Data-Driven Approaches to Insider Risk Mitigation

Dan Costa, Technical Manager, CERT National Insider Threat Center

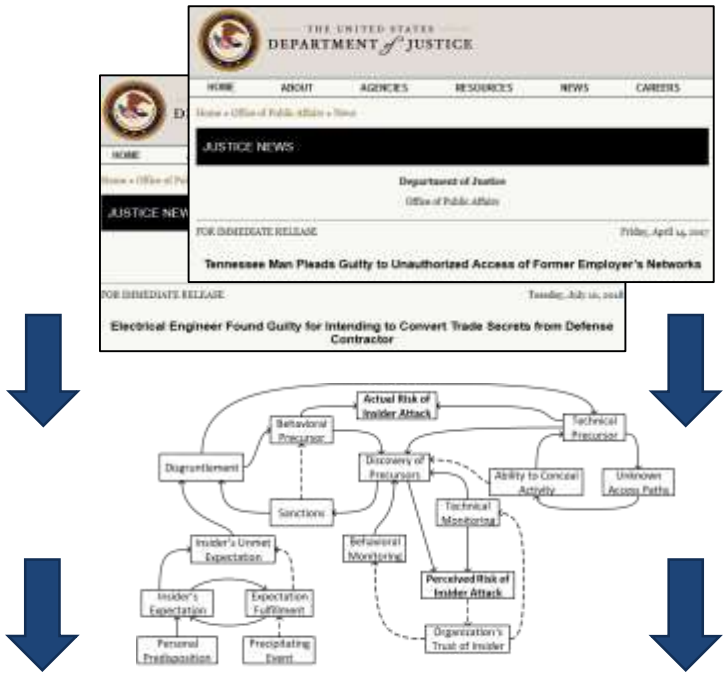
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

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.

DM20-0790

