Spotlight on Insider Fraud in the Financial Services Industry

Sarah Miller, CISSP, CIPT, CIPP/US

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.

DM21-0169

Presenter Biography

Sarah Miller (CISSP, CIPT, CIPP/US) is an Insider Threat Researcher supporting the CERT ® Division's National Insider Threat Center (NITC) at Carnegie Mellon University's Software Engineering Institute.

- Serves as the Chair of the Open Source Insider Threat (OSIT) information sharing group for industry insider threat practitioners.
- Develops detection and mitigation strategies for insider threat programs.
- Collaborate on insider threat program building for customers.
- Teaches public and custom insider threat courses.
- Conducts sector-specific, supply chain, cybersecurity best practices, collusion, kinetic threats, privacy, and other insider threat research.

Education

- MS in Information Security Policy and Management, Heinz College, Carnegie Mellon University
- MA in Rhetoric, Carnegie Mellon University
- BA in English and Psychology, McDaniel College

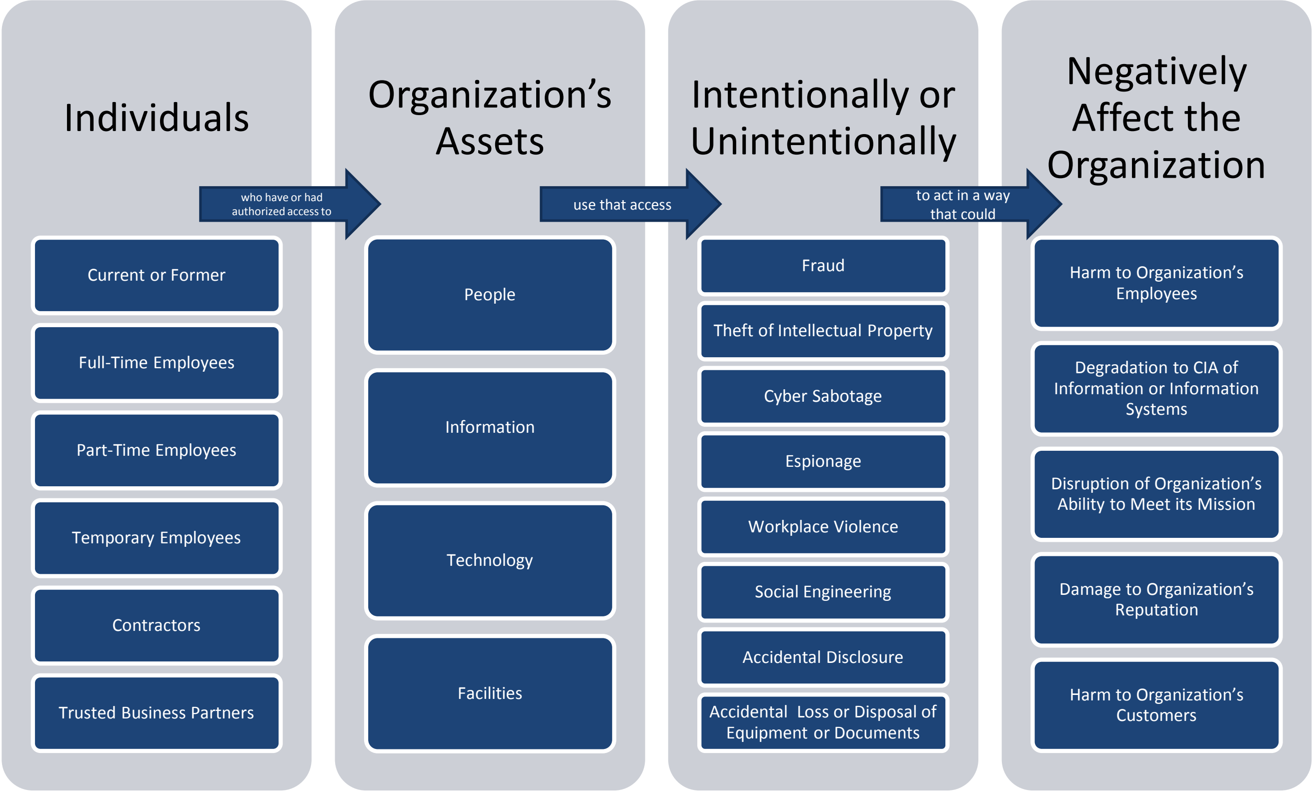
The CERT Division's National Insider Threat Center (NITC)

- **Focus:** Providing insider threat expertise across sectors
- **History:** Launched work in 2001 with the U.S. Secret Service and formalized as NITC in 2017
- **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 and transition socio-technical solutions to combat insider threats

The NITC Definition of Insider Threat

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.

What / Who Is an Insider Threat?



Individuals

who have or had authorized access to

- Current or Former
- Full-Time Employees
- Part-Time Employees
- Temporary Employees
- Contractors
- Trusted Business Partners

Organization’s Assets

use that access

- People
- Information
- Technology
- Facilities

Intentionally or Unintentionally

to act in a way that could

- Fraud
- Theft of Intellectual Property
- Cyber Sabotage
- Espionage
- Workplace Violence
- Social Engineering
- Accidental Disclosure
- Accidental Loss or Disposal of Equipment or Documents

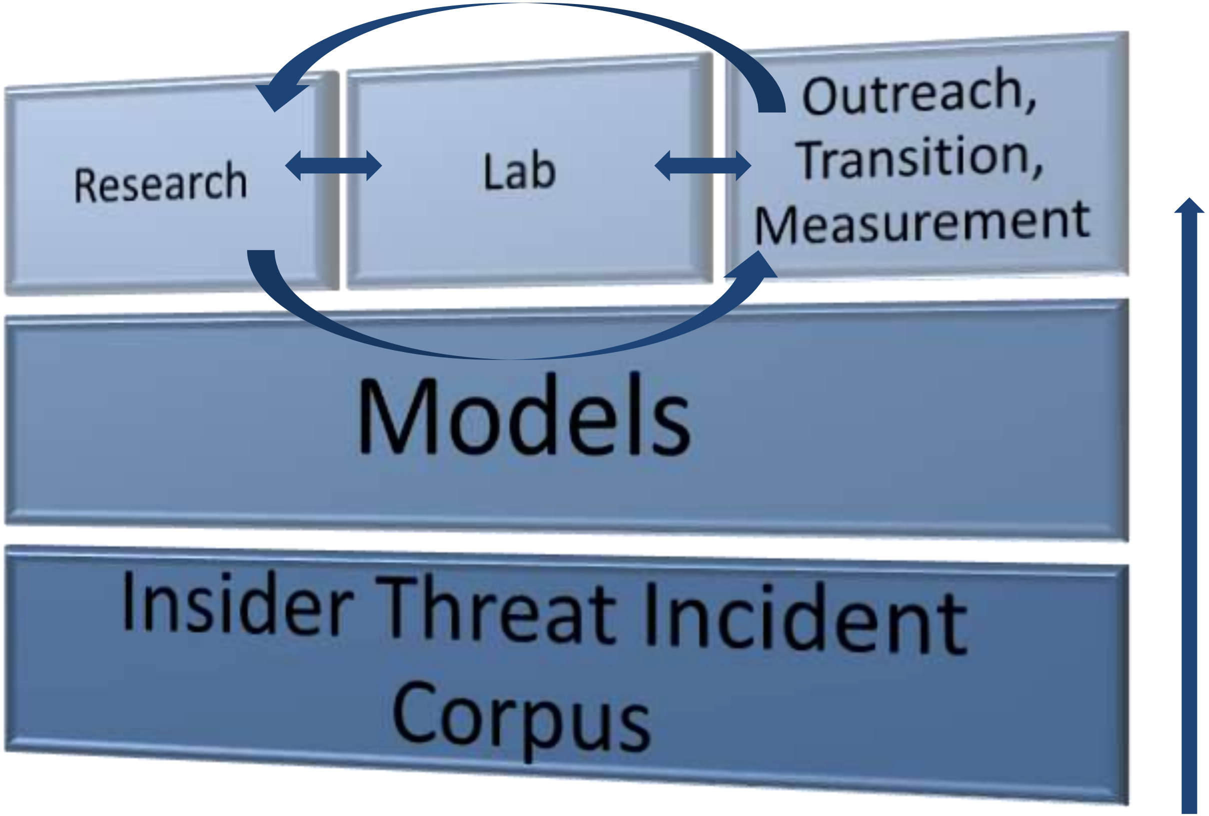
Negatively Affect the Organization

- Harm to Organization’s Employees
- Degradation to CIA of Information or Information Systems
- Disruption of Organization’s Ability to Meet its Mission
- Damage to Organization’s Reputation
- Harm to Organization’s Customers

Collaborations (Past, Current, Future)

Organizations	Focus Areas
Domain experts	• Psychology (Secret Service, FBI, DoD, NITC Visiting Scientists) • Espionage (DoD)
Interagency working group	• Espionage case collection and analysis • Identification of patterns of espionage indicators • Counterintelligence
Federal law enforcement	• Case analysis and information from victim organizations and perpetrators • Organizational vulnerabilities • Effective countermeasures
National labs, FFRDCs, critical infrastructure providers	• Automated detection enhancements • Sector-specific assessments
Tool vendors, infrastructure providers	• Automated detection enhancements • Emerging technologies (e.g., cloud computing)
Large auditing/consulting firms	• Assessments/follow-on guidance

The CERT National Insider Threat Center Approach to the Problem



Research

Lab

Outreach, Transition, Measurement

Models

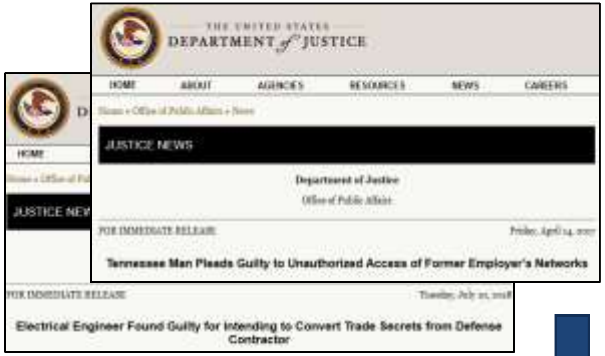
Insider Threat Incident Corpus

NITC Incident Corpus

Collection of over 1600 analyzed insider threat incidents, with hundreds more identified

Standardized incident coding methodology allows analysis of technical actions and observable behaviors

Body of empirical data provides a basis for threat models, technical and administrative control development, and risk quantification



