Leveraging Insider Threat Incident Data and Information Sharing for Increased Organizational Resiliency

Sarah Miller

National Insider Threat Center, CERT Division

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

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.

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.

DM20-0607

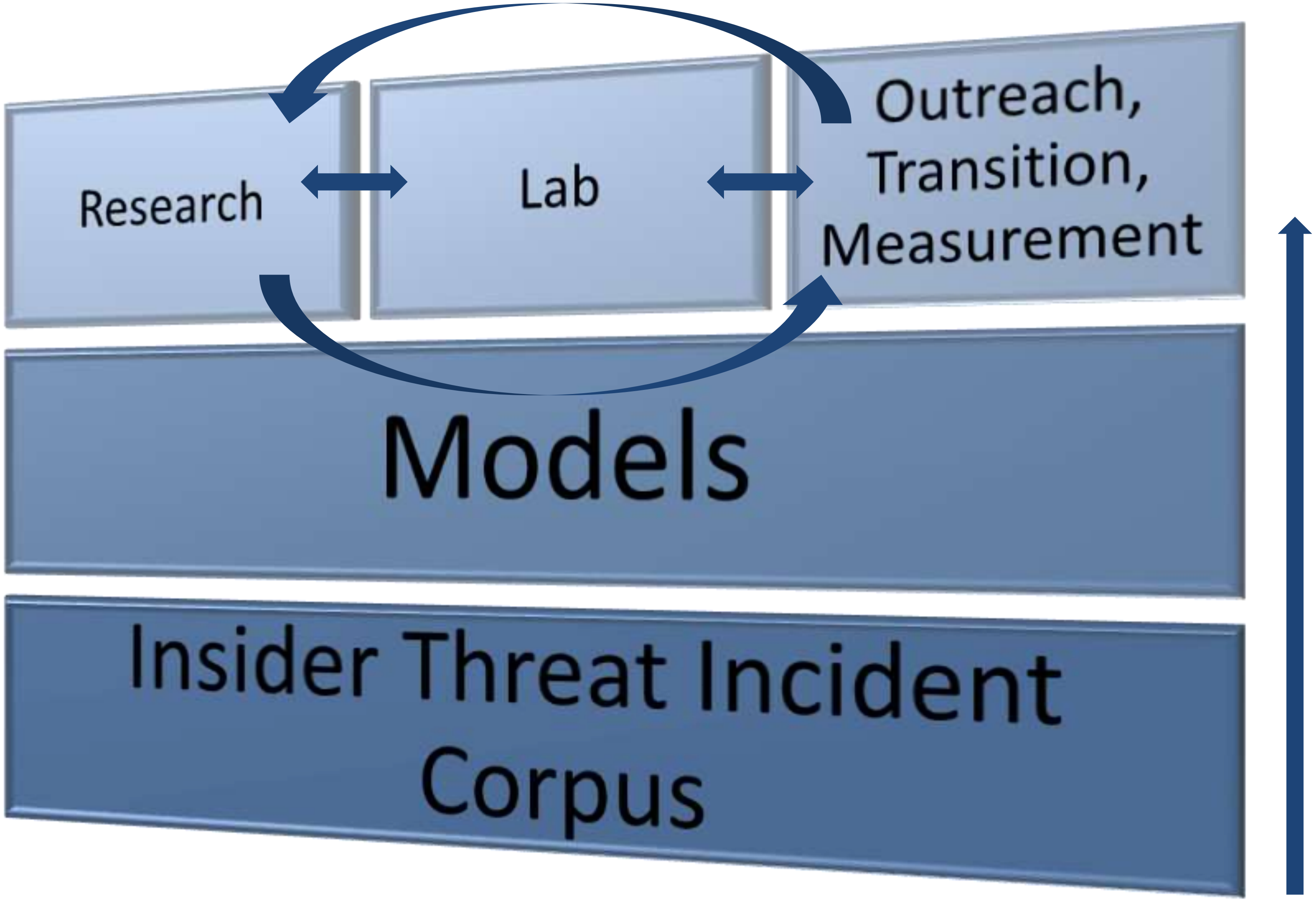
Abstract

To better prepare counter-insider threat programs for the future, organizations can leverage past incident data and artifacts to build insider threat incident corpora.

In this presentation, we will:

- Use the development and stewardship of CERT National Insider Threat Center's Insider Threat Incident Corpus as an exemplar of this process.
- Review supporting information and cyber security frameworks that reflect the need for information sharing, counter-insider threat programs, and incident corpora.
- Discuss the types of information sharing groups that organizations can join to assist their corpus development efforts.
- Demonstrate how these activities that can improve counter-insider threat program functions and organizational resiliency.