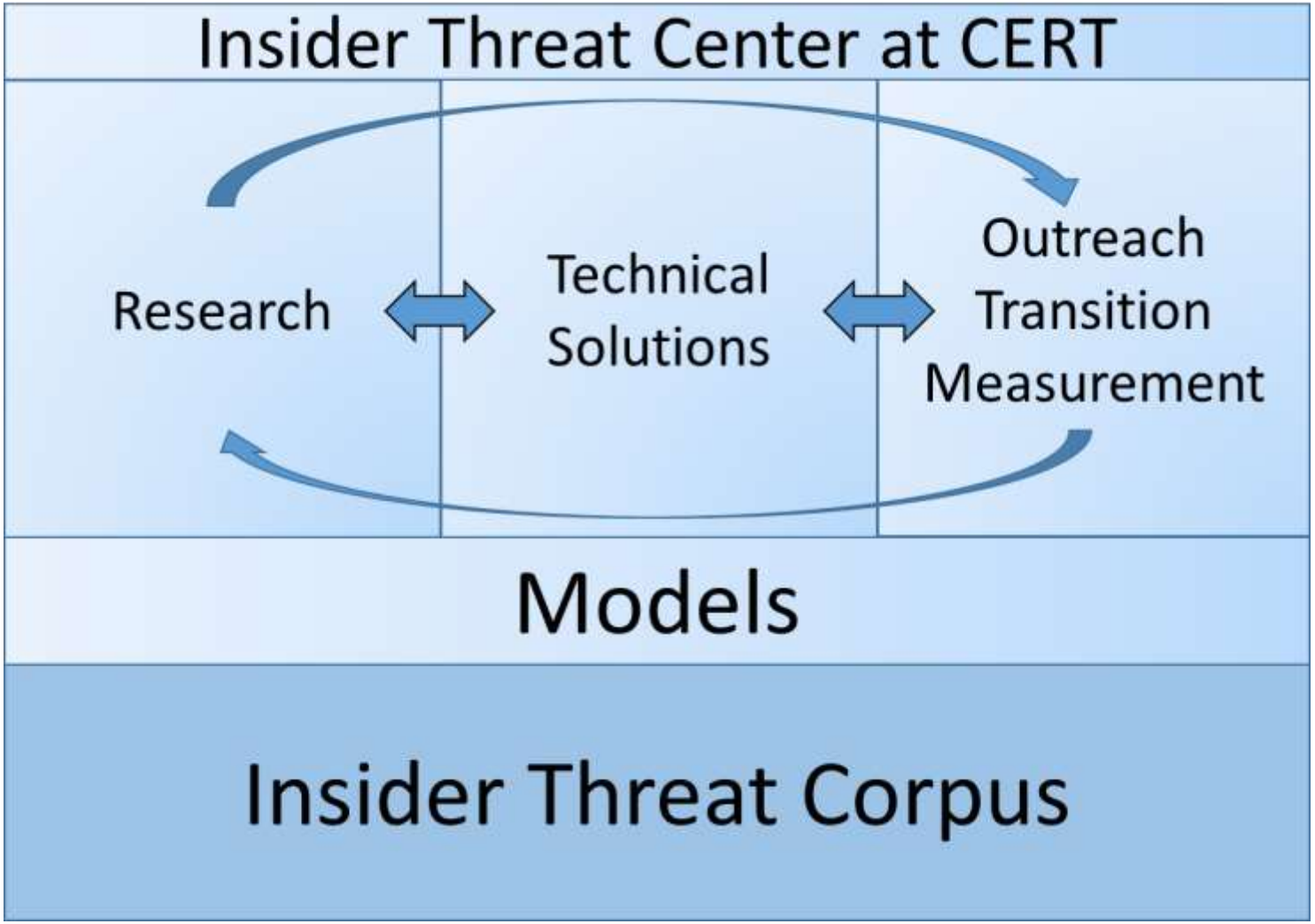
The CERT National Insider Threat Center




```
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

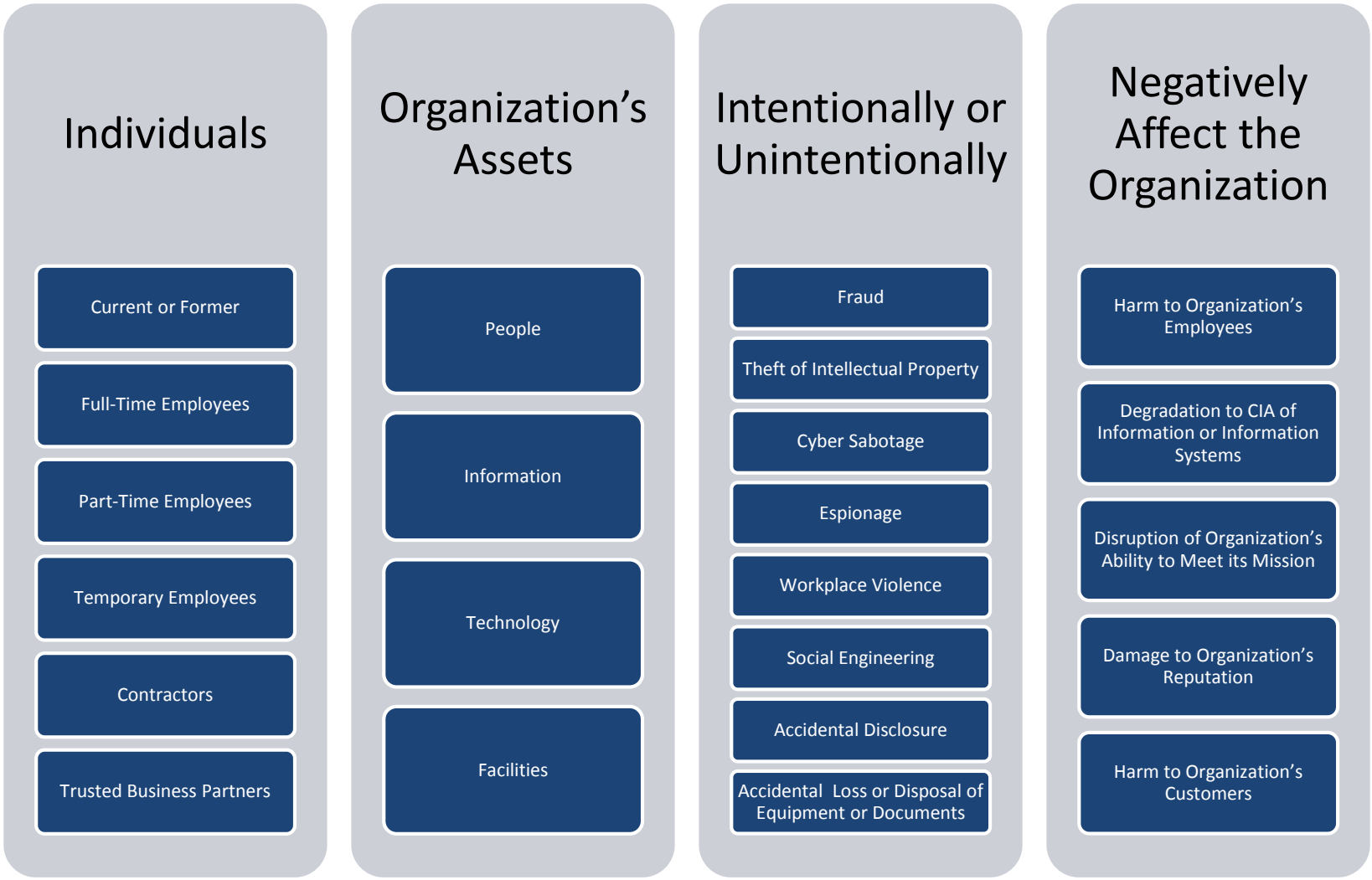
Our Approach



Definition of Insider Threat

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.

