Insider Threat or Insider Risk — What Are You Trying to Solve?

Michael C. Theis, CISSP, SAC (Retired)
Chief Engineer, Strategic Engagements,
National Insider Threat Center
in the CERT Program

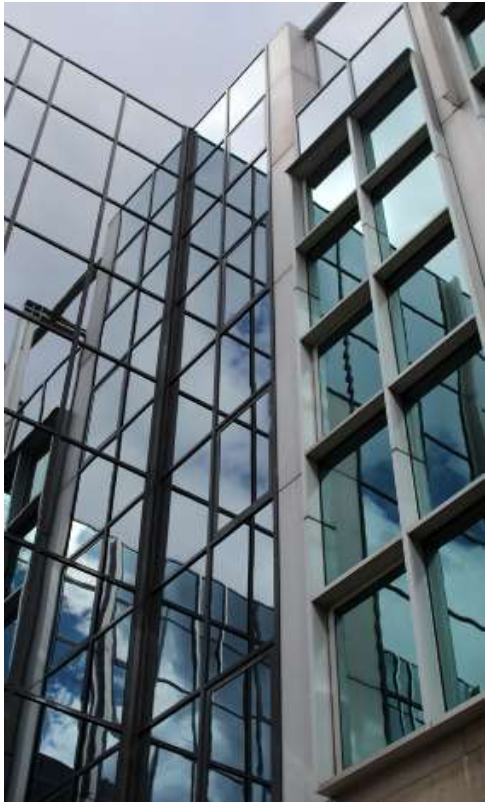
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

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.

DM20-0775

The National Insider Threat Center (NITC)



Center of insider threat expertise

Began working in this area in 2001 with the U.S. Secret Service

Mission: enable effective insider threat mitigation, incident management practices, and develop capabilities for deterring, detecting, and responding to evolving cyber threats

Action and Value: conduct research, modeling, analysis, and outreach to develop & transition socio-technical solutions to combat insider threats

About Insider Threat

There is not one “type” of insider threat

Threat is to an organization’s critical assets

- People
- Information
- Technology
- Facilities

Based on the motive(s) of the insider, impact is to Confidentiality, Availability, Integrity

