RELIABILITY FIRST

Insider Threats Webinar

September 30, 2020

Insider Threats Webinar - Information & Logistics

- **Facilitator – Ray Sefchik, Director Entity Engagement**
  - Opening Remarks – Bhesh Krishnappa (RF)
  - Presenters from Carnegie Mellon/SEI, FERC, MISO, NERC/E-ISAC, PJM, ReliabilityFirst
  - Time – 8:00am – 12:00pm
    - Morning Break at 9:55am

- **Audience Feedback, Questions/Answers, Polls**
  - Slido.com

OPENING REMARKS

Bheshaj Krishnappa

Program Manager, Risk & Resiliency, RF

Building a Culture of Preparedness through Awareness and Best Practices

- *Industry of 3,200 utilities, employs over 400,000 employees, 7,677 Power Plants, 55,000 Sub-stations, 450,000 miles of transmission.* *(Scott Wilson, DOE)*
- Resilient insiders are more likely to deter negative events

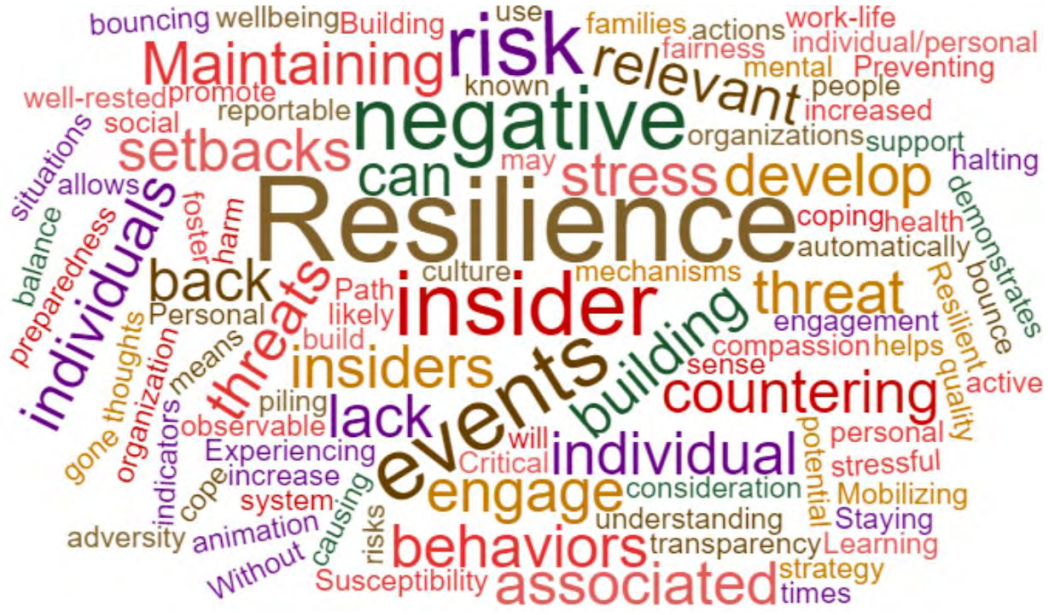


Image source: CDSE

Slido.com Poll

Does your organization have an Insider Threat Program?

Login to Slido.com using the event code

#RFInsiderThreat

All feedback is anonymous, but we will show the aggregate group feedback in real-time.

Slido.com Poll

How long has an Insider Threat Program been in place in your organization?

Login to Slido.com using the event code

#RFInsiderThreat

All feedback is anonymous, but we will show the aggregate group feedback in real-time.

INSIDER THREAT TRENDS IN THE ENERGY SECTOR

Dan Costa

Technical Manager, Carnegie Mellon/Software Engineering Institute

Insider Threat Trends in the Utilities Sector

Dan Costa

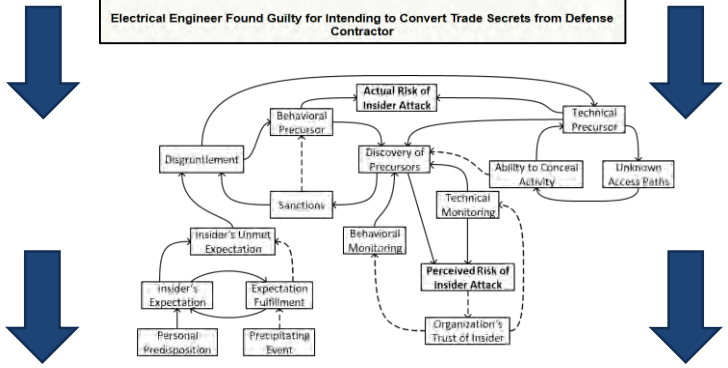
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

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

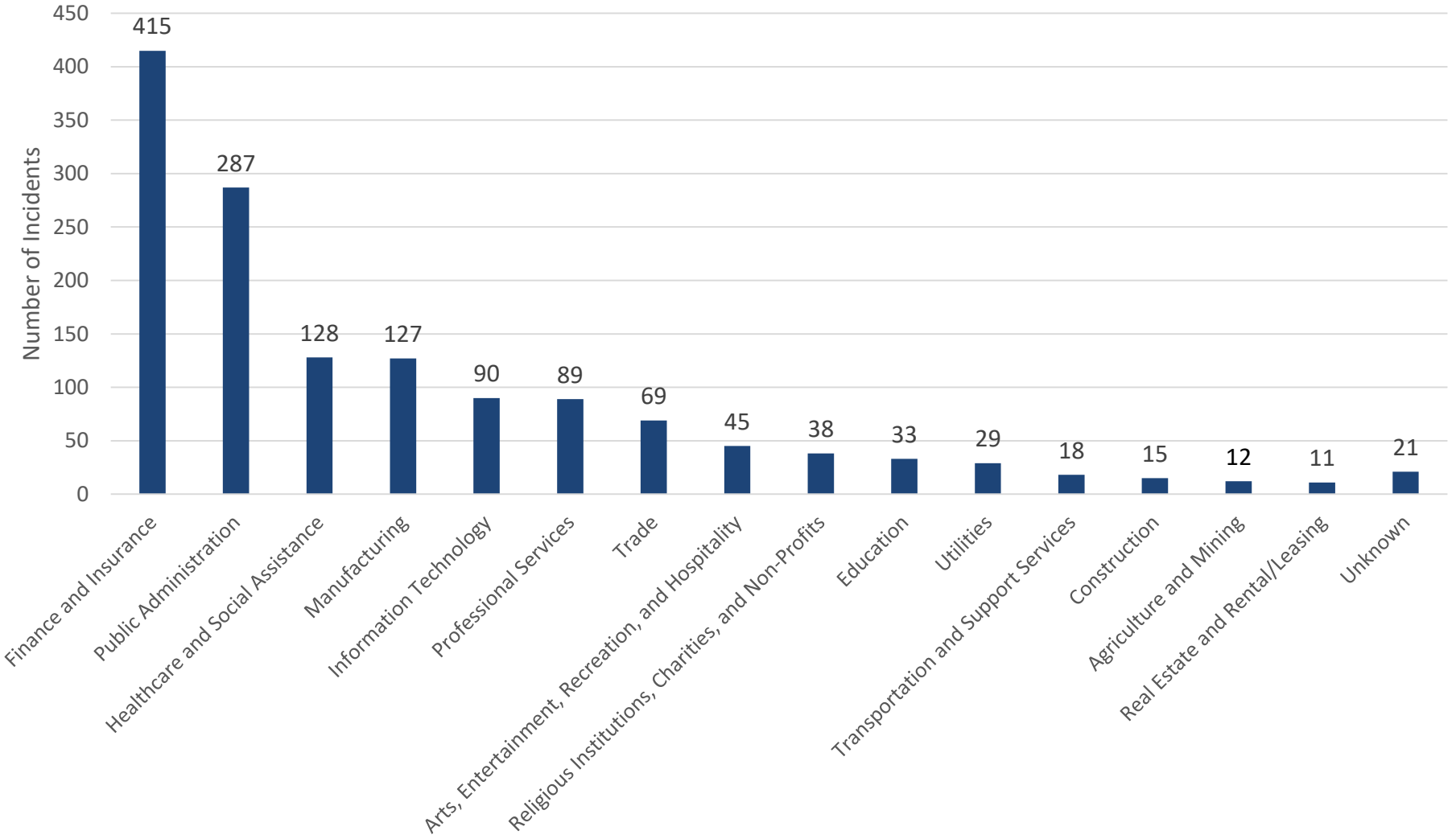
The CERT National Insider Threat Center




```
Splunk Query Name: Last 30 Days - Possible Theft of IP
Terms: 'host=HECTOR [search host="zeus.corp.merit.lab" Message="A user account was  disabled. *" |
eval Account_Name=mvindex(Account_Name, -1) | fields Account_Name | strcat Account_Name
"@corp.merit.lab" sender_address | fields - Account_Name] total_bytes > 50000 AND
recipient_address!="*corp.merit.lab" startdaysago=30 | fields client_ip, sender_address,
recipient_address, message_subject, total_bytes'
```

