



Understanding Insider Risk

Luke Osterritter

losterritter@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.

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.

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

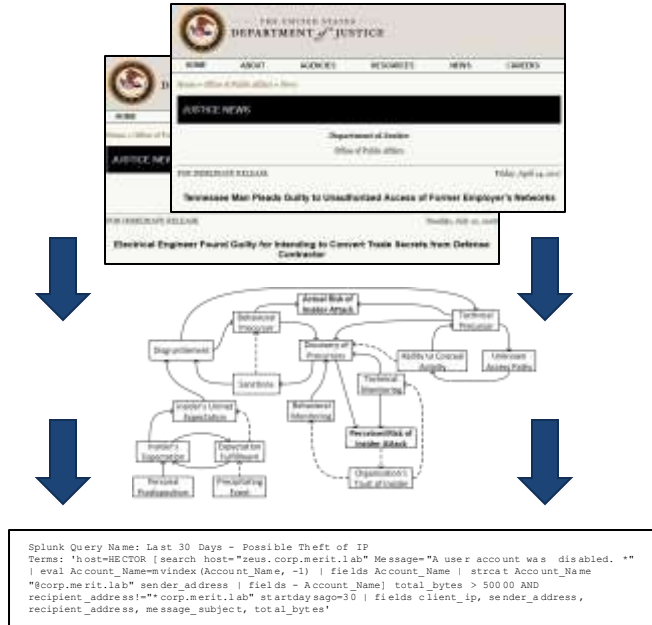
DM22-0155

The Software Engineering Institute



- A United States Department of Defense Federally Funded Research and Development Center (FFRDC)
- Vision: leading and advancing software engineering and cybersecurity to solve the nation's toughest problems
- Mission: to advance the technologies and practices needed to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring

Insider Risk at The CERT Division of Carnegie Mellon University's Software Engineering Institute



Conducting research, modeling,
analysis, and outreach to develop
socio-technical solutions to
combat insider threats since 2001

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

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

The Insider Threat Defined

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.

Untangling Insider Taxonomy

Insider: An *insider* of an organization is an employee, contractor, or other business partner who *has or had* authorized access to the organization's critical assets.

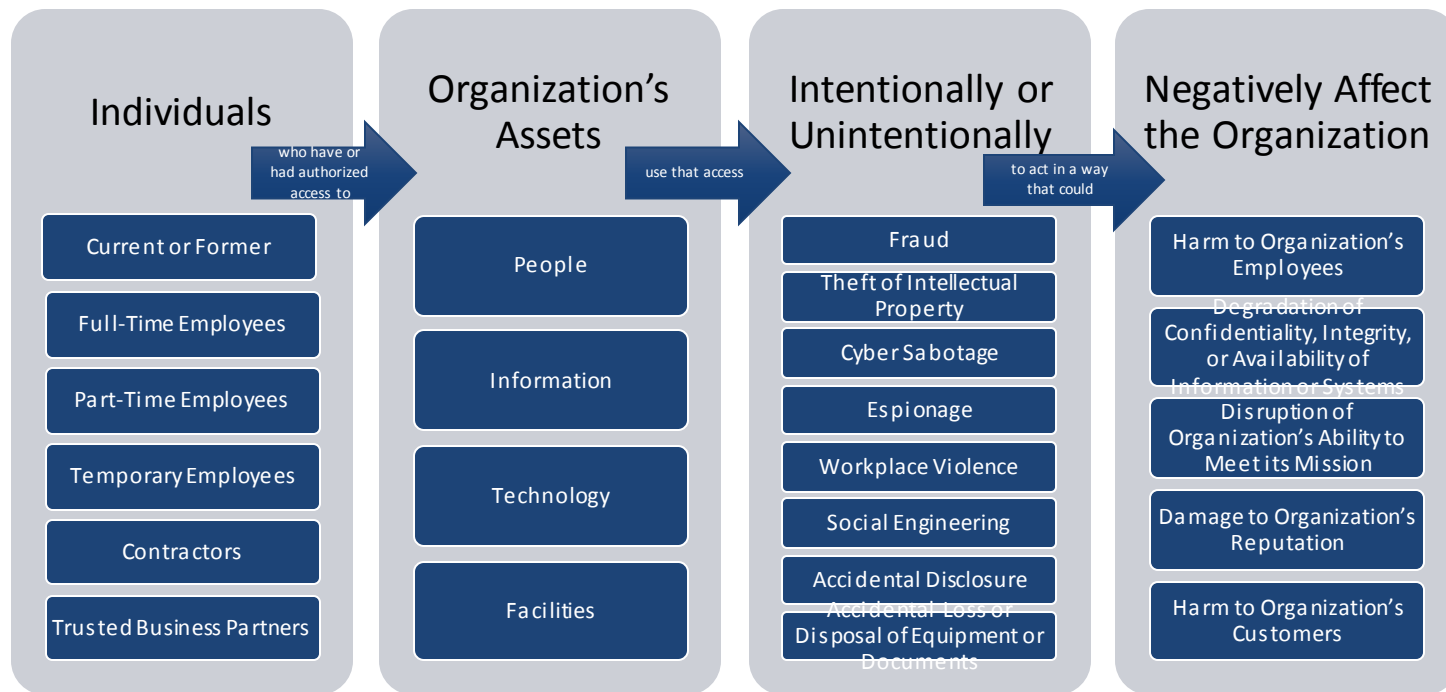
Insider Threat: *Insider threat* for an organization is the potential for an insider to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization.