Cyber attack = Cyber Impact

Kinetic attack = Kinetic Impact

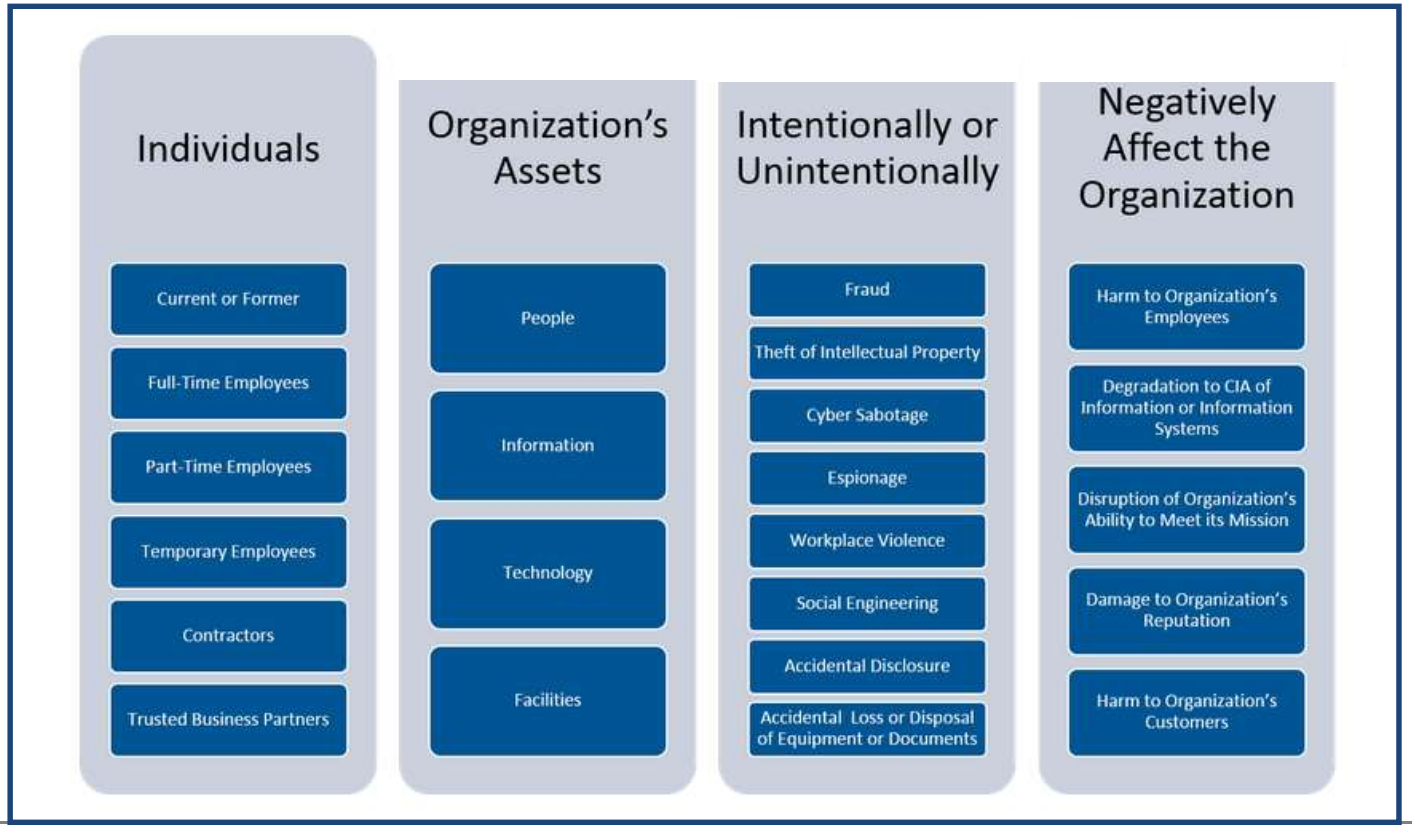
Cyber attack = Kinetic Impact

Kinetic attack = Cyber Impact

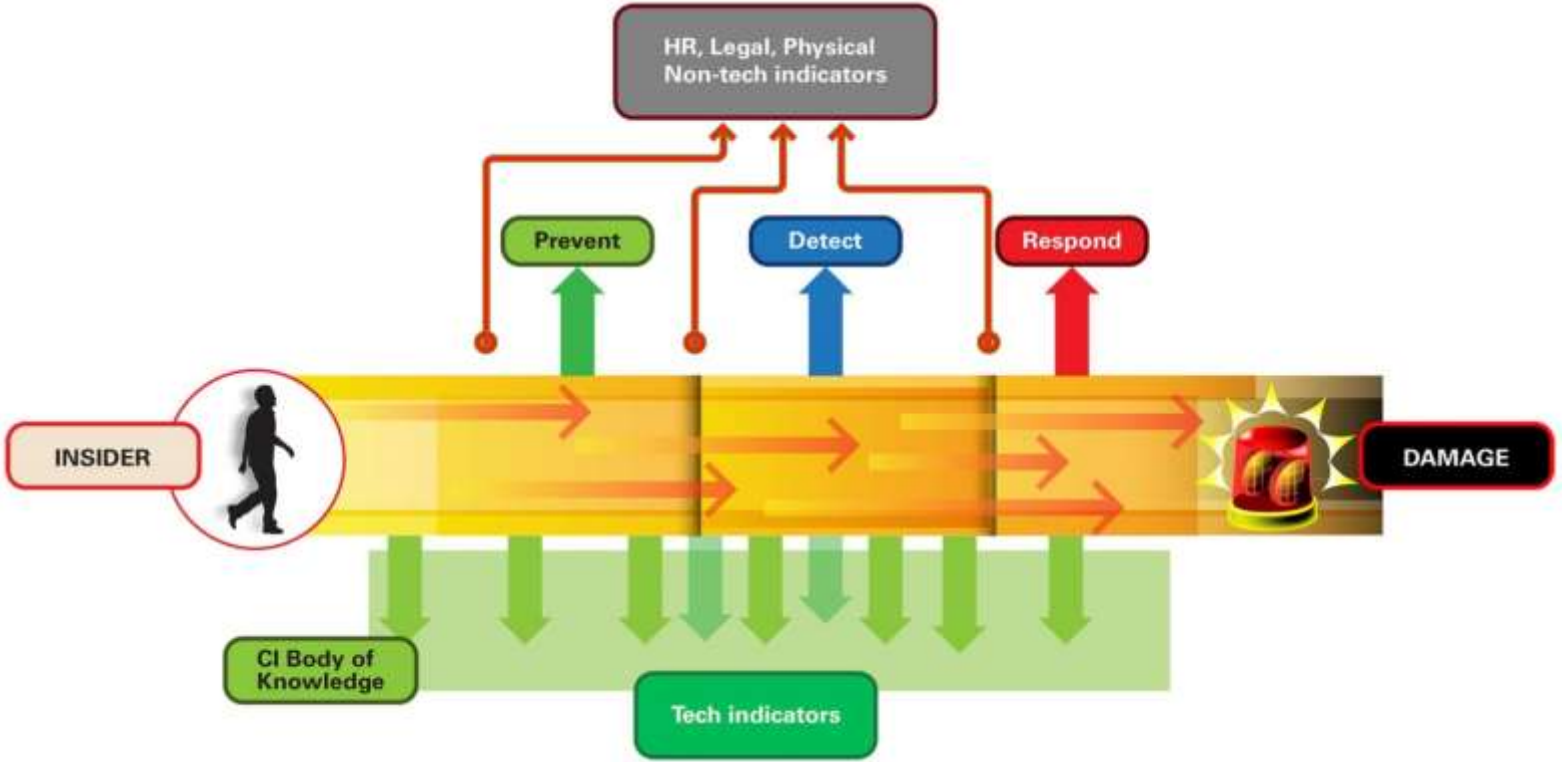
What / Who is an Insider Threat?

