Current Trends in Insider Threat Detection Capability - What Does an Effective Program Look Like?

Randall Trzeciak (rft@cert.org)

June 5, 2018

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

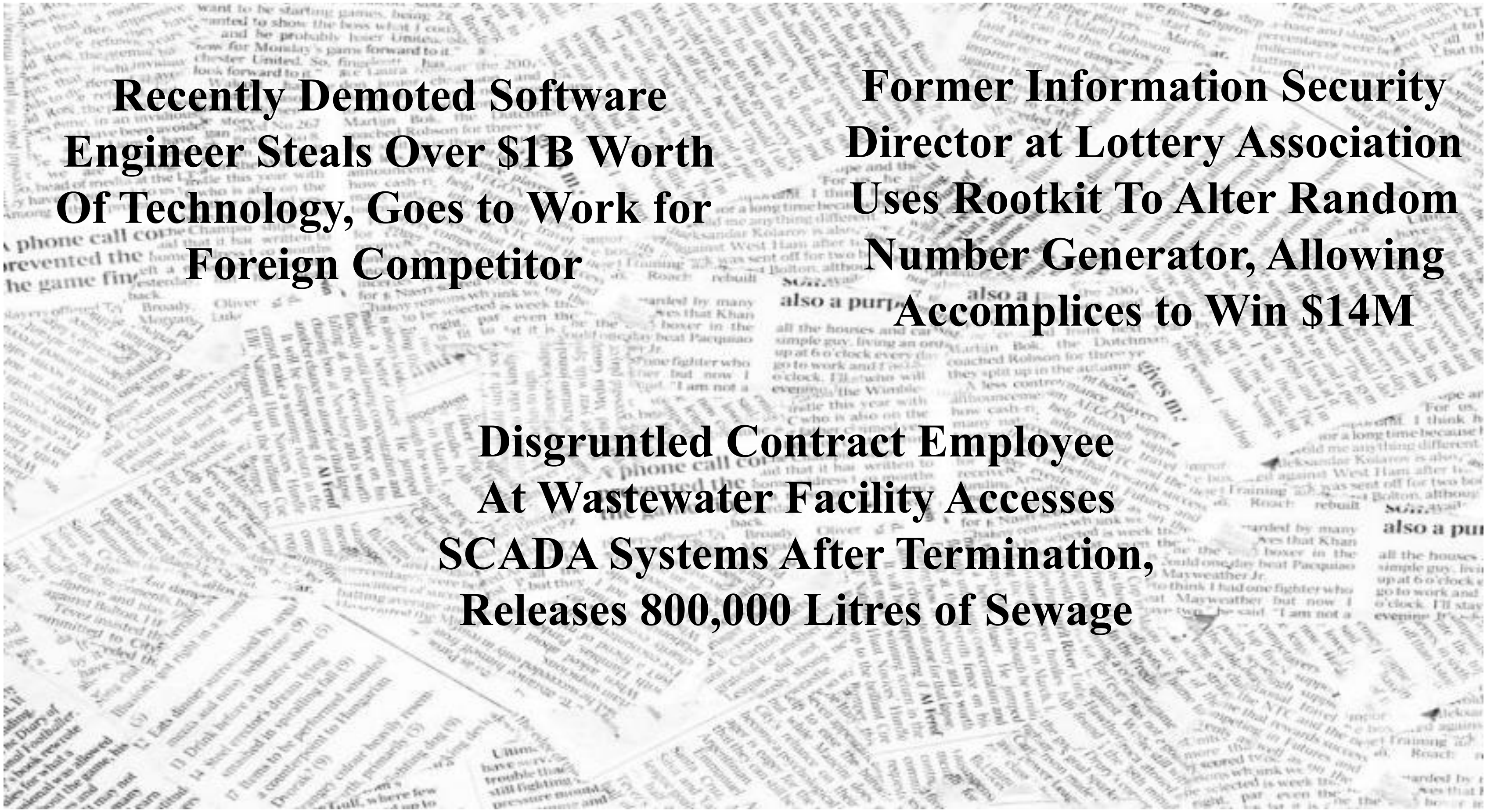
This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

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.