Insider Risk: *Insider risk* is the potential for loss associated with the realization of an insider threat.

Insider risk is unique in organizational security in that the potential threat agents play fundamental roles in accomplishing the organization's mission.

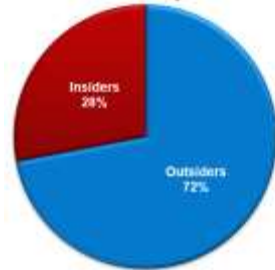
- Insider goodwill is essential to both keeping intentional insider risk to a minimum and ensuring organizational success generally.

Scope of the Insider Threat



Scale of the Insider Threat

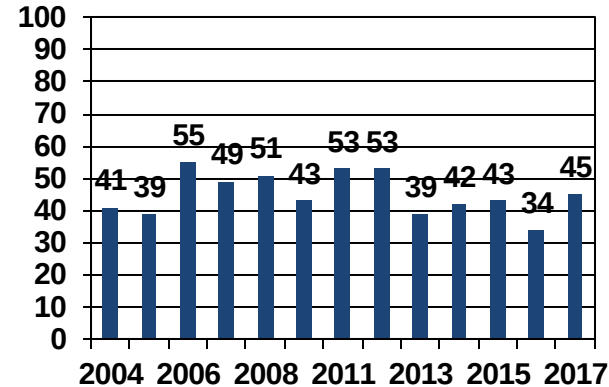
What percent of the electronic crime events are known or suspected to have been caused by :



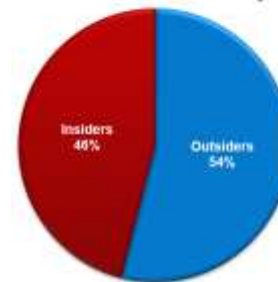
What percentage of certain types of security incidents were perpetrated by insiders?

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%

What percentage of organizations experienced an insider incident?

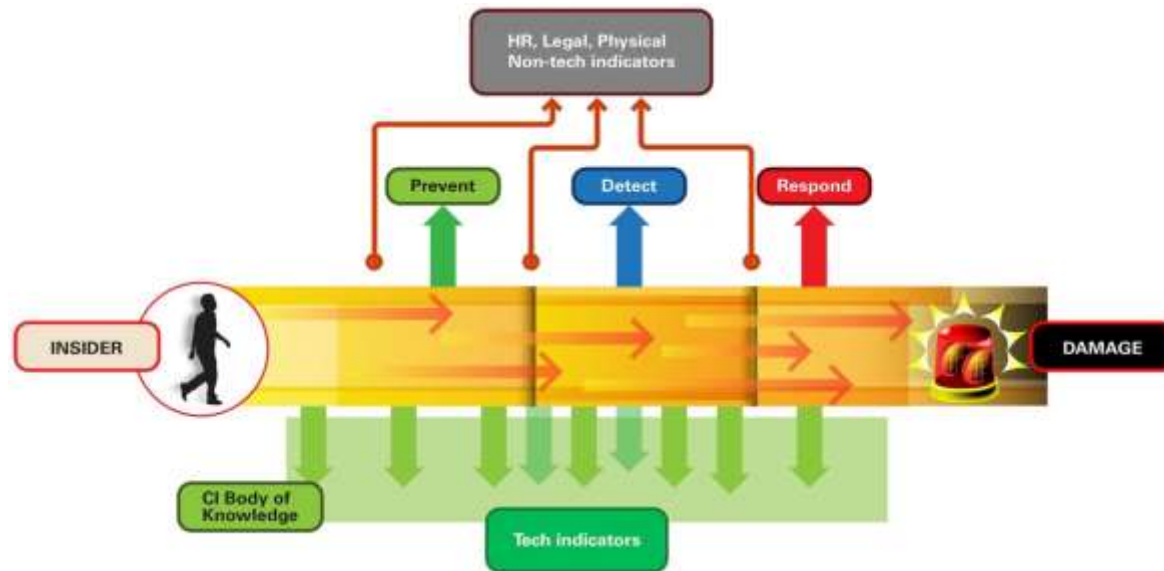


The most costly or damaging crimes were committed by:



Sources: 2004-2018 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

The Goal for an Insider Threat Program...