THE UNITED STATES DEPARTMENT of JUSTICE

JUSTICE NEWS

Department of Justice

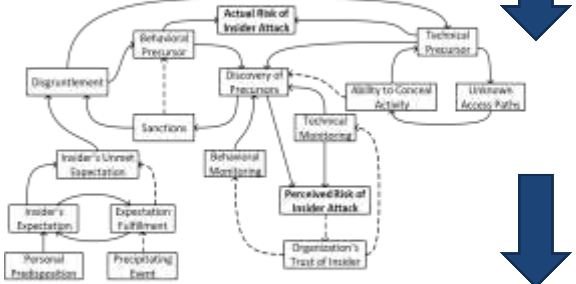
Office of Public Affairs

FOR IMMEDIATE RELEASE Friday, April 14, 2017

Tennessee Man Pleads Guilty to Unauthorized Access of Former Employer's Networks

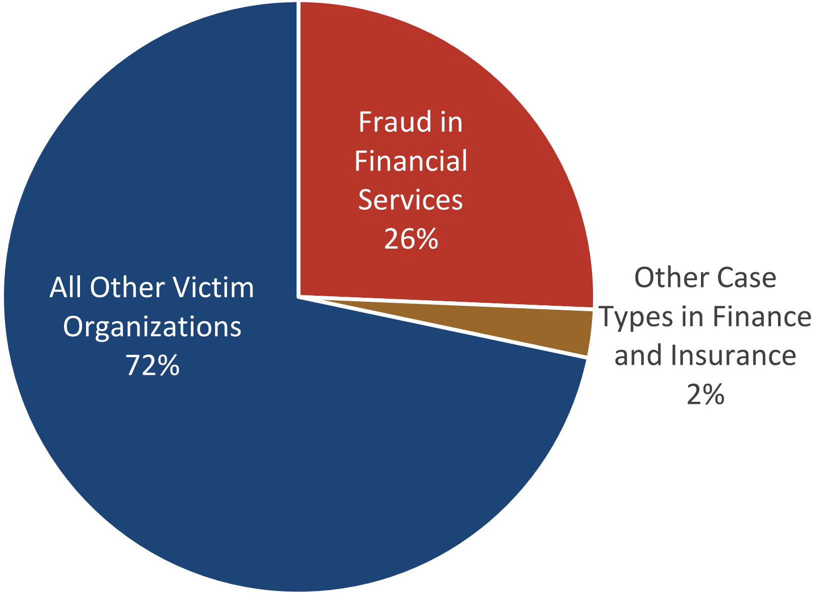
FOR IMMEDIATE RELEASE Tuesday, July 10, 2018

Electrical Engineer Found Guilty for Intending to Convert Trade Secrets from Defense Contractor