The CERT National Insider Threat Center Approach to the Problem



Research

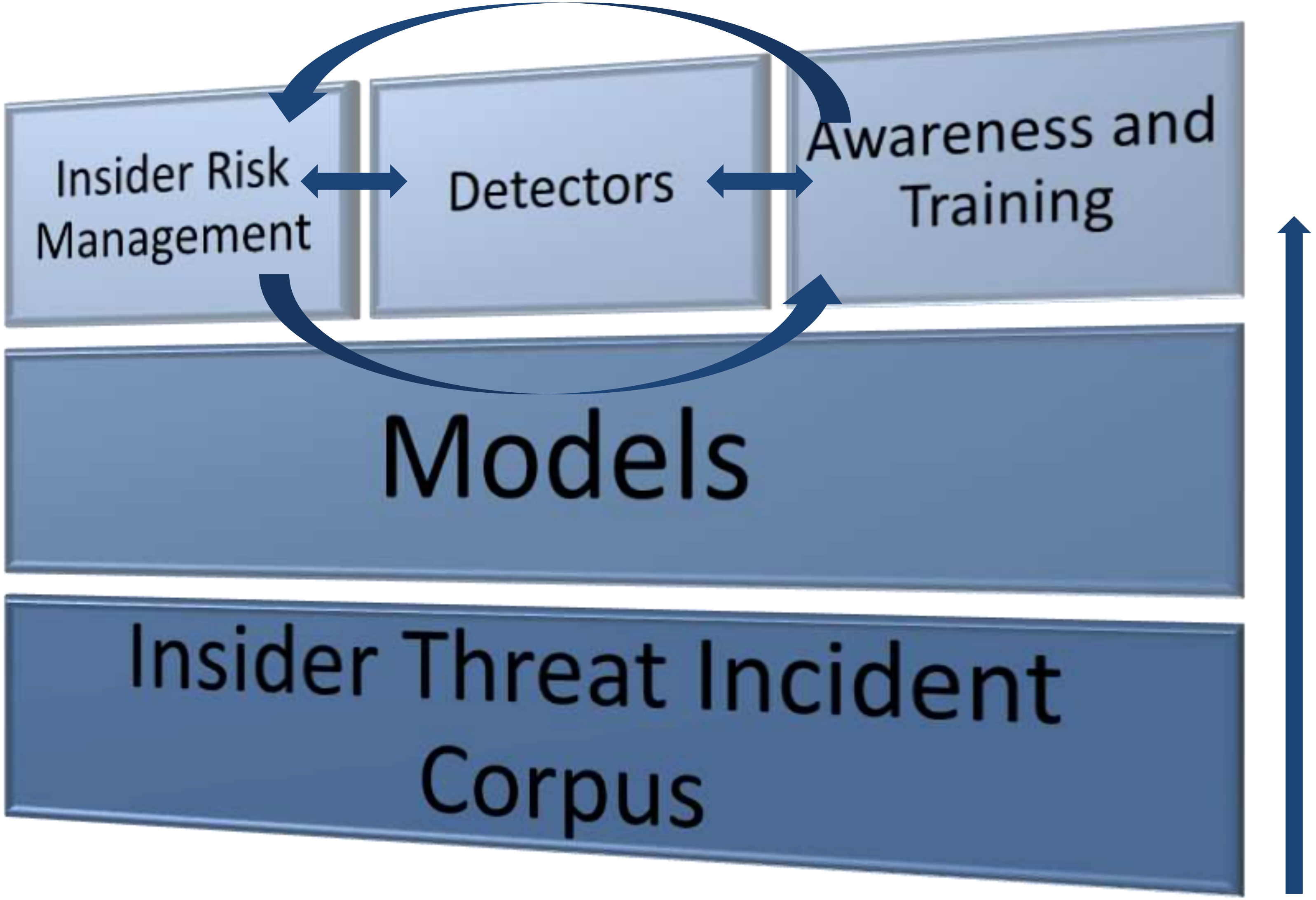
Lab

Outreach, Transition, Measurement

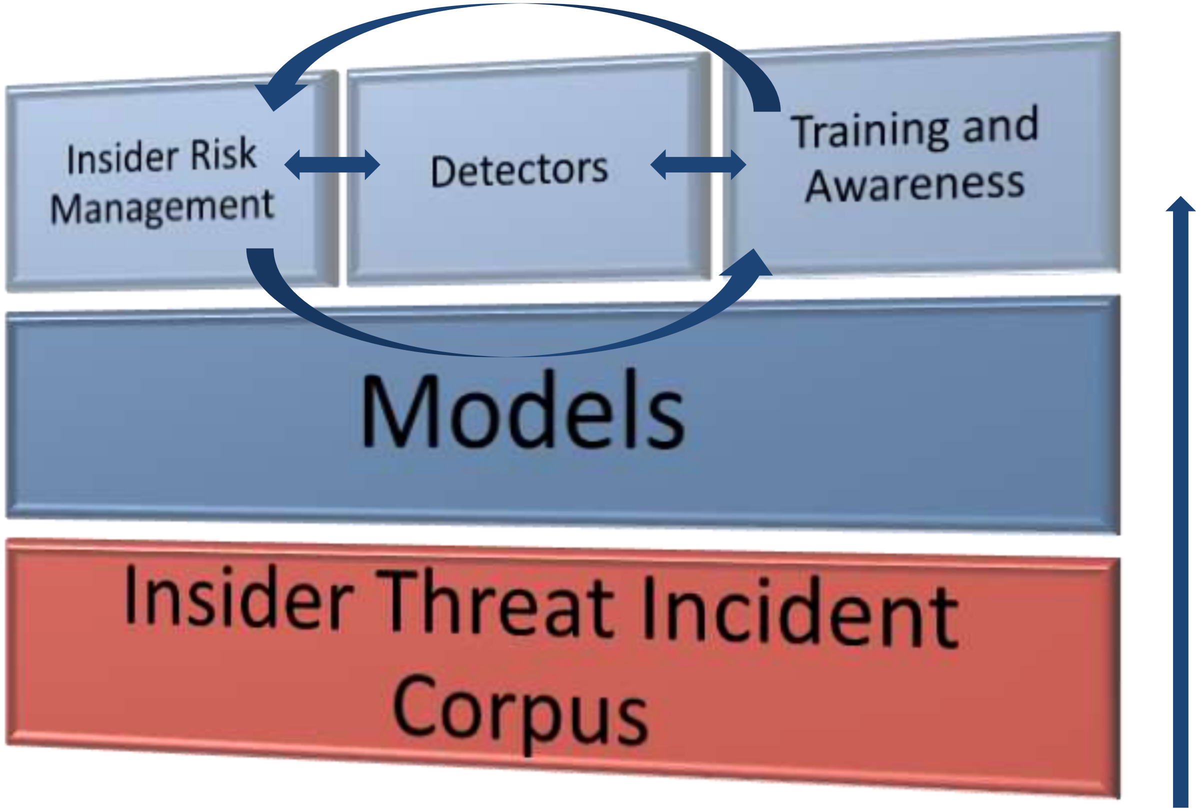
Models

Insider Threat Incident Corpus

Adapting the CERT National Insider Threat Center Approach to Insider Threat Program Operations



Knowledge Management Activities



Build a container for an incident corpus

- database, code repository, document repository, and/or incident tracker/management system