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.

What / Who is an Insider Threat?



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

Types of Insider Threat Activity

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Types of Insider Activities - 1

Insider IT Sabotage

An insider's use of IT to direct specific harm at an organization or an individual

- Deletion of information
- Bringing down systems
- Website defacement to embarrass organization

Insider Theft of Intellectual Property

An insider's use of IT to steal intellectual property from the organization

- Proprietary engineering designs, scientific formulas, etc.
- Proprietary source code
- Confidential customer information
- Industrial Espionage and Trade Secrets

Types of Insider Activities - 2

Insider Fraud

An insider's use of IT for the unauthorized modification, addition, or deletion of an organization's data (not programs or systems) for personal gain, or theft of information which leads to fraud

- Payroll
- Reimbursement
- Unauthorized acquisitions

Theft and sale of confidential information

- SSN, PII, etc.
- Credit card numbers

Modification of critical data for a fee

- Driver's license records
- Criminal records
- Qualification for welfare, etc.

Types of Insider Activities - 3

Insider National Security Espionage

- The act of communicating, delivering or transmitting information pertaining to the national defense of the United States to any foreign government or faction, with intent or reason to believe that is to be used to the injury of the United States or to the advantage of a foreign nation
  - Volunteers
  - Recruited in Place
  - Dispatched

Insider Miscellaneous

- Unauthorized disclosure (information insider believed should be in the public domain)
- Providing address of a person to an acquaintance who physically harmed the individual
- Accessing records of high-profile individuals

Types of Insider Activities - 4

Unintentional Insider Threat (UIT) - Four Categories:

DISC - accidental disclosure (e.g., via the Internet)

- sensitive information posted publicly on a website, mishandled, or sent to the wrong party via email, fax, or mail

PHISHING/SOCIAL - malicious code (UIT-HACKing, malware/spyware)

- an outsider's electronic entry acquired through social engineering (e.g., phishing email attack, planted or unauthorized USB drive) and carried out via software, such as malware and spyware