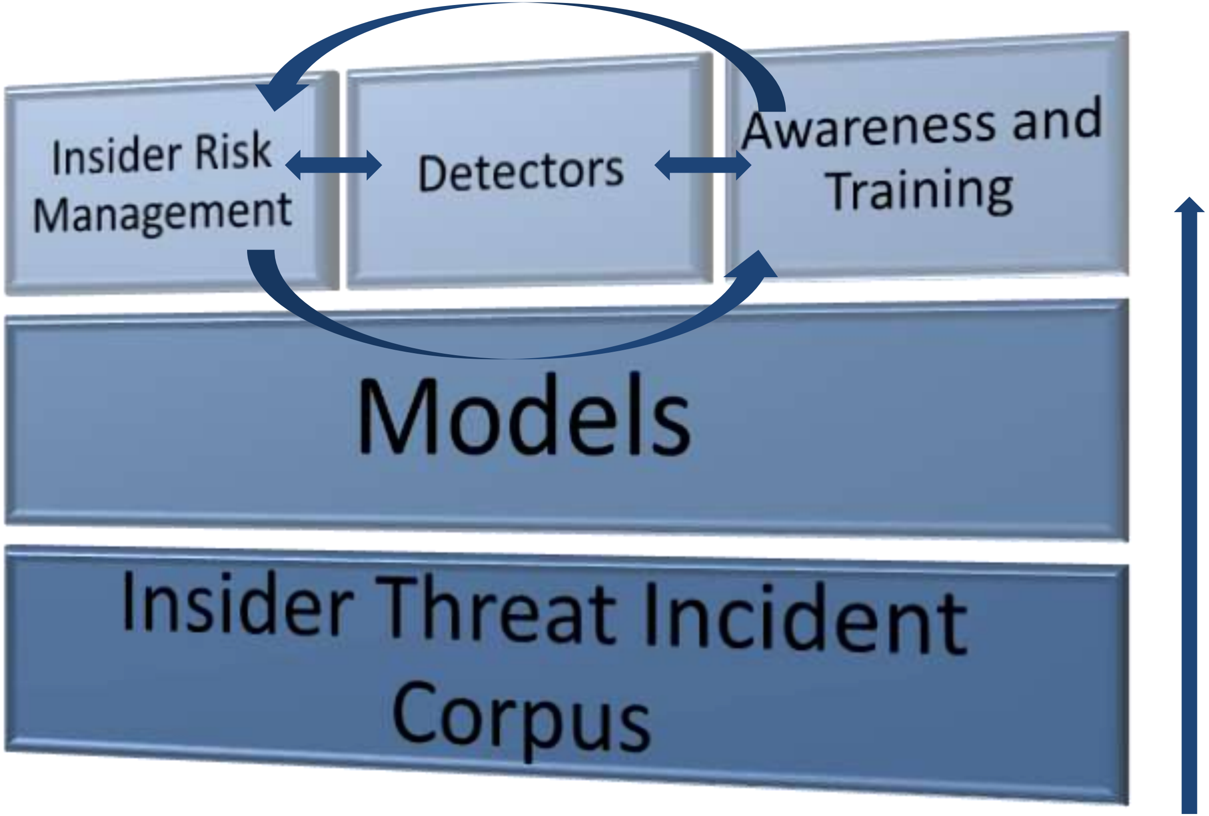
```
'host=HECTOR [search host="zeus.corp.merit.lab" Message="A user
account was  disabled. *" | eval Account_Name=mvindex(Account_Name, -
1) | fields Account_Name | strcat Account_Name "@corp.merit.lab"
sender_address | fields - Account_Name] total_bytes > 50000 AND
recipient_address!="*corp.merit.lab"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

Representation of Financial Services in Incident Corpus

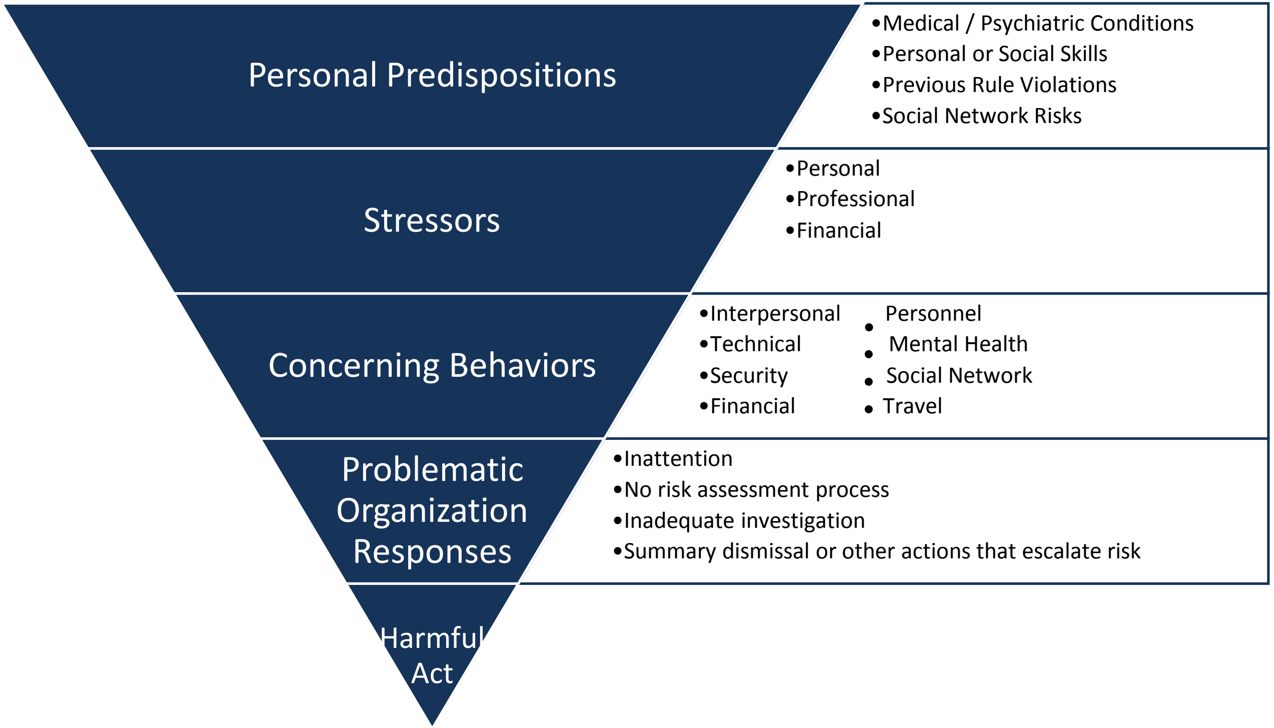


Over 1 in 4 victim organization records in the CERT Insider Threat Incident Corpus involves Fraud in the Financial Services sector.

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



NITC’s Critical Path to Insider Risk



- Medical / Psychiatric Conditions
- Personal or Social Skills
- Previous Rule Violations
- Social Network Risks

- Personal
- Professional
- Financial

- Interpersonal
- Technical
- Security
- Financial
- Personnel
- Mental Health
- Social Network
- Travel

- Inattention
- No risk assessment process
- Inadequate investigation
- Summary dismissal or other actions that escalate risk

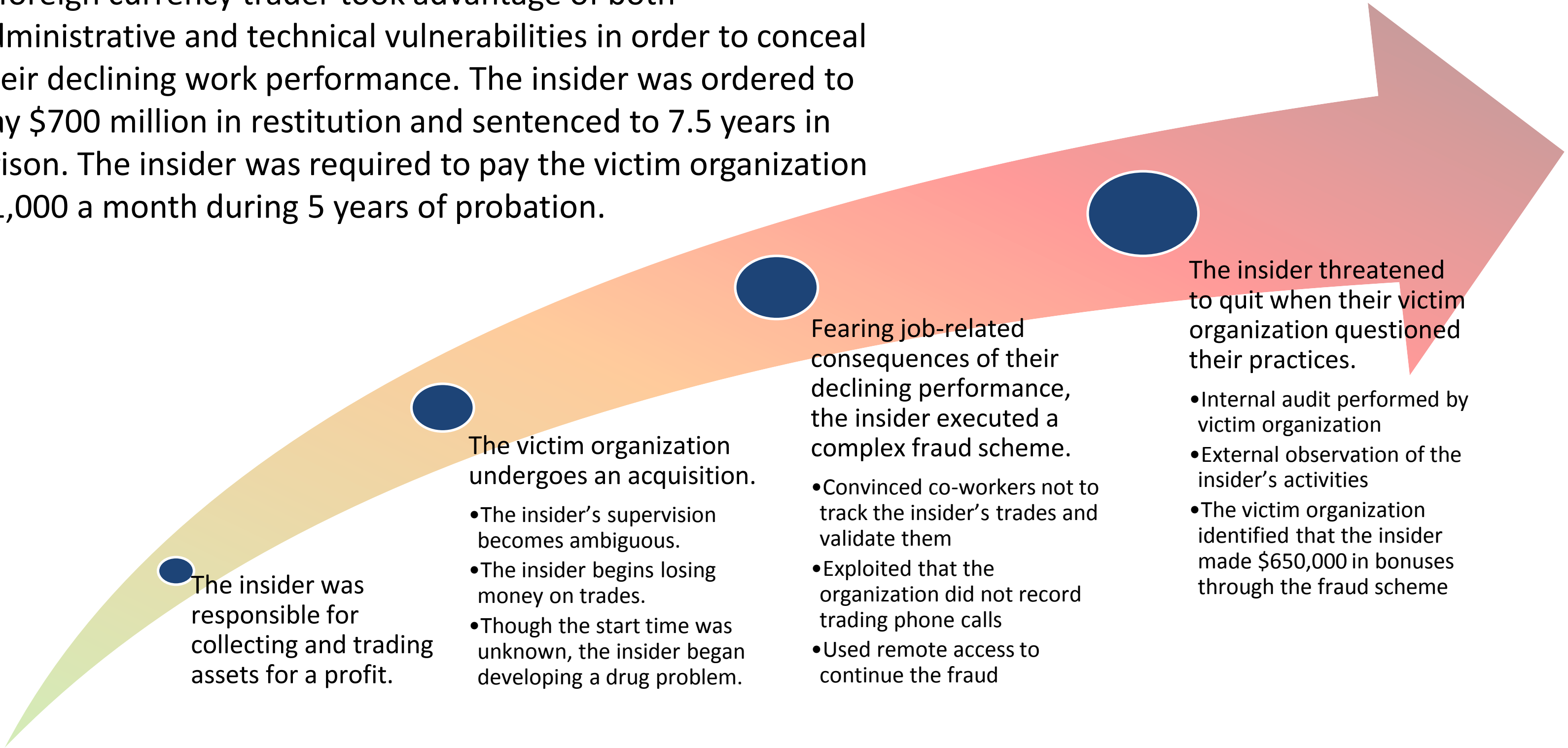
Source: Shaw, Sellers (2015) ; Carnegie Mellon University (2006)

Insider Threats Impacting Banks and Credit Unions

Case Examples

Fraud -1

A foreign currency trader took advantage of both administrative and technical vulnerabilities in order to conceal their declining work performance. The insider was ordered to pay $700 million in restitution and sentenced to 7.5 years in prison. The insider was required to pay the victim organization $1,000 a month during 5 years of probation.



The insider was responsible for collecting and trading assets for a profit.

The victim organization undergoes an acquisition.

- The insider's supervision becomes ambiguous.
- The insider begins losing money on trades.
- Though the start time was unknown, the insider began developing a drug problem.

Fearing job-related consequences of their declining performance, the insider executed a complex fraud scheme.

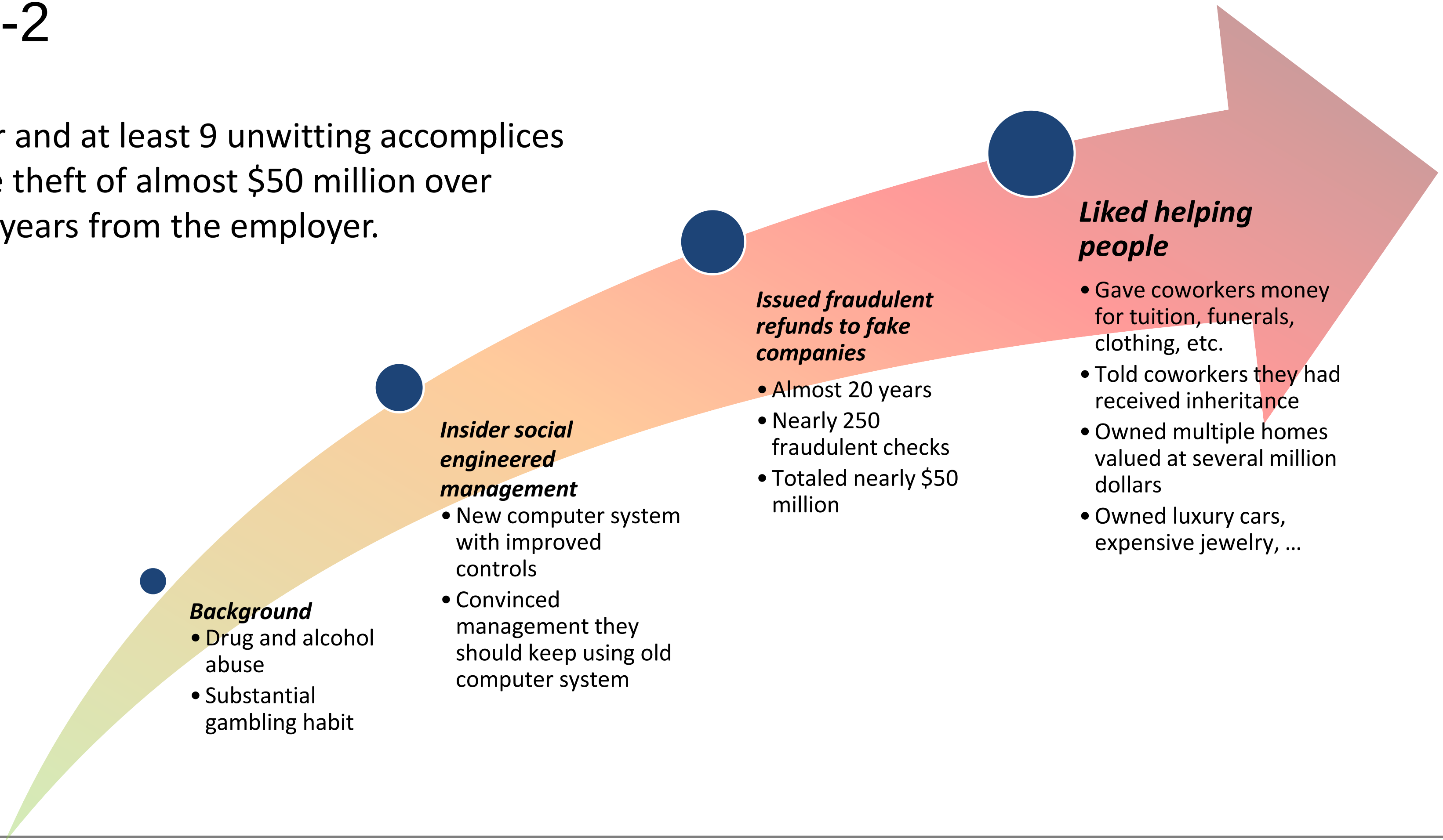
- Convinced co-workers not to track the insider's trades and validate them
- Exploited that the organization did not record trading phone calls
- Used remote access to continue the fraud

The insider threatened to quit when their victim organization questioned their practices.

- Internal audit performed by victim organization
- External observation of the insider's activities
- The victim organization identified that the insider made $650,000 in bonuses through the fraud scheme

Fraud -2

A manager and at least 9 unwitting accomplices enable the theft of almost $50 million over almost 20 years from the employer.



Background