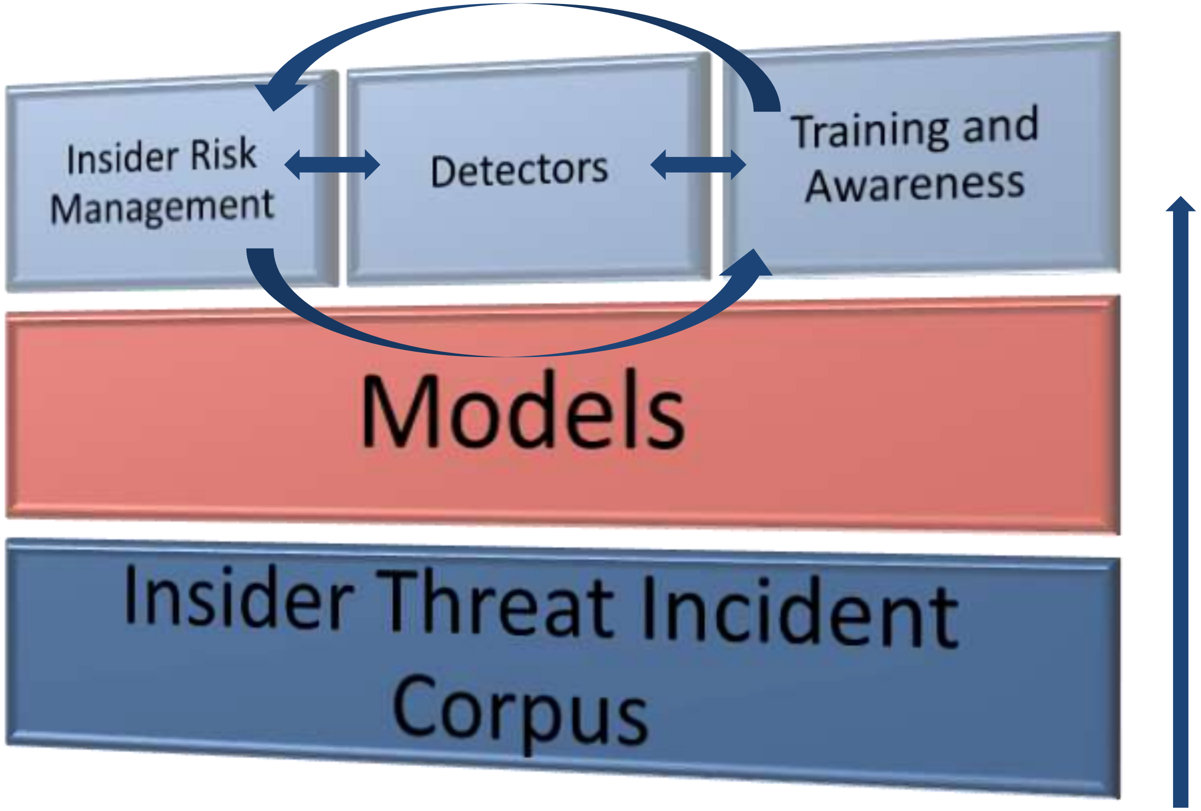
Collect publicly available information

- court records, media reports, social media online forums, and/or information security bulletins

Gather and share incident data with the broader counter-insider threat practitioner community

- abstracted incident data like indicators of compromise, tools, tactics, or procedures
- approaches for prevention, detection, mitigation, or response