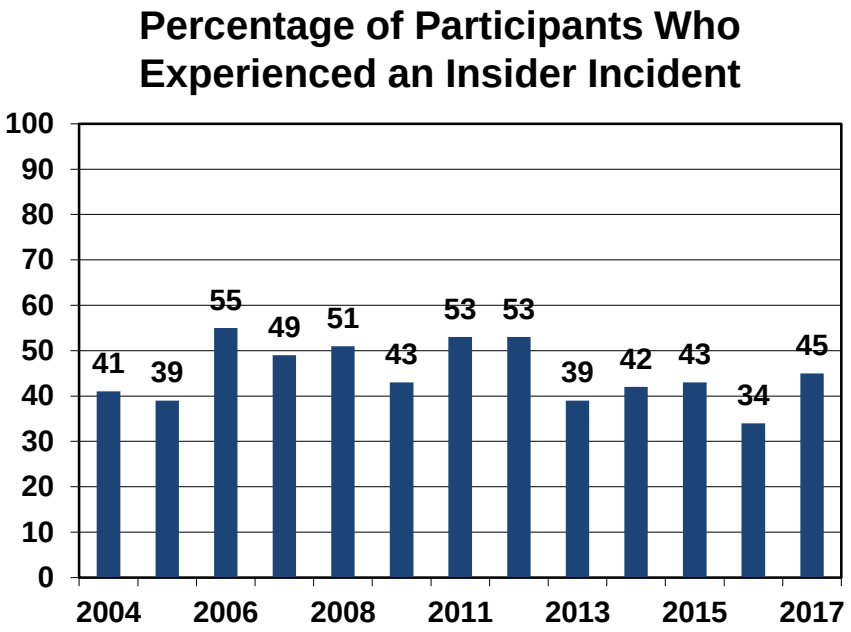
Scope of the Insider Threat



Scale of the Insider Threat

What 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%



Source: 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

Insider IT Sabotage

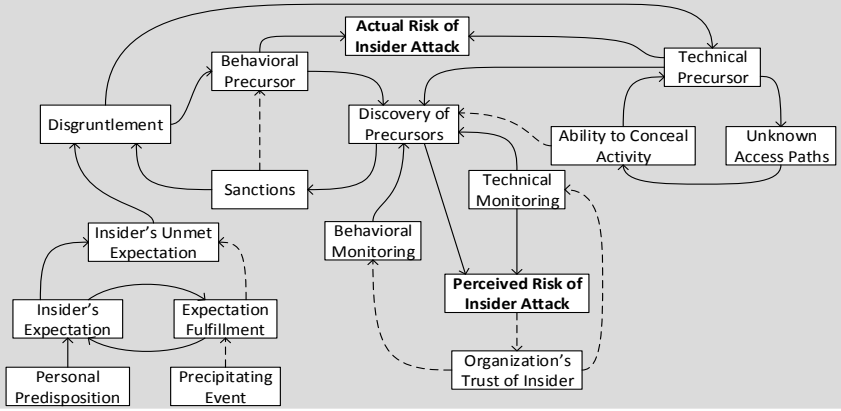
Background

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

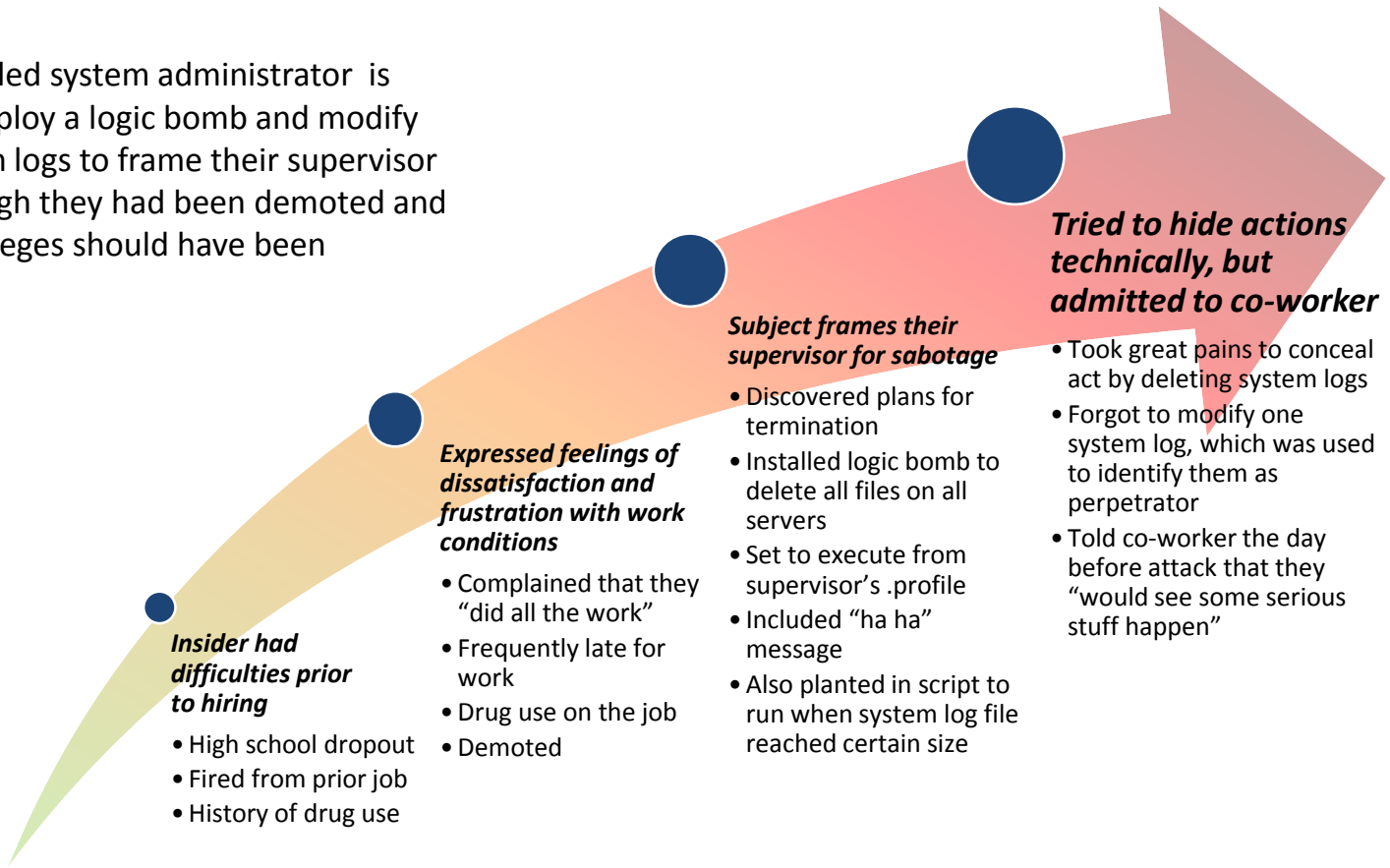
Personal Predispositions	• Repeated violation of organizational policies and procedures
Stressors	• Co-worker conflicts
Concerning Behaviors	• Sudden decline in job performance or work attendance • Aggressive or violent behavior
Harmful Act	• Unauthorized modification or deletion of critical system configurations • 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 IT Sabotage Example

A disgruntled system administrator is able to deploy a logic bomb and modify the system logs to frame their supervisor even though they had been demoted and their privileges should have been restricted.