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

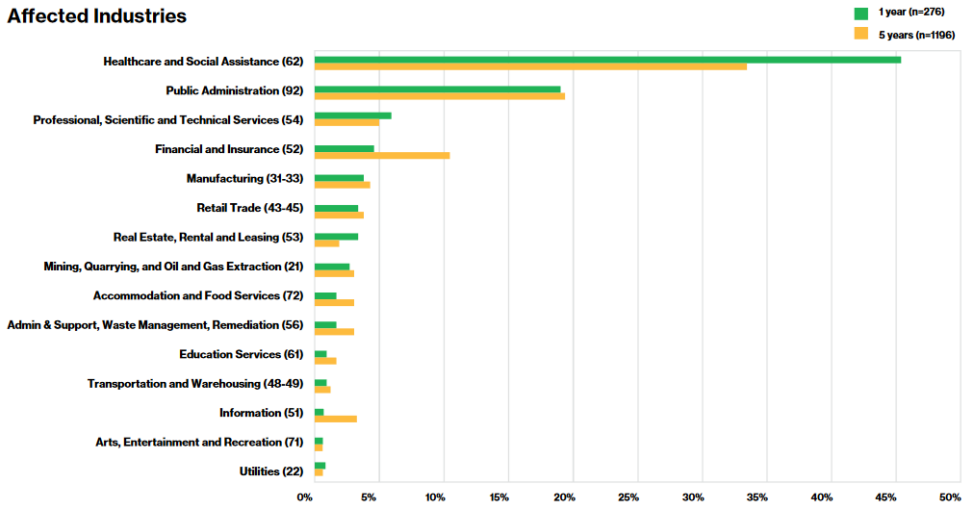


Verizon Insider Threat Study

VERIS — Affected Industries

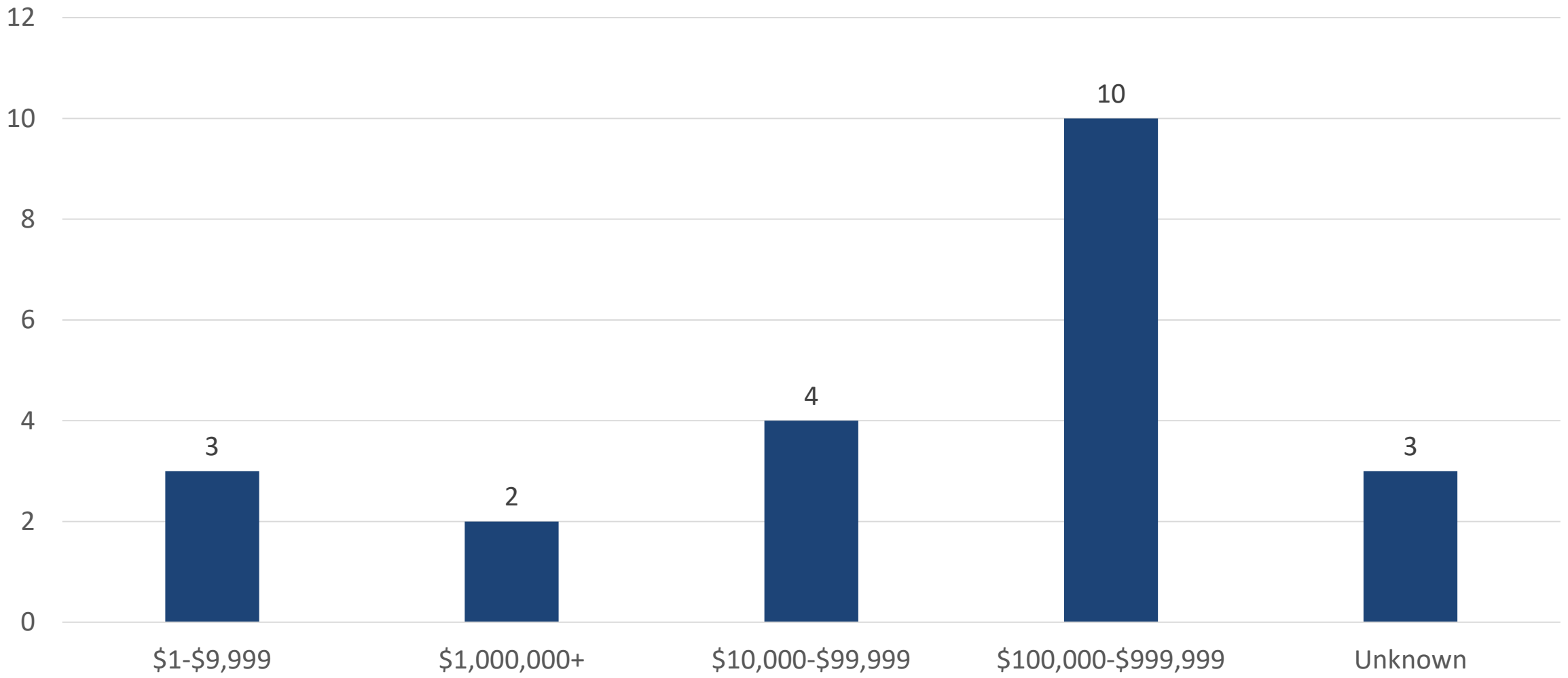
Viewing Insider and Privilege Misuse breaches over the previous year (2018), Healthcare and Social Assistance (46.4%) and Public Administration (18.5%) are the top industries involving privileged threat actors causing the most damage.

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:

