From Mitigating Insider Threats to Managing Insider Risk

Dan Costa

Sarah Miller

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.

DM20-0714

Where InTP's Have Succeeded

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

Where InTP'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

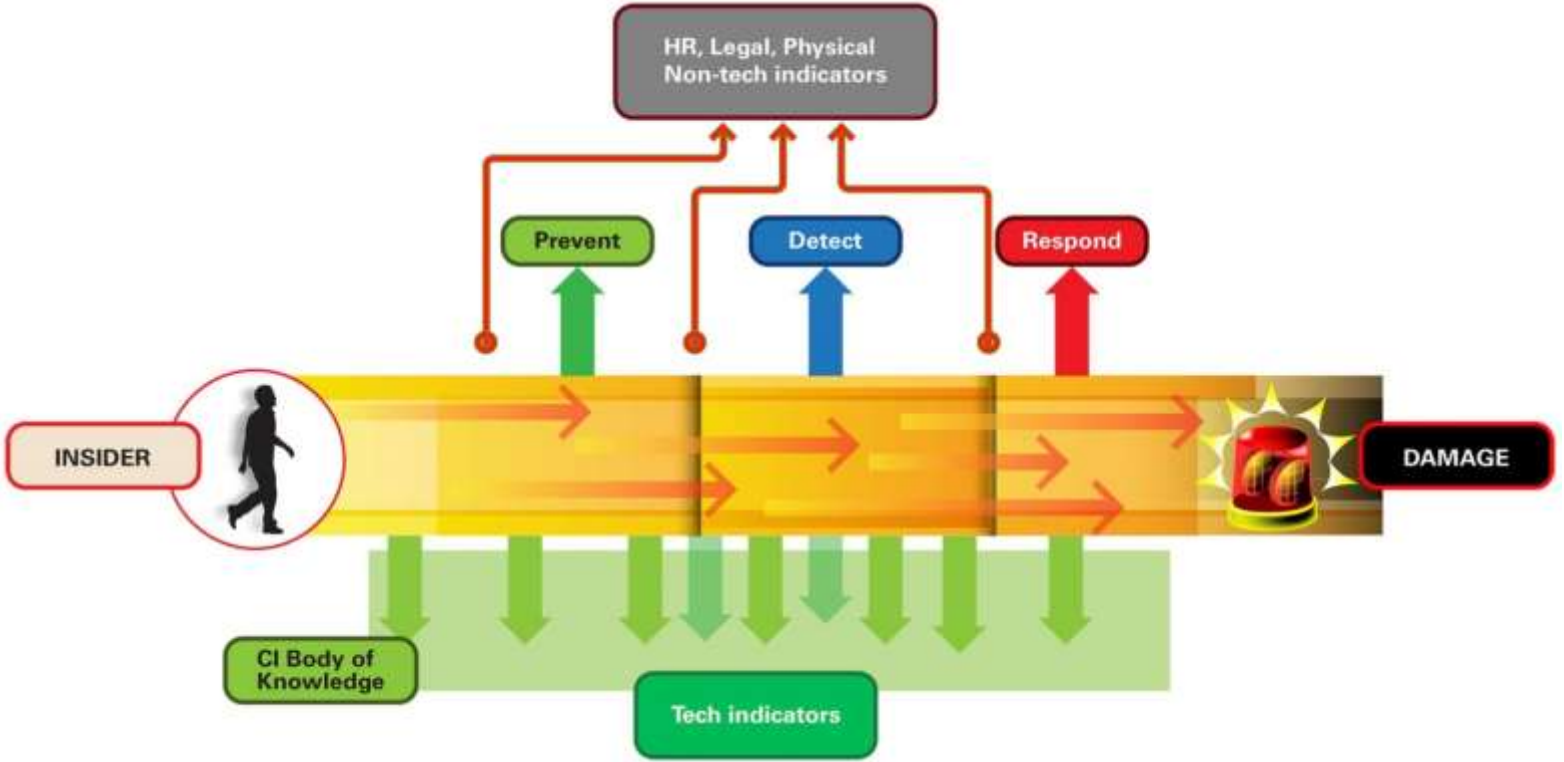
Operational resilience: The *emergent property* of an organization that can continue to carry out its mission in the presence of operational *stress* and *disruption* that does not exceed its limit.