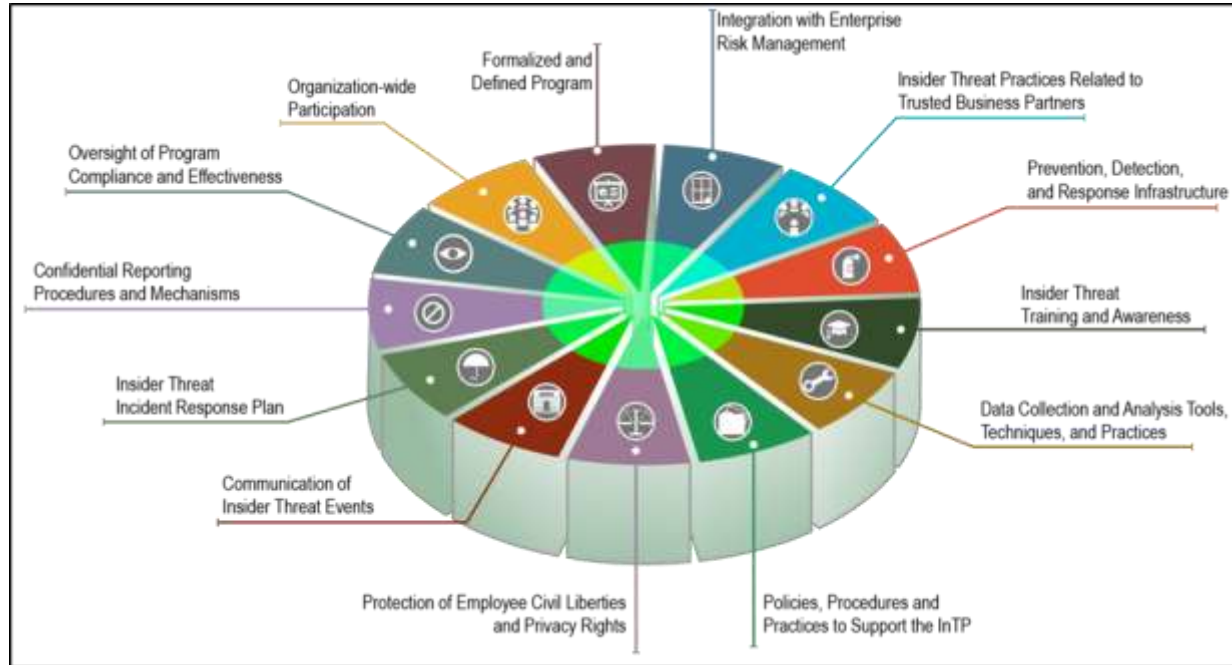
Is to reduce insider risks to critical assets to acceptable levels

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

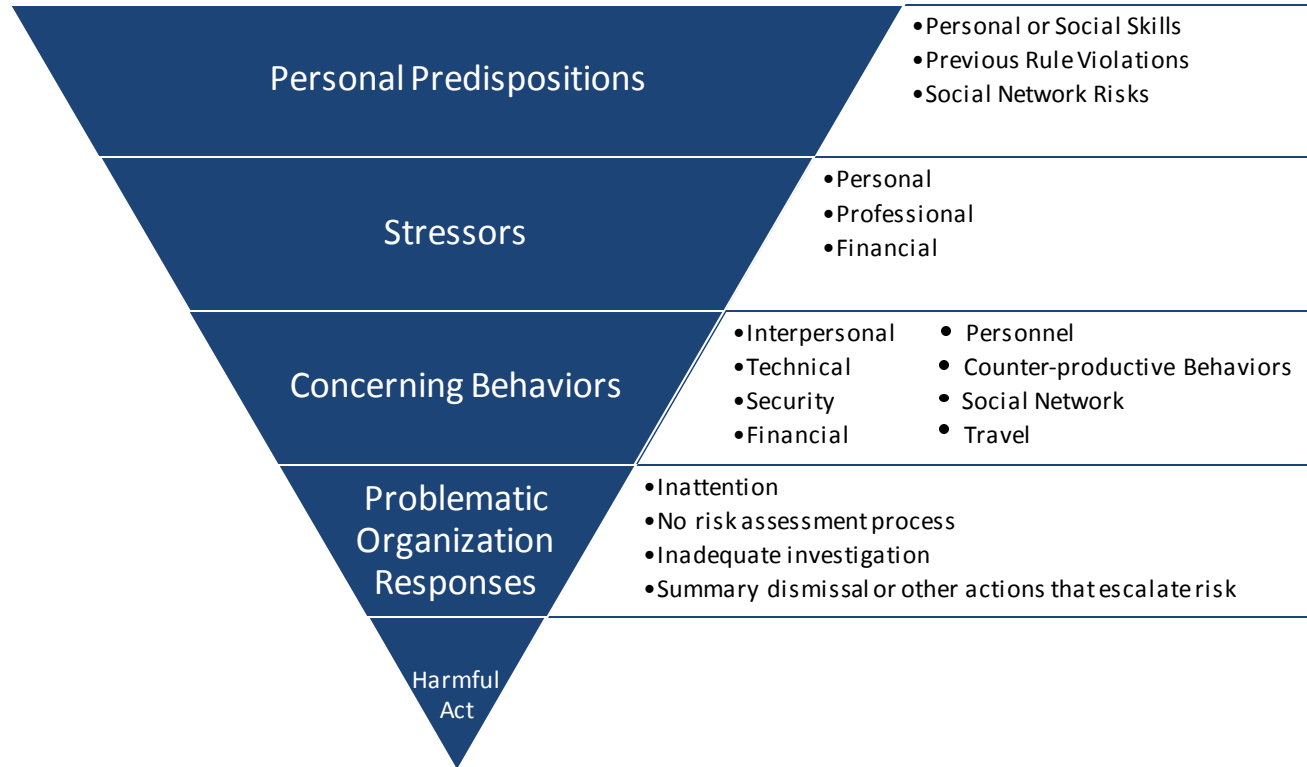
Best Practices from the CERT Common Sense Guide to Mitigating Insider Threats

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

Key Components of an Insider Threat Program



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 Importance of Positive Deterrence to Insider Risk Management