DM-0002495

Could This Happen to Your Organization?



Recently Demoted Software Engineer Steals Over $1B Worth Of Technology, Goes to Work for Foreign Competitor

Former Information Security Director at Lottery Association Uses Rootkit To Alter Random Number Generator, Allowing Accomplices to Win $14M

Disgruntled Contract Employee At Wastewater Facility Accesses SCADA Systems After Termination, Releases 800,000 Litres of Sewage

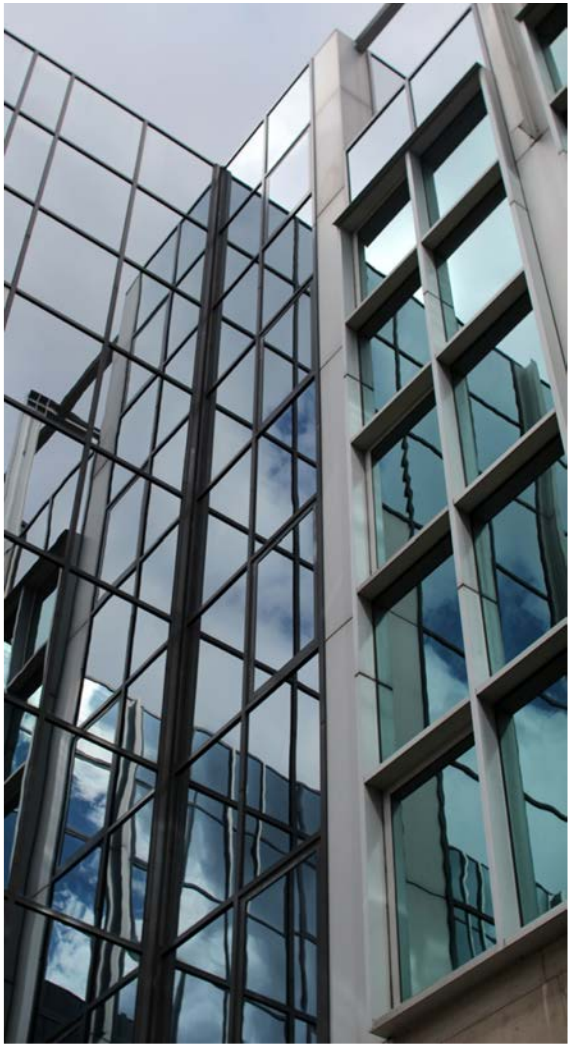
Established as a DoD FFRDC at Carnegie Mellon University in 1984

Only DoD R&D center focused on software and cybersecurity

Offices in Pittsburgh, Arlington, and Los Angeles

About 600 staff (~400 tech staff)

