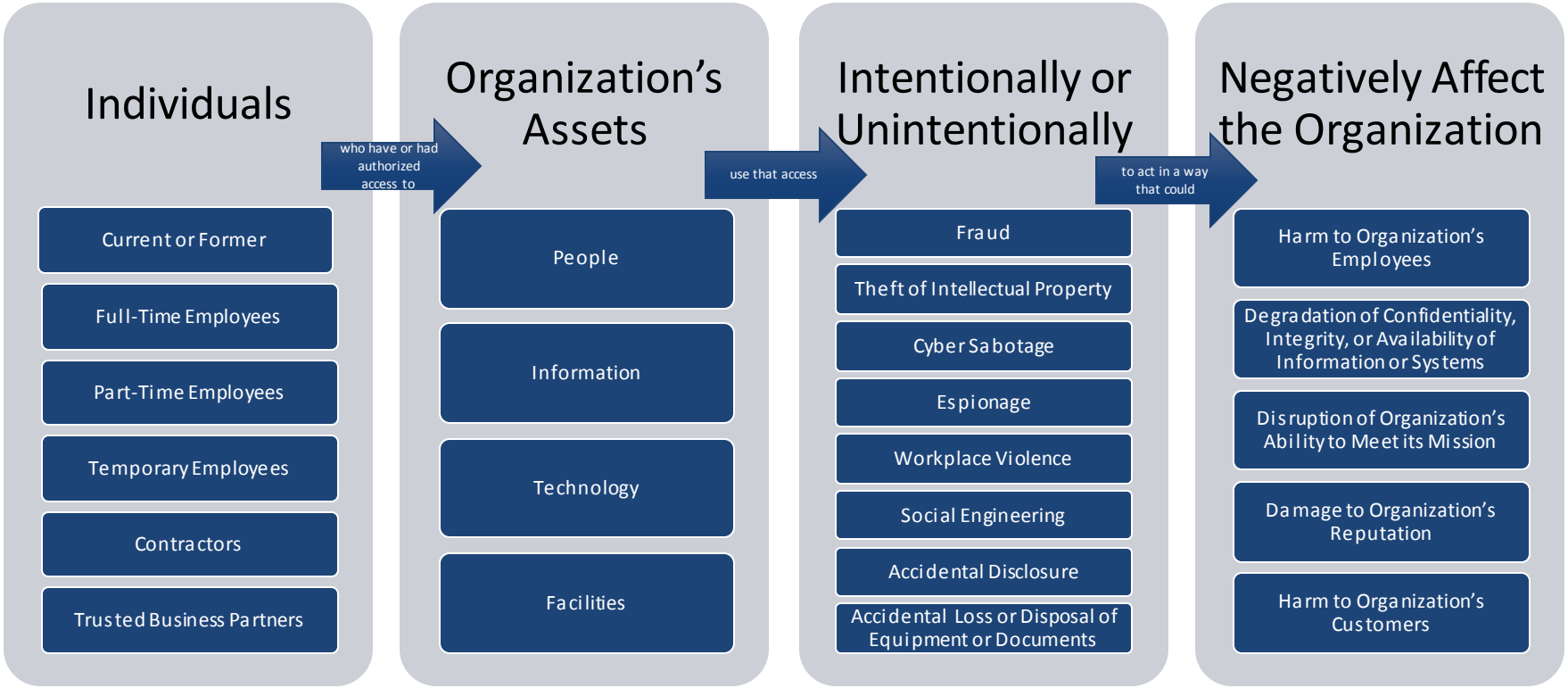

```
Splunk Query Name: Last 30 Days - Possible Theft of IP
Terms: 'host=HECTOR [search host="zeus.corp.merit.lab" Message="A user account was  disabled. *" |
eval Account_Name=mvindex(Account_Name, -1) | fields Account_Name | strcat Account_Name
"@corp.merit.lab" sender_address | fields - Account_Name]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

Conducting research, modeling, analysis, and outreach to develop socio-technical solutions to combat insider threats since 2001

The Insider Threat Defined

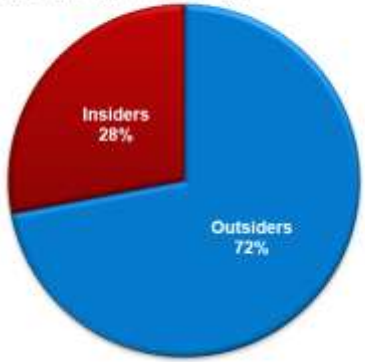
The potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.