Balanced Deterrence is Key

Balanced deterrence combines traditional security controls (command-and-control) with practices to increase employees' perceptions of organizational support (positive deterrence)

Command-and-Control

Workforce management practices that attempt to *force* employees to act in the interests of the organization

Employee Constraints,
Monitoring, Punishment

Positive Deterrence

Workforce management practices that attempt to *attract* employees to act in the interests of the organization

Value Employee Contributions,
Care about Well-Being, Treat Fairly

- Command-and-control *alone* can *exacerbate* the threat it is intended to mitigate
- Positive deterrence shown to reduce insider misbehavior through organizational justice, performance-based rewards/recognition, respectful communication, supervisor support
- **Both** positive and negative deterrence needed in *balance that is right* for organization
BUT organizational culture can be a significant barrier to adoption.

Why Augment Command-and-Control with Positive Deterrence?

1. Workforce management and security practices can undermine workforce goodwill
2. Positive deterrence can reduce insider incident rates over command-and-control alone
3. Promoting positive deterrence can significantly enhance the IRMP mission
4. Positive deterrence improves job performance generally

Three Categories of Positive Deterrence-Related Practices

People



Connected @ Work

Organization



Perceived Organizational
Support

Job



Job Engagement

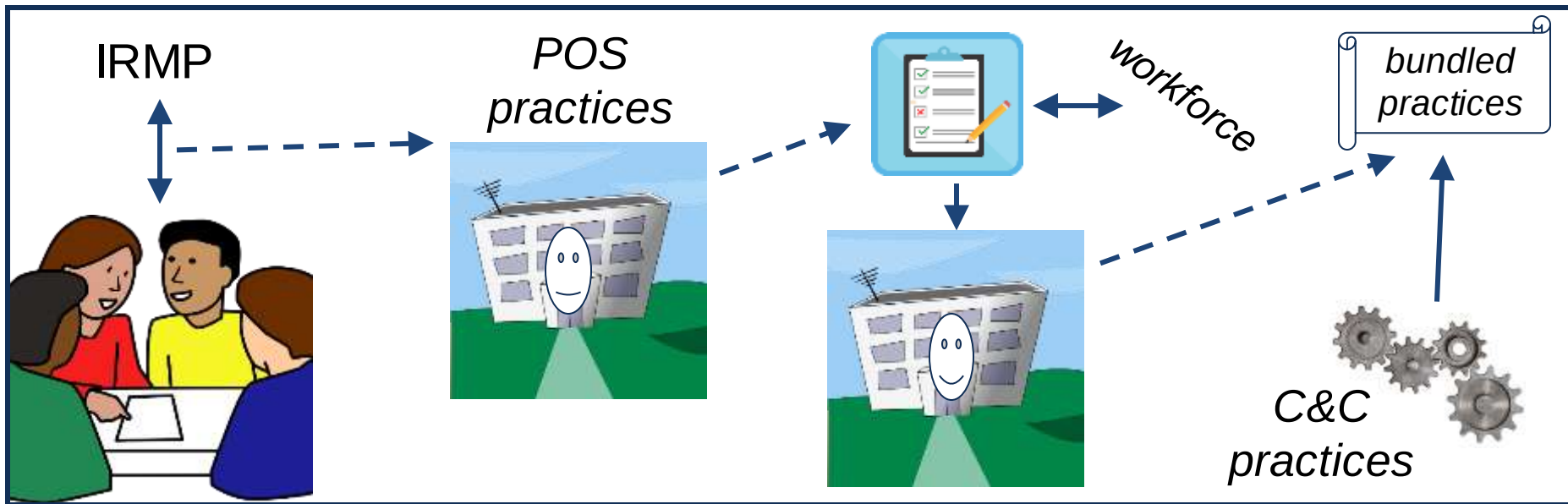
What Can Orgs Do Now to Implement Positive Deterrence

