Insider Threat Trends in the Utilities Sector

Dan Costa

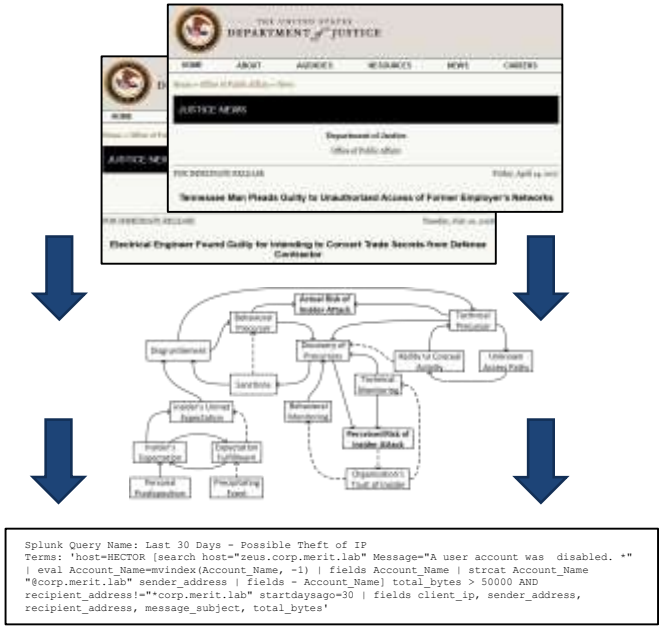
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

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.

