



# Relating Insider Cyber Sabotage and Workplace Violence

Dan Costa, Technical Manager, Enterprise Threat  
and Vulnerability Management | CERT Division

[dlcosta@sei.cmu.edu](mailto:dlcosta@sei.cmu.edu)

Software Engineering Institute  
Carnegie Mellon University  
Pittsburgh, PA 15213

# Document Markings

Copyright 2022 Carnegie Mellon University.

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.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM22-0239

# Insider Threat Research at the SEI

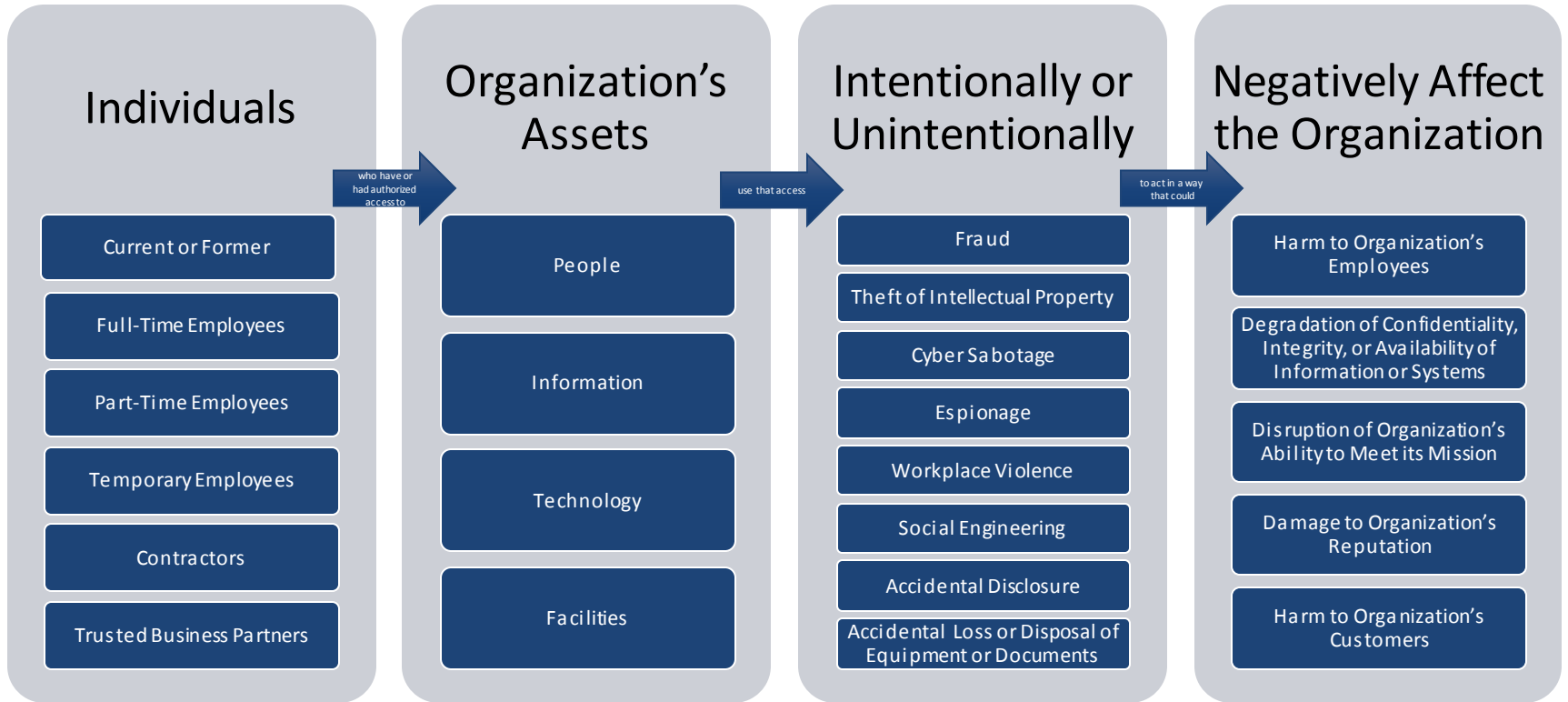


Conducting data collection, modeling, analysis, and outreach to develop socio-technical solutions to combat insider threats