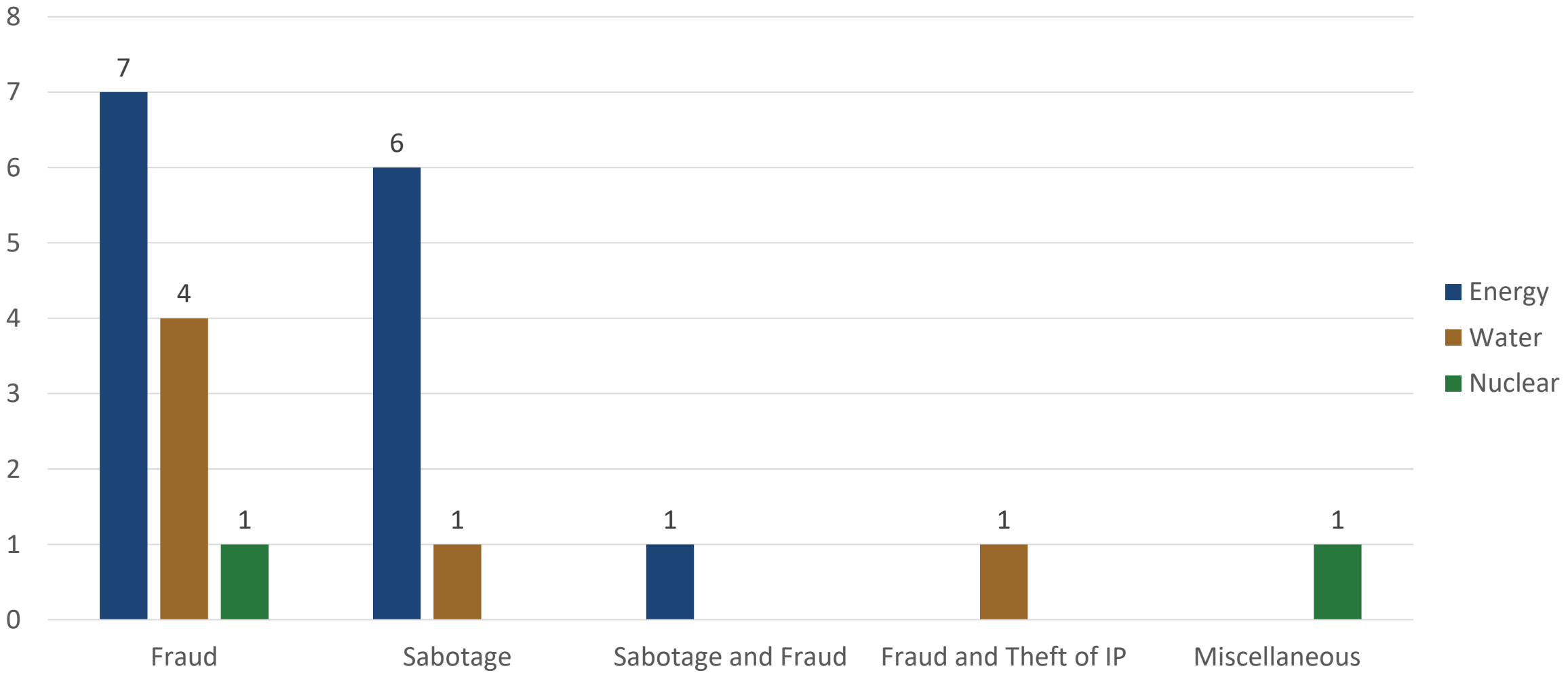


https://enterprise.verizon.com/resources/reports/insider-threat-report.pdf

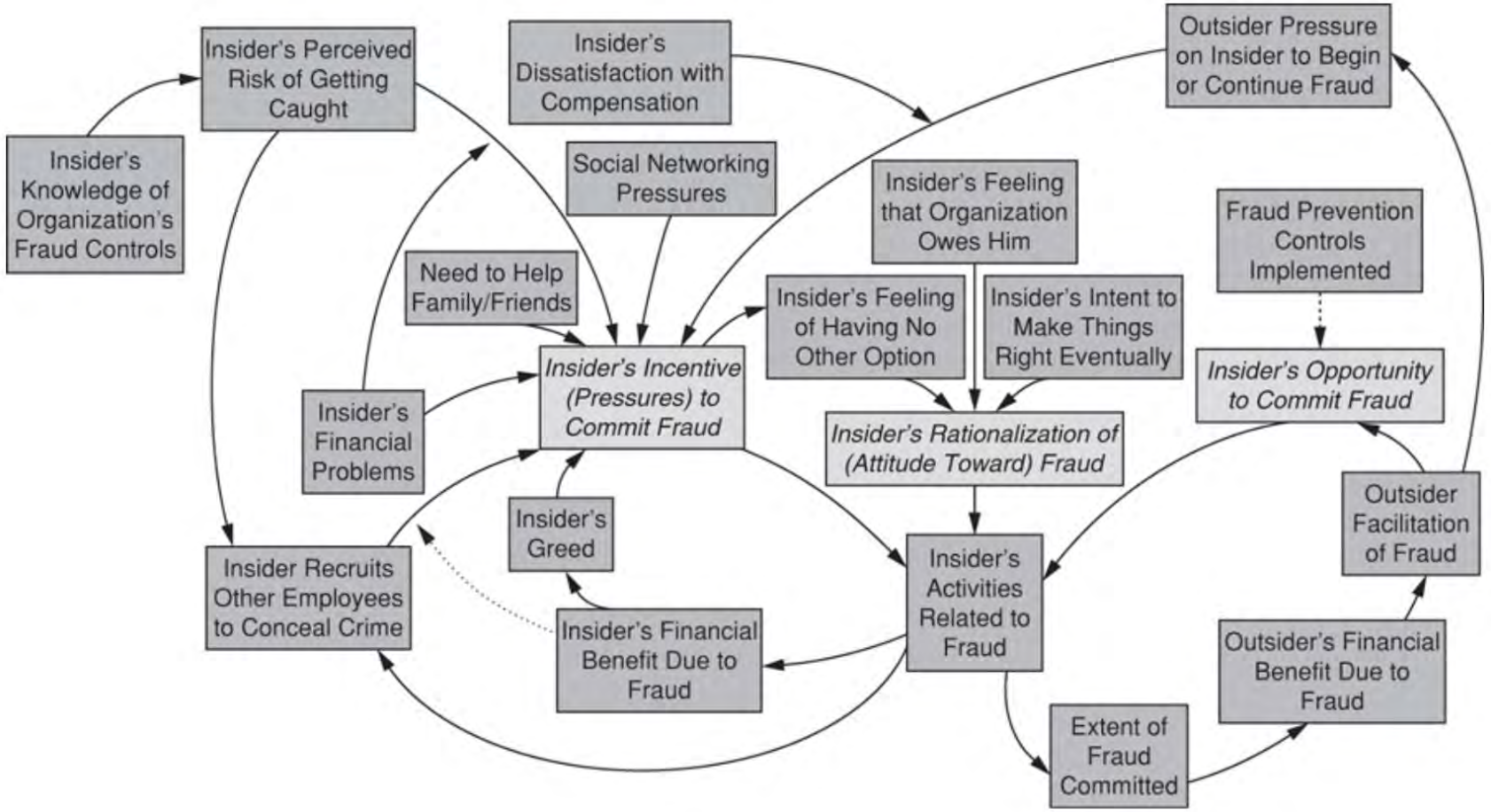
Financial Impact



Incident Types

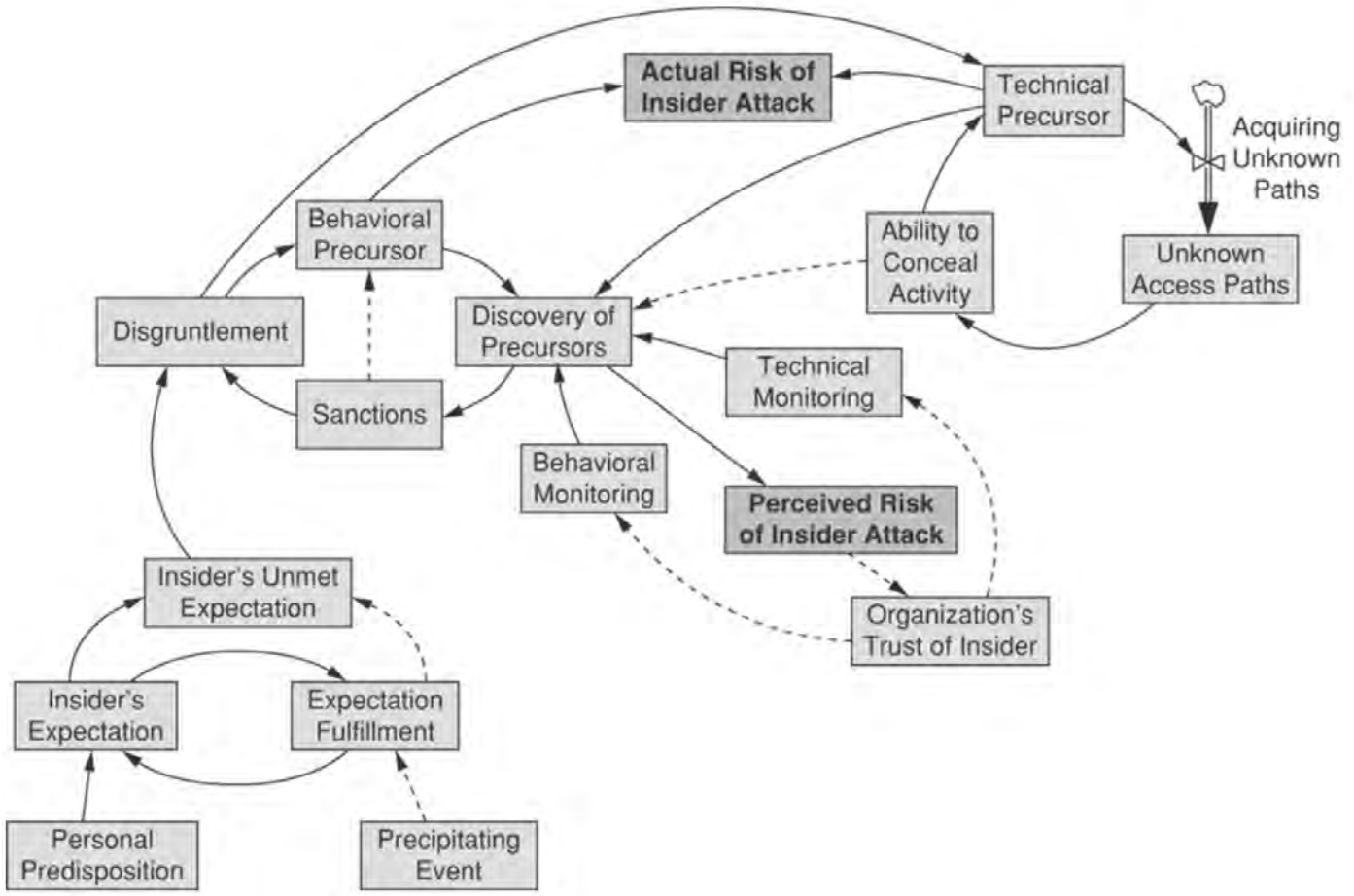


CERT's Insider Fraud Model



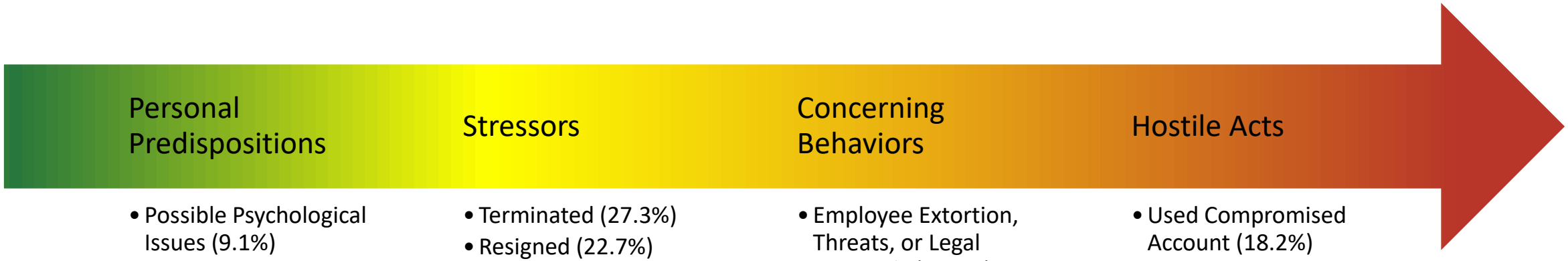
Source: The CERT® Guide to Insider Threats

CERT's Insider Sabotage Model



Source: The CERT® Guide to Insider Threats

Critical Path to Insider Risk – Utilities Observables



Personal Predispositions

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

Stressors

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

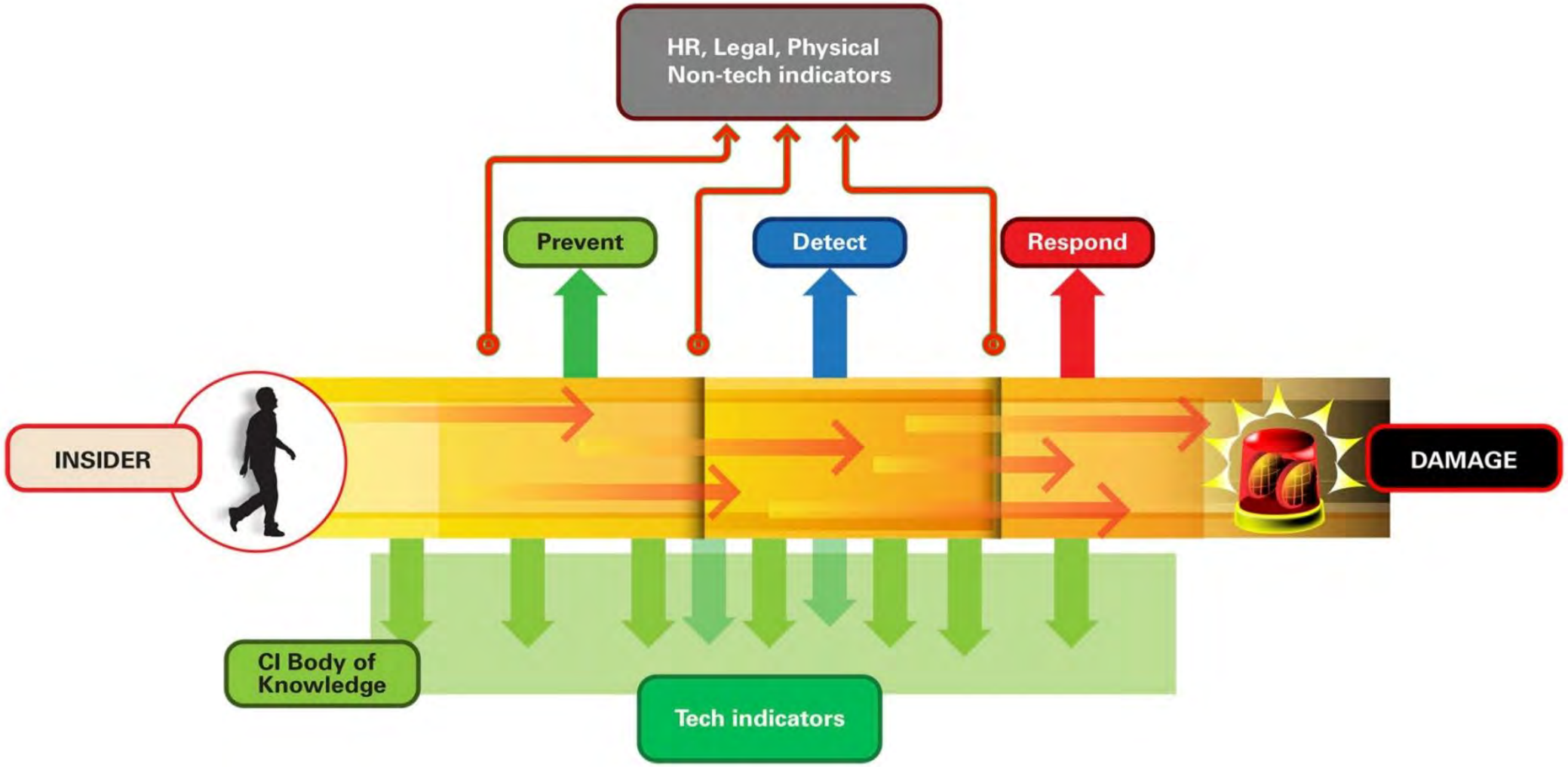
Concerning Behaviors

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

Hostile Acts

- 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…



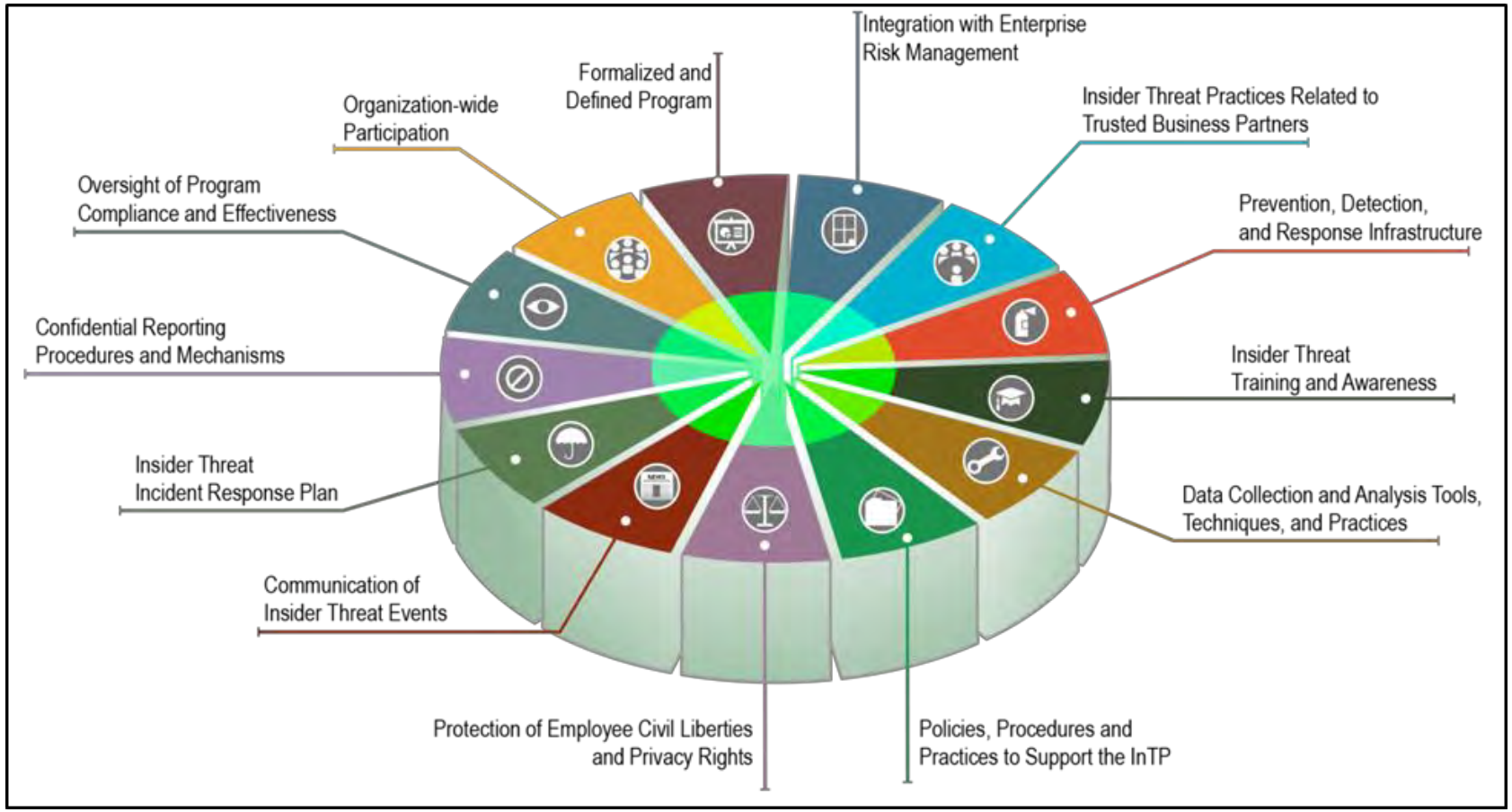
Is to reduce insider risks to critical assets to acceptable levels

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

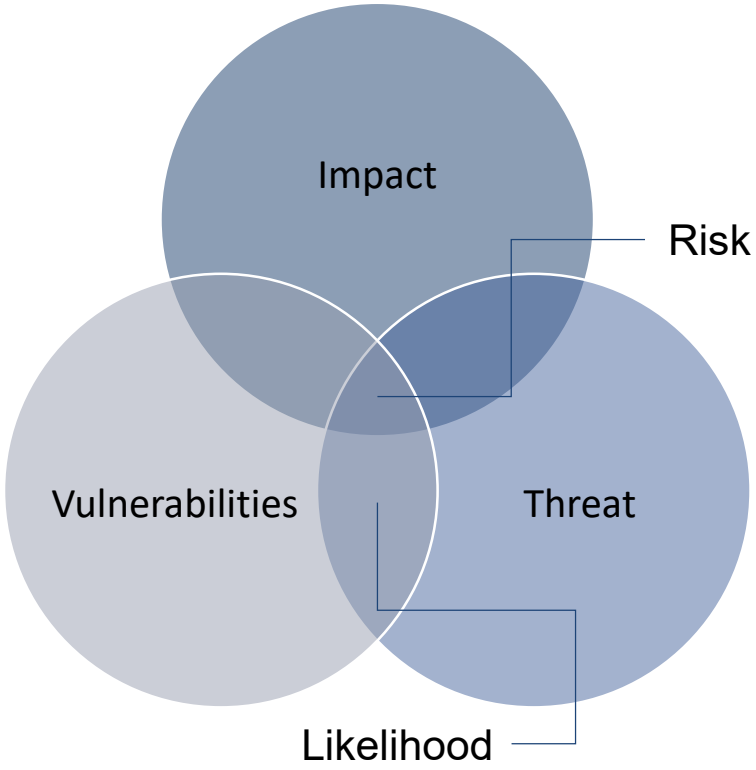


Acceptable Levels?