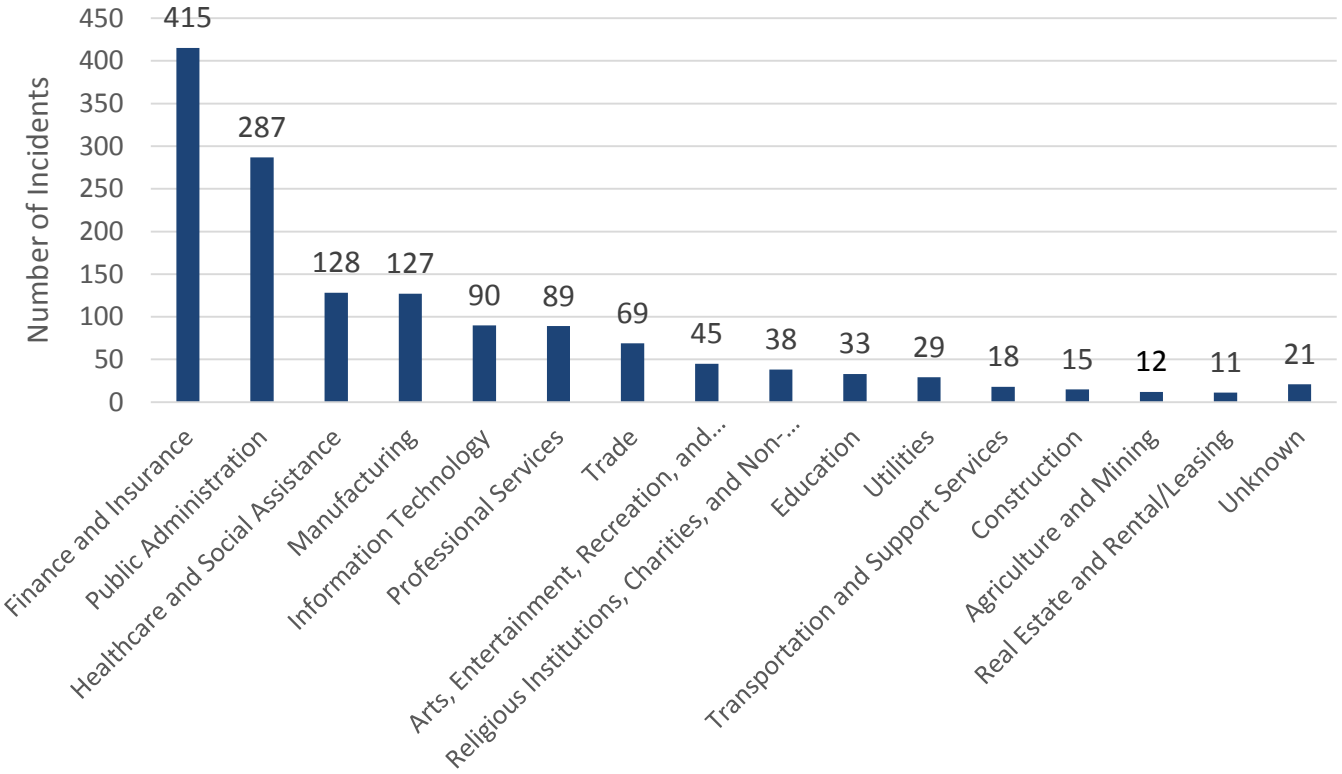
DM20-0857

The CERT National Insider Threat Center



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

NITC Corpus: Insider Threat Incidents by Industry / Sector

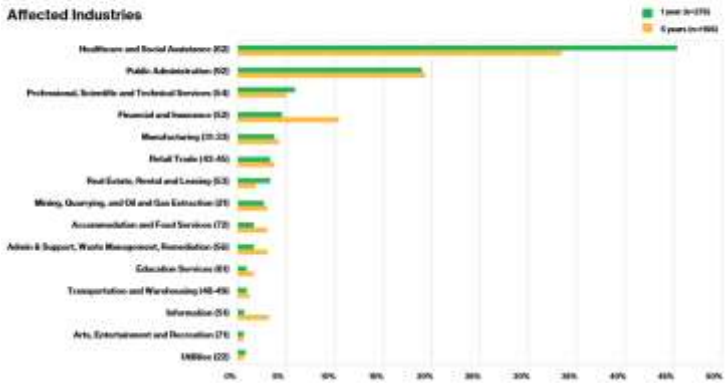


Verizon Insider Threat Study

VERIS — Affected Industries

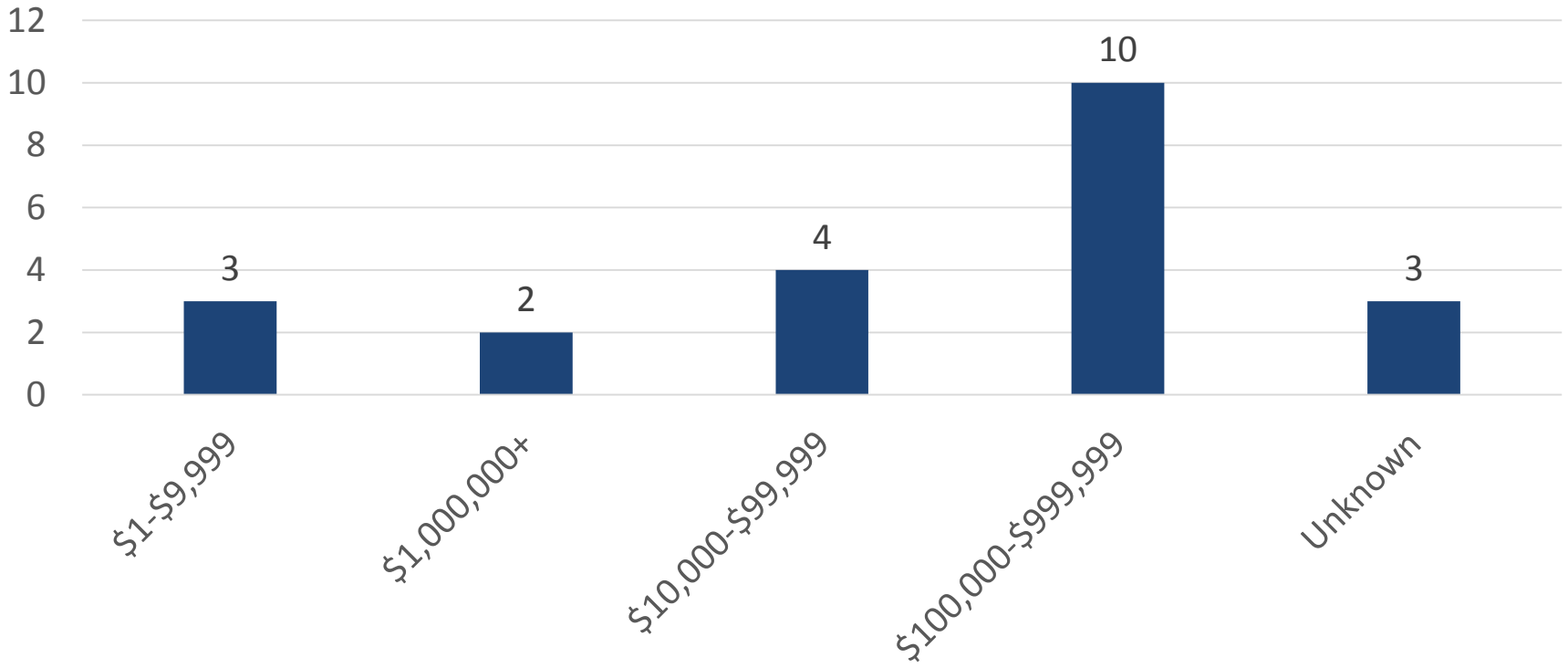
Viewing Insider and Privilege Misuse breaches over the previous year (2018), Healthcare and Social Assistance (46.4%) and Public Administration (18.5%) are the top industries involving privileged threat actors causing the most damage.