PHYS - improper/accidental disposal of physical records

- lost, discarded, or stolen non-electronic records, such as paper documents

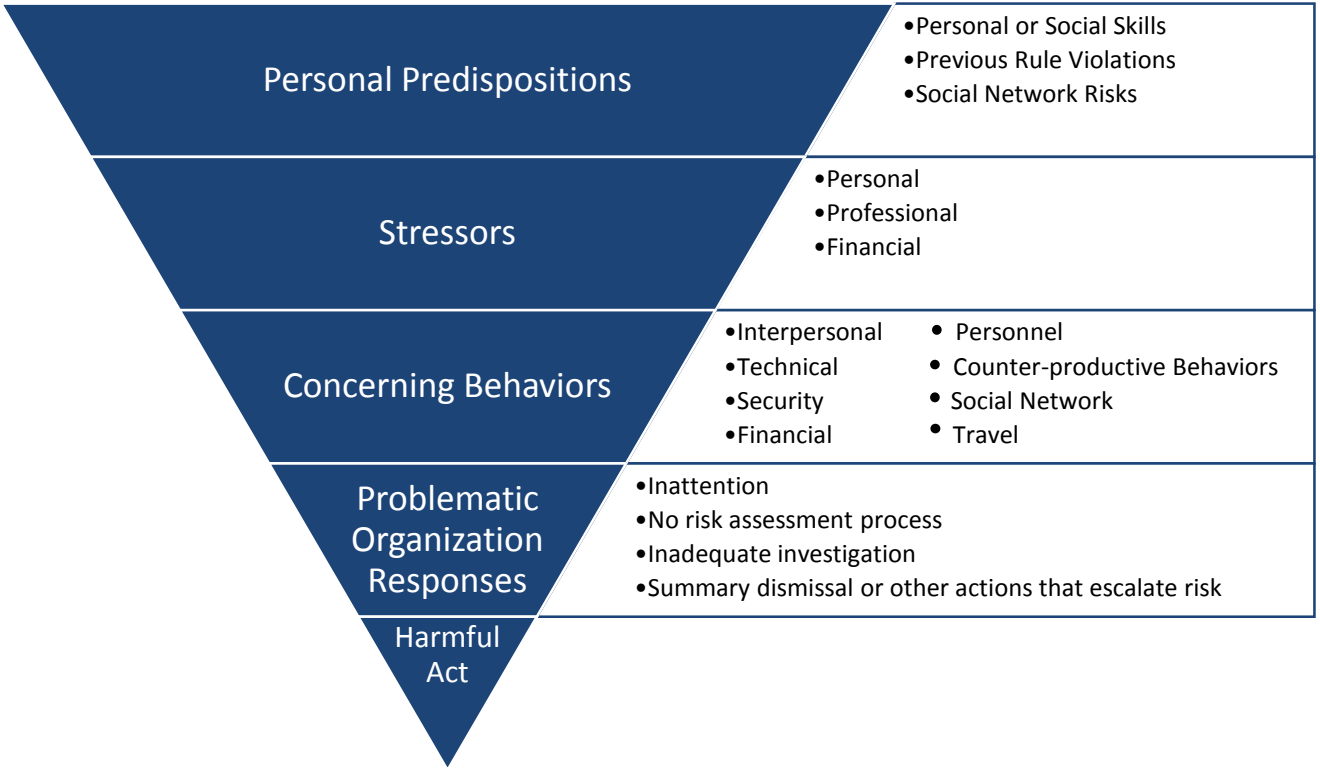
PORT - portable equipment no longer in possession

- lost, discarded, or stolen data storage device, such as a laptop, PDA, smart phone, portable memory device, CD, hard drive, or data tape

Bringing it together – Insiders are humans with behaviors

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

NITC's 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)

Behavioral Potential Risk Indicators (PRI)

Incident Type	Motivation	Behavioral PRIs
Fraud	Financial gain to overcome stress / need; Personal advantage	Significant debt; Living above one's means; Bankruptcy; Tardiness, insubordination, absences, complaints, poor performance
Theft of IP	Business Advantage	Announced resignation; Attempts to obtain information outside of job role; Post departure reach back to current employees; Deviation from typical working hours
IT Sabotage	Revenge for a perceived injustice	Individuals impacted by organization events, actions, conditions; Co-worker / supervisor conflicts; Poor performance; Tardiness; Absences; Previous rule volitions
Unintentional	Human error; fatigue; risk perception and risky decision making	Violation(s) of acceptable use policies; Previous rule violations; Failure to complete security awareness training