Insider IP Theft

Background

Insider IP Theft: insider incidents in which the insider uses information technology to steal intellectual property from an organization.

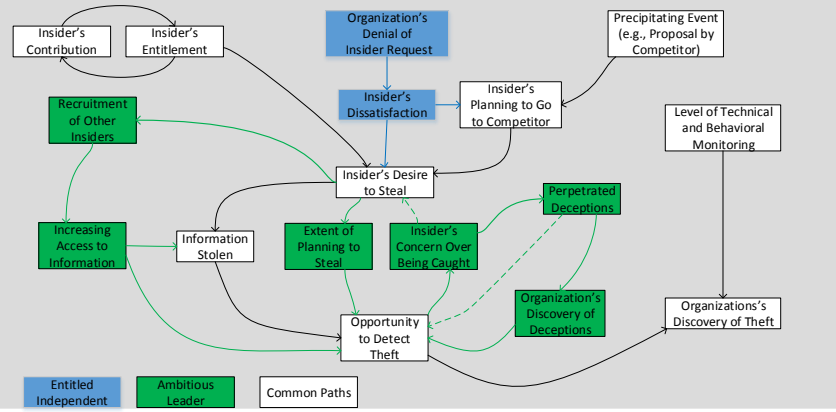
Motivations: Competitive business advantage, financial gain, benefit new employer, benefit foreign entity, or revenge.

Incident progression: in the case of an entitled independent, an insider begins to feel a degree of entitlement over his or her work products, and after experiencing some dissatisfaction (such as denied requests), the insider may decrease their sense of loyalty and compel them to seek other employment.

In the case of an ambitious leader, an insider plans to steal information and begins to increase their direct or indirect access to information, by recruiting others.

In both cases, without sufficient technical and behavioral monitoring, the organization may fail to discover the theft and deceptive activity leaving them unable to detect the overall attack.

Risk Model



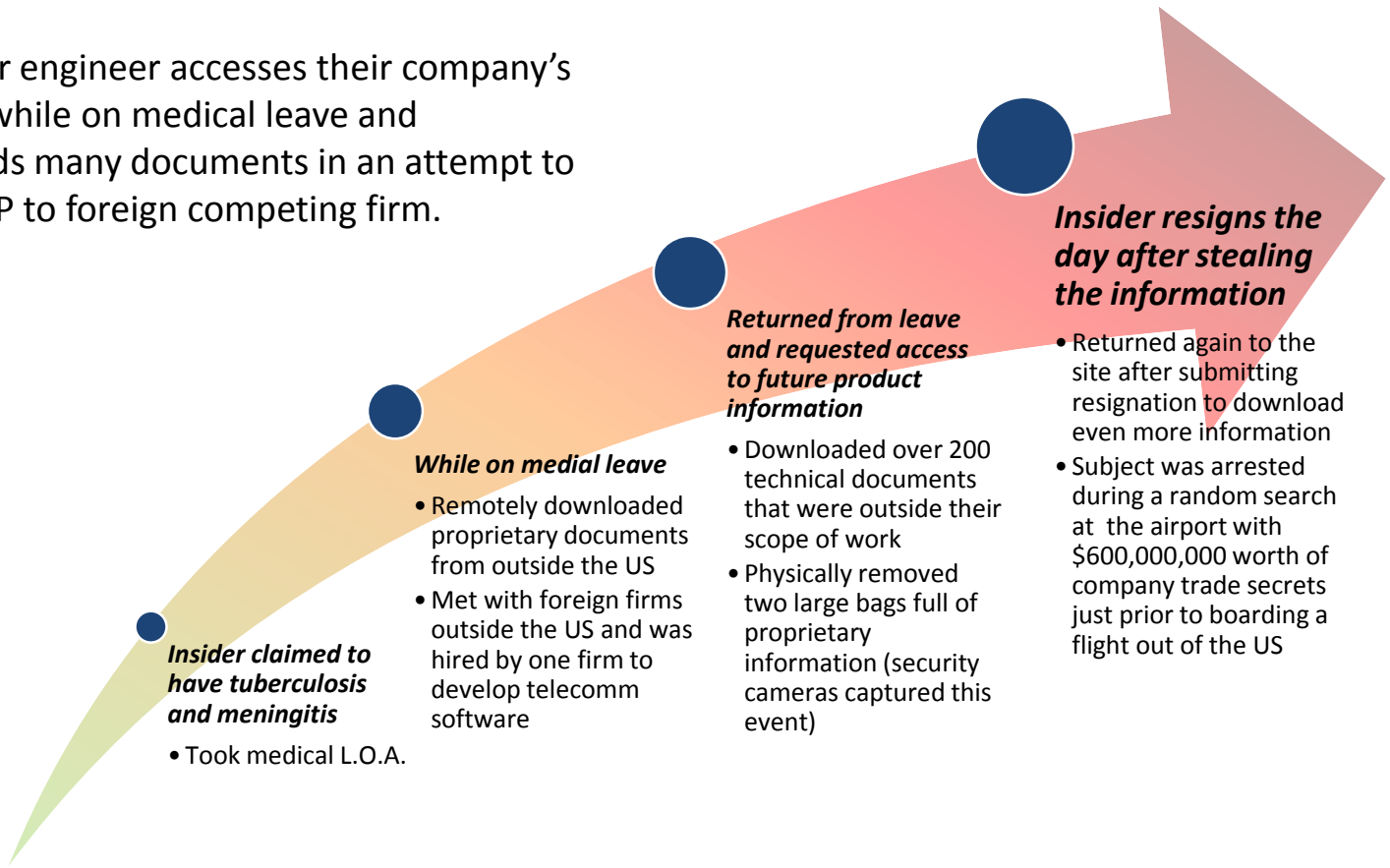
Associated Potential Risk Indicators

Applicable Data Sources

Email Logs	Chat Logs	Personnel Records
File Access Logs	User activity monitoring	Active Directory Logs
Anonymous Reporting	Background Investigations	DLP Logs