1. Engage and coordinate with stakeholders across the organization, especially HR

2. Work with stakeholders to implement practices proven to increase organizational support

3. Fine-tune practices by eliciting employee perspectives on IRMP and working environment

4. Bundle positive deterrence with command-and-control practices

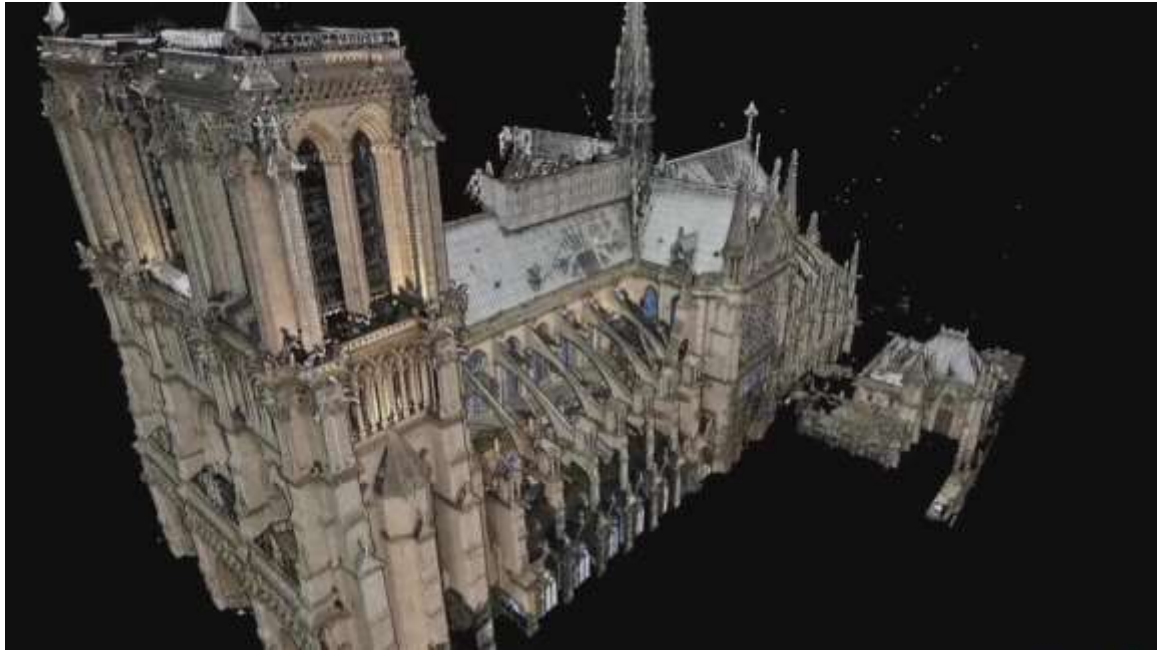


Digital Twins of Organizations – Future Research Direction

“A digital twin is a virtual model designed to accurately reflect a physical object.”

“The object being studied — for example, a wind turbine — is outfitted with various sensors related to vital areas of functionality.”

Real-world application:
Reconstruction of Notre Dame cathedral



Sources: “What Is a Digital Twin?” <https://www.ibm.com/topics/what-is-a-digital-twin>
“Reconstructing Notre Dame Cathedral” <https://www.cbsnews.com/news/reconstructing-notre-dame-cathedral/>

Digital Twins of Organizations – Future Research Direction

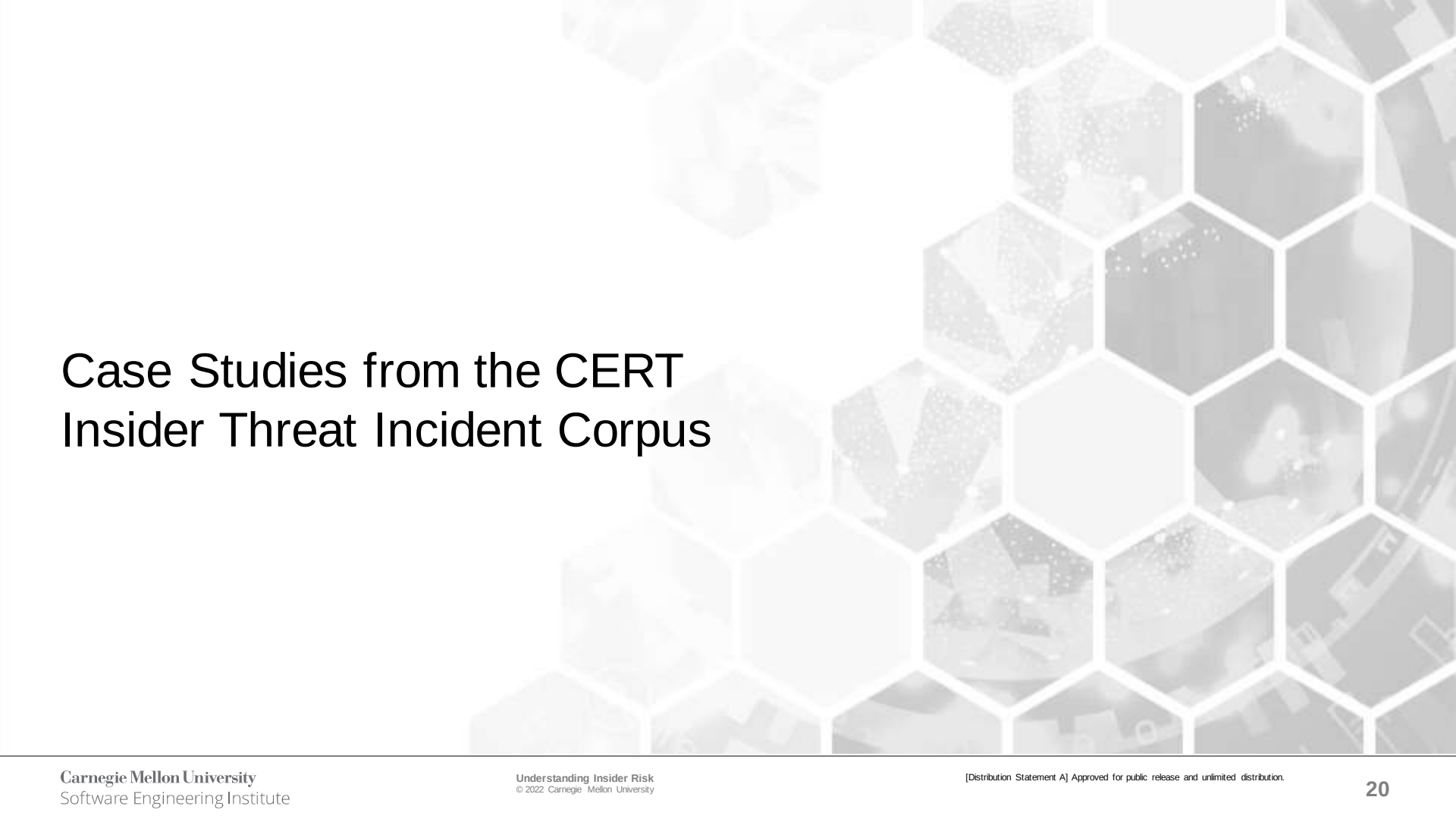
Parmer et al. suggests “that the concept of digital twins can be extended from digital representations of physical objects to digital representations of whole organizations” (2020)