- Drug and alcohol abuse
- Substantial gambling habit

Insider social engineered management

- New computer system with improved controls
- Convinced management they should keep using old computer system

Issued fraudulent refunds to fake companies

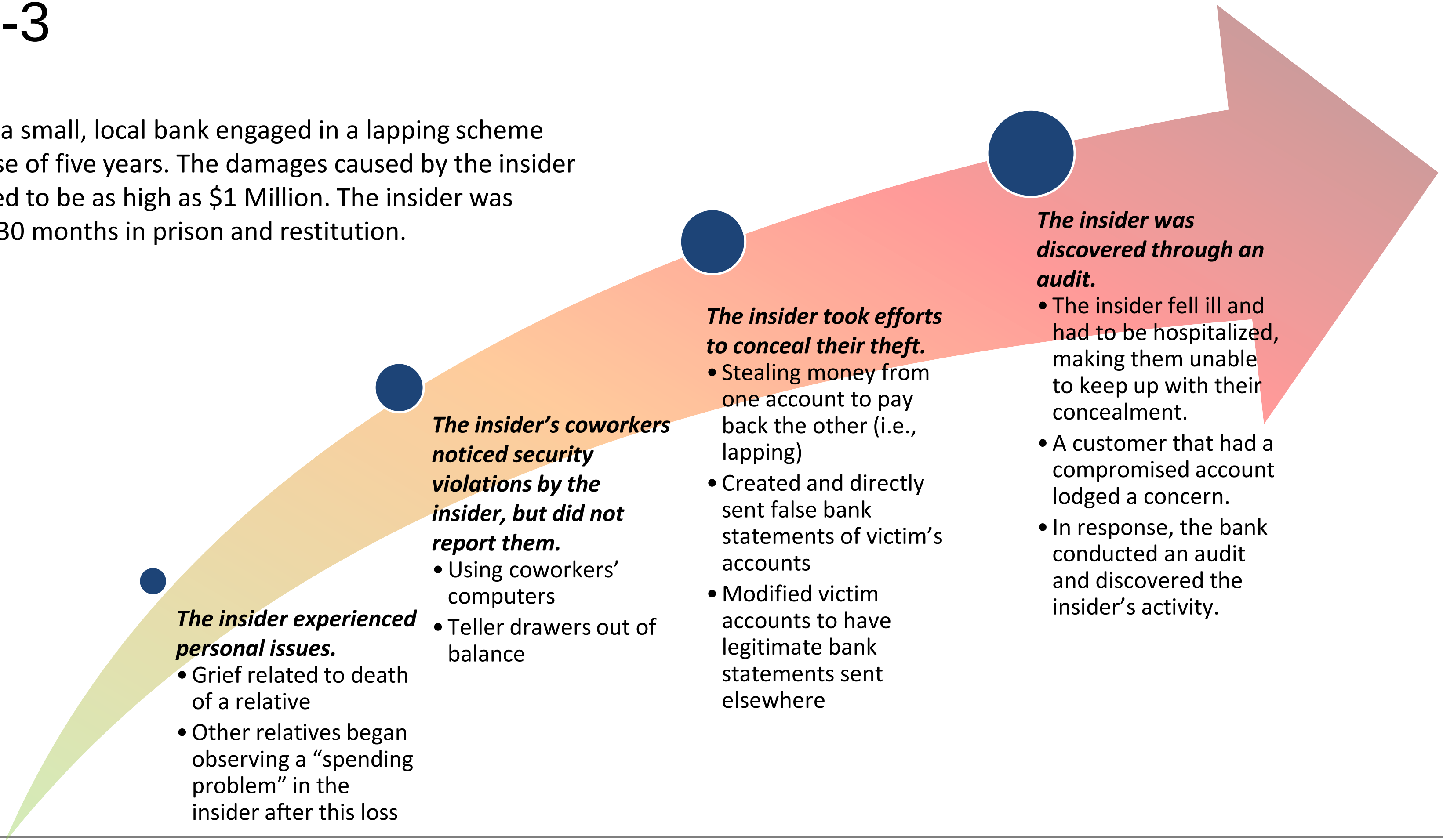
- Almost 20 years
- Nearly 250 fraudulent checks
- Totaled nearly $50 million

Liked helping people

- Gave coworkers money for tuition, funerals, clothing, etc.
- Told coworkers they had received inheritance
- Owned multiple homes valued at several million dollars
- Owned luxury cars, expensive jewelry, …

Fraud -3

A manager at a small, local bank engaged in a lapping scheme over the course of five years. The damages caused by the insider were estimated to be as high as $1 Million. The insider was sentenced to 30 months in prison and restitution.



The insider experienced personal issues.

- Grief related to death of a relative
- Other relatives began observing a "spending problem" in the insider after this loss

The insider's coworkers noticed security violations by the insider, but did not report them.

- Using coworkers' computers
- Teller drawers out of balance

The insider took efforts to conceal their theft.

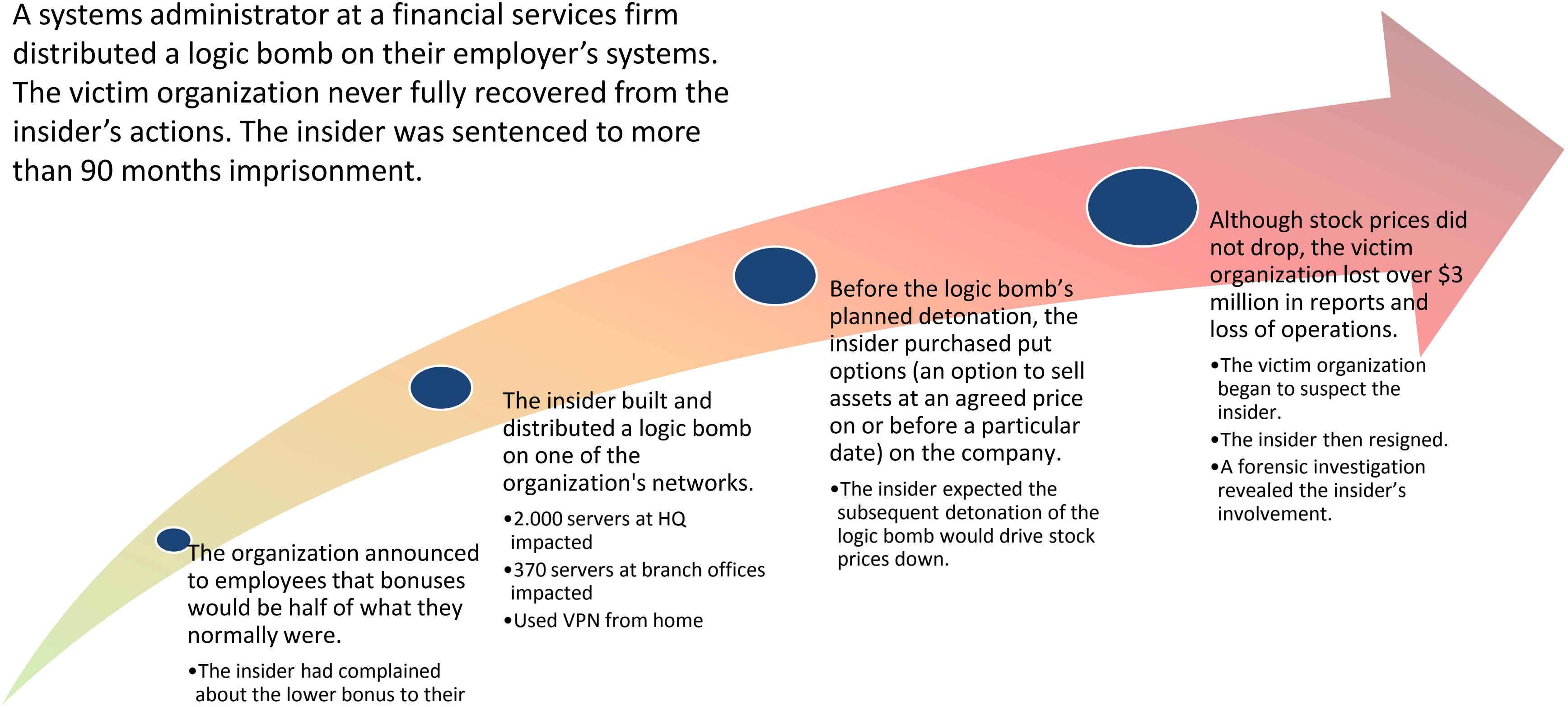
- Stealing money from one account to pay back the other (i.e., lapping)
- Created and directly sent false bank statements of victim's accounts
- Modified victim accounts to have legitimate bank statements sent elsewhere

The insider was discovered through an audit.

- The insider fell ill and had to be hospitalized, making them unable to keep up with their concealment.
- A customer that had a compromised account lodged a concern.
- In response, the bank conducted an audit and discovered the insider's activity.

Sabotage and Fraud

A systems administrator at a financial services firm distributed a logic bomb on their employer’s systems. The victim organization never fully recovered from the insider’s actions. The insider was sentenced to more than 90 months imprisonment.



The organization announced to employees that bonuses would be half of what they normally were.

- The insider had complained about the lower bonus to their supervisor.

The insider built and distributed a logic bomb on one of the organization's networks.

- 2.000 servers at HQ impacted
- 370 servers at branch offices impacted
- Used VPN from home

Before the logic bomb’s planned detonation, the insider purchased put options (an option to sell assets at an agreed price on or before a particular date) on the company.

- The insider expected the subsequent detonation of the logic bomb would drive stock prices down.

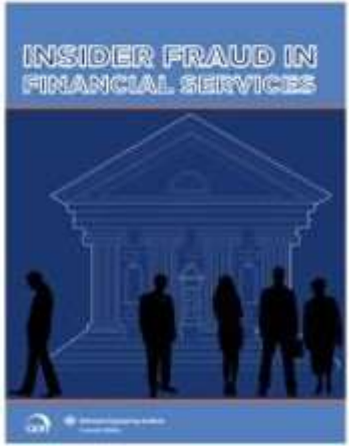