In the 2018 DBIR, a particular industry's representation in Figure 10 (below) isn't a security gauge; more doesn't correlate to less secure. The totals below are influenced by our sources: industry- or data-specific disclosure laws. The top 15 victim industries within Insider and Privilege Misuse for 2018 and for the previous five years (2014-2018) are:

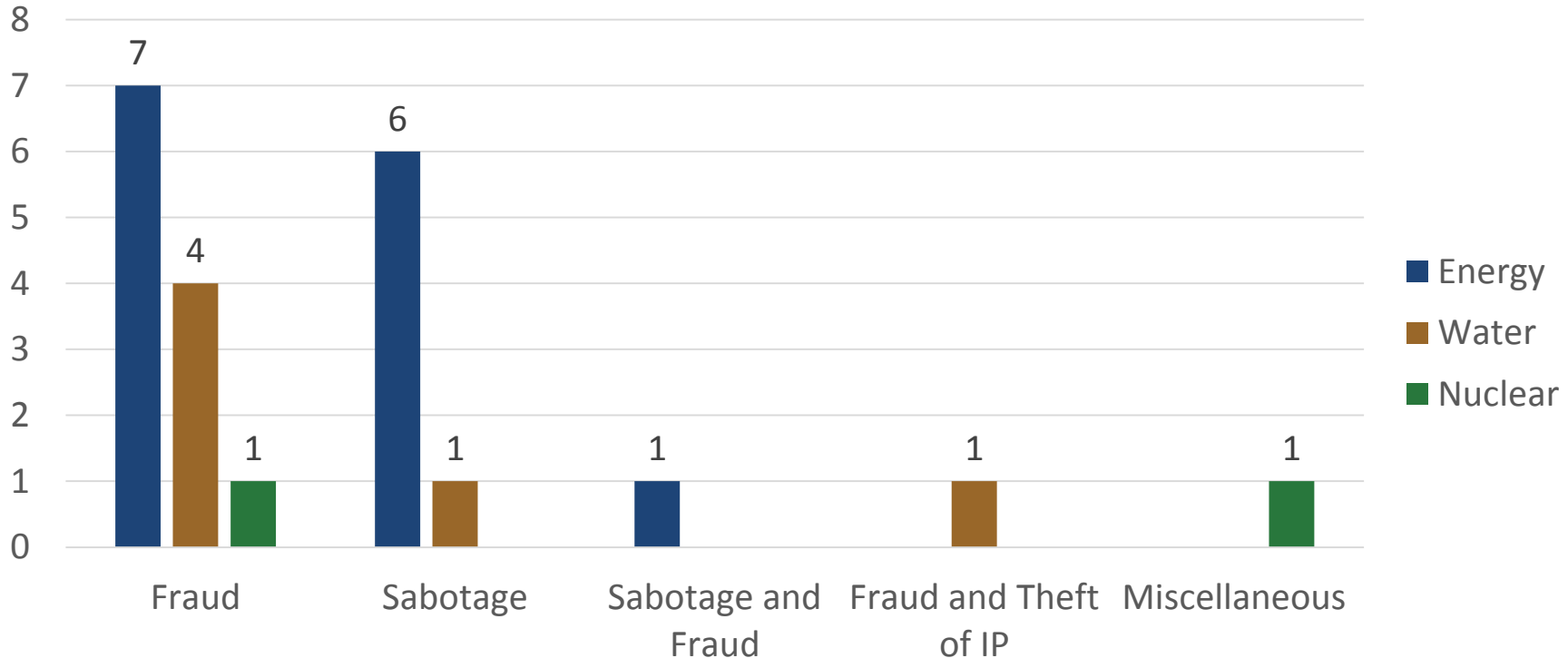