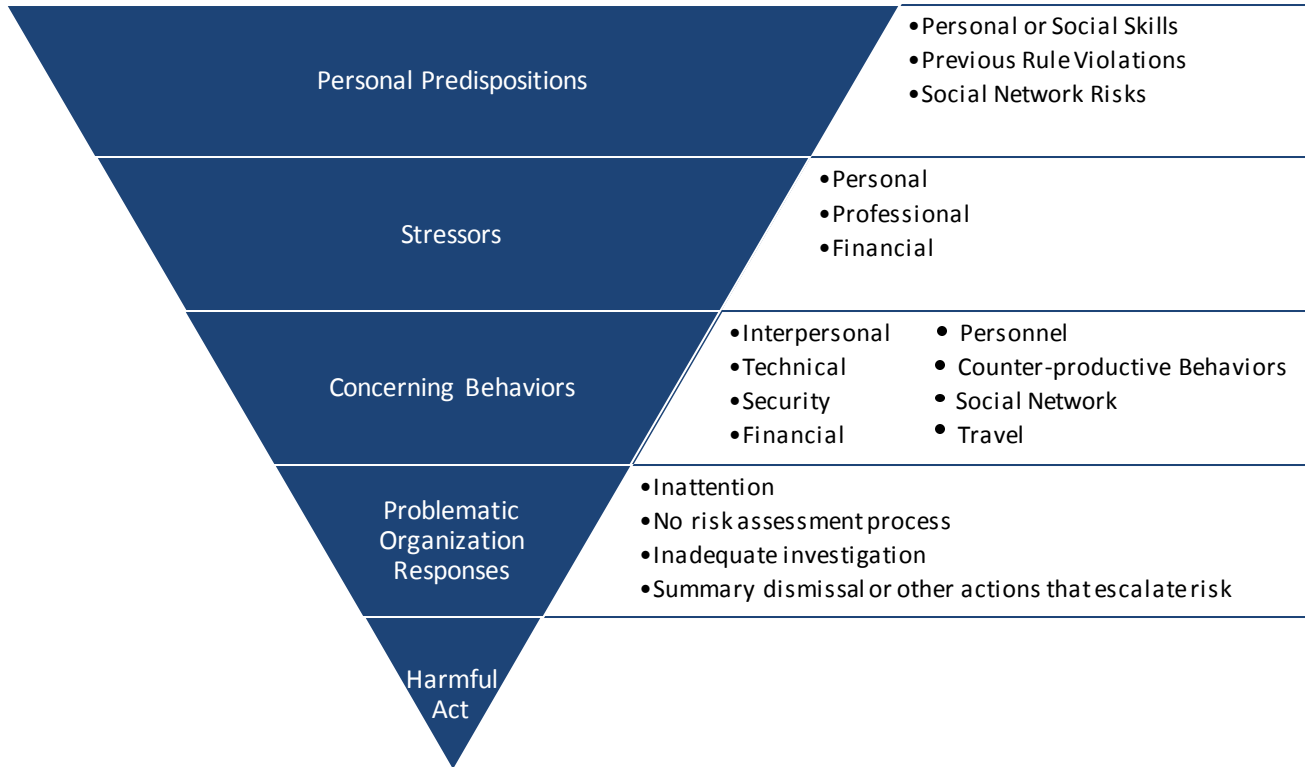


```
Splunk Query Name: Last 30 Days - Possible Theft of IP
Terms: 'host=HECTOR [search host="zeus.corp.merit.lab" Message="A user account was disabled. *" |
eval Account_Name=mvindex(Account_Name, -1) | fields Account_Name | streat Account_Name
"@corp.merit.lab" sender_address | fields - Account_Name]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

# Scope of the Insider Threat



# The Critical Path to Insider Risk



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

# 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



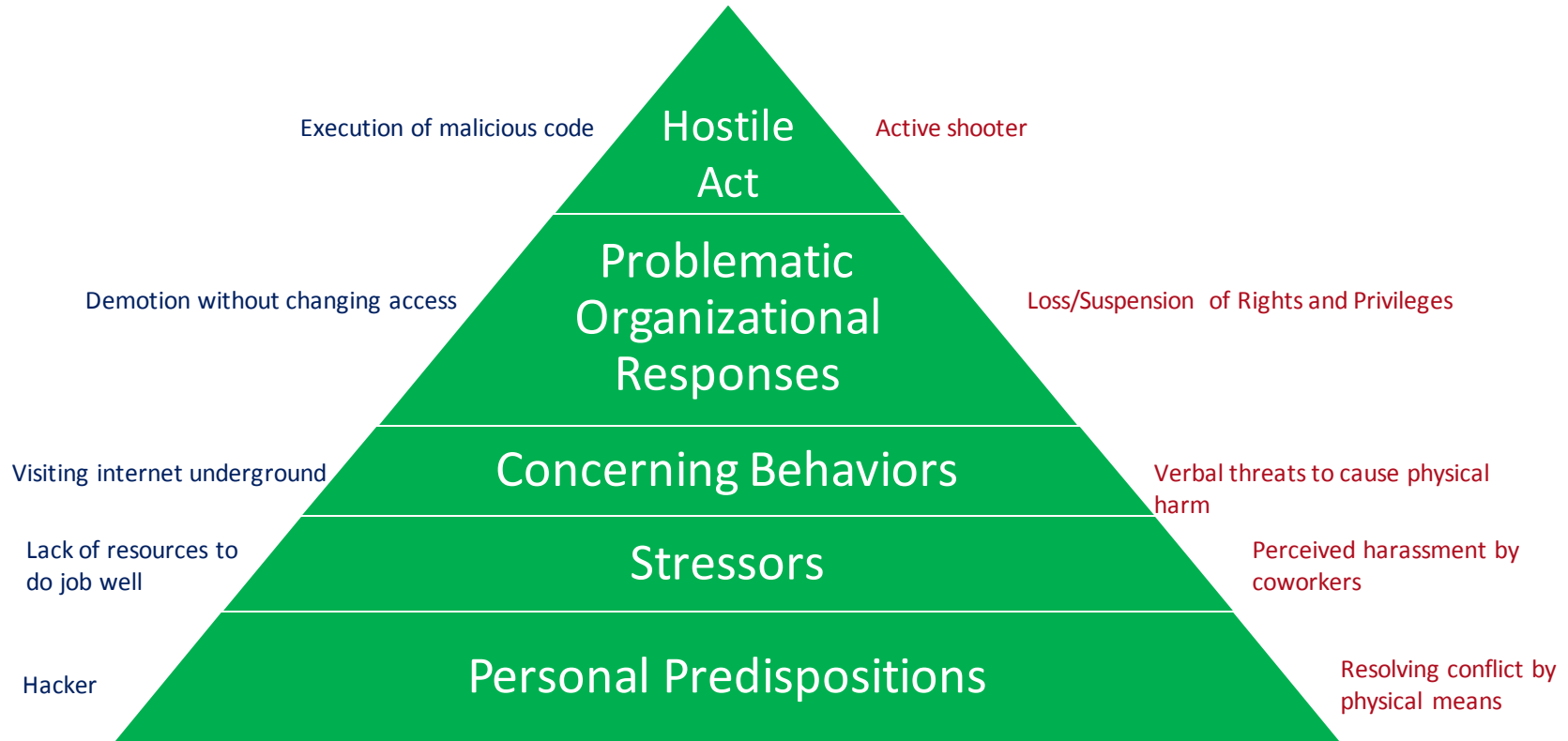
## Associated Potential Risk Indicators

Personal Predispositions	<ul style="list-style-type: none"> <li>Repeated violation of organizational policies and procedures</li> </ul>
Stressors	<ul style="list-style-type: none"> <li>Co-worker conflicts</li> </ul>
Concerning Behaviors	<ul style="list-style-type: none"> <li>Sudden decline in job performance or work attendance</li> <li>Aggressive or violent behavior</li> </ul>