Although stock prices did not drop, the victim organization lost over $3 million in reports and loss of operations.

- The victim organization began to suspect the insider.
- The insider then resigned.
- A forensic investigation revealed the insider’s involvement.

Insider Fraud Study and Updated Statistics

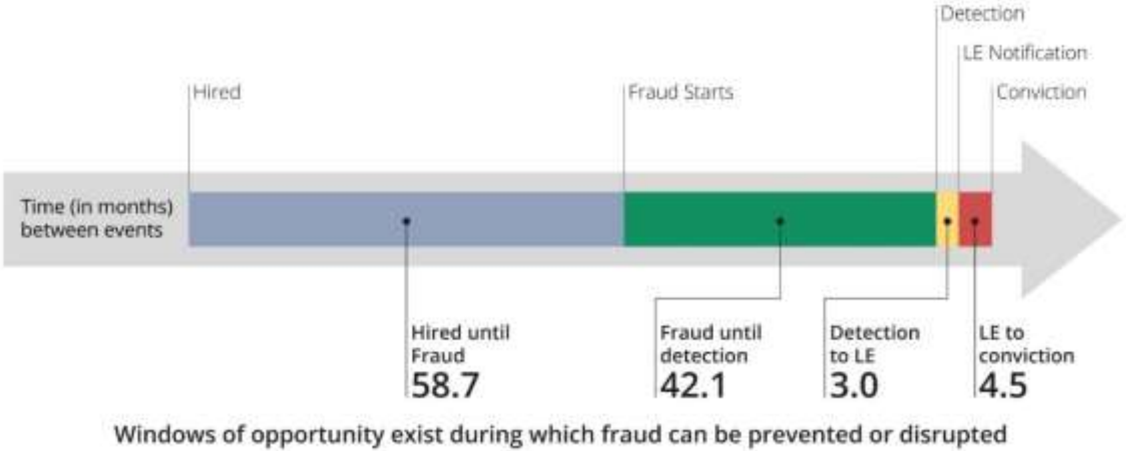
Insider Fraud Study

- Funded by U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T) (2012)
- Conducted by the NITC in collaboration with the U.S. Secret Service (USSS)
- Resulted in the report: Cummings, A.; Lewellen, T.; McIntire, D.; Moore, A.P.; & Trzeciak, R. (2012). Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector. CMU/SEI-2012-SR-004. Software Engineering Institute, Carnegie Mellon University.



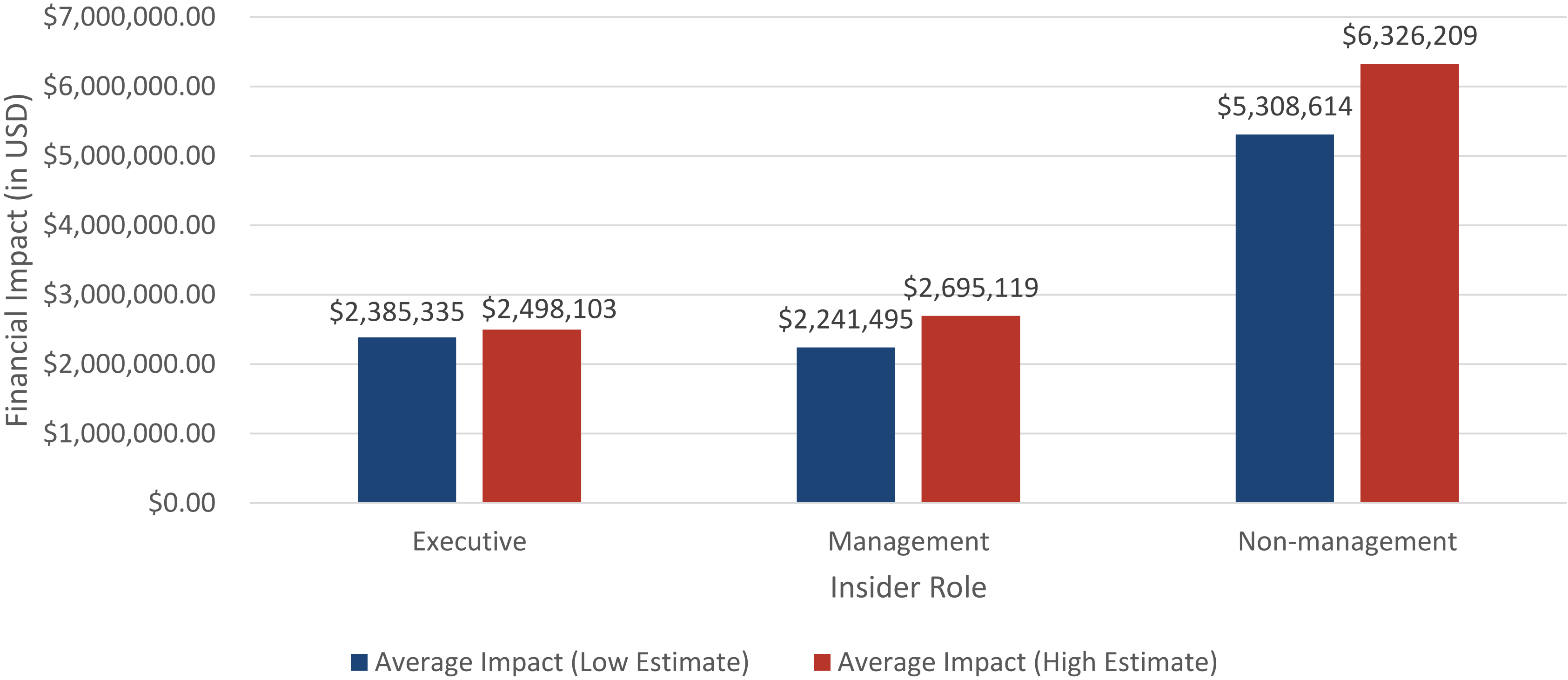
Low and Slow

Criminals who executed a “low and slow” approach accomplished more damage and escaped detection for longer.



There are, on average, approximately 5 years between a subject’s hiring and the start of the fraud. There are 42 months between the beginning of the fraud and its detection.

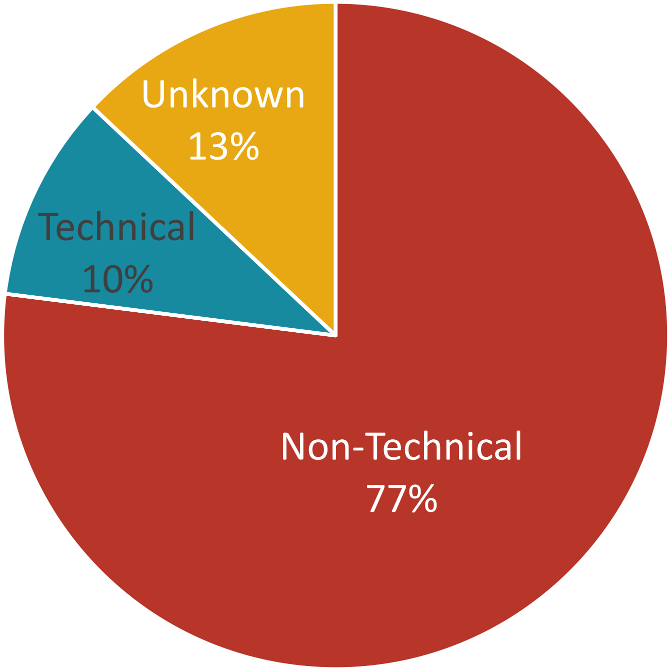
Average Financial Impact by Position Type in Finance and Insurance



General Fraud Trends from NITC Corpus

Non-Technical Positions

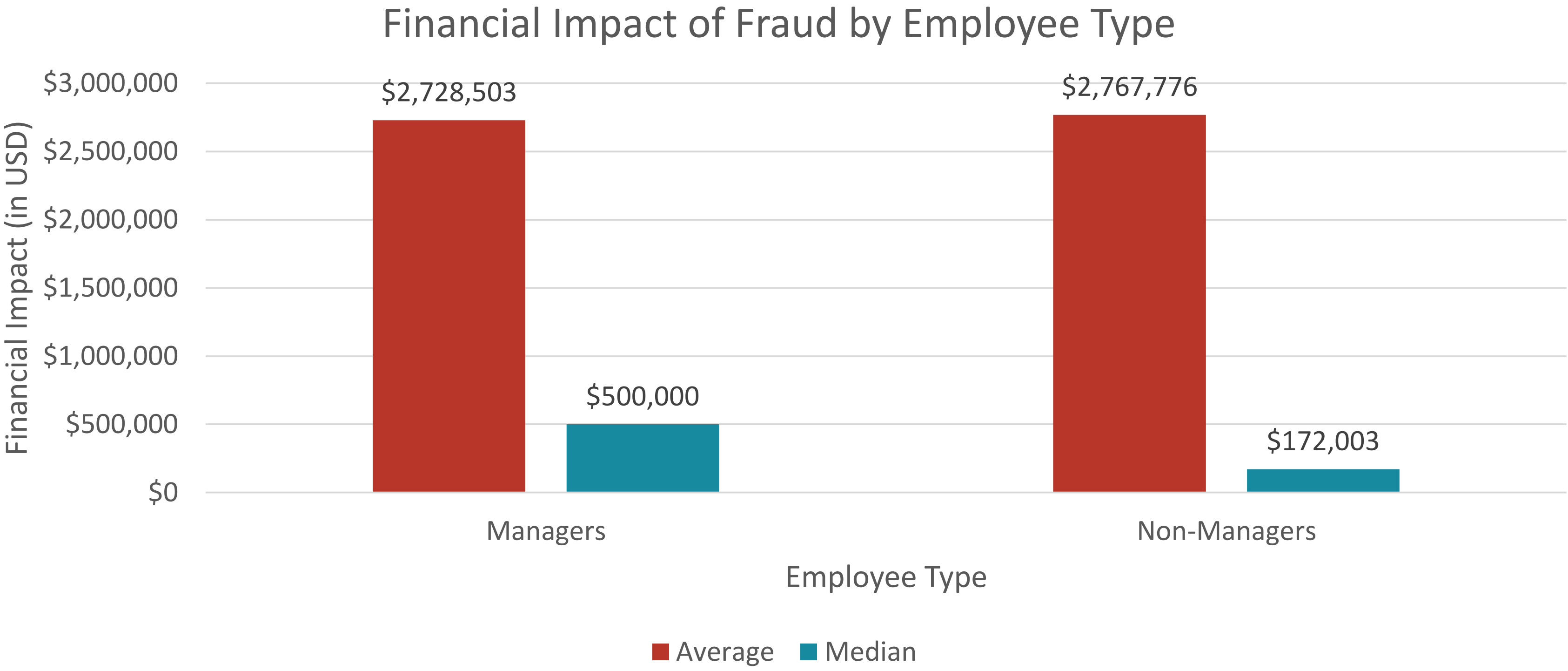
Positions Held by Insiders



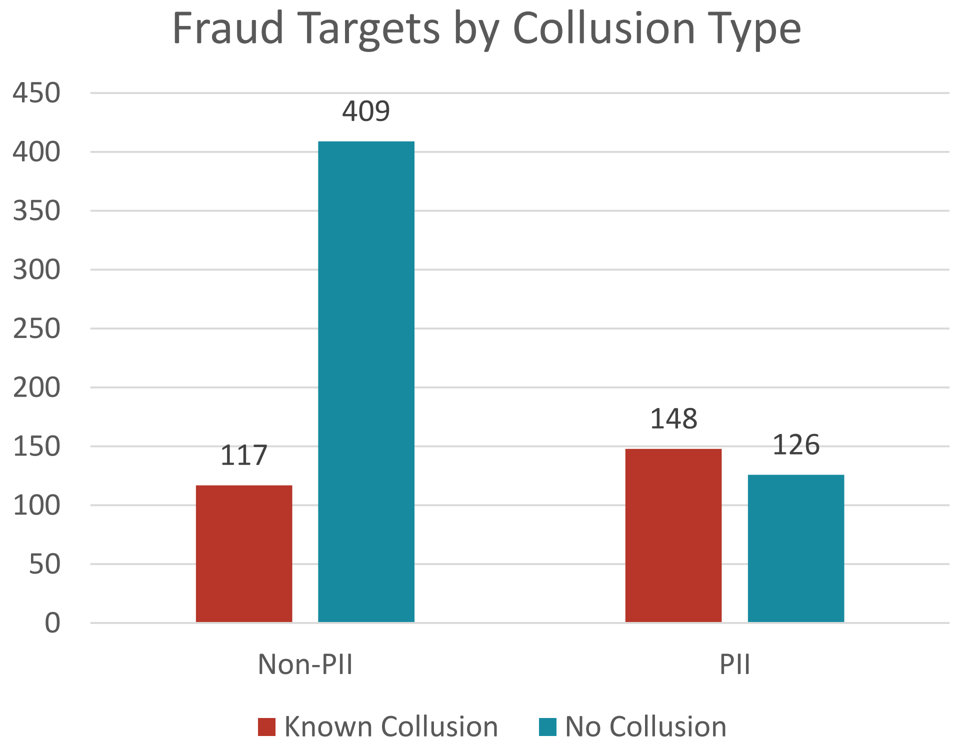
Over three-quarters of fraudsters occupied non-technical positions, such as

- Bank teller
- Bookkeeper
- Cashier
- Clerk
- Receptionist
- Secretary

Fraud by Non-Managers vs. Managers



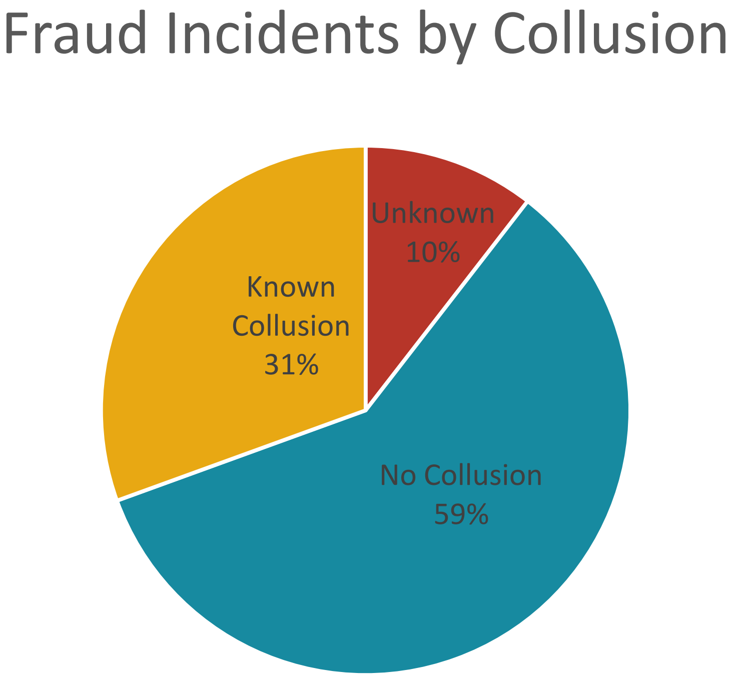
Fraud and PII



Personally identifiable information (PII) is a prominent target of those committing fraud.

Non-PII targets primarily involved money, accounting records, and payment systems.

Fraud and Collusion – 1



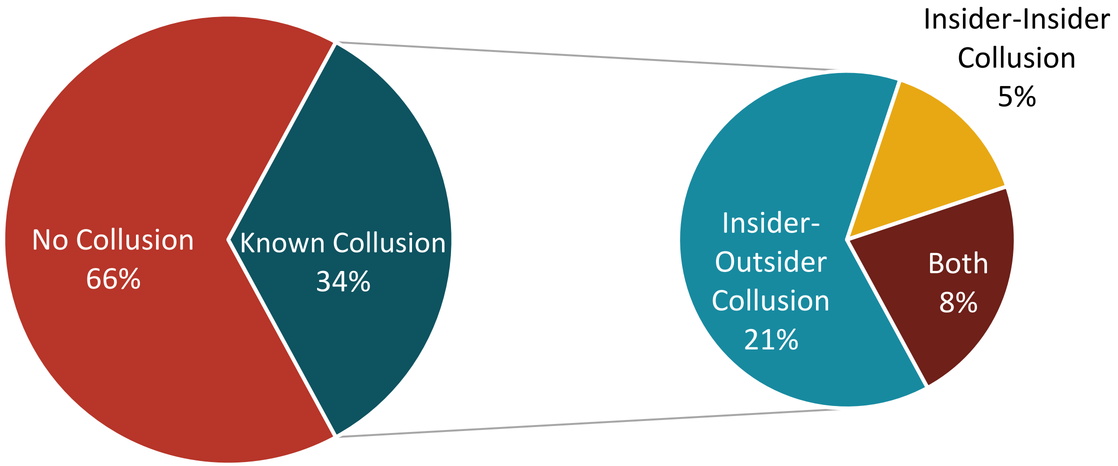
Most fraud cases do not involve collusion.

However, it is important to note that

- Approximately 31% of fraudsters do collude.
- Fraud involves collusion more often than other cases.

Fraud and Collusion – 2

External collusion is most common in fraud cases, i.e., a bank insider colluding with an external party to facilitate the crime.



Audits, Complaints, and Suspicions

Most incidents were detected through an audit, customer complaints, or co-worker suspicions.

- The most common way attacks were detected was through routine or impromptu audits.
- Over half of the insiders were detected by other victim organization employees, though none of the employees were members of the IT staff.
- As expected, most initial responders to the incidents were managers or internal investigators (75 percent).

Who were the Fraudsters?

Insider Demographics	
Position	Current employees in nontechnical positions