Scope of the Insider Threat

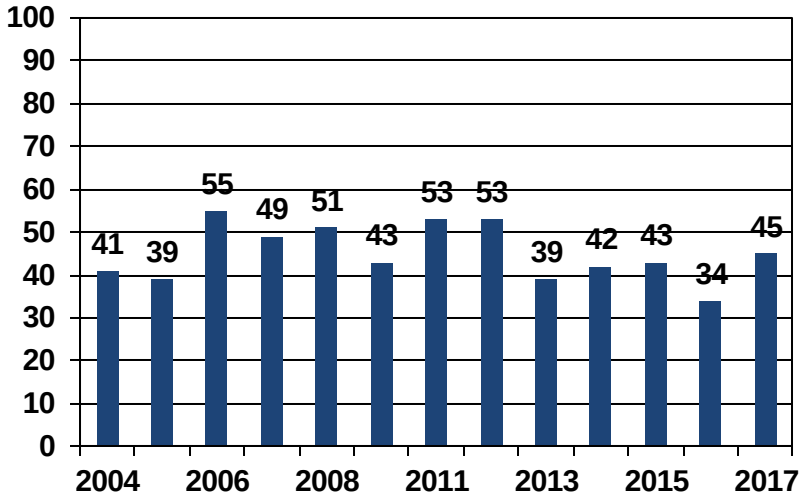


Scale of the Insider Threat

What percent of the electronic crime events are known or suspected to have been caused by :



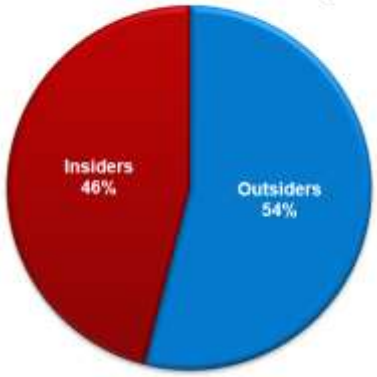
What percentage of organizations experienced an insider incident?



What percentage of certain types of security incidents were perpetrated by insiders?

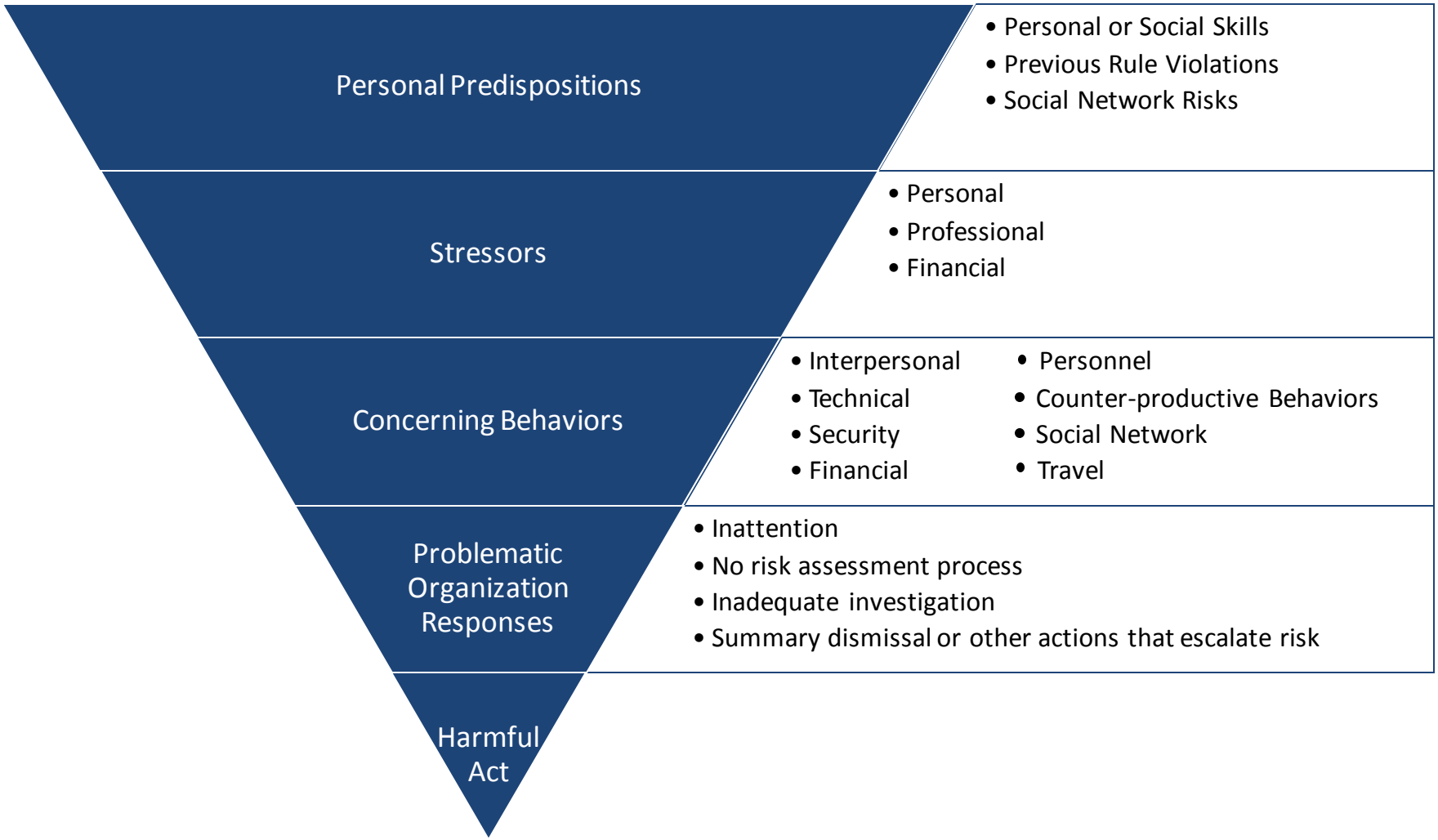
Confidential records (trade secrets or intellectual property) were compromised	79%
Customer records were compromised	79%
Private or sensitive information was intentionally exposed	70%
Theft of personally identifiable information (PII) (customer or partner data)	66%
Systems were sabotaged (deliberate disruption, deletion or destruction of information, systems or networks)	65%
Private or sensitive information was unintentionally exposed	56%