Insider Theft of IP Example

Computer engineer accesses their company's systems while on medical leave and downloads many documents in an attempt to transfer IP to foreign competing firm.



Insider claimed to have tuberculosis and meningitis

- Took medical L.O.A.

While on medial leave

- Remotely downloaded proprietary documents from outside the US
- Met with foreign firms outside the US and was hired by one firm to develop telecomm software

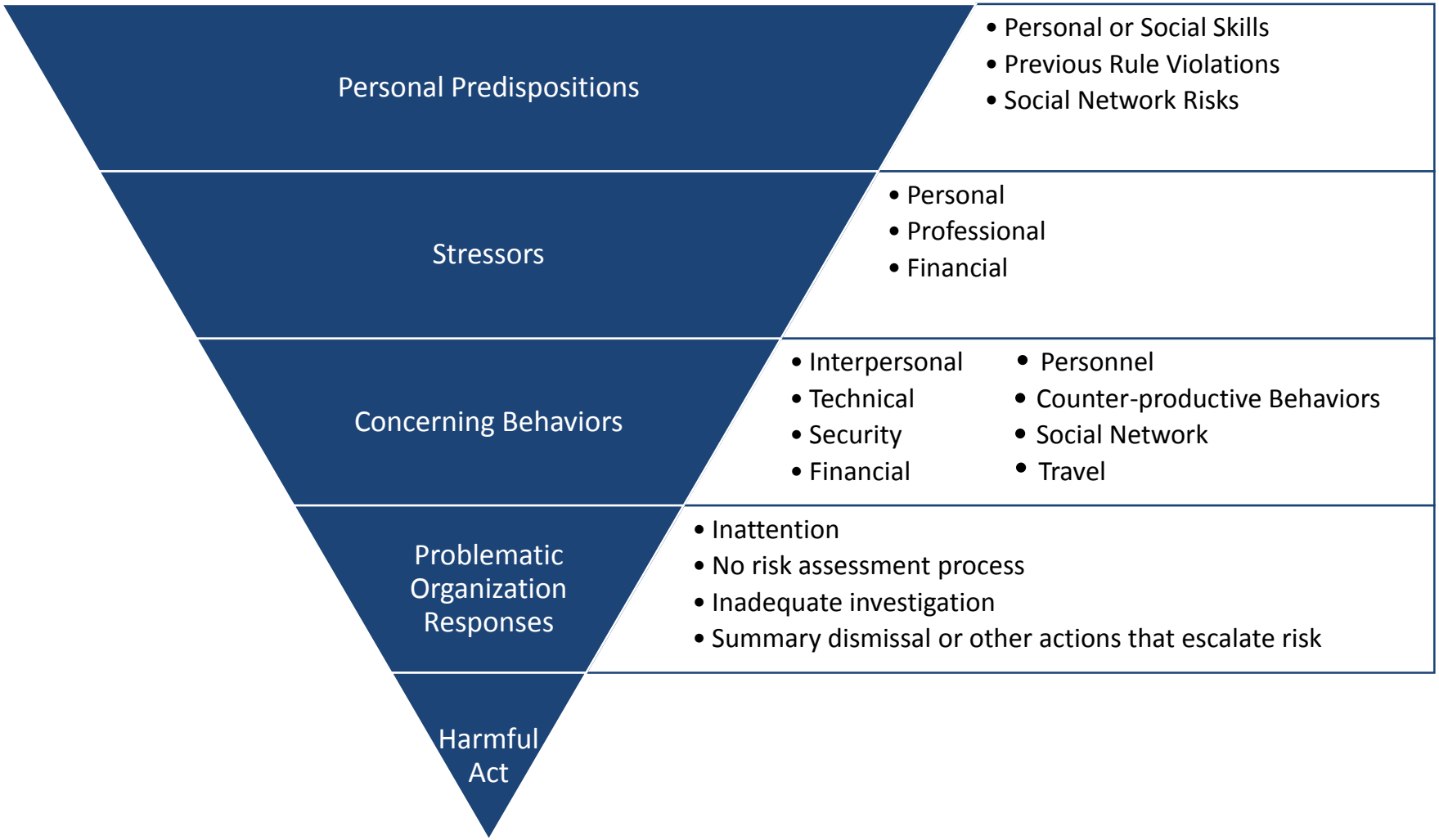
Returned from leave and requested access to future product information

- Downloaded over 200 technical documents that were outside their scope of work
- Physically removed two large bags full of proprietary information (security cameras captured this event)

Insider resigns the day after stealing the information

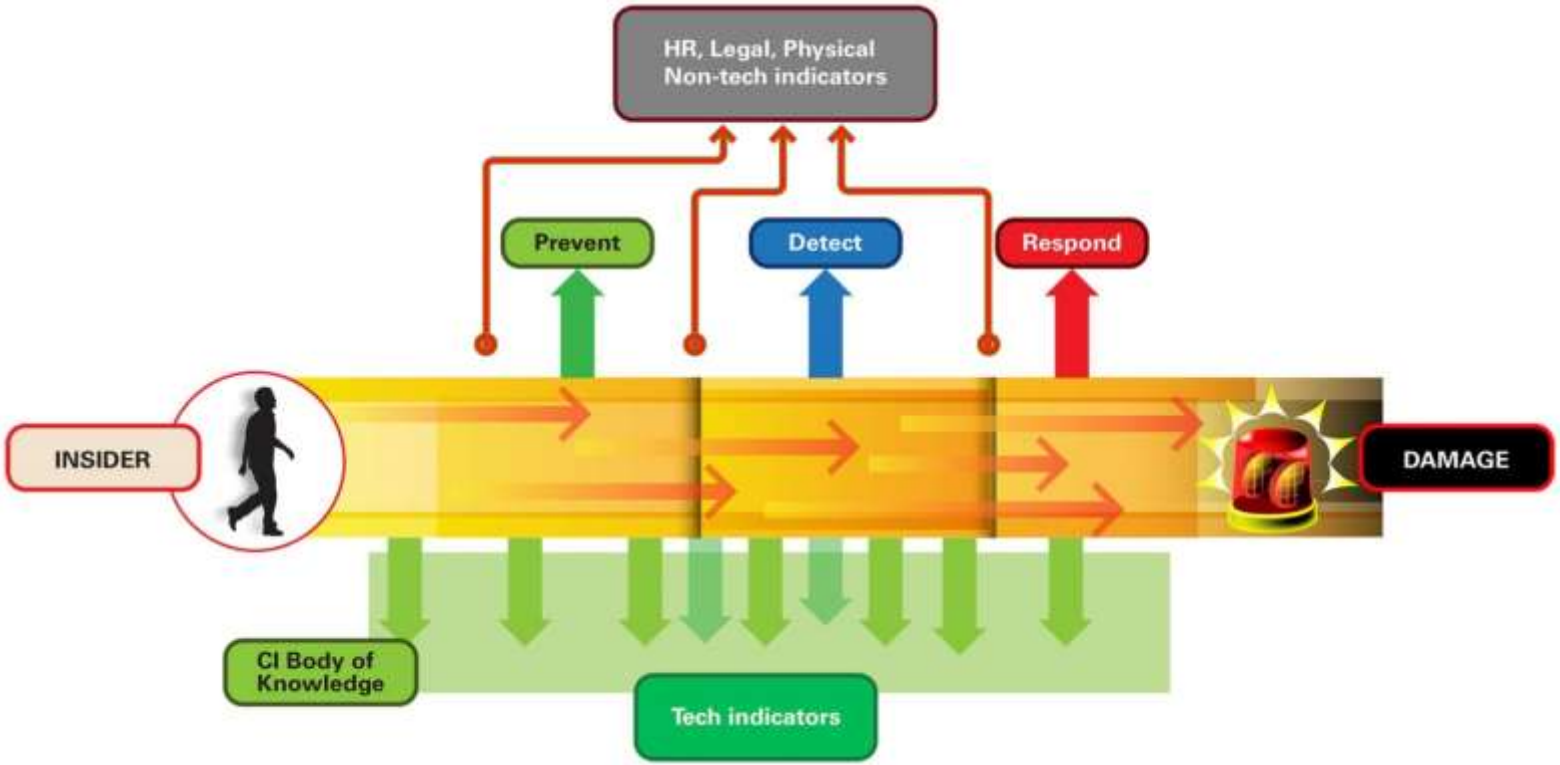
- Returned again to the site after submitting resignation to download even more information
- Subject was arrested during a random search at the airport with $600,000,000 worth of company trade secrets just prior to boarding a flight out of the US

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)

The Goal for an Insider Threat Program…



Is to reduce insider risks to critical assets to acceptable levels