Tenure	Typically 5 years or more
Age Range	Two-thirds are between the ages of 31 and 40
Gender	Fairly even split between male and female
Marital Status	Fairly even split between single and married

Attack Metrics	
Target(s)	Personally Identifiable Information (PII), Customer Information (CI), Accounting and Payment Systems
Method(s)	Authorized access
Location	On-site
Time	During normal working hours
Average Length	38.1 months
Impact	Average between $2 Million and $2.8 Million

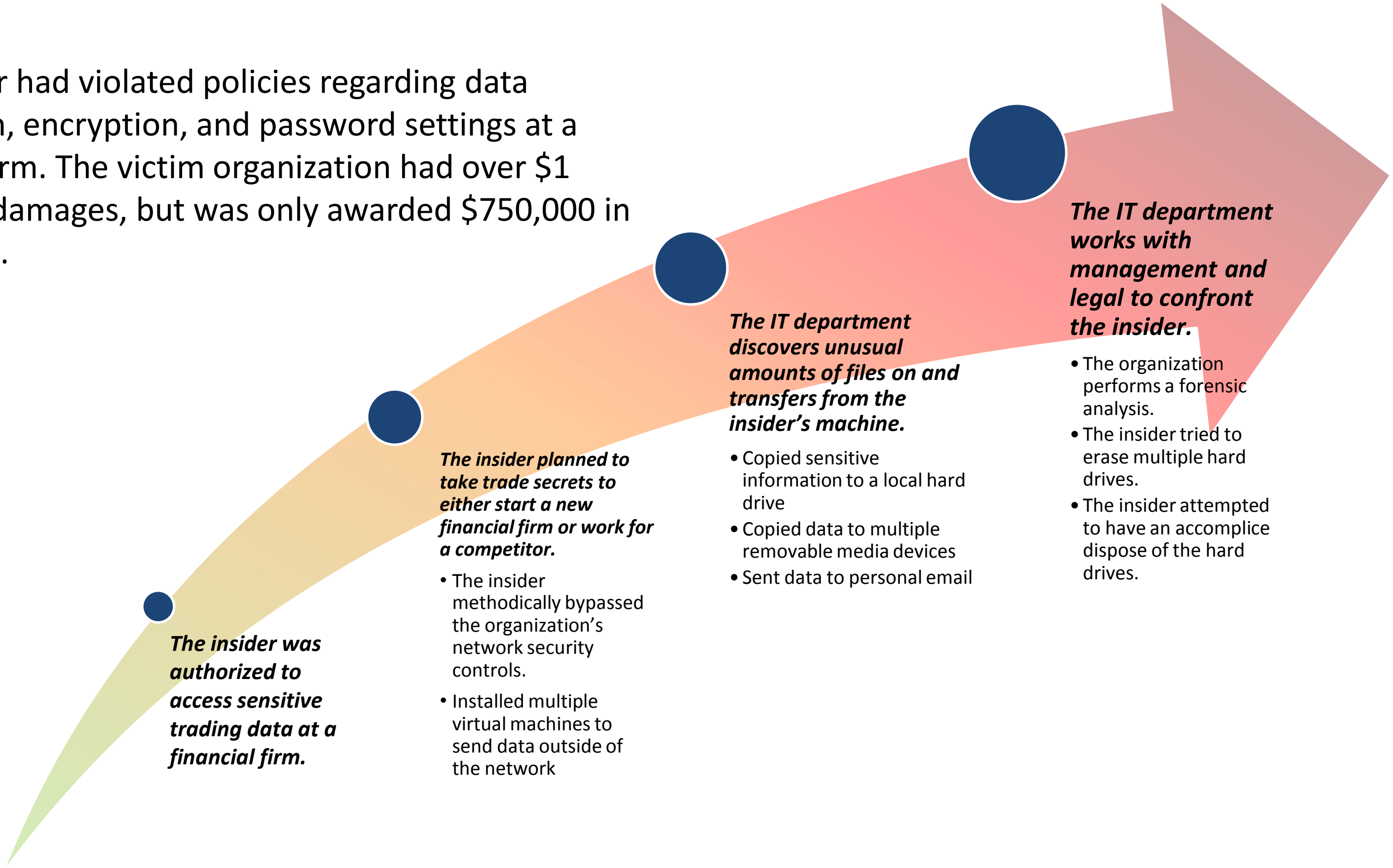
Countermeasures for Fraud

- Clearly document and consistently enforce policies and controls.
- Institute periodic security awareness training for all employees.
- Include unexplained financial gain in any periodic reinvestigation of employees.
- Log, monitor, and audit employee online actions.
- Pay special attention to accountants and managers.
- Restrict access to personally identifiable information.
- Develop an insider incident response plan.
- Provide an Employee Assistance Program or other recourse for employees experiencing personal or financial problems

Final Thoughts and Additional Case Examples

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.



The insider was authorized to access sensitive trading data at a financial firm.

The insider planned to take trade secrets to either start a new financial firm or work for a competitor.

- The insider methodically bypassed the organization's network security controls.
- Installed multiple virtual machines to send data outside of the network

The IT department discovers unusual amounts of files on and transfers from the insider's machine.

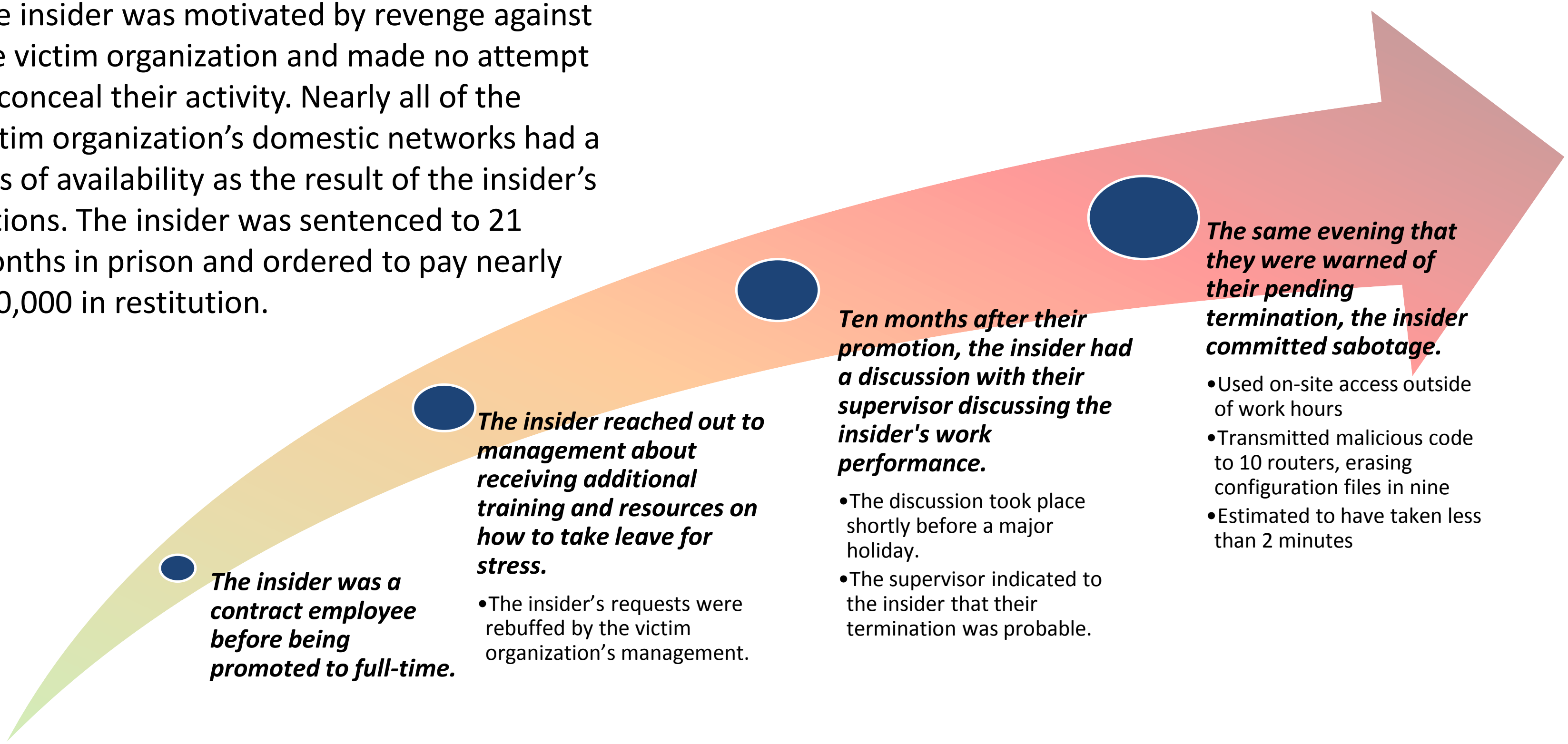
- Copied sensitive information to a local hard drive
- Copied data to multiple removable media devices
- Sent data to personal email

The IT department works with management and legal to confront the insider.

- The organization performs a forensic analysis.
- The insider tried to erase multiple hard drives.
- The insider attempted to have an accomplice dispose of the hard drives.

Sabotage

The insider was motivated by revenge against the victim organization and made no attempt to conceal their activity. Nearly all of the victim organization’s domestic networks had a loss of availability as the result of the insider’s actions. The insider was sentenced to 21 months in prison and ordered to pay nearly $80,000 in restitution.



The insider was a contract employee before being promoted to full-time.

The insider reached out to management about receiving additional training and resources on how to take leave for stress.

- The insider’s requests were rebuffed by the victim organization’s management.

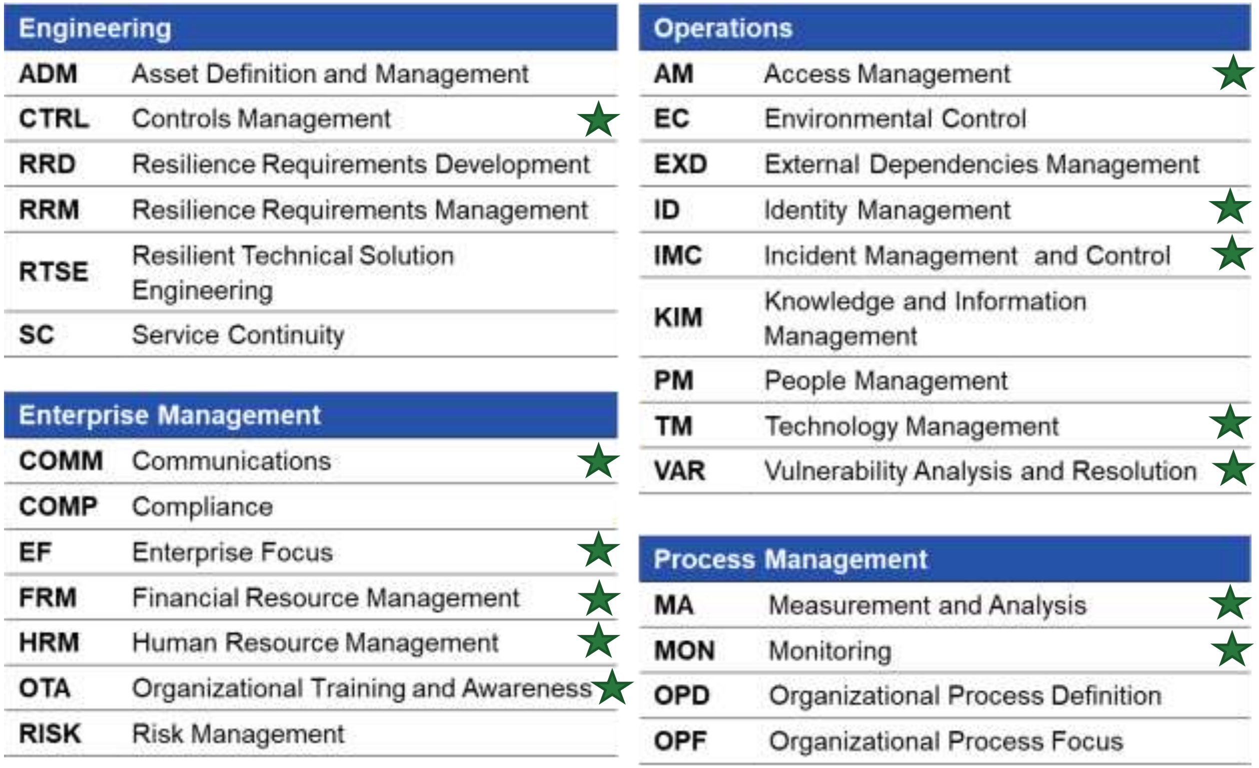