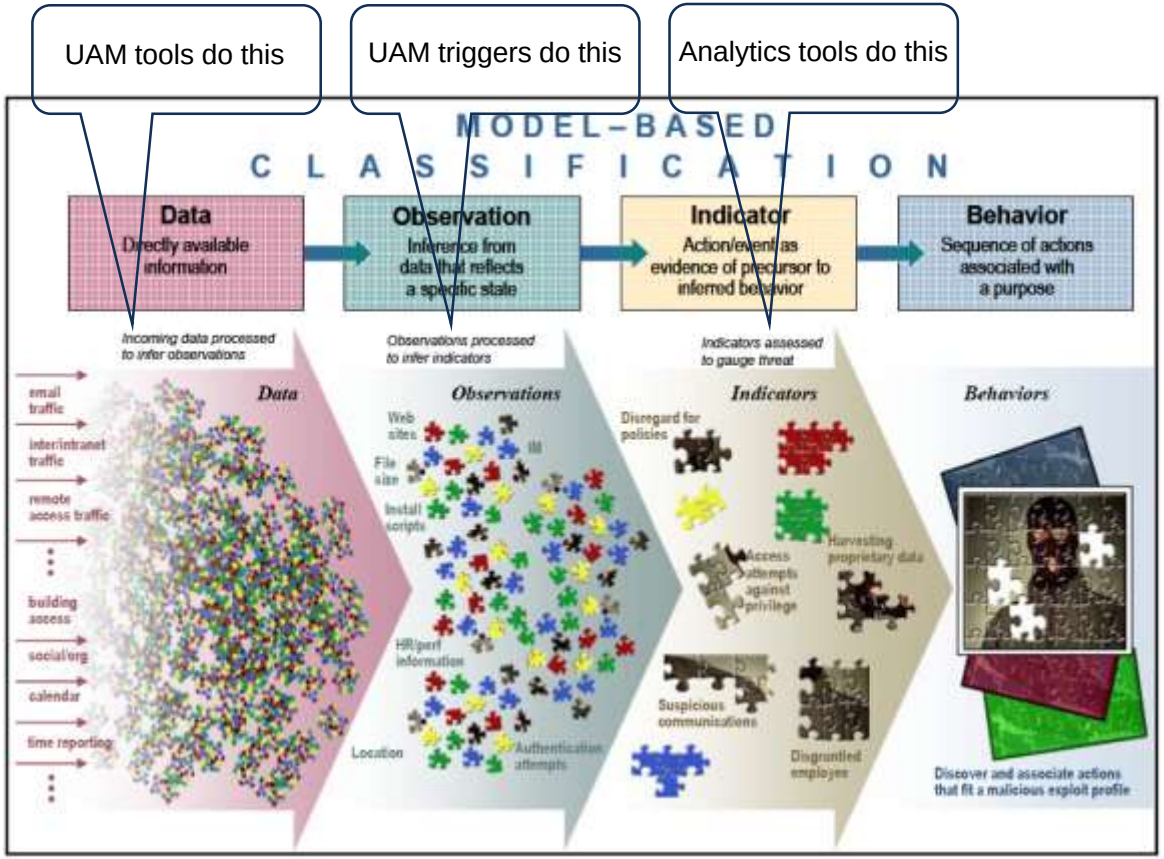
Why Include Behavioral Potential Risk Indicators?

- May provide insight into the motivations of an insider who is considering harming the organization.

- NITC's Corpus shows that behavioral observables were available before technical observables, as the insider progressed down the critical pathway.

- Reliance on technical indicators (alone) may only be effective at detecting an insider incident, which may be too late, rather than assisting in preventing an incident.

A Conceptual Model



Source: Greitzer, et al., “Predictive Modeling for Insider Threat Mitigation,” PNNL-SA-65204, April 2009.

Transitioning to Insider Risk and Resilience

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Where Insider Threat Program's Have Succeeded

- Connecting the dots
- Technical detection of blatant policy violations
- Identifying broken business processes

Where Insider Threat Program's Are Struggling

- Measures of Effectiveness / ROI
- Scoping
- Change management
- Proactive responses to the conditions that precede harmful acts

Where Insider Threat Programs Traditionally Focus

Engineering		
ADM	Asset Definition and Management	
CTRL	Controls Management	★
RRD	Resilience Requirements Development	
RRM	Resilience Requirements Management	
RTSE	Resilient Technical Solution Engineering	
SC	Service Continuity	

Enterprise Management		
COMM	Communications	★
COMP	Compliance	
EF	Enterprise Focus	★
FRM	Financial Resource Management	★
HRM	Human Resource Management	★
OTA	Organizational Training and Awareness	★
RISK	Risk Management	

Operations		
AM	Access Management	★
EC	Environmental Control	
EXD	External Dependencies Management	
ID	Identity Management	★
IMC	Incident Management and Control	★
KIM	Knowledge and Information Management	
PM	People Management	
TM	Technology Management	★
VAR	Vulnerability Analysis and Resolution	★

Process Management		
MA	Measurement and Analysis	★
MON	Monitoring	★
OPD	Organizational Process Definition	
OPF	Organizational Process Focus	

Where Insider Threat Programs Need To Expand

Engineering		
ADM	Asset Definition and Management	★
CTRL	Controls Management	
RRD	Resilience Requirements Development	★
RRM	Resilience Requirements Management	★
RTSE	Resilient Technical Solution Engineering	★
SC	Service Continuity	★