https://insights.sei.cmu.edu/insider-threat/2020/01/maturing-your-insider-threat-program-into-an-insider-risk-management-program.html

“Acceptable Levels”? Quantifiable and Actionable Risk Appetite Statements for Likelihood and Impact

Executive Attention

- Threat is between 75-99% likely to occur within the next year, or has occurred within the industry in the last year

Management Attention

- Threat is between 30-74% likely to occur within the next year, or has occurred within the industry in the last two years

Front Line Attention

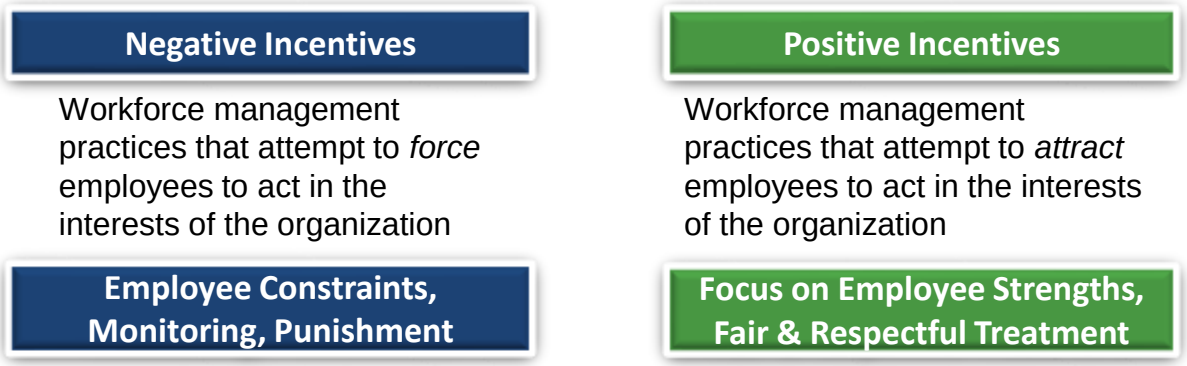
- Threat is between 1-29% likely to occur within the next year, or has occurred within the industry in the last 5 years

	Revenue (Operating Profit)	Safety	Operations	Reputation	Compliance	Human Capital	Projects
Escalate to Executive Attention	Any more than a 10% deviation from planned operating profit for a quarter	Loss of life or permanent disability	No more than three days of lost operations	Loss of market segment with multiple customers	Debarrment from a particular market segment linked to regulatory violation(s)	Any more than 5% high performer attrition from any business unit in a quarter	Liquidated damages that exceed contract value