Derive Insights from Incident Data – Foundational



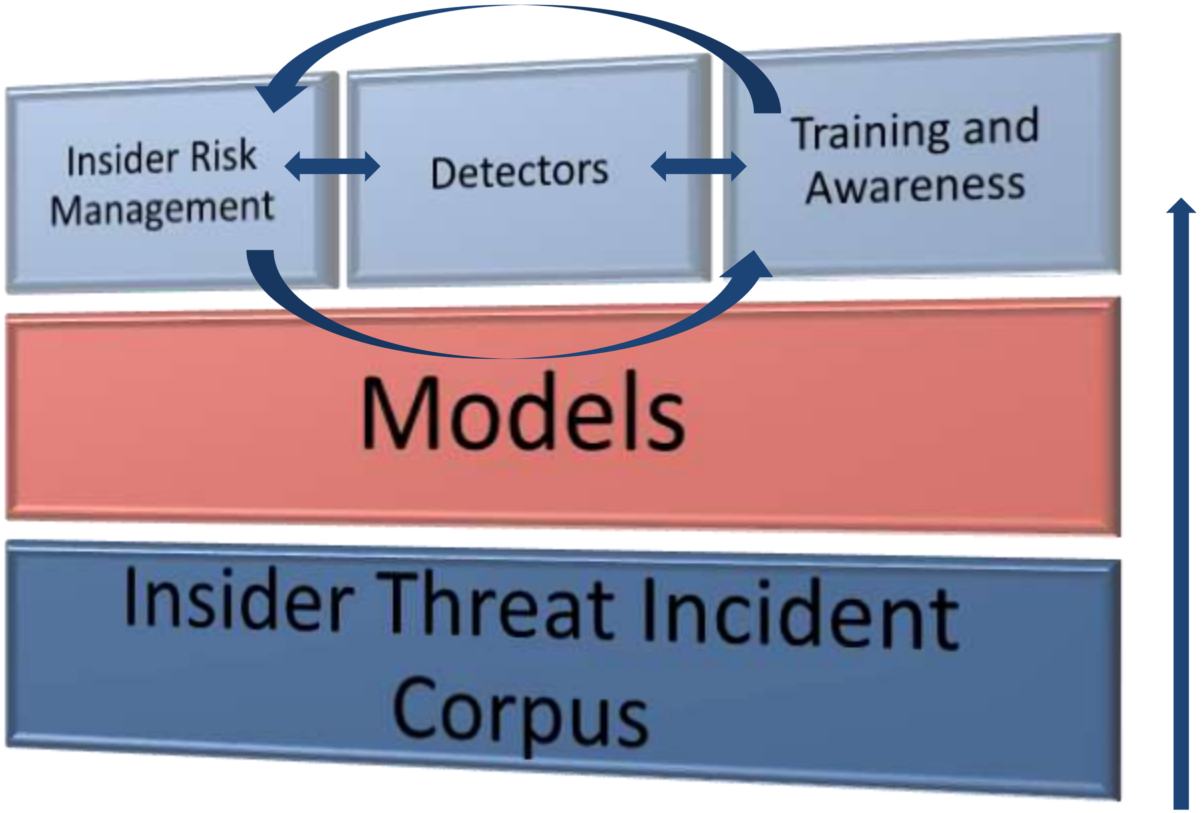
Summary statistics for each metric/category

- Statistical distributions and expected values
- Identifying outliers

Year-over-year trends for each metric

Case studies and lessons learned

Derive Insights from Incident Data – Advanced



Machine Learning (ML) to pre-process or “code” incident data into corpus

Identify statistically significant correlations

- Alternatively, identify co-occurrences approaching statistical significance to continue collecting data on

Named-entity recognition and other Natural Language Processing (NLP) to analyze unstructured text associated with an incident

Incorporate external data sources

- Compare trends and perform baselining
- Identify potential “macro” influences (outside of the organization) on insider incidents

Incident Corpus Project Manager Responsibilities

- Define scope for what will and will not be included
- Collaborate on requirements and use cases
- Acquire and allocate a budget for activities
- Research external sources and standards that can be leveraged to develop an initial data dictionary
- Identify potential stakeholders and Knowledge, Skills, and Abilities (KSAs) desired for team members
- Assign responsibilities for maintenance, analysis, and updates
- Develop documentation for data collection, incident curation, and analysis
- Establish a plan and process for change management
- Set expectations for ongoing stewardship and updates

Limitations of Using Past Incident Data

An incident corpus will only contain data…

- that you had available at the time
  - newer tools or data sources in use by the organization might not have been in place at the time, making it harder to validate that a particular source or tool would have been effective in detecting any one particular insider.
  - previous incidents before the collection process started will not be able to contribute to the overall picture of the threat posed to the organization or long-term trends in insider threats
- for insider threats that you or another organization were able to catch, meaning that you “don’t know what you don’t know.”
- on tools, tactics, techniques, or procedures previously used by insiders, which may change over time as new technologies emerge.

Types of Information Sharing Groups -1

Information Sharing and Analysis Centers (ISACs)

- Critical Infrastructure/Key Resources (CI/KR)
- Bidirectional sharing with government and industry (in theory)
- Many work within CISA CIOCC (formerly NCICC)
- National Council of ISACs has 21 of 33 sector-specific ISACs

Information Sharing and Analysis Organizations (ISAOs)

- Established by EO 13691
- Private sector (original intent)
  - While some may be fall within CI/KR (i.e., could reflect a subsector), they are not *obligated* to share with government or other ISAOs
  - Many still working with CISCP, AIS, ECS, and CISA CIOCC
- ISAO Standards Organization (ISAO SO) provides documentation and guidance
- Many geographically-based groups use term ISAO
  - Possible that some groups may be “classified” as ISAO or ISAC, but use a different name.
  - Not all are “officially” recognized.