Ten months after their promotion, the insider had a discussion with their supervisor discussing the insider's work performance.

- The discussion took place shortly before a major holiday.
- The supervisor indicated to the insider that their termination was probable.

The same evening that they were warned of their pending termination, the insider committed sabotage.

- Used on-site access outside of work hours
- Transmitted malicious code to 10 routers, erasing configuration files in nine
- Estimated to have taken less than 2 minutes

Programs Typically Focus on Insider Incident Management



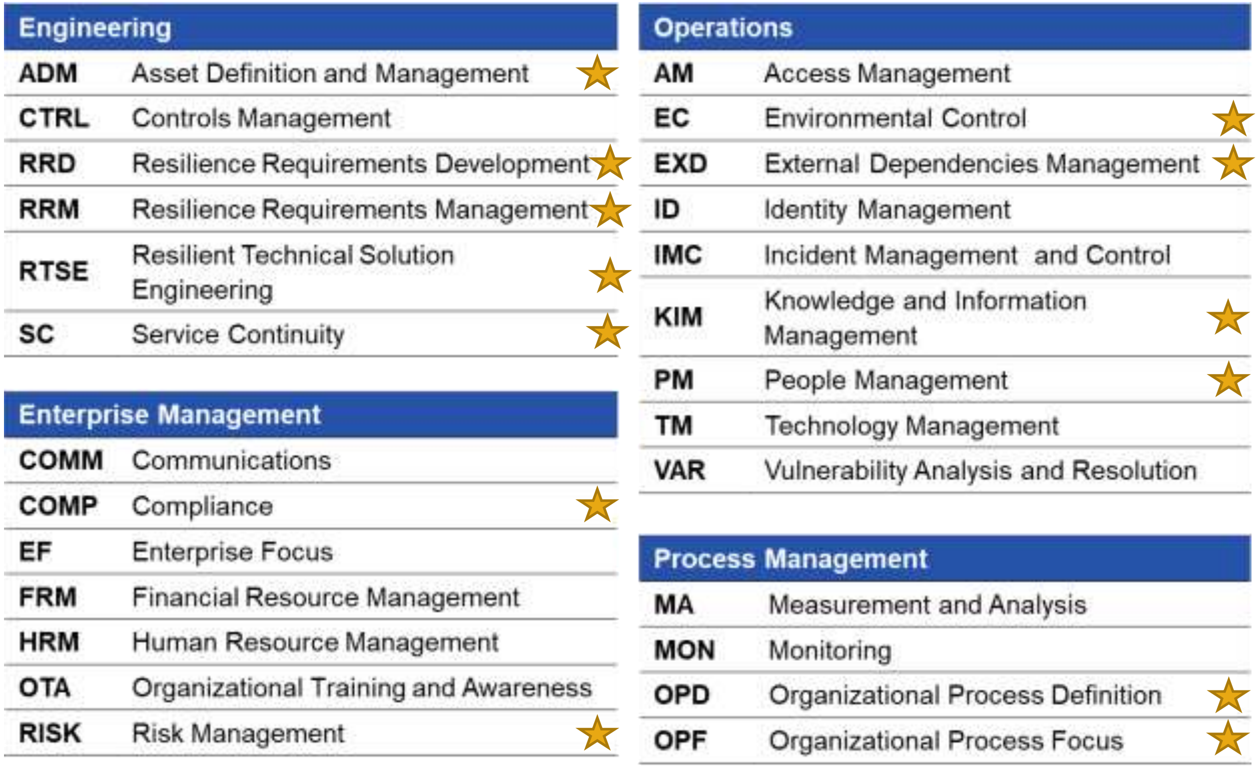
Engineering		
ADM	Asset Definition and Management	
CTRL	Controls Management	★
RRD	Resilience Requirements Development	
RRM	Resilience Requirements Management	
RTSE	Resilient Technical Solution Engineering	
SC	Service Continuity	

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	

Programs Need To Develop Insider Risk Management Capabilities



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	★

Recommended Best Practices for Insider Threat Mitigation

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.	*Upcoming:* 22 – Learn from insider threat incidents.

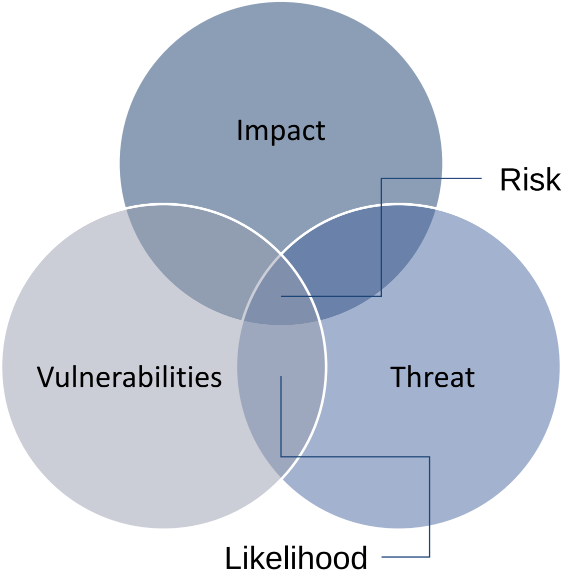
Acceptable Levels?

Risks can be expressed as a function of **impact** and **likelihood**

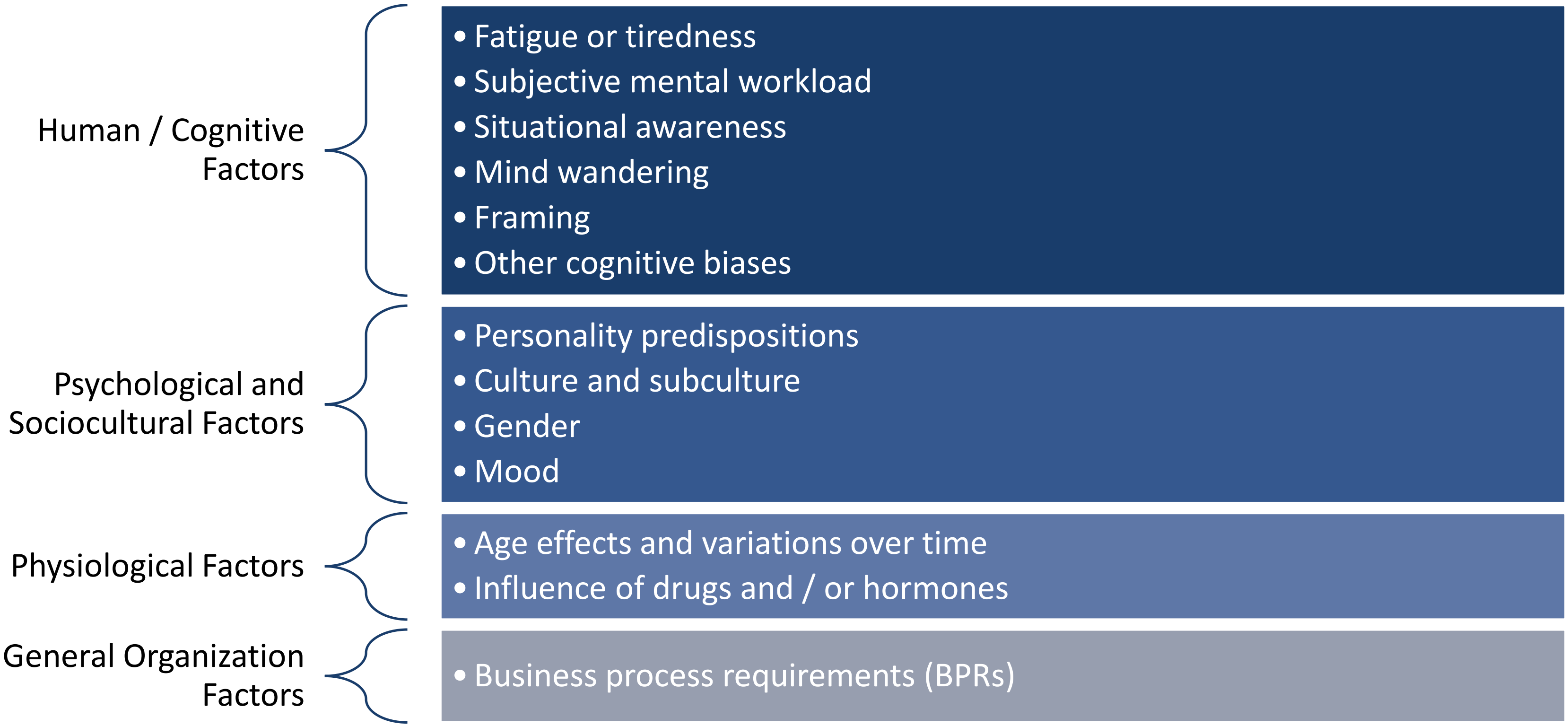
Deploying controls doesn’t necessarily reduce the likelihood of a threat occurring, especially for insider threats.

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



Contributing Factors in Risk Perception



Human / Cognitive Factors

- Fatigue or tiredness
- Subjective mental workload
- Situational awareness
- Mind wandering
- Framing
- Other cognitive biases

Psychological and Sociocultural Factors

- Personality predispositions
- Culture and subculture
- Gender
- Mood

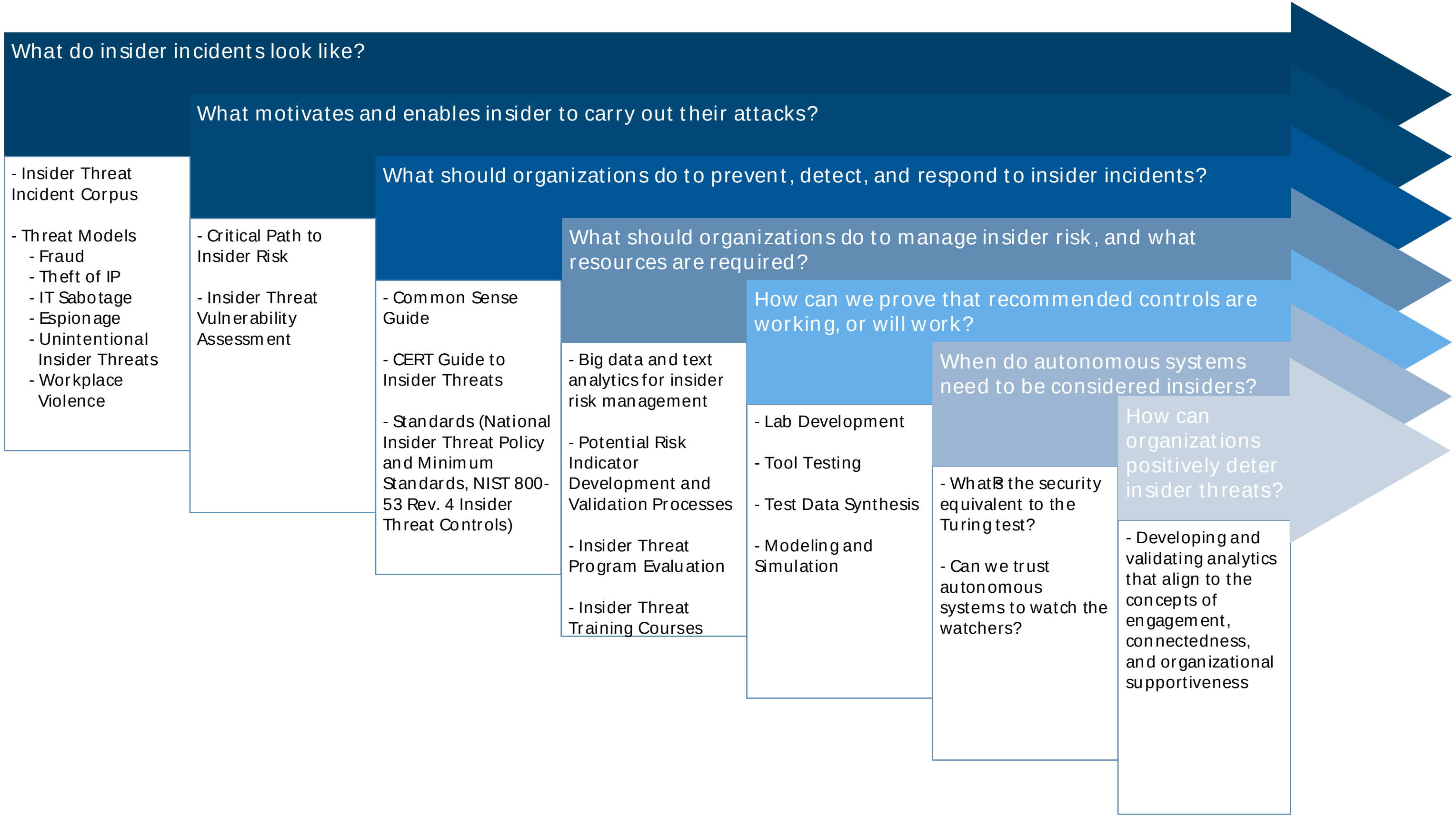
Physiological Factors

- Age effects and variations over time
- Influence of drugs and / or hormones

General Organization Factors

- Business process requirements (BPRs)

Past, Present, and Future Research



What do insider incidents look like?

- Insider Threat Incident Corpus
- Threat Models
  - Fraud
  - Theft of IP
  - IT Sabotage
  - Espionage
  - Unintentional Insider Threats
  - Workplace Violence

What motivates and enables insider to carry out their attacks?

- Critical Path to Insider Risk
- Insider Threat Vulnerability Assessment

What should organizations do to prevent, detect, and respond to insider incidents?

- Common Sense Guide
- CERT Guide to Insider Threats
- Standards (National Insider Threat Policy and Minimum Standards, NIST 800-53 Rev. 4 Insider Threat Controls)