https://enterprise.verizon.com/resources/reports/insider-threat-report.pdf

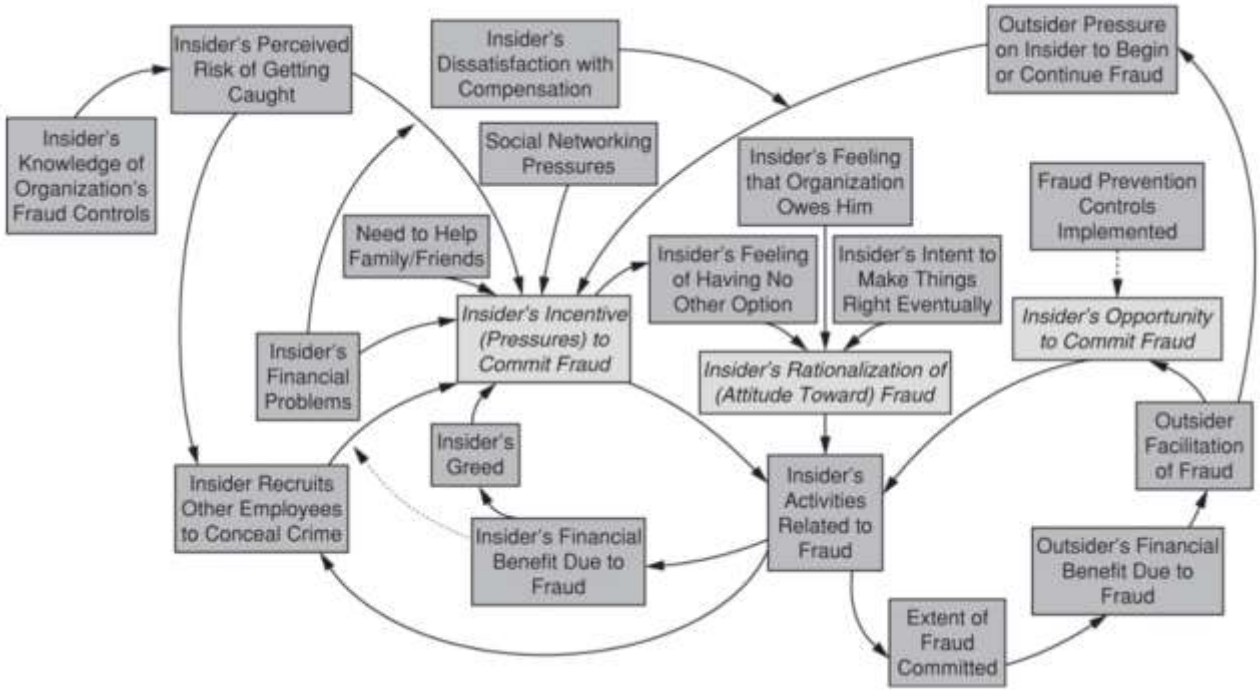
Financial Impact



Incident Types

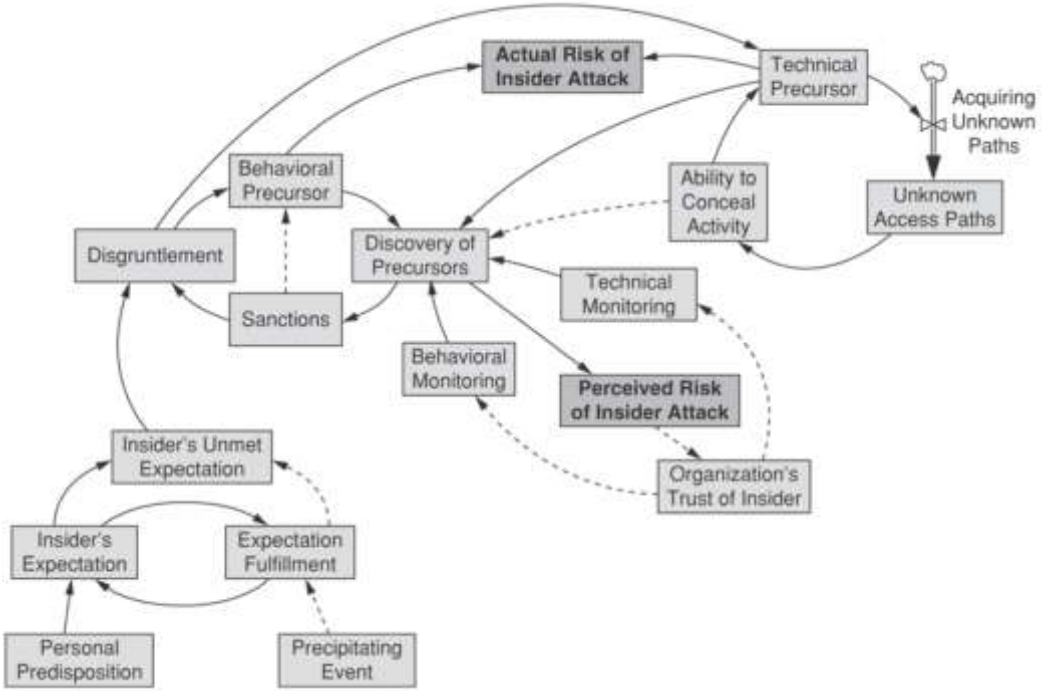


CERT's Insider Fraud Model



Source: The CERT® Guide to Insider Threats

CERT's Insider Sabotage Model



Source: The CERT® Guide to Insider Threats

Critical Path to Insider Risk – Utilities Observables