Types of Information Sharing Groups -2

Geographical

- National
- State
- Local
- International

Collaborative Structures

- e.g., ISAO SO, Global Resilience Federation

Sector-specific

Common interest

Common concern

Example Common Interest Groups: Insider Threat

- The Open Source Insider Threat (OSIT) information sharing group, operated by the CERT Division, is an industry-only group focused on vendor-free discussions of policies, procedures, tools, and techniques.
- The Association for Threat Assessment Professionals (ATAP) may be useful to organizations considering workplace violence as an insider threat use case.
  - Learn more at https://www.atapworldwide.org/
- The Intelligence and National Security Alliance (INSA) manages an Insider Threat Subcommittee that includes representation from the public and private sectors.
  - Learn more at https://www.insaonline.org/councils/insider-threatsubcommittee/

General Best Practices for Information Sharing

- Clarify goals for information sharing
  - e.g., how it fits into the overall information security, situational awareness, or insider threat program management strategy, etc.
- Establish Non-Disclosure Agreements (NDAs) with organizations that you would like to have enhanced or extended engagements with, especially beyond the standard agreement in place for any mutual information sharing groups
- Dedicate time and resources for participating in information sharing groups
- Incorporate information sharing with external partners or forums into your organization’s incident response process

Information and Cyber Security Frameworks

- Center for Internet Security Critical Security Controls
- CERT Resilience Management Model (CERT-RMM)
- Cybersecurity Capability Maturity Model (C2M2)
- Cybersecurity Maturity Model Certification (CMMC)
- NIST Cybersecurity Framework (CSF)

Conclusion

- Internal development of an insider threat incident corpus can help to inform insider threat program operations and in turn operational resilience more broadly.
  - Models inform insider risk management strategies and detectors.
  - Case studies inform training and awareness activities.
- Information sharing around not only insider threat incidents but program operations and best practices increases the overall state of the practice.
- Leveraging existing standards and practices to implement incident collection and information sharing makes the effort associated with those activities more manageable – and organizations compliant with those same standards in the process.
- The approach, activities, and frameworks described in this presentation will inform a new best practice in the planned *Common Sense Guide to Mitigating Insider Threats, Seventh Edition*.

References and Resources

BSI Group. (2017). Organizational Resilience Index Report 2017. Online: https://www.bsigroup.com/LocalFiles/zh-tw/organizational-resilience/Index-report-for-web.pdf

Cappelli, Dawn., Desai, Akash., Moore, Andrew., Shimeall, Timothy., Weaver, Elise., & Willke, Bradford. (2007). *Management and Education of the Risk of Insider Threat (MERIT): Mitigating the Risk of Sabotage to Employers Information, Systems, or Networks* (CMU/SEI-2006-TN-041). Retrieved July 30, 2020, from the Software Engineering Institute, Carnegie Mellon University website: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=8031

Software Engineering Institute. *CERT Resilience Management Model (CERT-RMM) Collection*. Available online: https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=514489

Theis, Michael., Trzeciak, Randall., Costa, Daniel., Moore, Andrew., Miller, Sarah., Cassidy, Tracy., & Claycomb, William. (2019). *Common Sense Guide to Mitigating Insider Threats, Sixth Edition* (CMU/SEI-2018-TR-010). Retrieved July 30, 2020, from the Software Engineering Institute, Carnegie Mellon University website: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=540644.

Trzeciak, Randy. (2017, November 29). "Announcing the National Insider Threat Center." *Insider Threat Blog*. Available online: https://insights.sei.cmu.edu/insider-threat/2017/11/announcing-the-national-insider-threat-center.html

Contact Information

Sarah Miller

Insider Threat Researcher

National Insider Threat Center

CERT Division

Software Engineering Institute

Carnegie Mellon University

Email: semiller@cert.org

Open Source Insider Threat (OSIT)

Email: osit-forum-support@cert.org

Leveraging Insider Threat Incident Data and Information Sharing for Increased Organizational Resiliency

Additional Materials for Review

Framework Comparison

Framework(s)	Inclusion Rationale	Details	Publisher	Year	Version
Critical Security Controls	Wide adoption by organizations across sectors	• 20 security controls	CIS	2018	7.1
CERT® Resilience Management Model (CERT-RMM)	Wide adoption by organizations across sectors	• 26 process areas	SEI	2016	1.2
Cybersecurity Capability Maturity Model (C2M2)	Not mapped to CMMC Critical Infrastructure Sector	• Cybersecurity capabilities • Maturity model • Evaluation tool	DOE	2014	1.1
Cybersecurity Maturity Model Certification (CMMC)	Mapped to other frameworks	• 17 domains • 43 capabilities • 5 levels per capability	DOD	2020	1.02
NIST Cybersecurity Framework (CSF)	Wide adoption by organizations across sectors	• Five functions • 23 categories • Four implementation tiers	NIST	2018	1.1

Relevant Practices -1

Framework	Domain / Control	Relevant Practice	Number/ID
CIS Controls	Incident Response and Management	Conduct Periodic Incident Scenario Sessions for Personnel	19.7
CIS Controls	Penetration Tests and Red Team Exercises	Conduct Regular External and Internal Penetration Tests	20.2
CIS Controls	Implement a Security Awareness and Training Program	Deliver Training to Fill the Skills Gap	17.2
CIS Controls	Incident Response and Management	Devise Organization-wide Standards For Reporting Incidents	19.4
CIS Controls	Implement a Security Awareness and Training Program	Implement a Security Awareness Program	17.3
CIS Controls	Implement a Security Awareness and Training Program	Train Workforce Members on Identifying and Reporting Incidents	17.9
CERT-RMM	Communications (COMM)	The types and extent of communications needed by the organization to support stakeholder and organizational information needs are identified.	COMM:SG1.SP2
CERT-RMM	Risk Management (RISK)	The sources of risk to assets and services are identified and the categories of risk that are relevant to the organization are determined.	RISK:SG1.SP1
CERT-RMM	Risk Management (RISK)	Collect risk management work products, measures, measurement results, and improvement information derived from planning and performing the process to support future use and improvement	RISK:GG3.GP2
C2M2	Event and Incident Response, Continuity of Operations: Detect Cybersecurity Events	There is a repository where cybersecurity events are logged based on the established criteria	MIL2.e