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

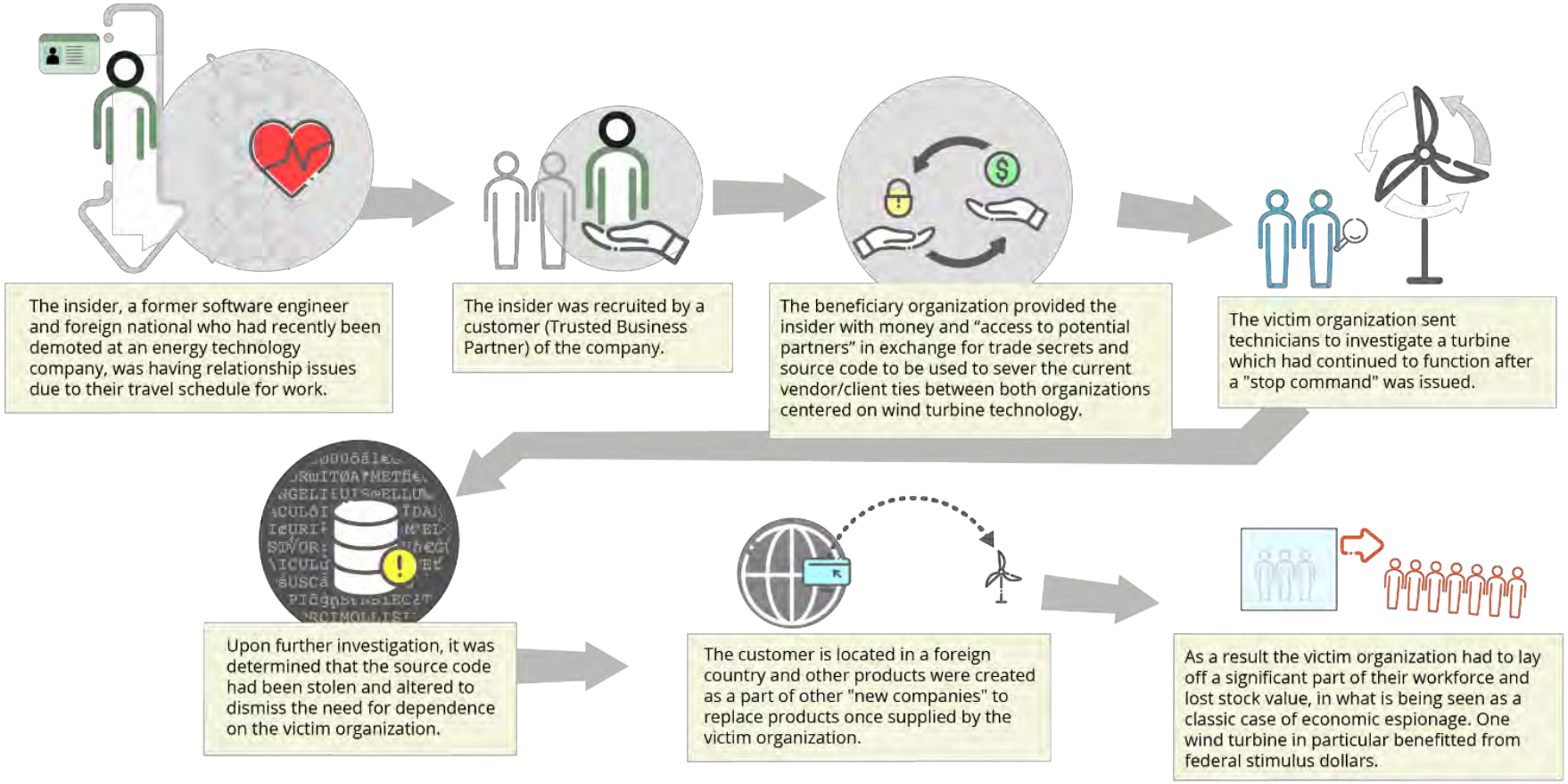
Technical Manager, CERT National Insider Threat Center

dlcosta@sei.cmu.edu

www.cert.org/insider-threat

Case Studies and Resources

Theft of IP

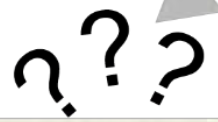


Fraud

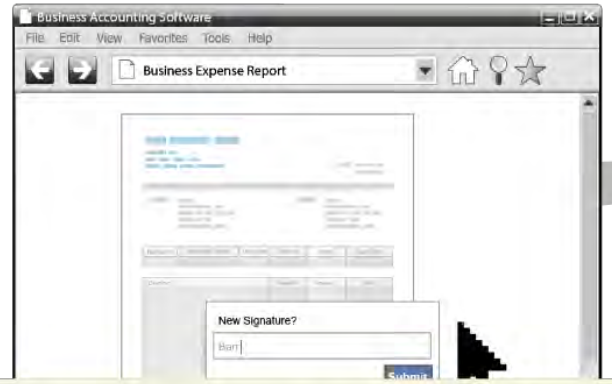
The insider was a current, full-time employee responsible for the operations of a privately-owned oil and natural gas company, the victim organization.

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.



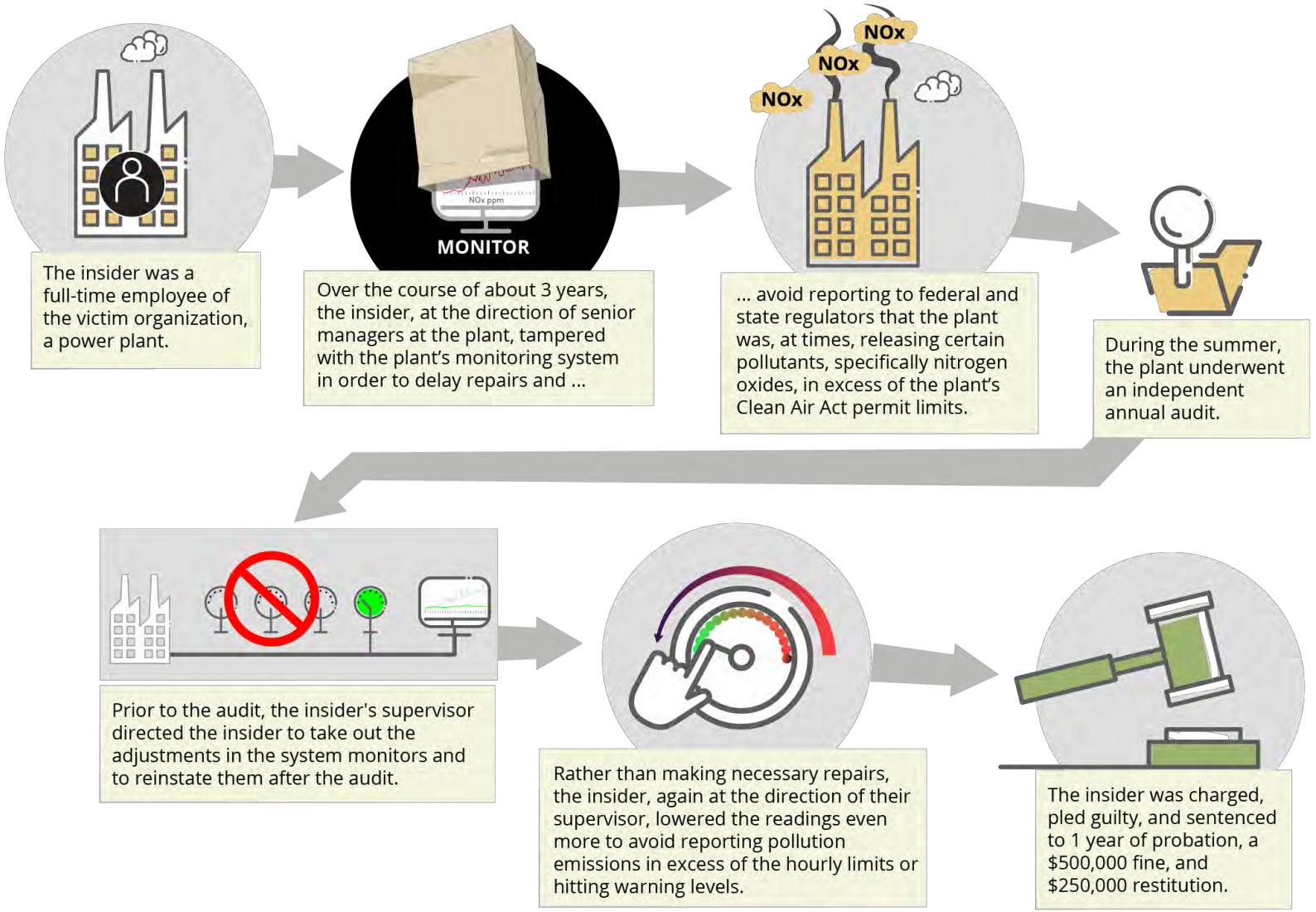
It is unclear how the insider was identified, nor how the fraud was detected.



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

INSIDER THREAT – A CASE STUDY

Matt Shultz

IT Security Specialist, FERC

RELIABILITY FIRST

Insider Threats Webinar

September 30, 2020

Insider Threat: A Case Study

DISCLAIMER

THE VIEWS I EXPRESS IN THIS PRENTATION DO NOT NECESSAIRLY REPRESENT THE VIEWS OF ANY COMMISSIONER OR THE COMMISSION, THEY ARE MY OWN.

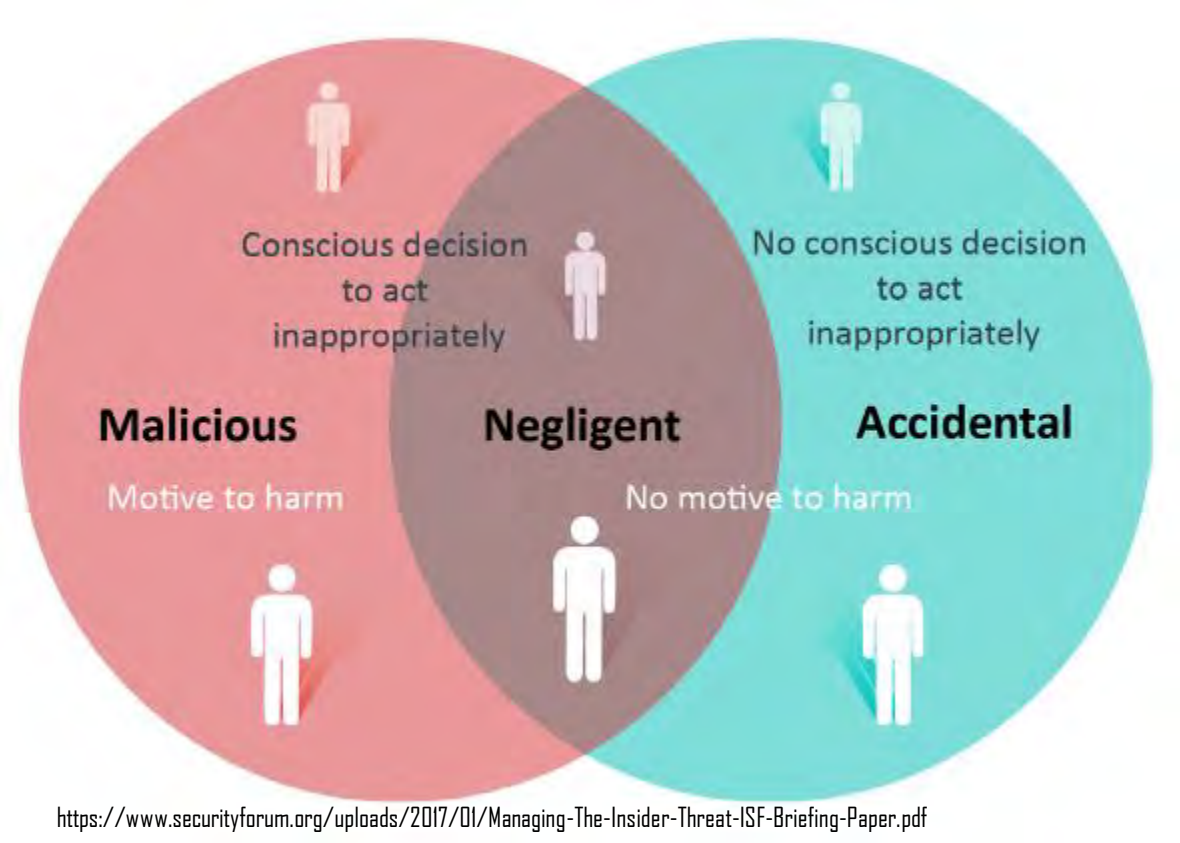
Agenda

- Introduction
- Motivations
- Case Study - IP Theft
- Nation State Doctrine
- Insider Threat Behaviors
- Relevant Assessment Findings
- How To Report
- Resources
- Wrap Up

whoami

- Matt Shultz
  - IT Security Specialist FERC/DEIS
    - Lead Assessor – Voluntary Cyber Architecture Assessments
  - Focus – Cybersecurity Best Practices Versus Standards
  - CISSP, CRISC, CDPSE, GRID, GCIA, & PMP certifications
  - 23 Years Defense Industrial Base
    - Component Level Repair
    - Hardware & Software Support
    - Network Engineering
    - Business Continuity
    - Security Operations
    - Program Management