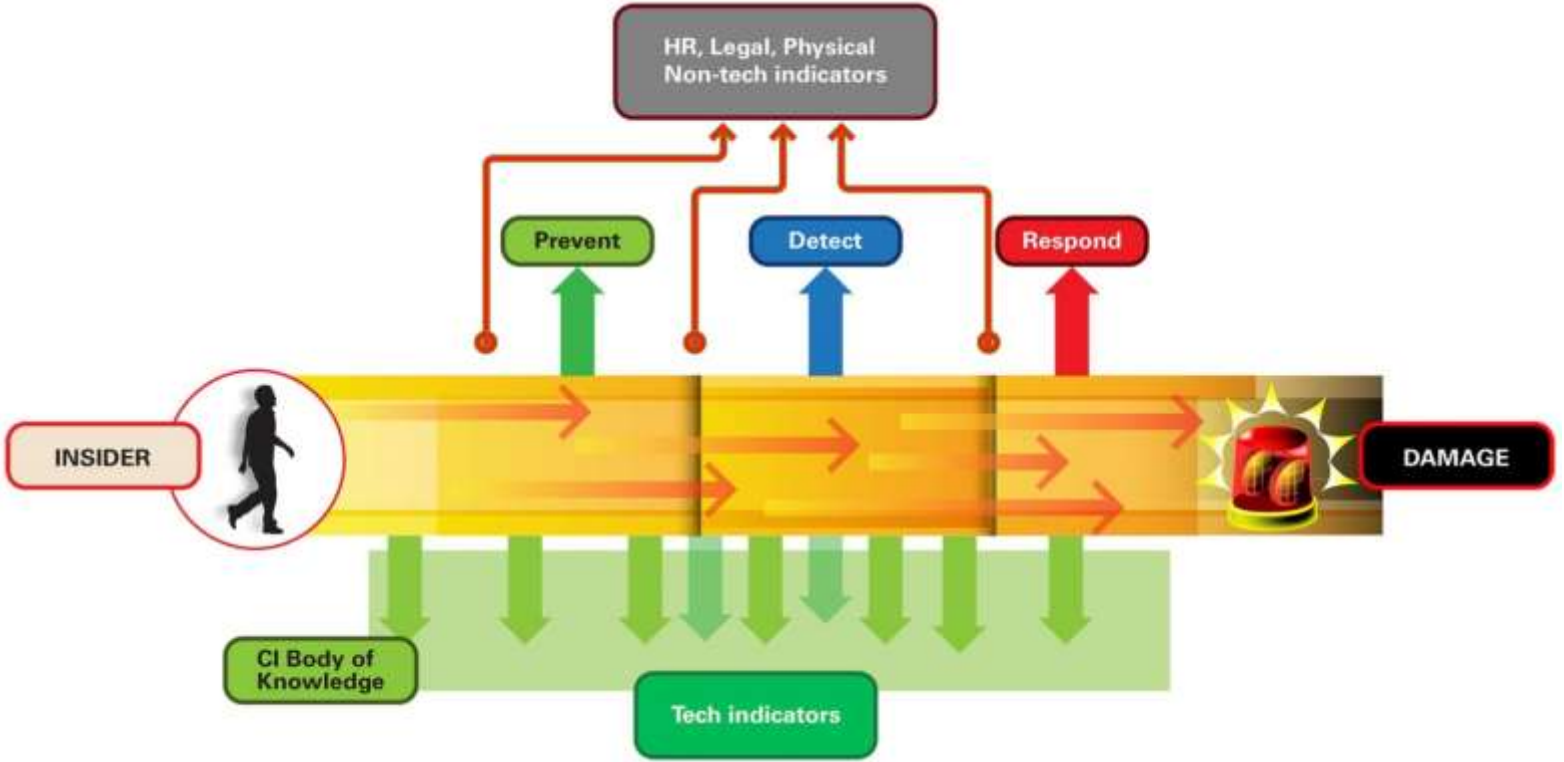
- Possible Psychological Issues (9.1%)
- Substance Abuse (4.5%)
- A History Of Financial Problems (4.5%)

- Terminated (27.3%)
- Resigned (22.7%)
- Changed Positions Internally (9.1%)

- Employee Extortion, Threats, or Legal Demands (18.2%)
- Suspicious Foreign Travel (13.6%)
- Bypassed Physical Security of Organization Facilities (9.1%)