“...data that flows from organizational assets, people, activities, and their interactions can be combined into a holistic digital model of the organization: an **organizational digital twin**.”

Research questions:

- Can a digital twin of an organization (DTO) afford the ability to facilitate what-if assessments of organizational policy changes and insider risk outcomes as a result of balanced deterrence strategies?
- How do digital twin modeling languages and technologies need to evolve to support such a capabilities?

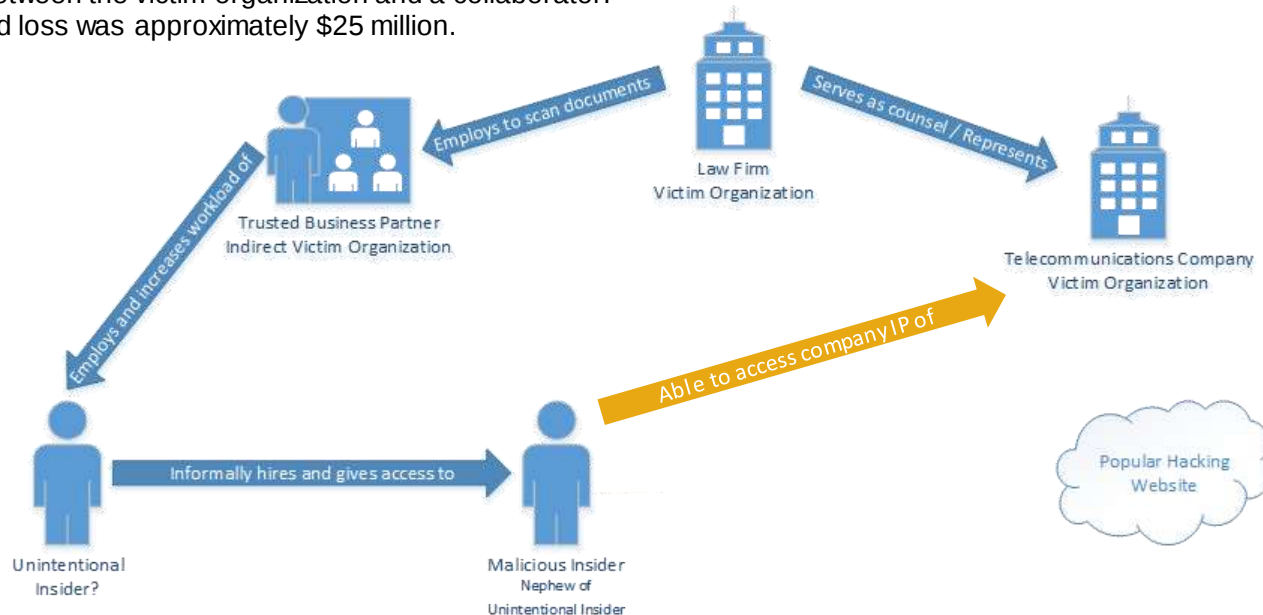
Source: Parmar, R., Leiponen, A., & Thomas, L. D. (2020). Building an organizational digital twin. *Business Horizons*, 63(6), 725-736.