The most costly or damaging crimes were committed by:



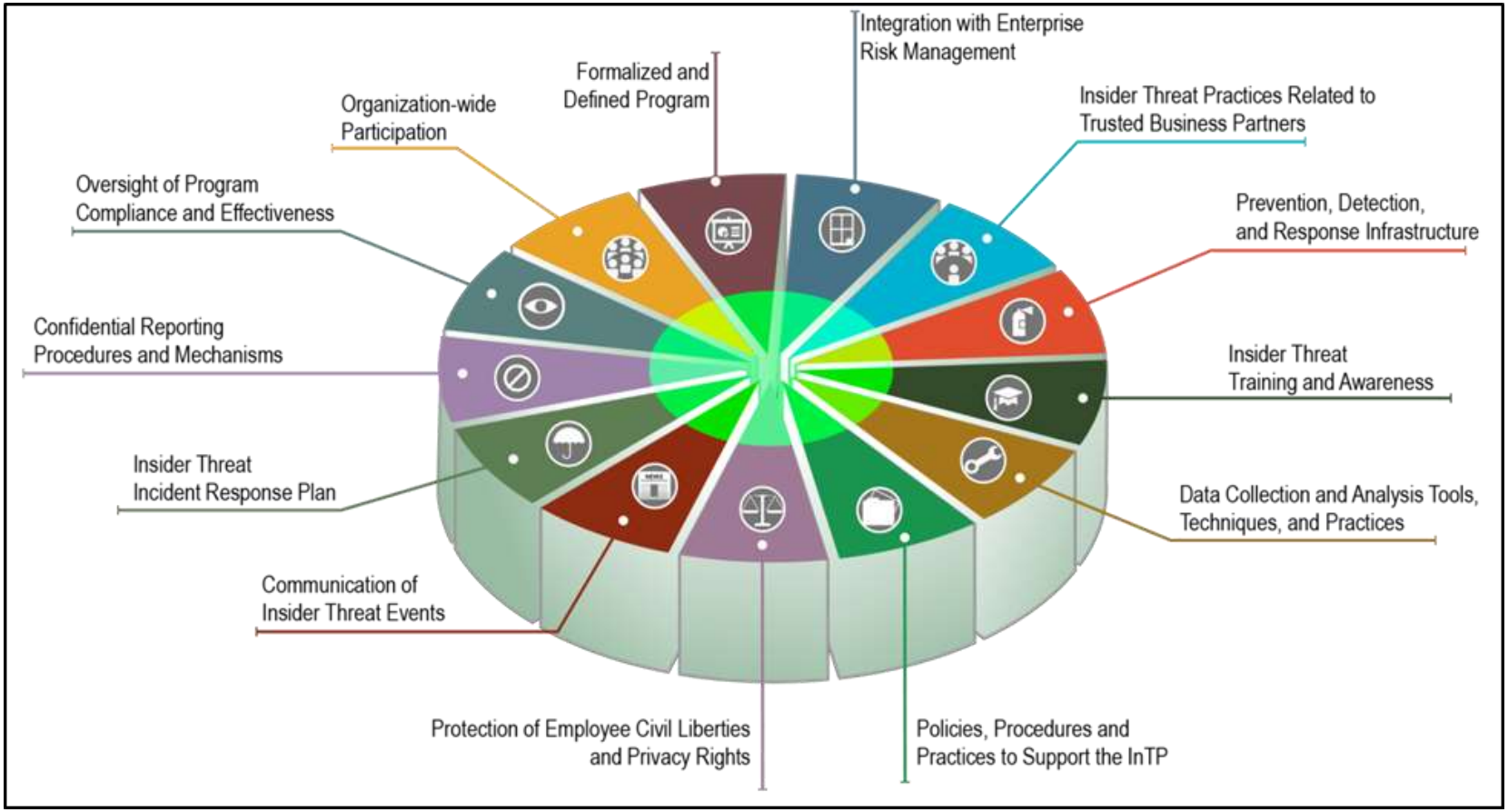
Sources: 2004-2018 U.S. State of Cybercrime Survey, in partnership with KnowBe4, CSO, U.S. Secret Service, and CERT Division of Software Engineering Institute at Carnegie Mellon University

The Critical Path to Insider Risk



Adapted from Shaw, Eric, and Laura Sellers. "Application of the Critical-Path Method to Evaluate Insider Risks." *Studies in Intelligence* 59.2 (Extracts, June 2015)

Key Components of an Insider Threat Program



Challenges to InTP Building

How extensive is the challenge of achieving each of the following for insider risk programs?

Challenge	Respondent Count	Low	Medium Low	Medium	Medium High	High
Coordinating and communicating across business / operational units	50				✓	
Establishing the insider threat program scope and organizational structure	50			✓		
Ensuring compliance with all applicable legal requirements	50			✓		
Developing policy and formalizing the program	50			✓		
Incorporating insider threat controls for trusted business partners	49				✓	
Obtaining adequate funding for program operation	50				✓	
Developing and administering insider threat awareness training	50			✓		
Hiring and retaining qualified insider threat program personnel	48			✓		
Sharing information across the organization's departments / units, including Human Resources (HR)	50				✓	

https://www.cylab.cmu.edu/_files/documents/irm-survey-results-20210331.7.pdf

Best Practices from the CERT Common Sense Guide to Mitigating Insider Threats

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

Questions / Open Discussion

Contact Information

Dan Costa, CISSP, PSEM

Technical Manager, CERT National Insider Threat Center

dlcosta@sei.cmu.edu

https://www.sei.cmu.edu/our-work/insider-threat/index.cfm