Relevant Practices -2

Framework	Domain / Control	Relevant Practice	Number/ID
C2M2	Workforce Management: Control the Workforce Life Cycle	A formal accountability process that includes disciplinary actions is implemented for personnel who fail to comply with established security policies and procedures	MIL3.h
C2M2	Workforce Management: Increase Cybersecurity Awareness	Cybersecurity awareness content is based on the organization’s threat profile (TVM-1d)	MIL4.c
C2M2	Risk Management: Manage Cybersecurity Risk	A risk register (a structured repository of identified risks) is used to support risk management activities	MIL3.j
CMMC	Risk Management (RM)	Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria.	RM.3.144
CMMC	Awareness & Training (AT)	Provide awareness training focused on recognizing and responding to threats from social engineering, advanced persistent threat actors, breaches, and suspicious behaviors; update the training at least annually or when there are significant changes to the threat.	AT.4.059
CMMC	Situational Awareness (SA)	Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders.	SA.3.169
CMMC	Incident Response (IR)	Use knowledge of attacker tactics, techniques, and procedures in incident response planning and execution.	IR.4.100
CMMC	Incident Response (IR)	Test the organizational incident response capability.	IR.3.099
CMMC	Access Control (AC)	Verify and control/limit connections to and use of external information systems.	AC.1.003

Relevant Practices -3

Framework	Domain / Control	Relevant Practice	Number/ID
CMMC	Awareness & Training (AT)	Provide security awareness training on recognizing and reporting potential indicators of insider threat.	AT.3.058
CMMC	Situational Awareness (SA)	Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders.	SA.3.169
CMMC	System & Information Integrity (SI)	Use threat indicator information relevant to the information and systems being protected and effective mitigations obtained from external organizations to inform intrusion detection and threat hunting.	SI.4.221
CMMC	System & Communications Protection (SC)	Prevent unauthorized and unintended information transfer via shared system resources.	SC.3.182
NIST CSF	Analysis (AN)	Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	RS.AN-5
NIST CSF	Information Protection Processes and Procedures (PR.IP)	Protection processes are improved	PR.IP-7
NIST CSF	Improvements (RC.IM)	Recovery plans incorporate lessons learned	RC.IM-1
NIST CSF	Improvements (RC.IM)	Recovery strategies are updated	RC.IM-2
NIST CSF	Information Protection Processes and Procedures (PR.IP)	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	PR.IP-9
NIST CSF	Risk Management Strategy (ID.RM)	Risk management processes are established, managed, and agreed to by organizational stakeholders	ID.RM-1

Relevant Practices -4

Framework	Domain / Control	Relevant Practice	Number/ID
NIST CSF	Detection Processes (DP)	Detection processes are tested	DE.DP-3
NIST CSF	Communications (CO)	Incidents are reported consistent with established criteria	RS.CO-2
NIST CSF	Communications (CO)	Information is shared consistent with response plans	RS.CO-3
NIST CSF	Risk Assessment (RA)	Cyber threat intelligence is received from information sharing forums and sources	ID.RA-2
NIST CSF	Risk Assessment (RA)	Threats, both internal and external, are identified and documented	ID.RA-3
NIST CSF	Supply Chain Risk Management (ID.SC)	Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	ID.SC-1
NIST CSF	Mitigation (MI)	Newly identified vulnerabilities are mitigated or documented as accepted risks	RS.MI-3
NIST CSF	Awareness and Training (AT)	Physical and cybersecurity personnel understand their roles and responsibilities	PR.AT-5

Organizational Resiliency -1

People

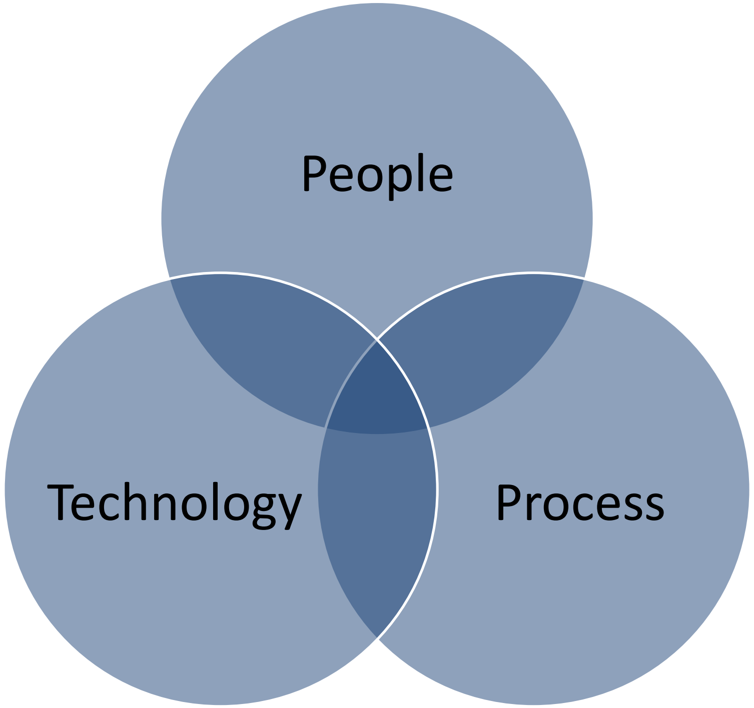
- Leadership
- Community Engagement
- Awareness, Training, and Testing