Motivations



https://www.securityforum.org/uploads/2017/01/Managing-The-Insider-Threat-ISF-Briefing-Paper.pdf

https://twitter.com/jromeropwc/status/451072338478784512

Case Study Background

- Xiaoqing Zheng
  - The Insider
- Zhaoxi Zhang
  - The accomplice
- Liaoning Tianyi Aviation Technology Co., Ltd. (LTAT)
  - Focus on development
- Nanjing Tianyi Avi Tech Co., Ltd. (NTAT)
  - Focus on manufacturing

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF NEW YORK

STATES OF AMERICA	)	Criminal No. 1:19-CR-156 (MAD)
	)	
v.	)	Indictment
	)	
NG Xiaoqing and ANG Zhaoxi	)	Violation(s): 18 U.S.C. §§ 1831, 1832, 1001
	)	

What Was Stolen

- Design models
- Engineering drawings
- Material specifications
- Performance test rigs
- Turbine sealing and optimizing technology
- Other information related to metal brush seals, turbine blades, and combustion chamber

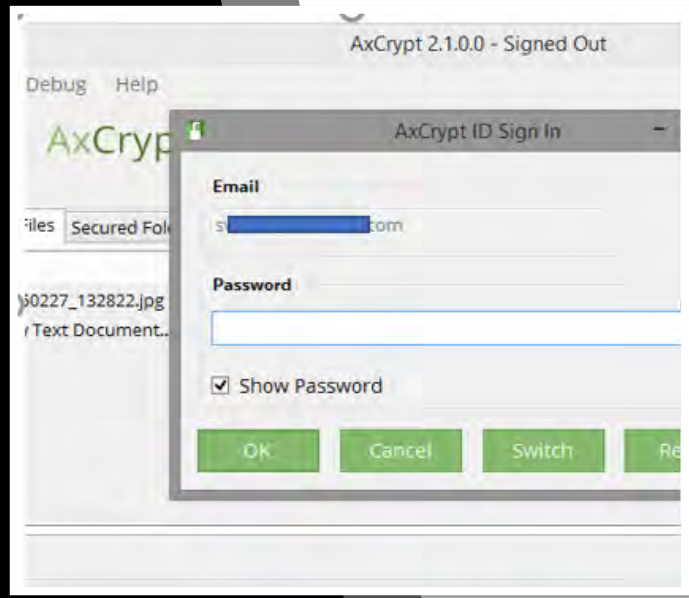
[Y]ou must be extremely careful to avoid using GE intellectual property, proprietary information or proprietary processes. Although you should not use knowledge and skills acquired as a GE employee, before your company becomes or if your company has become a part supplier to a company which may compete with GE Aviation, be sure to fully inform your manager and ask your GE business' Legal/Compliance counsel for advice. Should the situation change in the future, please notify your manager and complete another on-line submission of the conflict of interest form.

- GE Power Counsel to Zheng

How Was It Stolen

Protection Measures

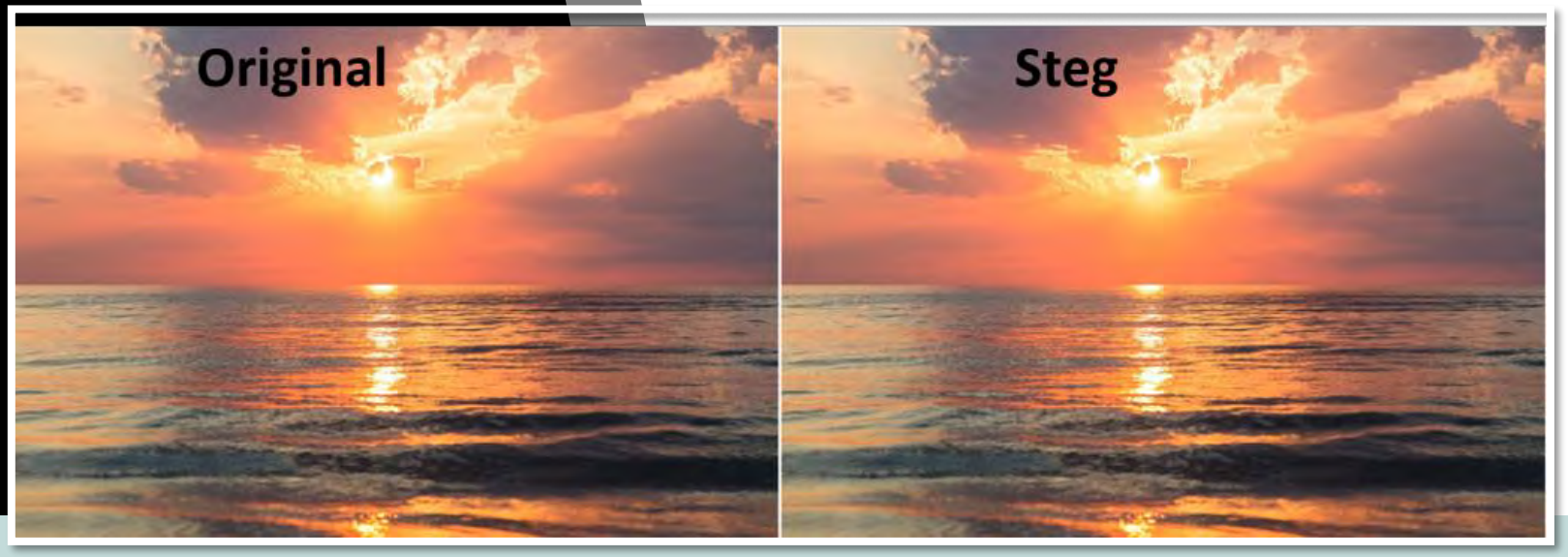
- Physical security
- Administrative security
- Security policy
- Technical controls



2. Requirements and Limitations

AxCrypt requires very little and is compatible with all current versions of Windows.

Resource	Value
Memory (RAM)	About 5 Mega bytes of virtual memory when active.
Hard disk space	3 Mega byte
Temporary disk space	Up to about 1.5 x the size of a file being encrypted.
Processor	Any x86 or x64
Operating System	Windows XP, 2003, 2008, Vista, 7. 32-bit or 64-bit.
User permissions	Any user can run AxCrypt
Installation permissions	Administrator privileges required to install.
Maximum file size	Only limited by disk space or file system.
Maximum number of encrypted files	Only limited by disk space or file system.
Development environment	To recompile AxCrypt from downloaded source code you need Visual Studio 2010 express or later/better.



Why Was It Stolen

- 13th 5 Year Plan
- Made in China 2025
- Thousand Talents Program

China's 13th 5 Year Plan (2016–2020)

- Innovation
- Coordinated Development
- Green Growth
- Openness
- Inclusive Growth

The 13th Five-Year Plan places aerospace development as a priority among its strategic key technology projects. A year has since passed. I feel the sense of urgency more than ever. Therefore, I am here to ask the leadership to give the development of this national key technology project the special attention it deserves, without reservation. Please do the extraordinary and move this strategic industry and advanced manufacturing technology forward in the area, rightly making it a Liaoyang specialty industry.

Zheng encrypted message to Zhang 22 JAN 17

Made in China 2025

BUSINESS TECHNIQUES:

- **Visitors**
- Academic Collaboration
- Talent Recruitment Programs
- **Trade Shows and Conferences**
- Foreign Travel
- **Elicitation**

DIFFERENCES IN BUSINESS PRACTICES	
UNITED STATES	**CHINA**
GENERALLY ACCESSIBLE MARKET	HIGHLY RESTRICTIVE MARKET
MARKET ECONOMY	STATE-RUN ECONOMY
DEVELOPMENT BY INNOVATION	DEVELOPMENT BY THEFT, REPLICATION, AND COMMERCIALIZATION
INDEPENDENT JUDICIARY AND SEPARATION OF POWERS	JUDICIARY SUBORDINATE TO THE GOVERNMENT
LAWS PROTECTING INTELLECTUAL PROPERTY	THEFT OF INTELLECTUAL PROPERTY
NO GOVERNMENT-SPONSORED ECONOMIC ESPIONAGE	GOVERNMENT-SPONSORED ECONOMIC ESPIONAGE

Source: FBI China: The Risk to Corporate America

The Program Formerly Known as China's "Thousand Talents Program"

Recruitment programs are often part of broader whole-of-government strategies to reduce costs associated with basic research while focusing investment on military development or dominance in emerging technology sectors.

Distinguishing features of a foreign government talent recruitment program:

1. Compensation provided by the foreign state to the targeted individual in exchange for the individual transferring their knowledge and expertise to the foreign country.

- Cash
- Research funding
- Honorific titles
- Career advancement opportunities
- Promised future compensation
- Other types of remuneration or consideration

2. The targeted individual may be employed and located in the U.S., or in the foreign state.

3. Possible incentivization of the targeted individual to physically relocate to the foreign state. Of particular concern are those programs that allow for continued employment at U.S. research facilities or receipt of DOE research funds while concurrently receiving compensation from the foreign state

Text Source: https://www.directives.doe.gov/directives-documents/400-series/0486.1-BOrder/@@images/file
Image Source: https://www.scmp.com/news/china/article/1631317/chinas-programme-recruiting-foreign-scientists-comes-under-scrutiny

Insider Threat Behaviors

- Displays suitability issues, such as alcohol abuse or illegal drug use
- Insists on working in private
- Volunteers to help on classified* or sensitive work
- Expresses an interest in covert activity
- Has unexplained or prolonged absences

- Is disgruntled to the point of wanting to retaliate against the company
- Rummages through others' offices or desks
- Misuses computer or information systems
- Unnecessarily photocopies sensitive material
- Takes classified* or sensitive material home

- Attempts a computer network intrusion
- Has criminal contacts or associates Employs elicitation techniques
- Displays unexplained affluence
- Fails to report overseas travel, if required*
- Works unusual hours

- Conceals foreign contacts
- Lacks concern for or violates security protocols
- Attempts to gain access without a need to know
- Shows unusual interest in information outside the scope of his or her job

Relevant Architectural Assessment Findings

- Contract workforce
  - Actor identification of critical facilitates (espionage)
- Periodic reinvestigations
- Open source information collection
- Network architecture
- Elevated privilege accounts
- Shadow IT

How to Report

- Internally
  - Clear reporting guidelines supported by insider threat policy
  - Including anonymous reporting
  - Incorporate multiple communication channels
    - Phone hotline
    - Email
    - Website
    - Supervisors
    - Human resources
    - Insider threat program office open-door policy
  - Ensure reporting protects the privacy of all concerned
  - Provide quick feedback to those reporting concerning behavior
- Externally
  - Don't tip off / terminate the employee