What should organizations do to manage insider risk, and what resources are required?

- Big data and text analytics for insider risk management
- Potential Risk Indicator Development and Validation Processes
- Insider Threat Program Evaluation
- Insider Threat Training Courses

How can we prove that recommended controls are working, or will work?

- Lab Development
- Tool Testing
- Test Data Synthesis
- Modeling and Simulation

When do autonomous systems need to be considered insiders?

- What’s the security equivalent to the Turing test?
- Can we trust autonomous systems to watch the watchers?

How can organizations positively deter insider threats?

- Developing and validating analytics that align to the concepts of engagement, connectedness, and organizational supportiveness

NITC Publications and References

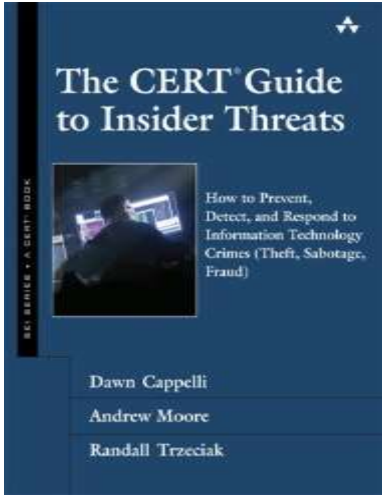
Kessel, E. “Benford’s Law: Potential Applications for Insider Threat Detection.” (2020). Insider Threat Blog. Software Engineering Institute, Carnegie Mellon University.

Theis, M.; Trzeciak, R.; Costa, D.; Moore, A.; Miller, S.; Cassidy, T.; & Claycomb, W. (2019). Common Sense Guide to Mitigating Insider Threats, Sixth Edition. Pittsburgh: Software Engineering Institute.

Miller, S. “Insider Threats in Finance and Insurance (Part 4 of 9: Insider Threats Across Industry Sectors).” (2018). Insider Threat Blog. Software Engineering Institute, Carnegie Mellon University.

Moore, A.; Savinda, J.; Monaco, E.; Moyes, J.; Rousseau, D.; Perl, S.; Cowley, J.; Collins, M.; Cassidy, T.; VanHoudnos, N.; Buttles-Valdez, P.; Bauer, D.; & Parshall, A. (2016). The Critical Role of Positive Incentives for Reducing Insider Threats. CMU/SEI-2016-TR-014. Software Engineering Institute, Carnegie Mellon University.

Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). The CERT® Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud). Addison-Wesley Professional.



SEI SERIES • A CERT® BOOK
The CERT® Guide to Insider Threats
How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)
Dawn Cappelli
Andrew Moore
Randall Trzeciak

Open Source Insider Threat (OSIT) Information Sharing Group

- Community of Interest for insider threat program practitioners across industry organizations
- Over 550 members from over 220 organizations
- Supports volunteer-run special interest groups
  - Data Analytics (DA SIG)
  - Financial Services (FinSer SIG)
- Launched a “partner” community of interest, the Privacy Special Interest Group (PSIG)

Questions?

Contact Information

Sarah Miller

Insider Threat Researcher

CERT® National Insider Threat Center

Email: semiller@cert.org

osit-forum-support@cert.org

privacy-sig-owner@cert.org

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-3890