Process

- Supply Chain
- Information and Knowledge Management
- Reputational Risk
- Adaptive Capacity

Technology

- Resource Management

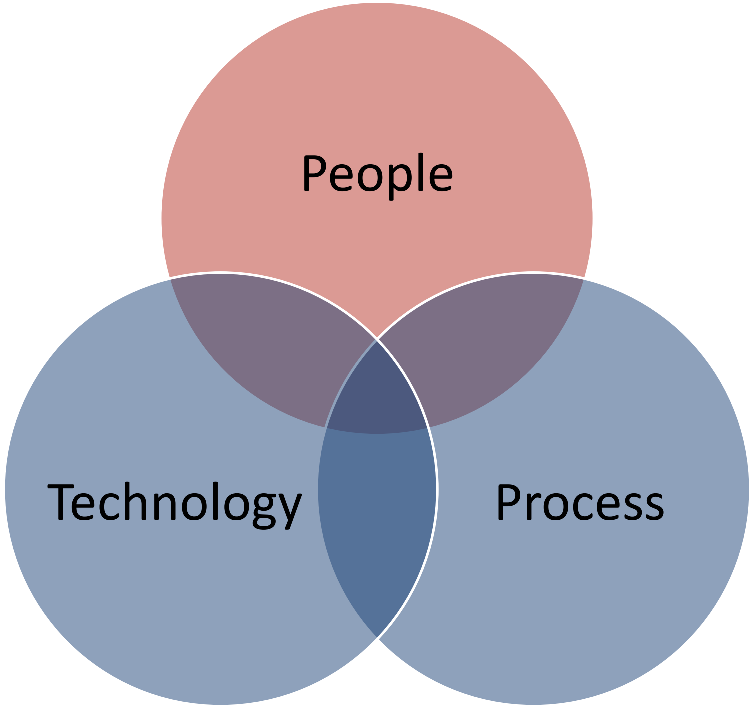


Adapted from “16 Elements of Organizational Resilience” (BSI, 2017)

Organizational Resiliency -2

People

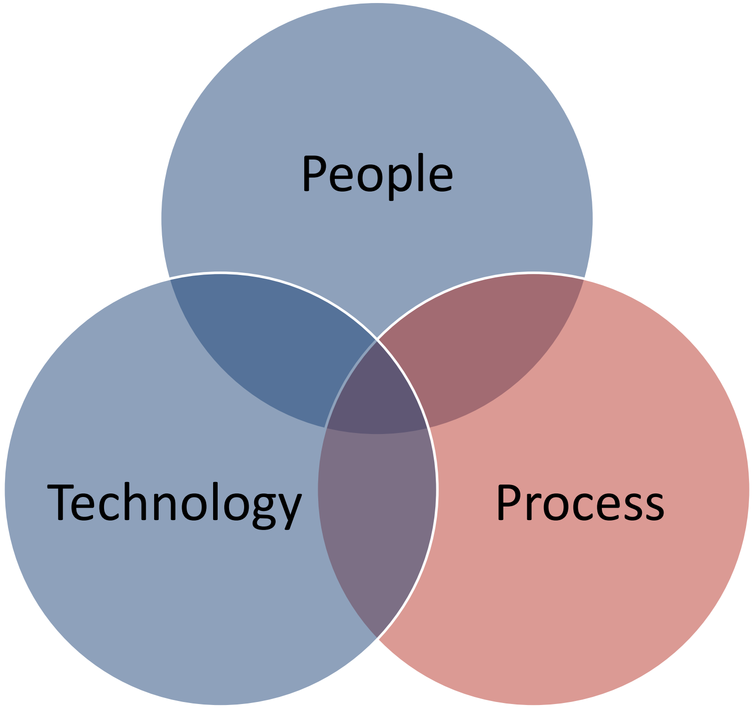
- Leadership
  - Trends from an **incident corpus** or **information sharing groups** can inform decision-making by leadership
- Community Engagement
  - **Information sharing** can engage the organization with your industry or an insider threat community, allowing for opportunities to “give back”
- Awareness, Training, and Testing
  - **Incident corpus** case studies can be used in training and awareness activities
  - **Information sharing groups** can be a source of case studies or best practices