Domestic Security Alliance Council

- https://www.dsac.gov/

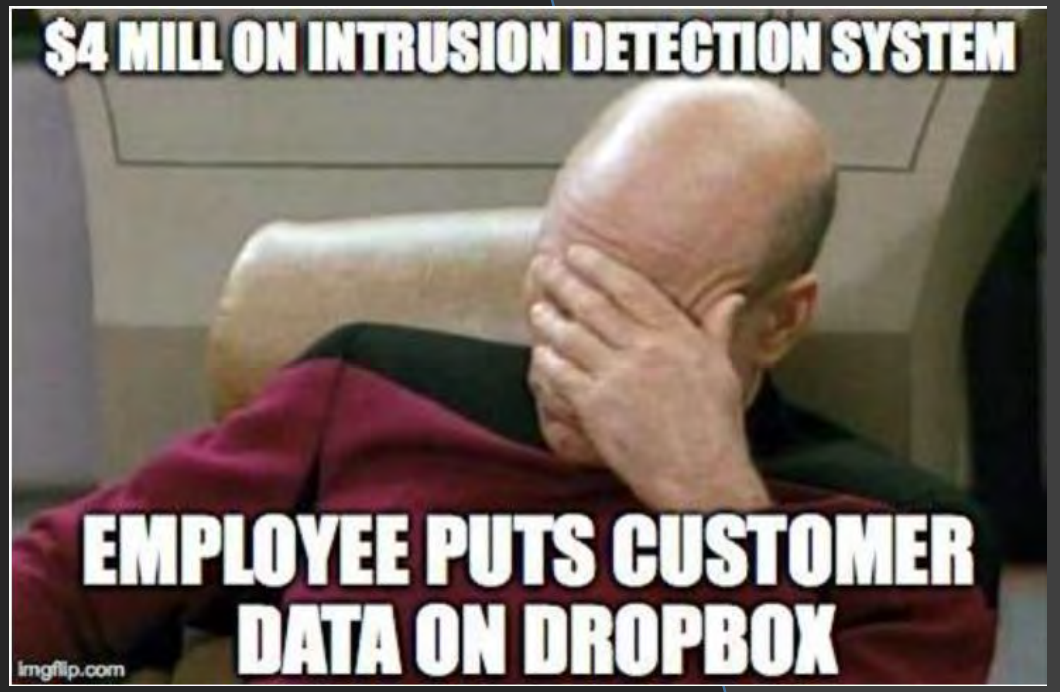
Infragard

- https://infragard.org

or: https://www.ic3.gov

Resources (for the before time)

- Director of National Intelligence (DNI)
  - National Insider Threat Task Force (NITTF)
  - https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf
- Department of Homeland Security (DHS)
  - Cybersecurity and Infrastructure Security Agency (CISA)
  - Insider Threat Mitigation Website
  - https://www.cisa.gov/insider-threat-mitigation
- U.S. Department of Defense (DOD)
  - Center for Development of Security Excellence (CDSE)
  - https://www.cdse.edu/
- Carnegie Mellon University (CMU)
  - Software Engineering Institute – Insider Threat
  - https://www.sei.cmu.edu/research-capabilities/all-work/display.cfm?customel_datapageid_4050=21232
- Employee Assistance Programs (EAP)



Wrap Up

Key Takeaways

- From the top
- 'Physician heal thyself'
- Cyber is hard
- Listen to your people
- You are not 'Big Brother'
- Bring out your Feds
- You Got This

Questions ??

Contact:

matthew (dot) shultz (at) ferc (dot) gov

No 'C' here

INSIDER THREAT AWARENESS

Benjamin Gibson

Senior Analyst, NERC/E-ISAC

A DIVISION OF NERC

E-ISAC

ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

Insider Threats

Benjamin Gibson
Senior Analyst
Physical Security

RF Insider Threat Briefing
September 30, 2020




What is an Insider Threat?

- **What is an Insider Threat?**
  - Meanings
  - Examples

- **Definitions**
  - National Insider Threat Task Force (NITTF)
  - Design Basis Threat

- **Types of Insider Threat:**
  - Passive Insider
  - Active Nonviolent Insider
  - Active Violent Insider

Five Main Categories of Insider Threat

The National Insider Threat Task Force (NITTF) defines five main categories of insider threat which we will discuss:

- Leaks
- Spills
- Espionage
- Sabotage
- Targeted Violence

Leaks

Intentional, unauthorized disclosure of classified or proprietary information to a person or an organization that does not have a "need-to-know."

Spills

Unintentional transfer of classified or proprietary information to unaccredited or unauthorized systems, individuals, applications, or media.

- Spills are the most common form of insider threat
- Spills do not require malicious intent to cause damage
- Spills can be cyber or physical

Espionage

Unauthorized transmittal of classified or proprietary information to a competitor, foreign nation, or entity with the intent to harm.

Sabotage

Means to deliberately destroy, damage, or obstruct, especially for political or military advantage.

Targeted Violence

Any form of violence that is directed at an individual or group, for a specific reason.

Protecting Information From Adversaries

- **Adversaries**
- **What They Want to Know**
- **How Adversaries Gather Information**

Indicators and Vulnerabilities

We all have vulnerabilities. But not everyone who exhibits vulnerabilities represents a potential insider threat. However, some vulnerabilities could increase the risk that an insider could be exploited or make the decision to leak, commit espionage, or engage in sabotage and/or targeted violence.

Technology Considerations

- **Technology Impact**
- **Social Media Impact**
- **Technology Considerations**
- **Social Media Considerations**
- **Countermeasures**

Electricity Industry Incidents

How to Share

- Members can share directly with the E-ISAC by posting to the portal www.eisac.com;
- Emailing the E-ISAC operations@eisac.com or physicalsecurity@eisac.com; or
- Calling the Watch Floor 202-790-6000

Questions and Answers

DEVELOPING AN INSIDER THREAT PROGRAM: WHO CAN WE TRUST?

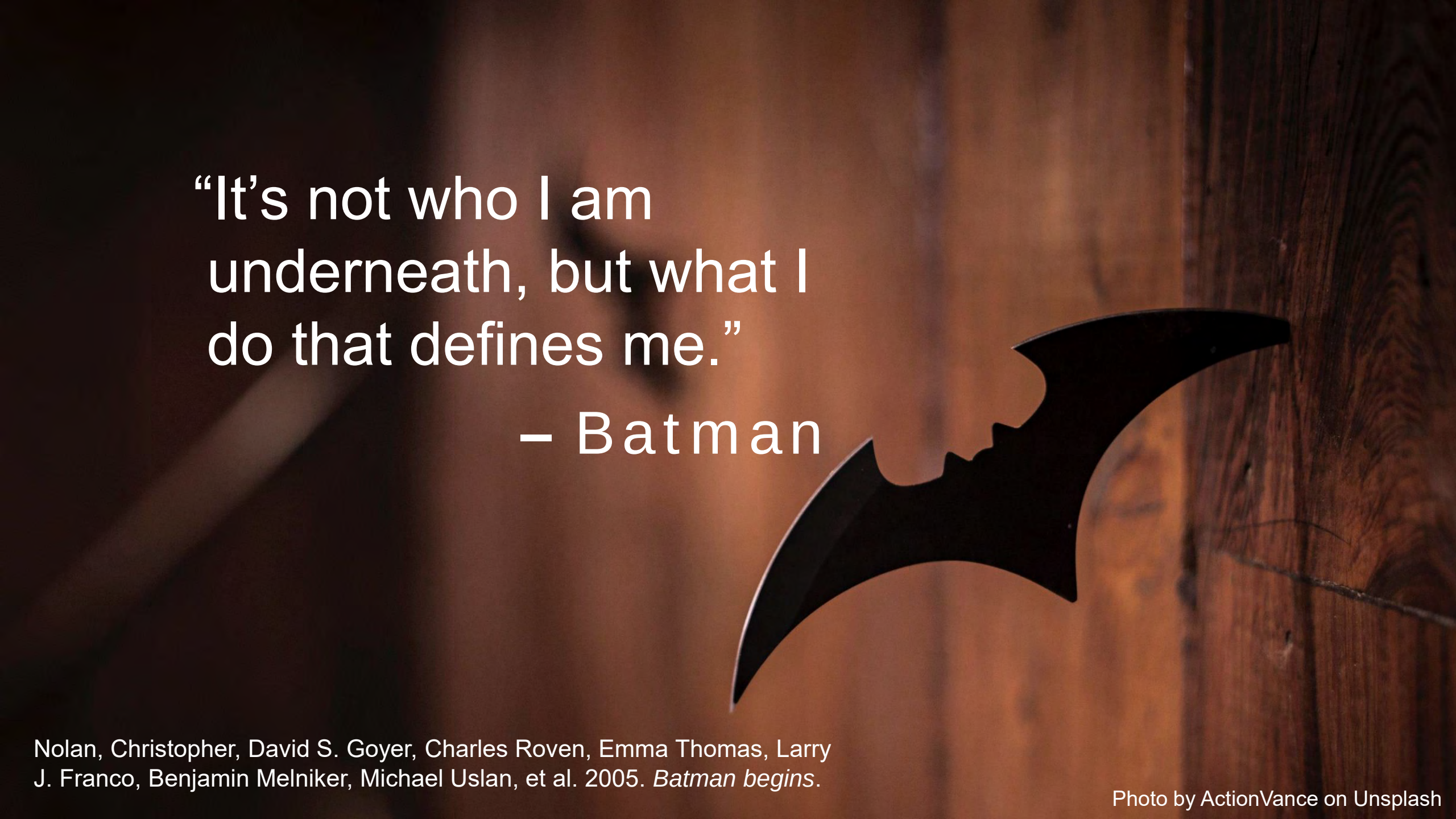
Steven McElwee

Chief Information Security Officer, PJM

Developing an Insider Threat Program: Who Can You Trust?

ReliabilityFirst Insider Threats Webinar
September 30, 2020

Steven McElwee, Ph.D.
Chief Information Security Officer



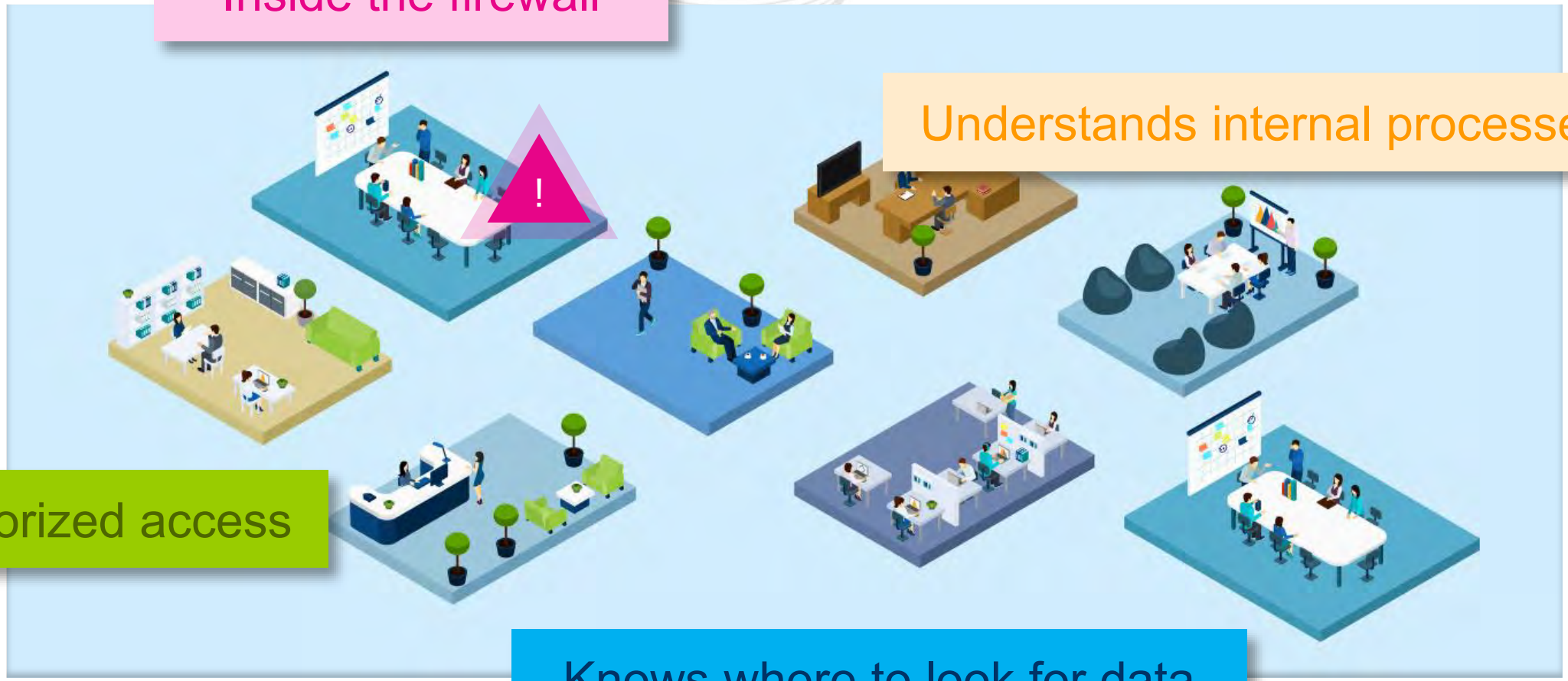
Nolan, Christopher, David S. Goyer, Charles Roven, Emma Thomas, Larry J. Franco, Benjamin Melniker, Michael Uslan, et al. 2005. *Batman begins*.