Enterprise Management		
COMM	Communications	
COMP	Compliance	★
EF	Enterprise Focus	
FRM	Financial Resource Management	
HRM	Human Resource Management	
OTA	Organizational Training and Awareness	
RISK	Risk Management	★

Operations		
AM	Access Management	
EC	Environmental Control	★
EXD	External Dependencies Management	★
ID	Identity Management	
IMC	Incident Management and Control	
KIM	Knowledge and Information Management	★
PM	People Management	★
TM	Technology Management	
VAR	Vulnerability Analysis and Resolution	

Process Management		
MA	Measurement and Analysis	
MON	Monitoring	
OPD	Organizational Process Definition	★
OPF	Organizational Process Focus	★

Operational Resilience

Operational resilience: The *emergent property* of an organization that can continue to carry out its mission in the presence of operational *stress* and *disruption* that does not exceed its limit.

Stress and *disruption* come from **risk**

Risk is the impact and likelihood associated with a threat occurring

Operational resilience emerges from effective **risk management**

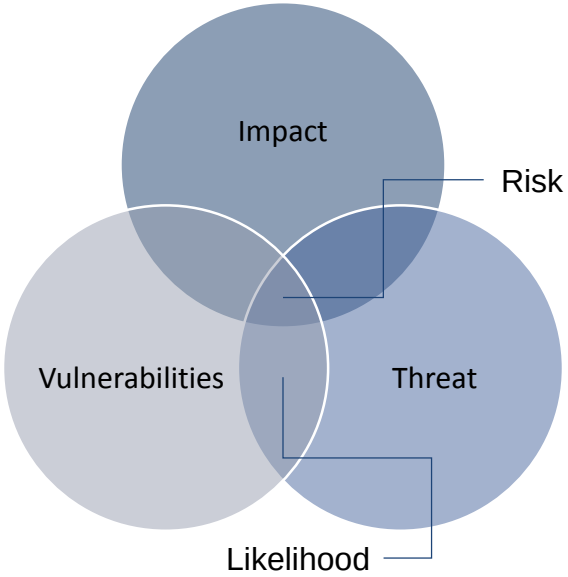
Acceptable Levels?

Risks can be expressed as a function of **impact** and **likelihood**

Deploying controls doesn't necessarily reduce the likelihood of a threat occurring, especially for insider threats.

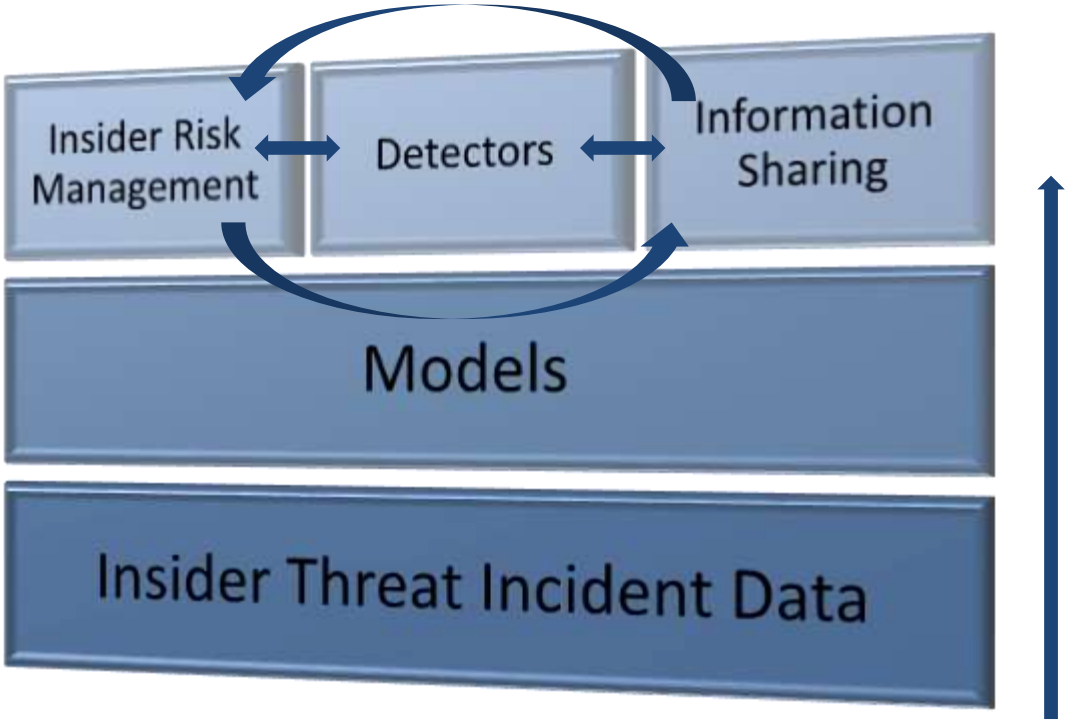
How much insider risk is our organization willing or able to withstand while still carrying out its mission?