Case Studies from the CERT Insider Threat Incident Corpus

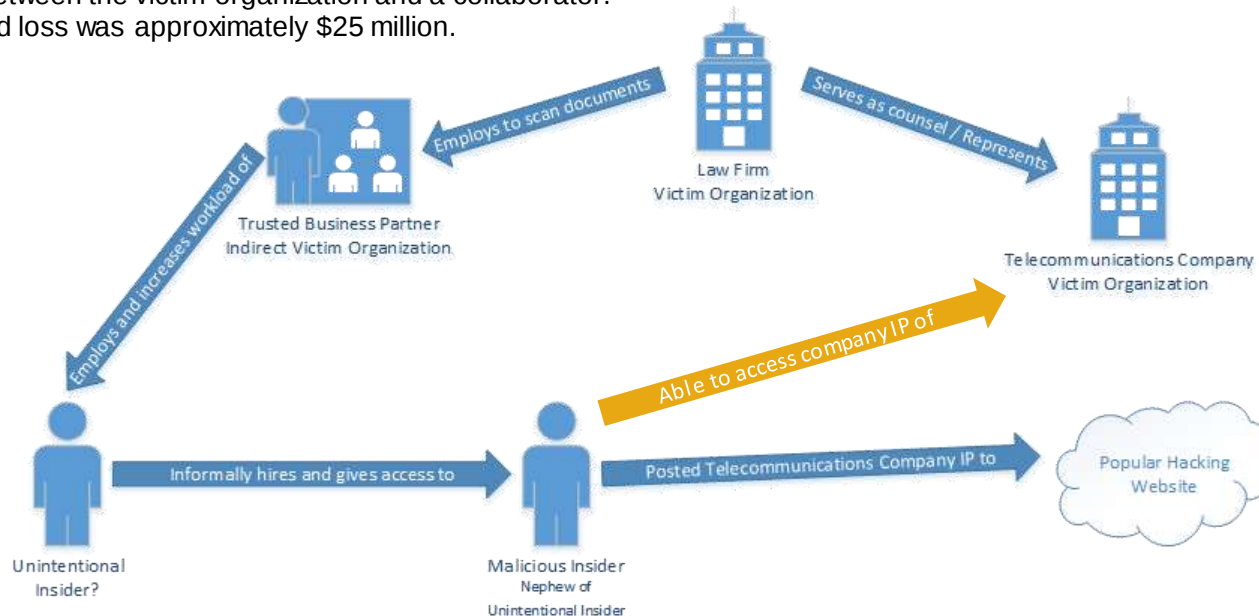
Insider Threat Incident Scenario

A contractor was unofficially working for the company's TBP, a document imaging company. The victim organization was a high technology company. The TBP was hired to copy trade secrets in preparation for litigation. The insider was hired informally by a family member, to assist with the high workload. The insider stole and posted trade secrets, design notes, and correspondence between the victim organization and a collaborator. The incident related loss was approximately \$25 million.



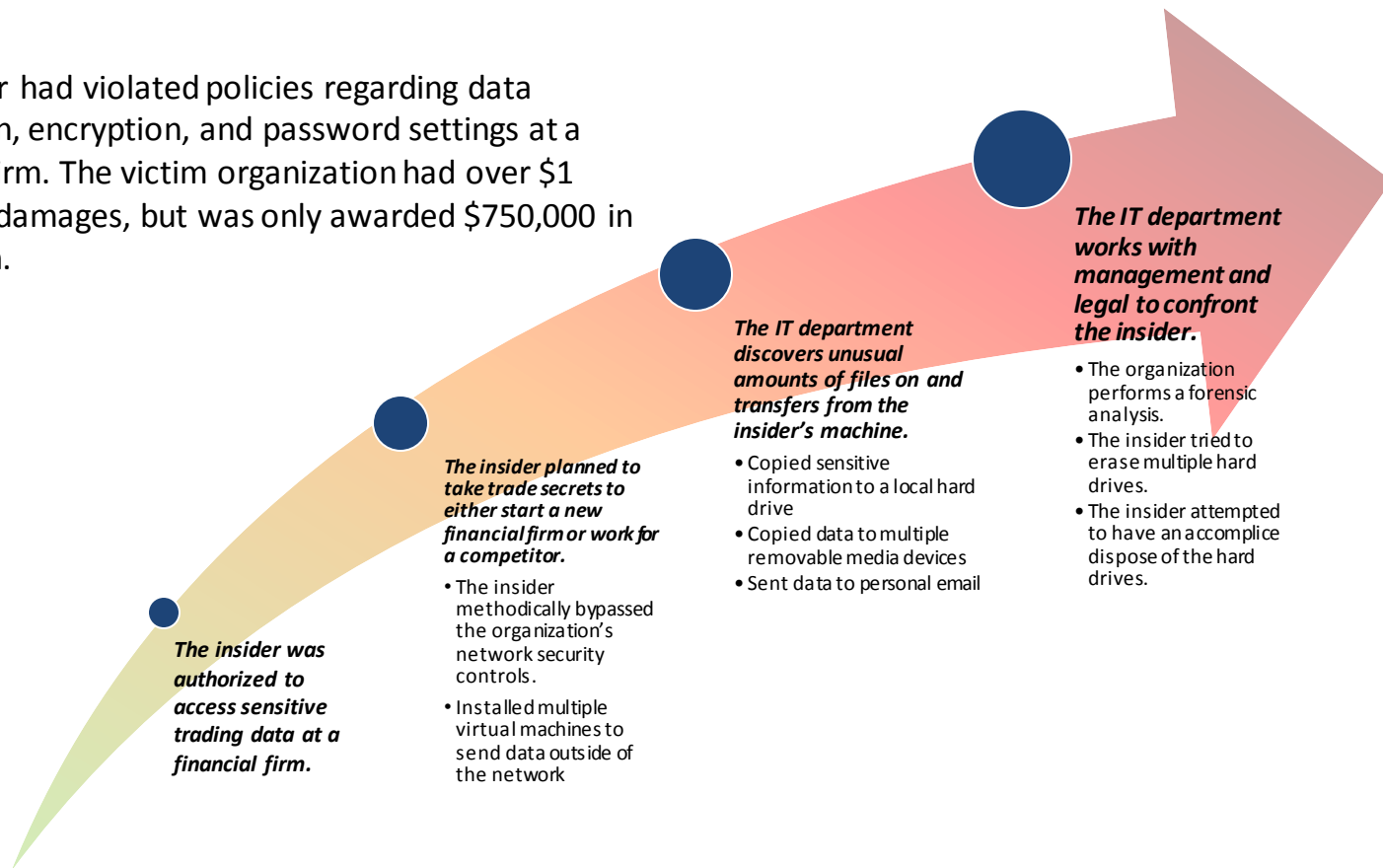
Insider Threat Incident Scenario

A contractor was unofficially working for the company's TBP, a document imaging company. The victim organization was a high technology company. The TBP was hired to copy trade secrets in preparation for litigation. The insider was hired informally by a family member, to assist with the high workload. The insider stole and posted trade secrets, design notes, and correspondence between the victim organization and a collaborator. The incident related loss was approximately \$25 million.