Photo by ActionVance on Unsplash

Photo by Massimo Botturi on Unsplash

Insider Advantage

Inside the firewall



Understands internal processes

Authorized access

Knows where to look for data

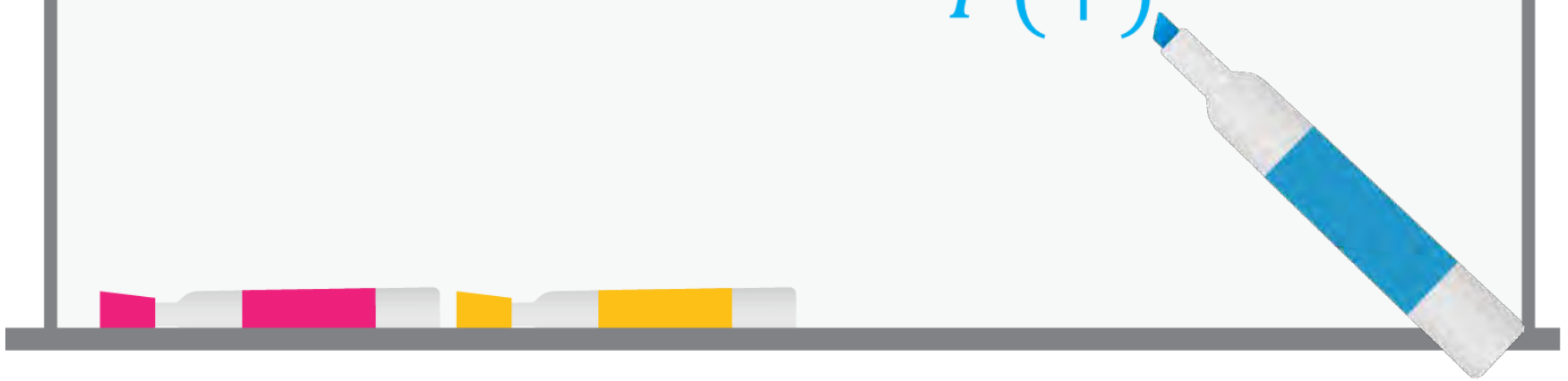
Photo by Ali Shah Lakhani on Unsplash

Why Detecting Insider Threats Is Challenging

Even with high accuracy given a positive detection, there is a low probability that the user is actually a threat.

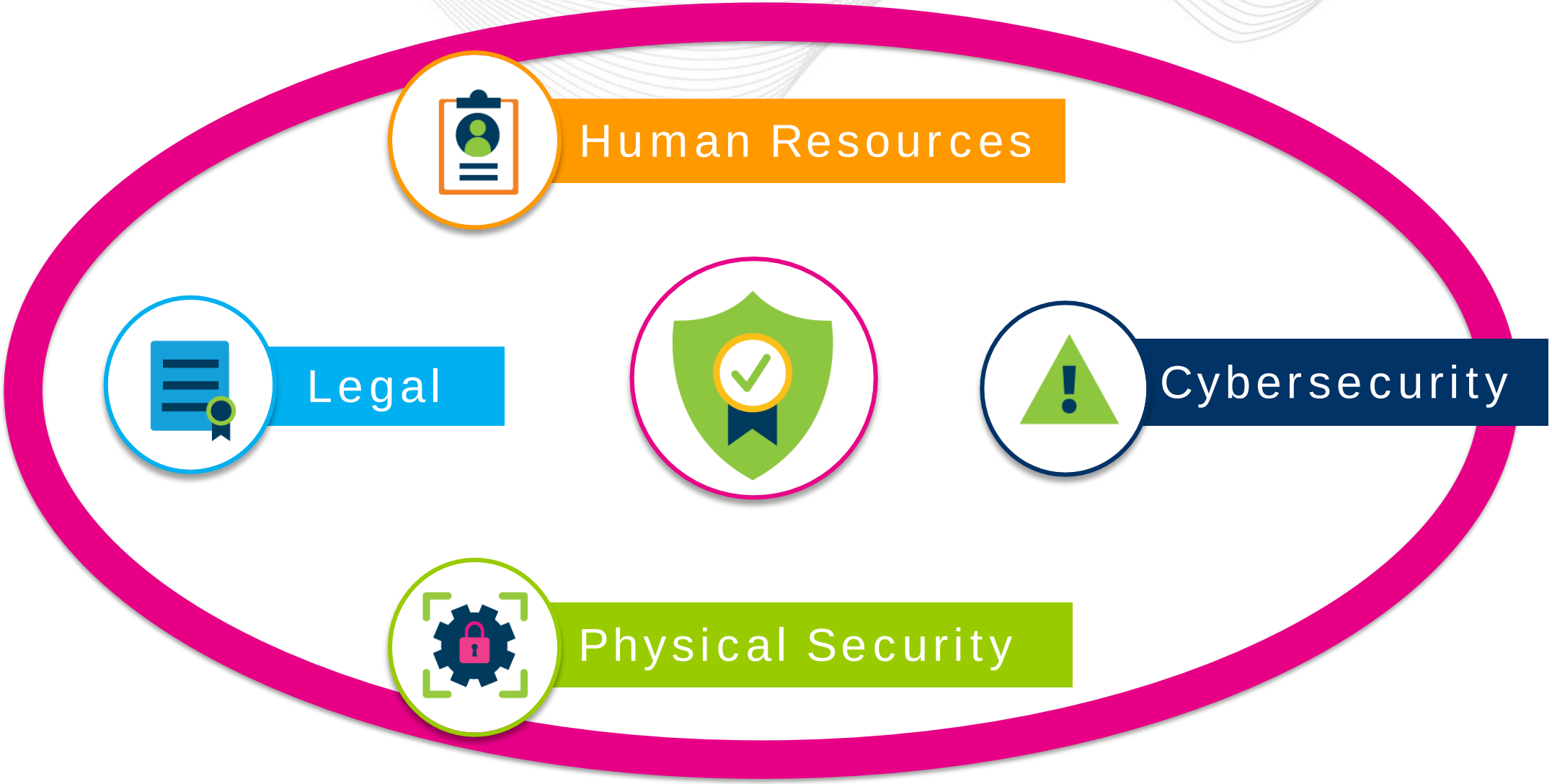
If one in 1,000 users is an insider threat, the probability that a user is an insider threat P(user) is 0.001.

$$P(user|+) = \frac{P(+|user)P(user)}{P(+)}$$




“HR professionals consider and protect the rights of individuals, especially in the acquisition and dissemination of information while ensuring truthful communications and facilitating informed decision-making.”
– Society for Human Resource Management
Photo by Romain V on Unsplash

Building Trust With Internal Business Partners



Pieces of an Insider Threat Program

Thank You

RF'S INTP MATURITY ASSESSMENT AND HELPFUL RESOURCES

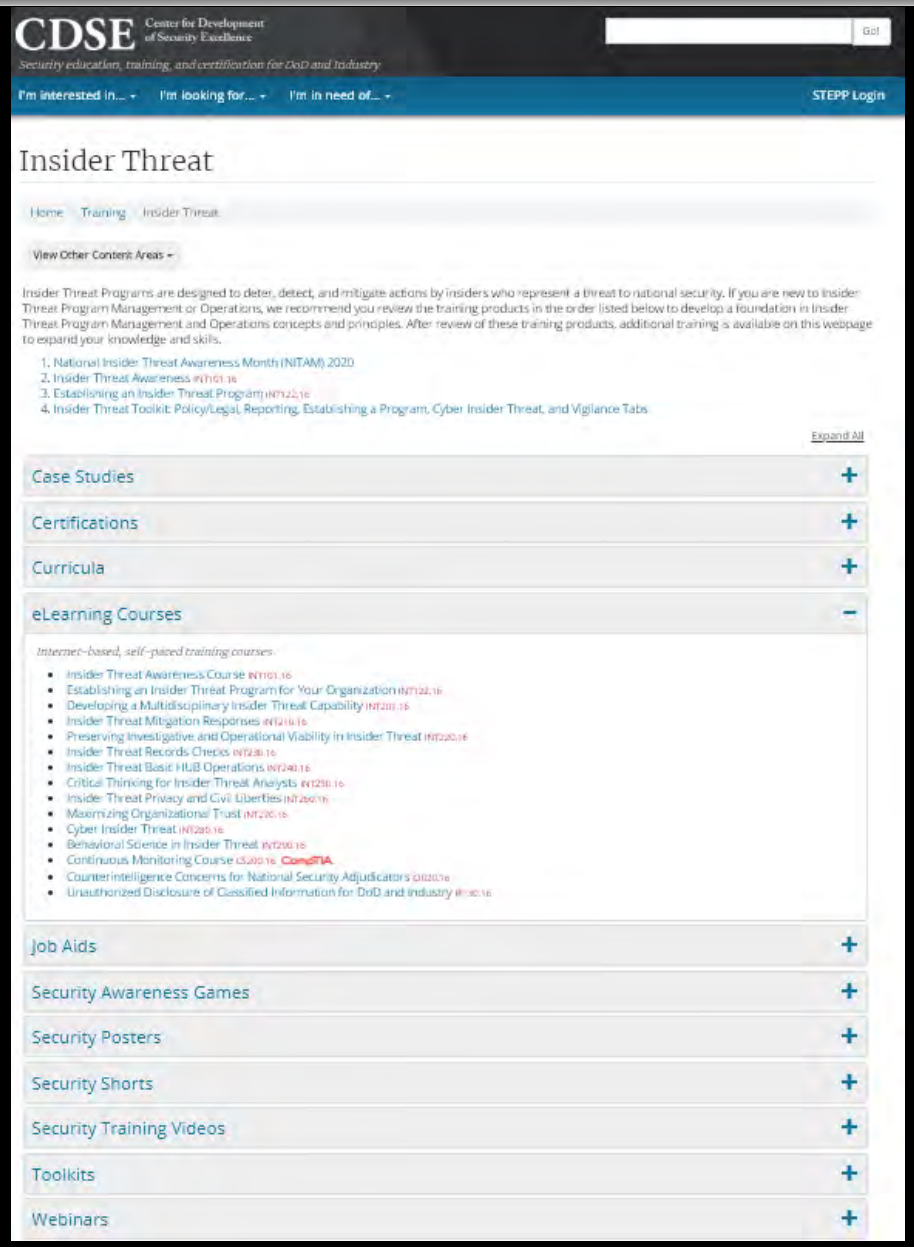
Bheshaj Krishnappa

Program Manager, Risk & Resiliency, RF

Agenda

- Insider Threat Resources
- Insider Threat
- RF's Insider Threat Program Maturity Assessment

Center for Development of Security Excellence (CDSE)



https://www.cdse.edu/catalog/insider-threat.html

Posters

Not every company has resources to have a full fledged InTP, awareness, training and posters can help.