- To begin to answer this question, we need quantifiable and actionable **risk appetite statements**
  - To do this, we need reliable, sound methods for measuring the likelihood and impact of insider threats



How Do We Get There?

- Business impact analysis
- Continuous measurement of current security posture
- Broadening the scope of what's considered a 'security control'
- Using our data
- Information sharing

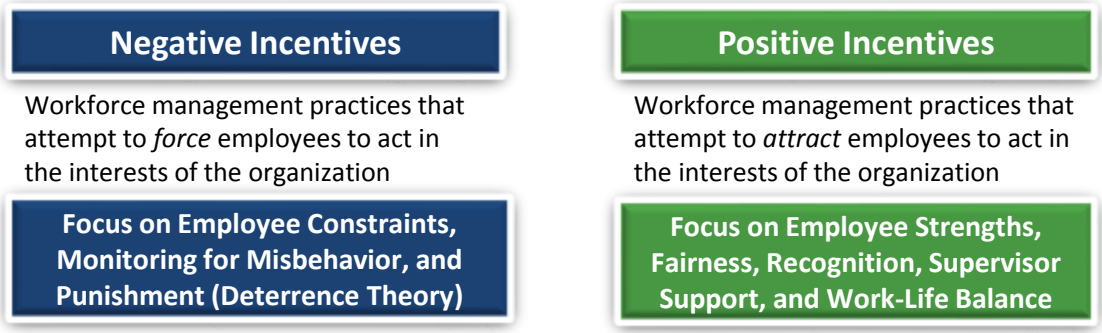


Consider Using Positive Deterrence

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Background of NITC Research Project

Incentives are the means to change attitudes and the (hypothesized) result is deterrence.



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

The influence of positive attitudes and certain positive incentives on certain beneficial organizational outcomes is well-studied in organizational behavior literature, but not specifically for insider threat deterrence.

Basic Belief: Organizations should *explicitly* consider a *mix of positive and negative incentives* to build insider threat programs to optimize the efficacy of insider threat defense.

Moore et al – The Critical Role of Positive Incentives for Reducing Insider Threats https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=484917