Escalate to Management Attention	Any more than a 5% deviation from planned operating profit for a quarter	Time away or other reportable incident	No more than one day of lost operation	Loss of customer	Any fines or other penalties linked to regulatory violation(s)	Any more than 3% high performer attrition from any business unity in a quarter	Liquidated damages that erode the margin as sold
Provide Front Line Attention	Any deviations from planned operating profit for a quarter	Bumps, strains, bruises	No more than one shift of lost operation	Customer complaints or negative social media buzz	Any warnings linked to regulatory violation(s)	Any developing trend in high performer attrition	Minor disputes with limited contractual impact

https://www.rsaconference.com/industry-topics/presentation/finding-the-right-answersfacilitating-insider-threat-analysis-using-octave

A Balanced Approach to Insider Risk Management

Organizations typically focus their insider threat programs almost exclusively on negative incentives.

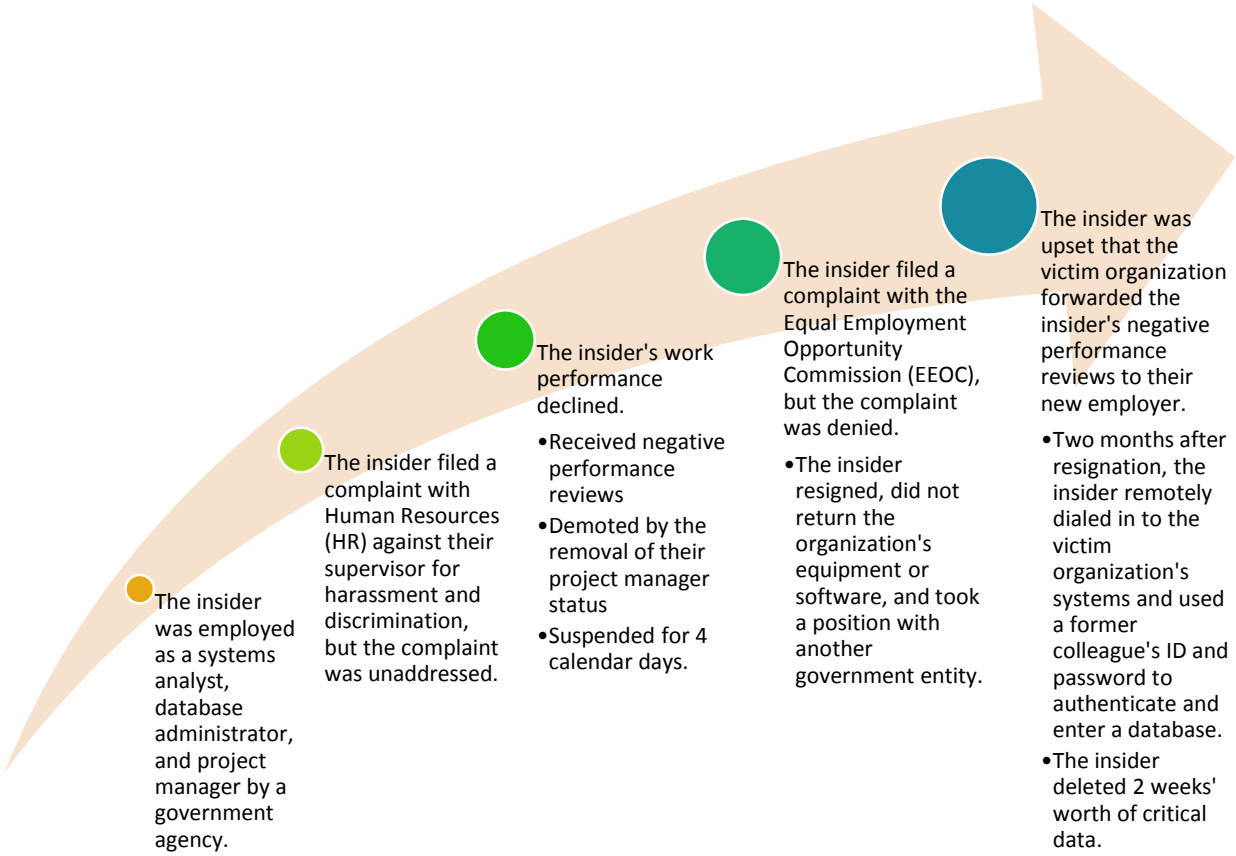


Negative incentives alone can exacerbate the threat they are intended to mitigate.*

Basic Tenet: Organizations should explicitly consider a mix of positive and negative incentives to build insider threat programs that are a net positive for employees and the organization.