Harmful Act	<ul style="list-style-type: none"> <li>Unauthorized modification or deletion of critical system configurations</li> <li>Unauthorized modification or deletion of logs or backups</li> <li>Creating and using backdoor, shared, non-attributable, and unauthorized accounts</li> <li>Downloading and installing malicious code and / or hacking tools</li> <li>Tampering with, disabling, or attempting to disable security controls</li> </ul>

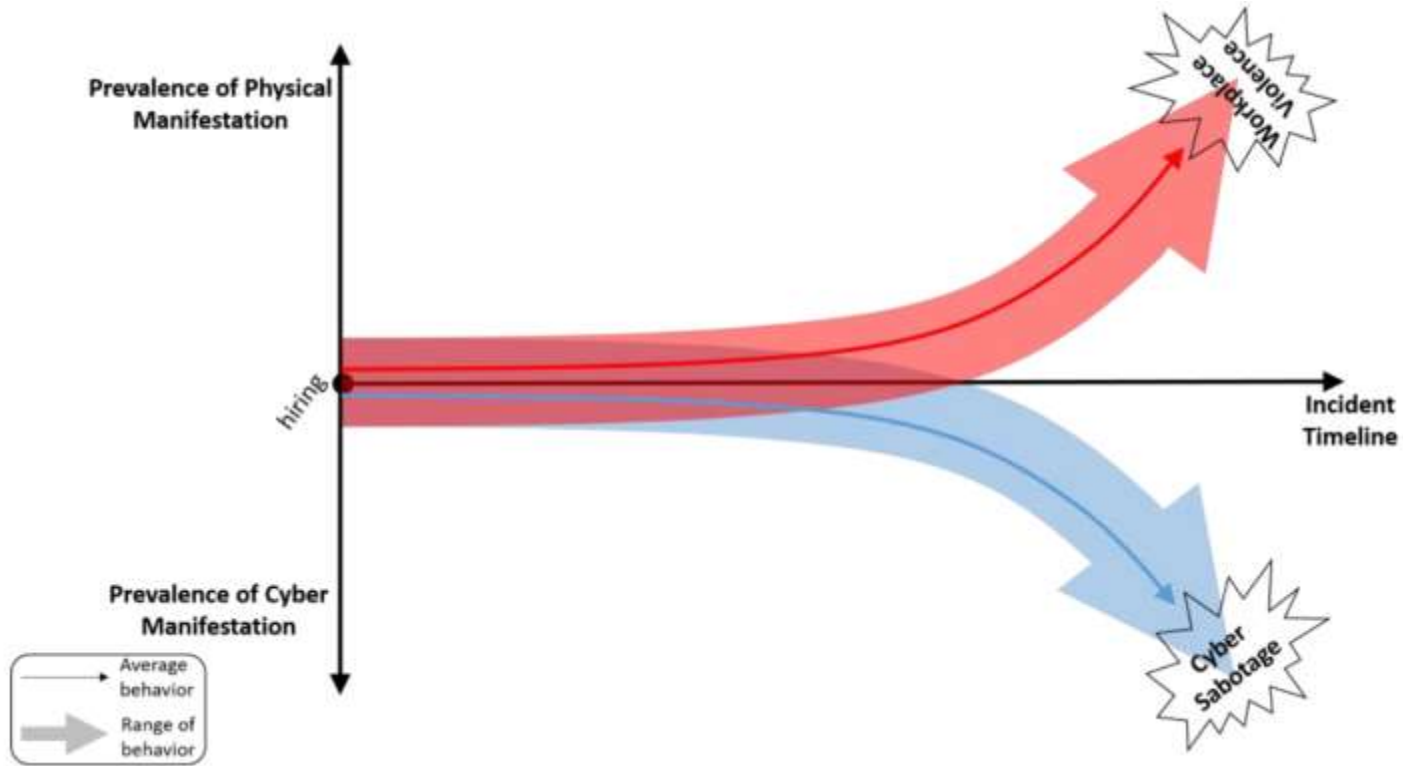
## Applicable Data Sources

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

# Workplace Violence and Insider Cyber Sabotage: Two Sides of the Same Coin?



# Hypothesis: Common Path Before Divergence



# If Correct, So What?

- Cost savings in controls
- Better risk models
- Increased value for cross-organization collaboration

# Insider Harm to Others Overview

## Background

**Insider Harm to Others:** insider incidents in which the insider exploits physical security gaps to direct potentially lethal force at an organization's employees or