Organizational Resiliency -3

Process

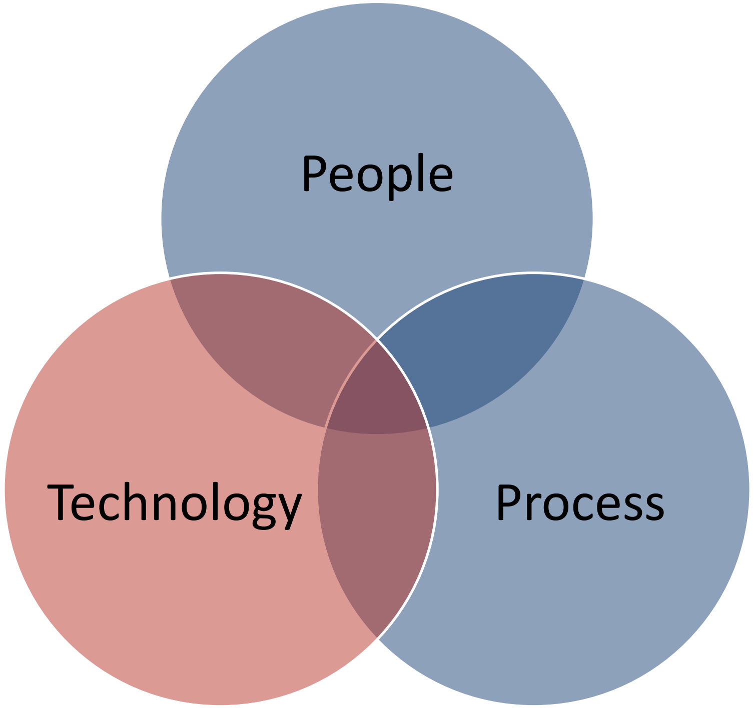
- Supply Chain
  - Supply chain security management processes may be informed by previous incidents captured in an **incident corpus** or intelligence received from **information sharing** relationships
- Information and Knowledge Management
  - **Insider threat incident corpus and information sharing management** are inherently knowledge management activities
- Reputational Risk
  - An **insider threat incident corpus** can help to limit reputation risk by supporting faster detection of incidents
- Adaptive Capacity
  - Engagement with **information sharing groups** can help an organization stay more attuned to potential changes in their environment



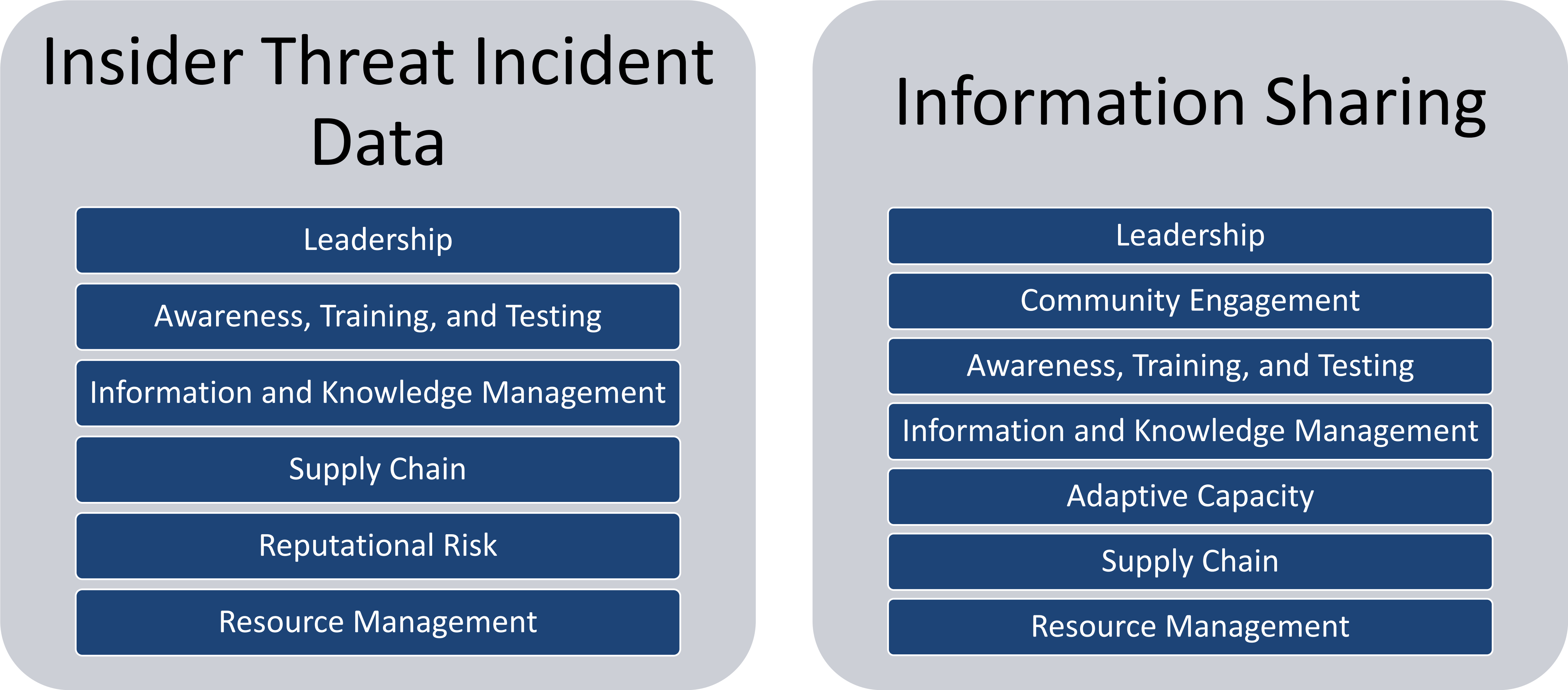
Organizational Resiliency -4

Technology

- Resource Management
  - Engaging in **information sharing groups** can provide insights on data sources to monitor or tool configurations
  - Aggregated data from an **insider threat incident corpus** may highlight potential high-risk networks/environments on which to deploy enhanced monitoring or tools



Organizational Resiliency -5



Insider Threat Incident Data

- Leadership
- Awareness, Training, and Testing
- Information and Knowledge Management
- Supply Chain
- Reputational Risk
- Resource Management

Information Sharing

- Leadership
- Community Engagement
- Awareness, Training, and Testing
- Information and Knowledge Management
- Adaptive Capacity
- Supply Chain
- Resource Management