True Story: Theft of IP

The insider had violated policies regarding data exfiltration, encryption, and password settings at a financial firm. The victim organization had over \$1 million in damages, but was only awarded \$750,000 in restitution.



TRUE STORY: *Theft of IP*

Simulation software for the reactor control room in a U.S. nuclear power plant was being run from a country outside the U.S. ...

A former software engineer born in that country took it with him when he left the company.



TRUE STORY: *Theft of IP*

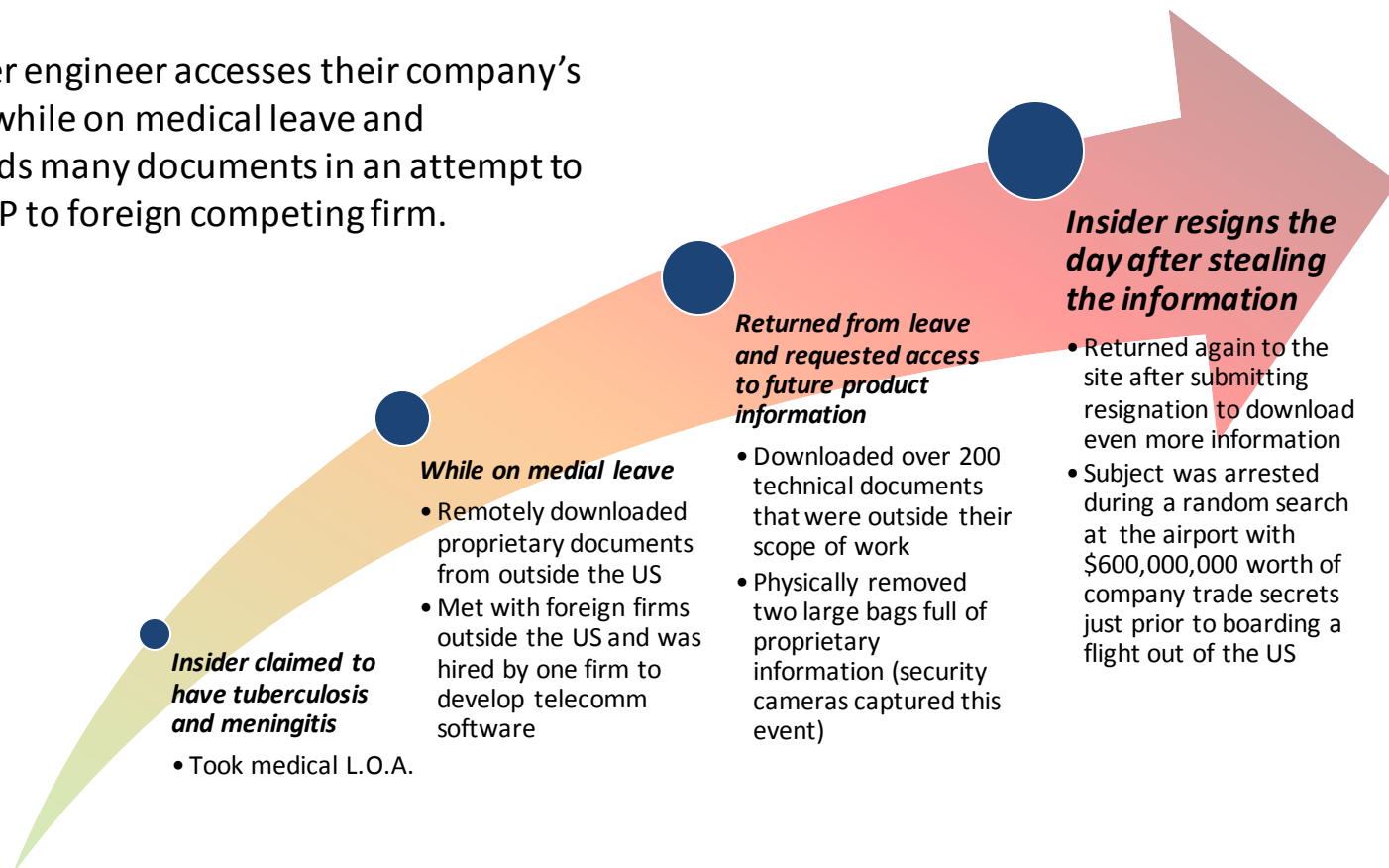
Research scientist downloads 38,000 documents containing his company's trade secrets before going to work for a competitor...

Information was valued at \$400 Million.



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.



Contact Information

Luke Osterritter, MSIS, CISSP

Cyber Security Researcher, CERT Division

Software Engineering Institute

Carnegie Mellon University

losterritter@sei.cmu.edu

<https://www.sei.cmu.edu/our-work/insider-threat/index.cfm>

Featured Research from the CERT Insider Risk – 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 CERT Insider Risk – 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 CERT Insider Risk – 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>

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>