Frameworks

National Insider Threat Task Force
Insider Threat Program
Maturity Framework

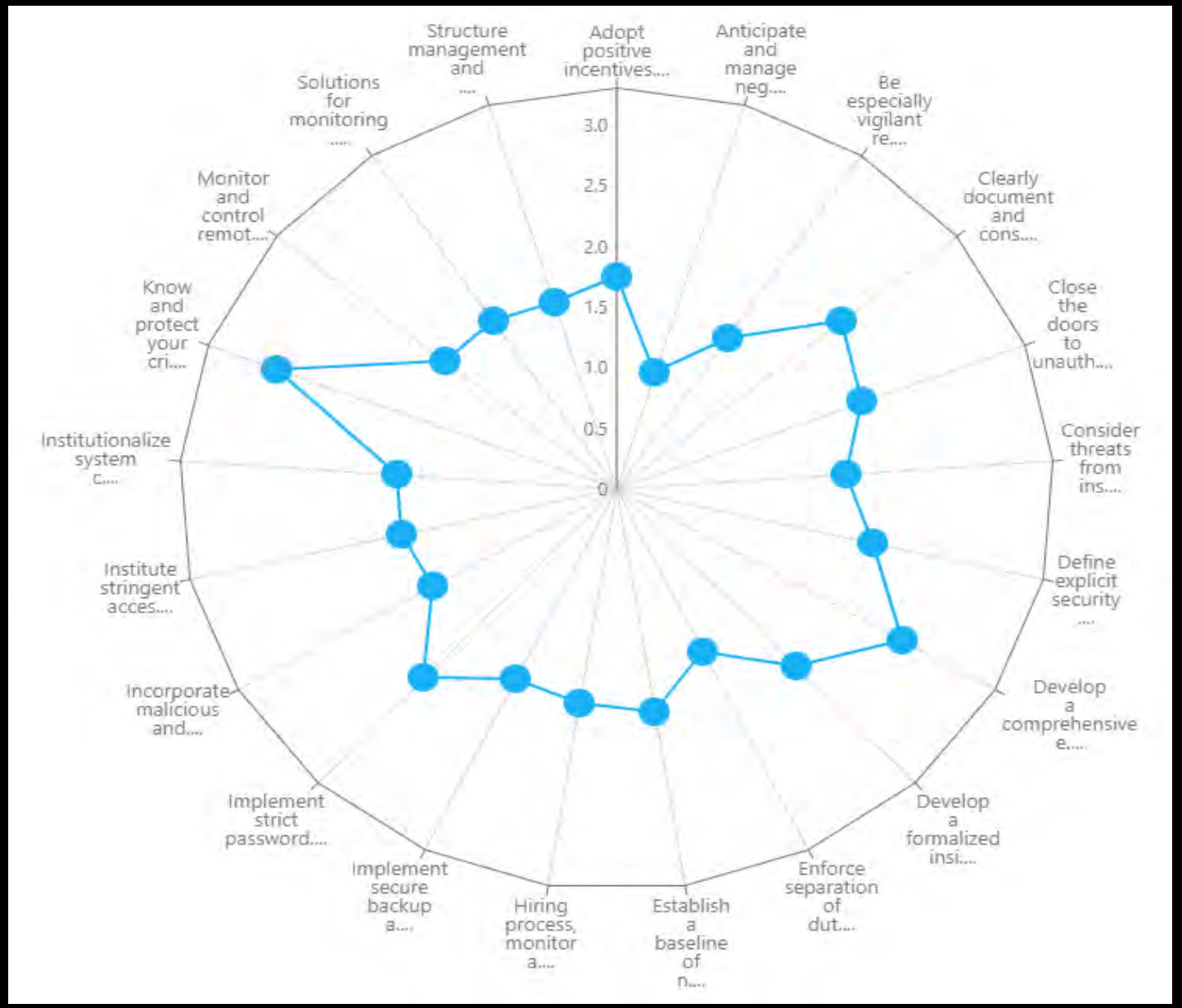
CERT National Insider Threat Center's
Sixth Edition of Common Sense Guide
to Mitigating Insider Threats

RF's Insider Threat Program Maturity Assessment

- **A web-based self-assessment based on 21 best practice areas under SEI CERT's Common Sense Guide to Mitigating Insider Threats.**
  - A comprehensive report containing assessment summary analysis, areas for improvement, resources to improve the program, benchmarking, etc.,
- **Entity/User data is protected to maintain confidentiality and integrity.**
- **Tool security**
  - Securely hosted in RF at https://insiderthreat.rfirst.org
  - Data is encrypted at storage and transit
  - Multifactor authentication and stringent password policy

Available to all entities in the RF footprint!

Polar chart


Adopt positive incentives....
Anticipate and manage neg....
Be especially vigilant re....
Clearly document and cons....
Close the doors to unauth....
Consider threats from ins....
Define explicit security ....
Develop a comprehensive e....
Develop a formalized insi....
Enforce separation of dut....
Establish a baseline of n....
Hiring process, monitor a....
Implement secure backup a....
Implement strict password....
Incorporate malicious and....
Institute stringent acces....
Institutionalize system c....
Know and protect your cri....
Monitor and control remot....
Solutions for monitoring ....
Structure management and ....
3.0
2.5
2.0
1.5
1.0
0.5
0

Practice Area vs Maturity Distribution

Practice area Heatmap

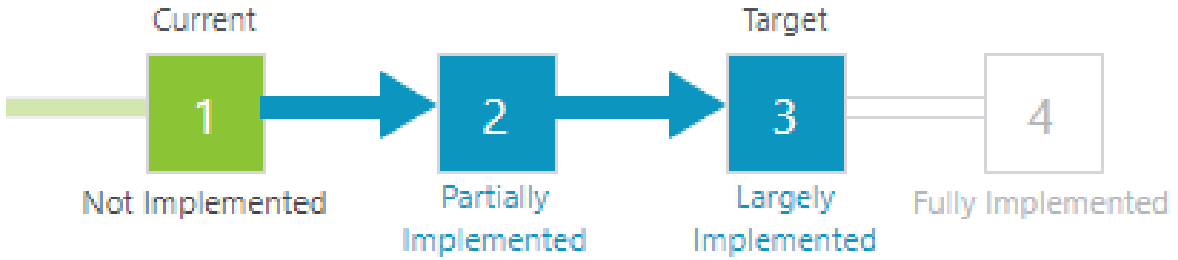
Assessment - Entity A

Insider Threat Program Checklists of Quick Wins and High-Impact Solutions

Know and protect your critical assets 2.75(Largely Implemented)	**Anticipate and manage negative issues in the work environment** **1.00(Not Implemented)**	Incorporate malicious and UIT awareness into periodic security training 1.60(Partially Implemented)	Monitor and control remote access from all end points, including mobile devices 1.67(Partially Implemented)	Establish a baseline of normal behavior for both networks and employees 1.86(Partially Implemented)	Enforce separation of duties and least privilege 1.50(Partially Implemented)
Develop a formalized insider threat program 2.00(Partially Implemented)	Consider threats from insiders and business partners in enterprise wide risk assessments 1.75(Partially Implemented)	Implement strict password and account management policies and Ps 2.14(Partially Implemented)	Define explicit security agreements for any cloud services 2.00(Partially Implemented)	Implement secure backup and recovery processes 1.75(Partially Implemented)	Close the doors to unauthorized data exfiltration 2.00(Partially Implemented)
Clearly document and consistently enforce policies and controls 2.20(Partially Implemented)	Be especially vigilant regarding social media 1.50(Partially Implemented)	Institute stringent access controls and monitoring policies on privileged users 1.67(Partially Implemented)	Institutionalize system change controls 1.67(Partially Implemented)	Develop a comprehensive employee termination procedure 2.50(Largely Implemented)	Adopt positive incentives to align the workforce with the organization 1.75(Partially Implemented)
Hiring process, monitor and respond to suspicious or disruptive behavior 1.80(Partially Implemented)	Structure management and tasks to minimize insider stress and mistakes 1.60(Partially Implemented)	Solutions for monitoring employee actions and correlating information from multiple sources 1.67(Partially Implemented)			

Areas of Improvement

Anticipate and manage negative issues in the work environment

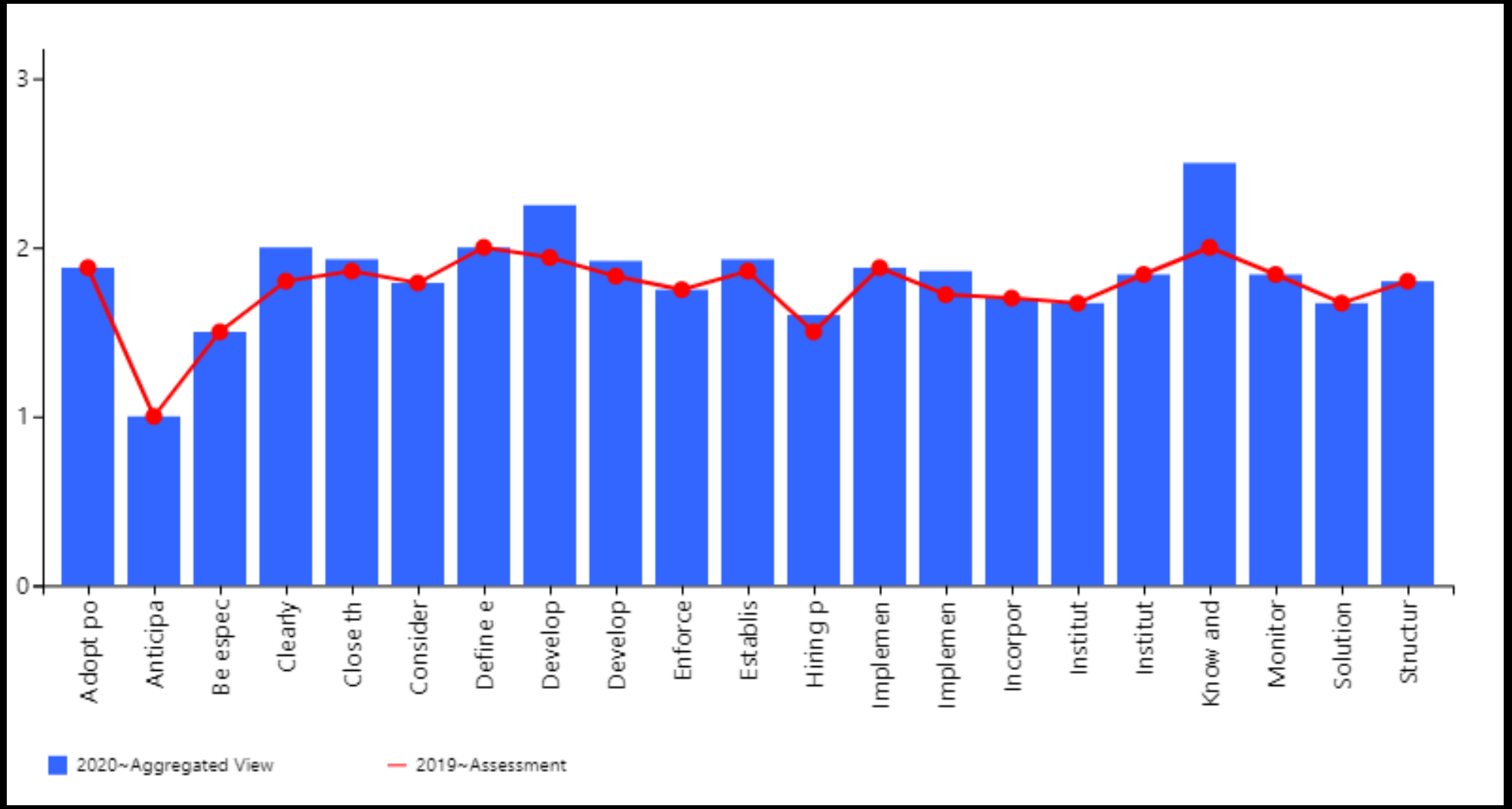


Improve from 1-Not Implemented --> 2-Partially Implemented

Recommended Areas of Improvement

Group Level 3	Description	Maturity Level
Practice Area 5.1	My organization uses enhanced monitoring of employees with an impending or ongoing personnel issue, in accordance with organizational policy and laws. Enable additional auditing and monitoring controls outlined in policies and procedures. Regularly review audit logs to detect activities outside of the employee's normal scope of work. Limit access to these log files to those with a need to know.	1.00
Practice Area 5.2	My organization at all levels of management regularly communicates organizational changes to all employees. This allows for a more transparent organization, and employees can better plan for their future.	1.00

Benchmarking Performance



RF can help

Please visit https://www.rfirst.org
Contact Us page and choose Resilience from the list of Areas.

Slido.com Poll

Would you be interested in an RF Insider Threat Program Maturity Assessment Tool?

Login to Slido.com using the event code

#RFInsiderThreat

All feedback is anonymous, but we will show the aggregate group feedback in real-time.

Slido.com Poll

Would you be interested in participating in an RF Insider Threat Community of Practice?

Login to Slido.com using the event code

#RFInsiderThreat

All feedback is anonymous, but we will show the aggregate group feedback in real-time.

Questions & Answers

Forward Together ReliabilityFirst

CLOSING REMARKS

Ray Sefchik

Director Entity Engagement, RF

Wrap Up

- A big thank you to all of presenters!
- Also, a big thank you to all attendees!
- Please be on the lookout for an RF survey for this webinar.