Three Broad Categories of Positive Incentives

People

Connected @ Work

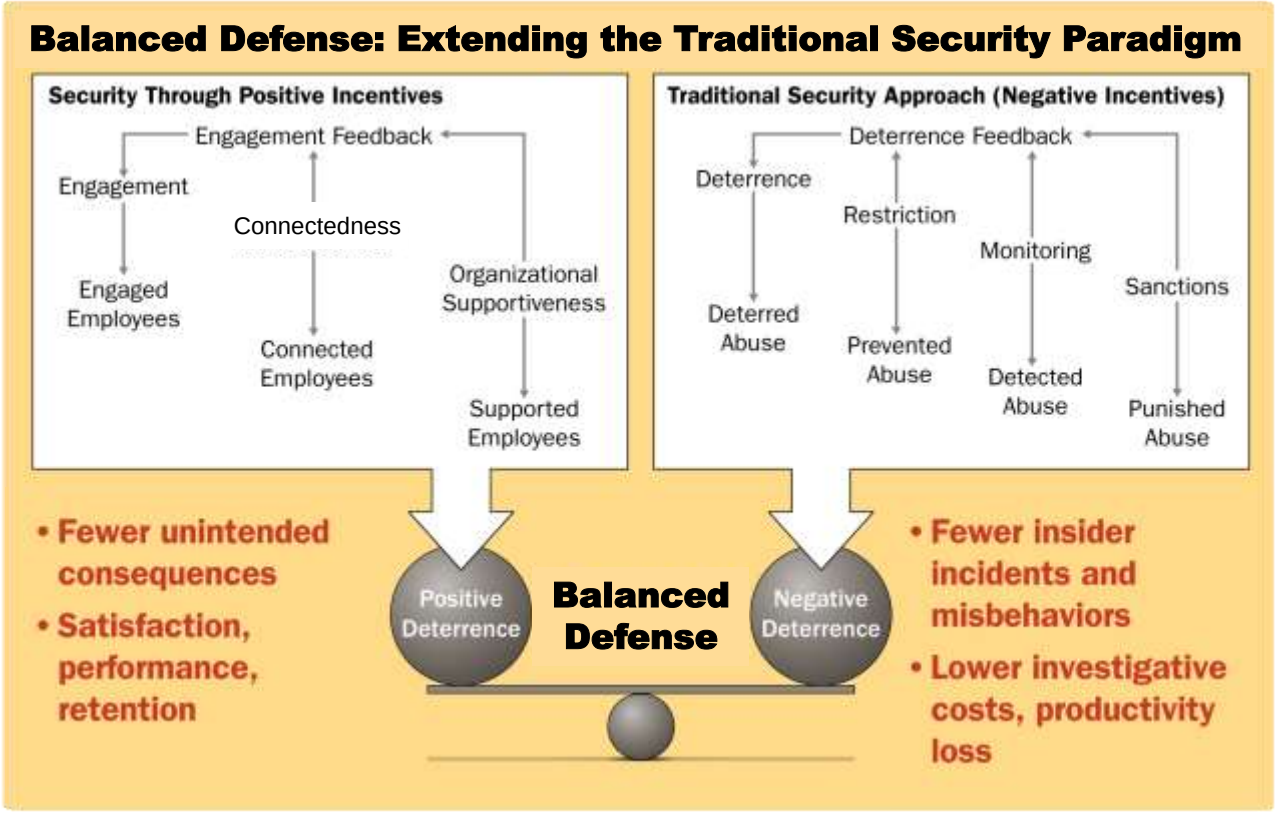
Job

Job Engagement

Organization

Perceived Organizational Support

Vision for Integrating Positive and Negative Incentives



The Future

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

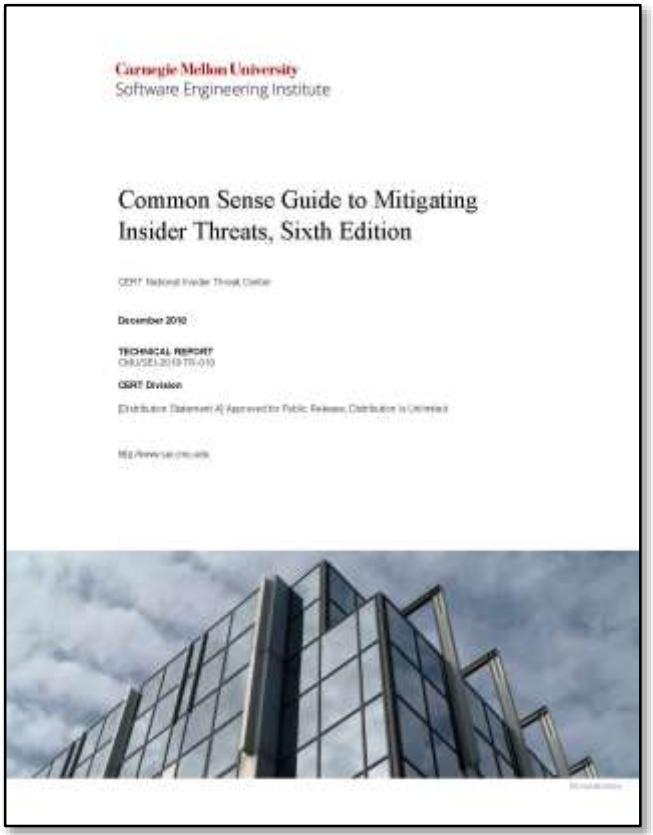
This future state can be realized by:

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

Common Sense Guide, Sixth Edition

A Mitigation Strategy

Common Sense Guide, Sixth Edition



CERT's Common Sense Guide to Mitigating Insider Threats, Sixth Edition https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=540644

Contact Information

CERT National Insider Threat Center

Website: http://www.cert.org/insider-threat/

Blog: http://www.cert.org/blogs/insider-threat/

Email: insider-threat-feedback@cert.org

Contact

Michael Theis

Chief Engineer, Strategic Engagements

CERT National Insider Threat Center

Email: mctheis@cert.org