* See “Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls,” SEI Digital Library, March 2015.

Case Example: Failure to ensure employee concerns are heard and acted upon.



Conclusion

The Counter-Insider Threat Program of the future is an integrated, proactive, risk-based mission enabler that makes its organization operationally resilient against insider threats.

How do we get there?

- By expanding relationships with traditionally under-represented insider threat program stakeholders
- By clearly articulating program goals and risk appetite
- By placing an emphasis on process institutionalization, yielding more stable processes that produce consistent results over time that are retained during times of stress

References / Resources

Featured Research from the CERT National Insider Threat Center – 1

The Common Sense Guide to Mitigating Insider Threats, Sixth Edition – a collection of 21 best practices for insider threat mitigation, complete with case studies and statistics

- https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=540644

Balancing Organizational Incentives to Counter Insider Threat – a study on how positive incentives can complement traditional security practices to provide a better balance for organizations' insider threat programs

- https://ieeexplore.ieee.org/abstract/document/8424655

Featured Research from the CERT National Insider Threat Center – 2

Navigating the Insider Threat Tool Landscape: Low Cost Technical Solutions to Jump-Start an Insider Threat Program – an exploration of the types of tools that organizations can use to prevent, detect, and respond to multiples types of insider threats

- https://resources.sei.cmu.edu/asset_files/WhitePaper/2018_019_001_521706.pdf

Insider Threats Across Industry Sectors – a multi-part blog series that contains the most up-to-date statistics from our database on sector-specific insider threats

- https://insights.sei.cmu.edu/insider-threat/2018/10/insider-threat-incident-analysis-by-sector-part-1-of-9.html

Featured Research from the CERT National Insider Threat Center – 3

Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls

- https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=446367

Analytic Approaches to Detect Insider Threats

- https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=451065

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

- https://web.archive.org/web/20170122065908/http:/resources.sei.cmu.edu/library/asset-view.cfm?assetid=48668

Featured Research from the CERT National Insider Threat Center – 4

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

- https://resources.sei.cmu.edu/asset_files/Presentation/2016_017_001_474306.pdf

An Insider Threat Indicator Ontology

- https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=454613

Resources and Tools for Operational Resilience Management

- CERT Resilience Management Model
  - https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419
- RMM Code of Practice Crosswalk
  - https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084
- RMM NIST SP 800 Series Crosswalk
  - https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=93044
- Operationally Critical Threat, Asset, and Vulnerability Evaluation
  - https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=309051

Where We'll Be Presenting This Month

- Three presentations available in the week two materials of the Department of Defense Counter-Insider Threat Social & Behavioral Science Research Summit
  - https://sbssummit.com/week-two/
- September 17 – Keynote Address - Insider Risk Summit
  - https://www.insiderrisksummit.com/
- September 22 - Insider Risk Quantification - National Insider Threat Task Force Tech Talk series
  - https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf
- September 22 – Building and Effective Insider Risk Management Program – National White Collar Crime Center Webinar Series
  - https://www.nw3c.org/webinars/Register?id=11535
- September 24 – Technical Detection Methods for Insider Risk Mitigation – National White Collar Crime Center Webinar Series
  - https://www.nw3c.org/webinars/Register?id=11536
- September 30 – Insider Incidents in the Energy Sector - Reliability First Insider Threat Webinar
  - https://www.eventbrite.com/e/insider-threat-webinar-tickets-118341477545

Training from the CERT National Insider Threat Center

Our insider threat program manager, vulnerability assessor, and program evaluator certificate programs and insider threat analyst training courses are now available in live-online delivery formats!

For more information, please visit www.sei.cmu.edu/education-outreach/courses/index.cfm

For More Information

Over 125 publications are available at our website, www.cert.org/insider-threat

We're updating our blog (www.insights.sei.cmu.edu/insider-threat) weekly this month

Any other questions or comments? Email us at insider-threat-feedback@cert.org.