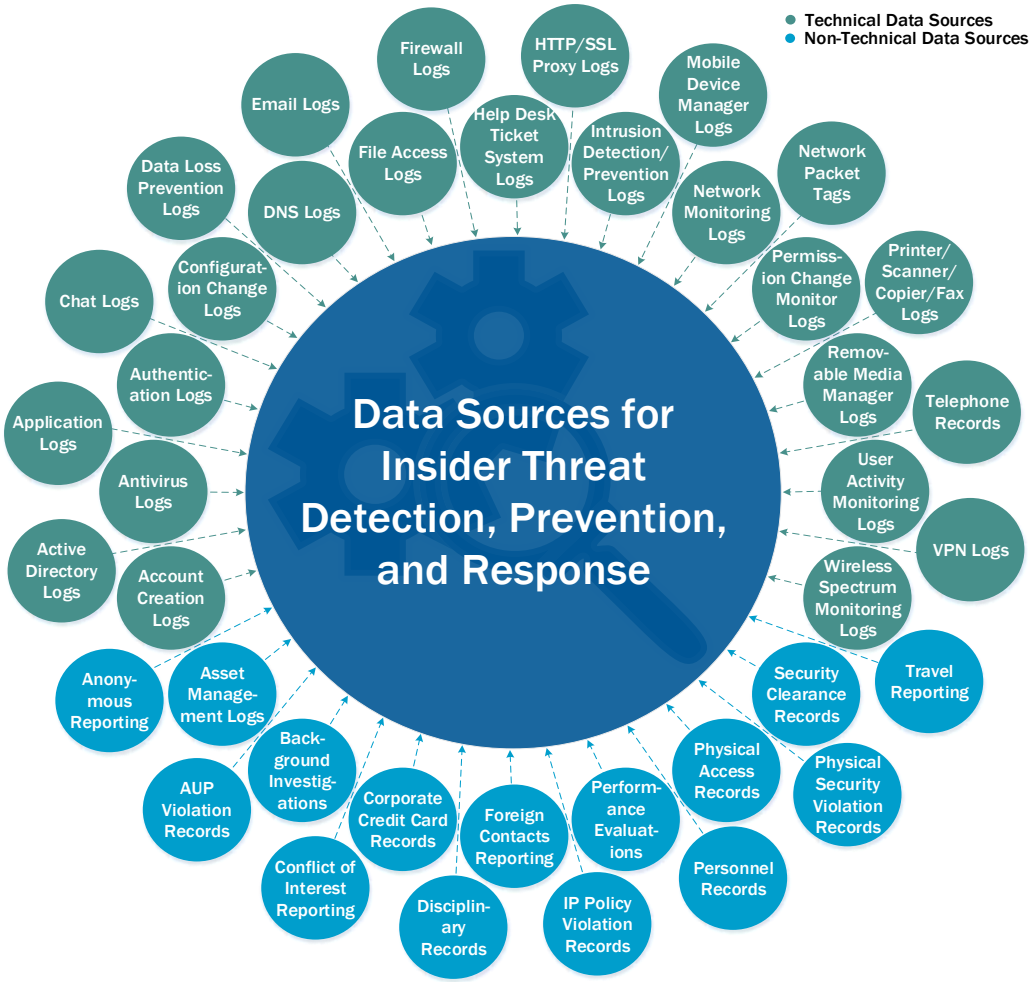
- Used Compromised Account (18.2%)
- Denial of Service Attack (18.2%)
- Used Their Account After Termination/Resignation (13.6%)
- Privileged Access Abuse (13.6%)
- Deleted Critical Data (13.6%)
- Modified Critical Data (9.1%)

The Goal for an Insider Threat Program…



Is to reduce insider risks to critical assets to acceptable levels

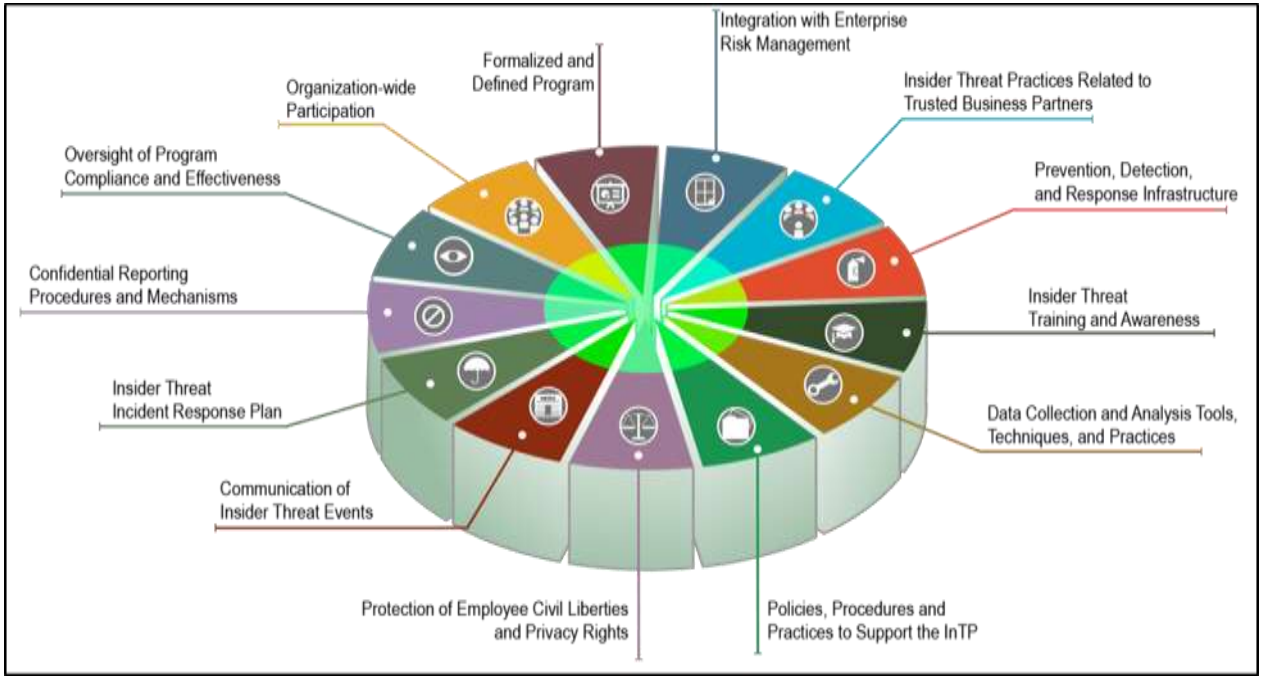
https://insights.sei.cmu.edu/insider-threat/2020/01/maturing-your-insider-threat-program-into-an-insider-risk-management-program.html