other bystanders

**Motivations:** revenge, primarily in response to a negative work-related event such as a demotion, transfer, dispute with a co-worker, or termination; in some circumstances, the insider may misdirect anger related to a personal life event toward the organization in response to the perceived wrongdoing of the organization

**Incident progression:** an insider's unmet expectations (pay, promotion, workload, etc.), combined with personal predispositions (history of aggression and violence, low self-monitoring behavior, etc.), may lead to disgruntlement, desperation, or distress. Disgruntled insiders may begin to exhibit behavioral precursors (decline in work performance / attendance, etc.), which may be discovered by the organization, who in turn may or may not impose sanctions. Failure to implement appropriate sanctions related to specific, lower-consequence harmful acts (stalking, attempted violent acts, "boundary-pushing," etc.), which act as a form of reconnaissance for the insider, may push the insider to more extreme harmful acts.

## Risk Model



## Associated Potential Risk Indicators

Personal Predispositions	<ul style="list-style-type: none"> <li>• History of aggression and violence</li> </ul>
Stressors	<ul style="list-style-type: none"> <li>• Changes in employment status</li> <li>• Changes in relationship status or loss of partner</li> <li>• Financial stress</li> </ul>
Concerning Behaviors	<ul style="list-style-type: none"> <li>• Threats to others or self</li> <li>• Sudden decline in job performance or work attendance</li> <li>• Sudden or dramatic shifts in mood</li> <li>• Access or attempts to access weapons</li> <li>• "Energy burst" of activity</li> </ul>
Harmful Act	<ul style="list-style-type: none"> <li>• Workplace stalking</li> <li>• Attempted or completed violent acts</li> <li>• Violations of physical security policies ("boundary-pushing")</li> </ul>

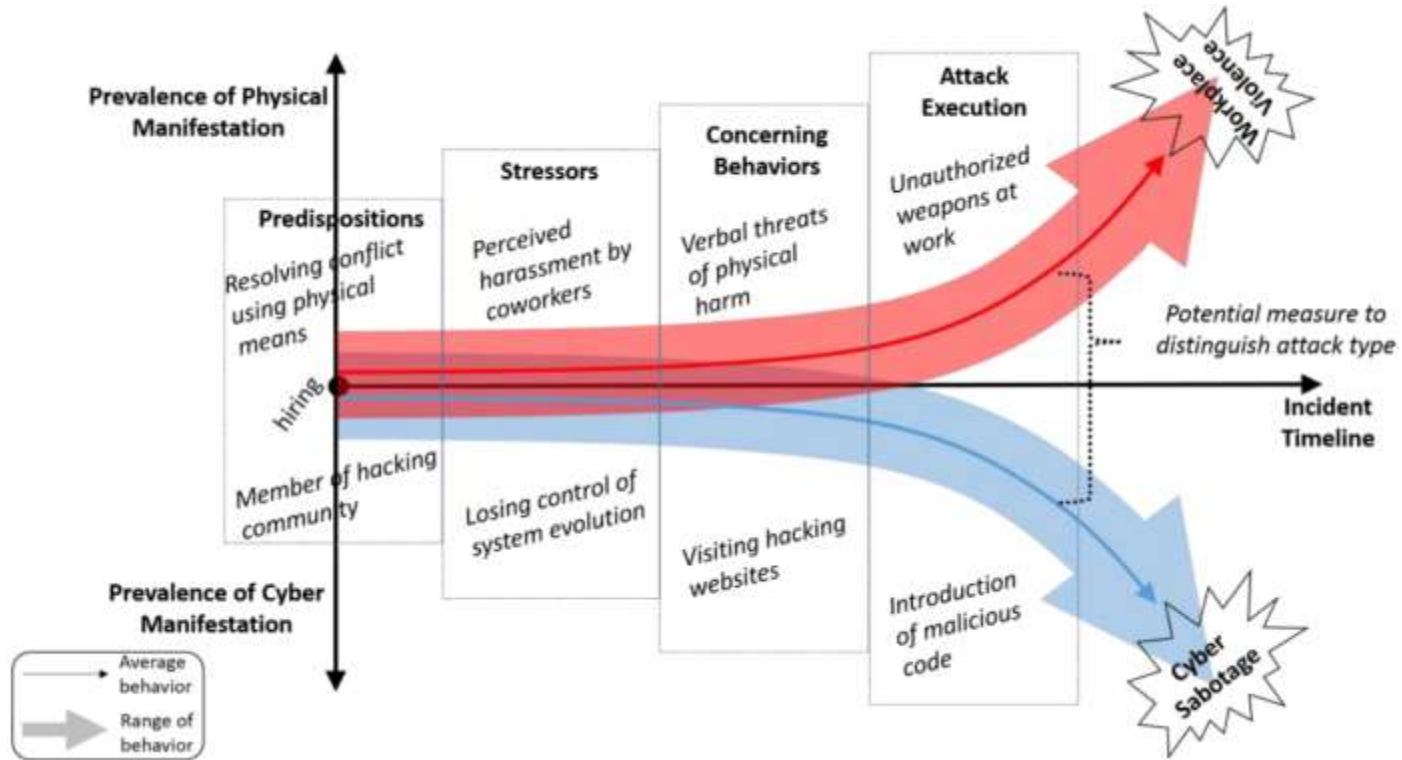
## Applicable Data Sources

User activity monitoring	Performance evaluations	Security clearance records