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

Risk is the impact and likelihood associated with a threat occurring

Operational resilience emerges from effective **risk management**

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

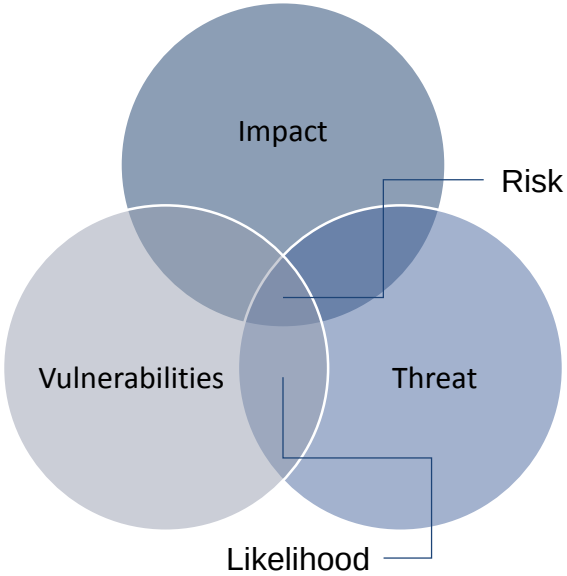
Acceptable Levels?

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.

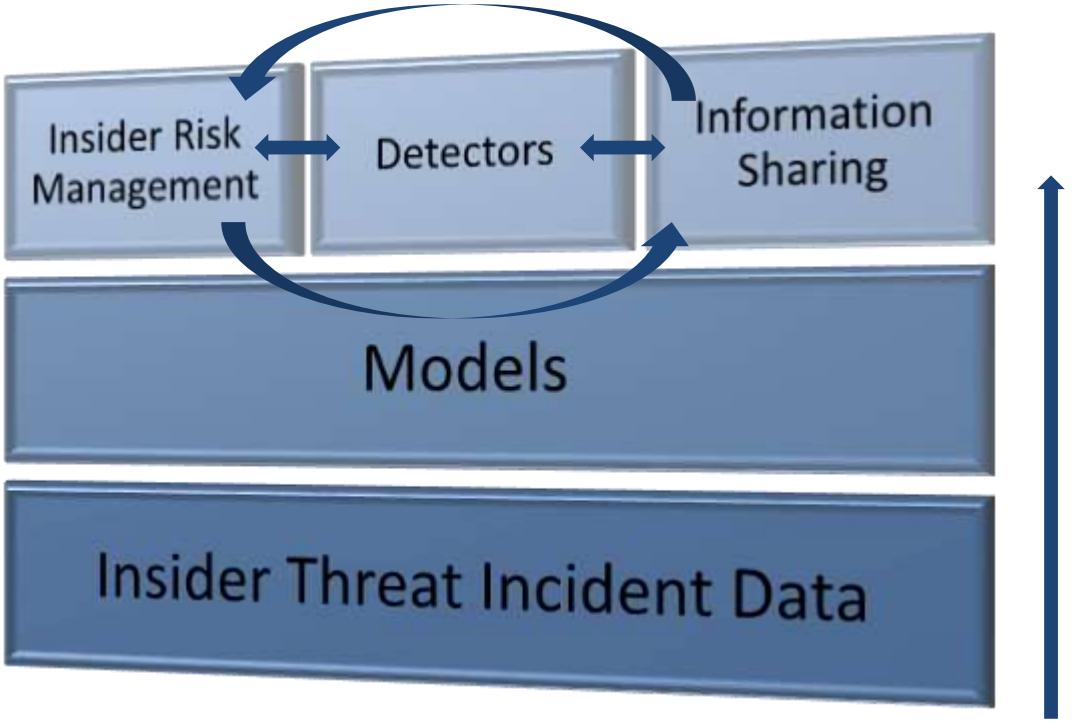
How much insider risk is our organization willing or able to withstand while still carrying out its mission?

- 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



Conclusion

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