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

An Overview of Insider Threat Program Components

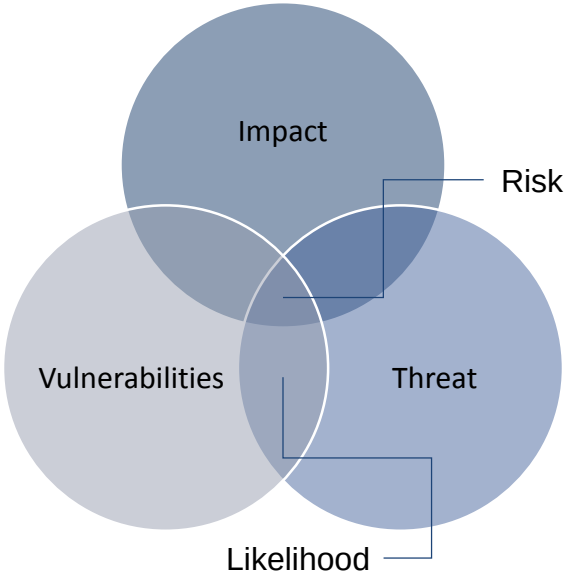


Acceptable Levels?

Deploying controls doesn't necessarily reduce the likelihood of a threat occurring to 0%, 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



Questions / Presenter Contact Information

Dan Costa, CISSP, PSEM

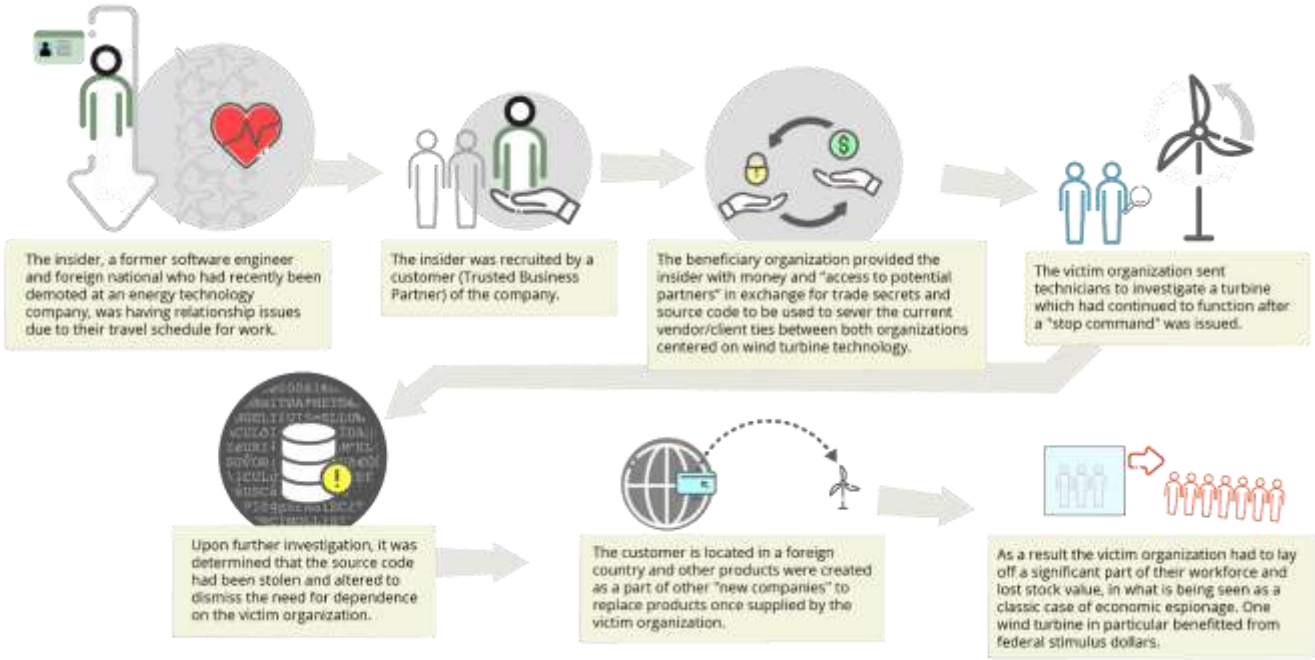
Technical Manager, CERT National Insider Threat Center