Background investigations	Personnel records	Employee performance management systems
Disciplinary records	Confidential / anonymous reporting systems	Human resource management systems

# Stressors by ICS and WPV



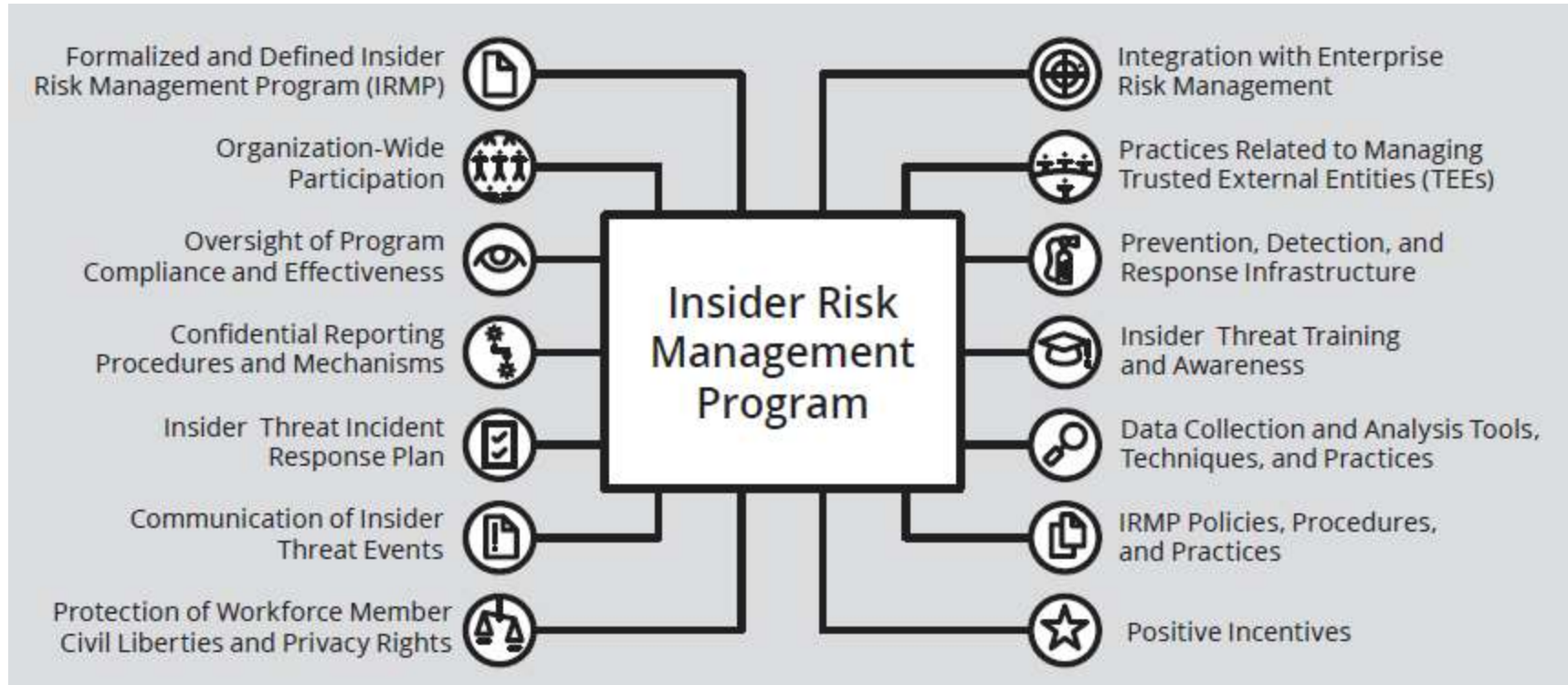
# Findings



# 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.
<b>5 - Anticipate and manage negative issues in the work environment.</b>	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.	<b>21 - Adopt positive incentives to align the workforce with the organization.</b>
11 - Institute stringent access controls and monitoring policies on privileged users.	<a href="http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=540644">http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=540644</a>

# 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 Threat Program Manager Certificate](#)

[Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls](#)

[Analytic Approaches to Detect Insider Threats](#)

[Workplace Violence & IT Sabotage: Two Sides of the Same Coin?](#)

# Questions / Discussion