dlcosta@sei.cmu.edu

www.cert.org/insider-threat

Case Studies and Resources

Theft of IP

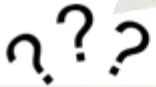


Fraud

The insider was a current, full-time employee responsible for the operations of a privately-owned oil and natural gas company, the victim organization.

Over the course of four years, the insider used their role in maintaining financial operations to transfer in excess of $200,000 to themselves.

The insider used the stolen funds to pay for personal expenses, vehicle purchases for themselves, and education expenses for their young-adult children. The insider concealed their fraud by making false entries into the accounting software used by the victim organization.

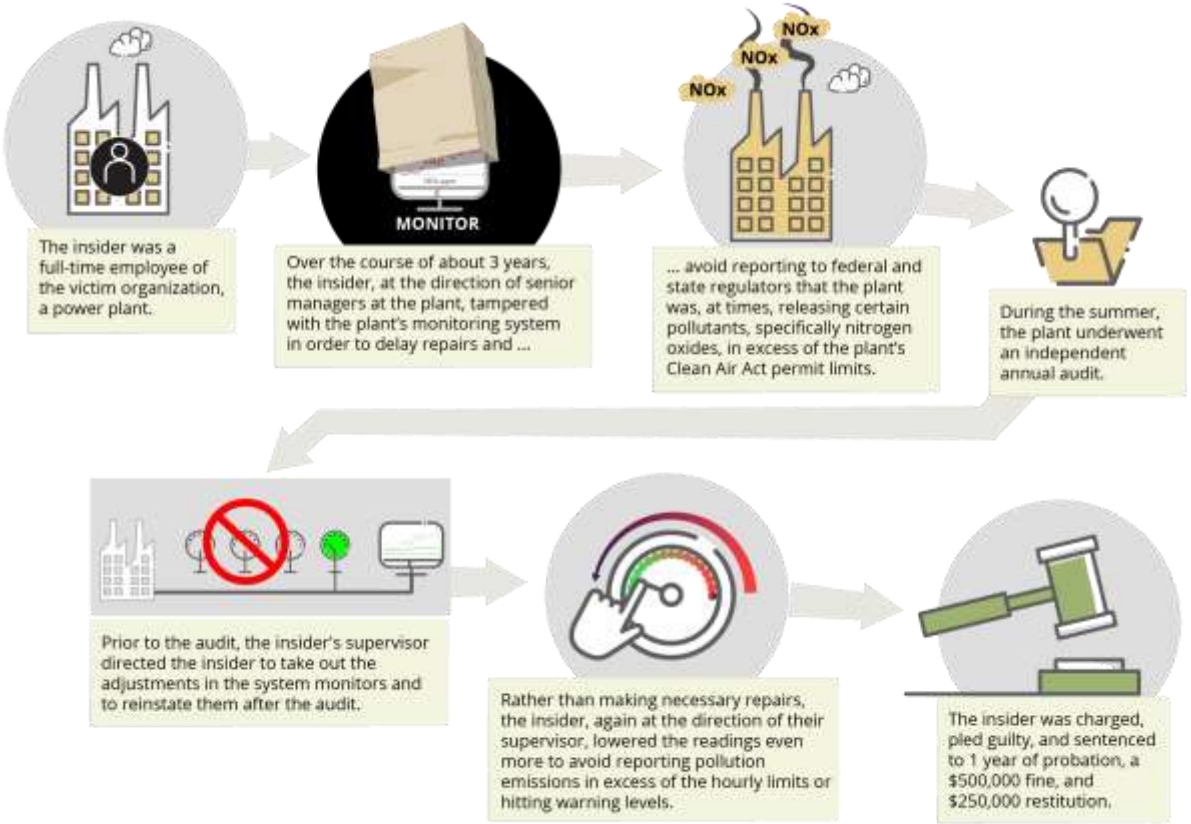


It is unclear how the insider was identified, nor how the fraud was detected.

However, court documents related to the incident suggest that the insider concealed the fraud only by changing the name of the expense in the accounting software, allowing investigators to identify one-to-one matches between expenses the insider approved with fraudulent purchases.

The insider was indicted on 1 count Wire Fraud, 1 count Mail Fraud, 1 count Impeding and obstructing the IRS, and 4 counts Income Tax Evasion.

Sabotage and Fraud



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

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