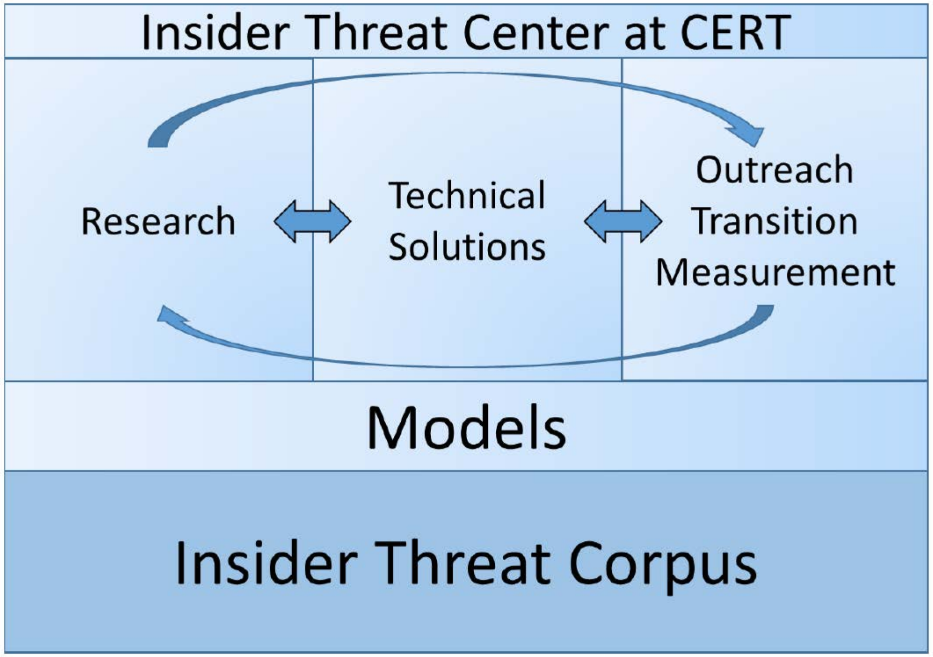
The CERT Insider Threat Center



- Center of insider threat expertise
- Began working in this area in 2001 with the U.S. Secret Service
- 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

Insider Threat Incident Corpus

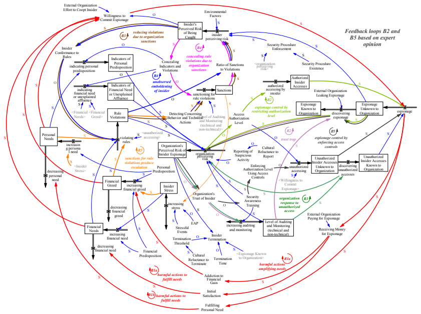
- Database of over 1600 insider threat incidents
  - Includes interviews of actual offenders
- Coded to allow analysis of technical actions & behaviors observables
- Development of technical controls to baseline and detect anomalous actions
- Research into areas of
  - Sentiment analysis
  - Workplace violence
  - Typing heuristics
  - Biometrics


Insider Threat Center at CERT
Research
Technical Solutions
Outreach Transition Measurement
Models
Insider Threat Corpus

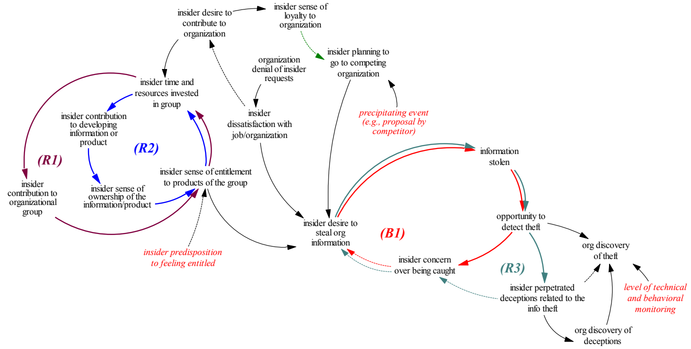
CERT Insider Threat Center Methodology

Collect, code, and empirically analyze incidents

Develop Causal Models



Deriving Candidate Controls and Indicators


insider desire to contribute to organization
insider sense of loyalty to organization
insider planning to go to competing organization
organization denial of insider requests
insider time and resources invested in group
insider contribution to developing information or product
insider dissatisfaction with job/organization
precipitating event (e.g., proposal by competitor)
(R1)
(R2)
insider contribution to organizational group
insider sense of ownership of the information/product
insider sense of entitlement to products of the group
information stolen
opportunity to detect theft
insider desire to steal org information
(B1)
org discovery of theft
insider predisposition to feeling entitled
insider concern over being caught
(R3)
insider perpetrated deceptions related to the info theft
level of technical and behavioral monitoring
org discovery of deceptions

Our lab transforms that into this…

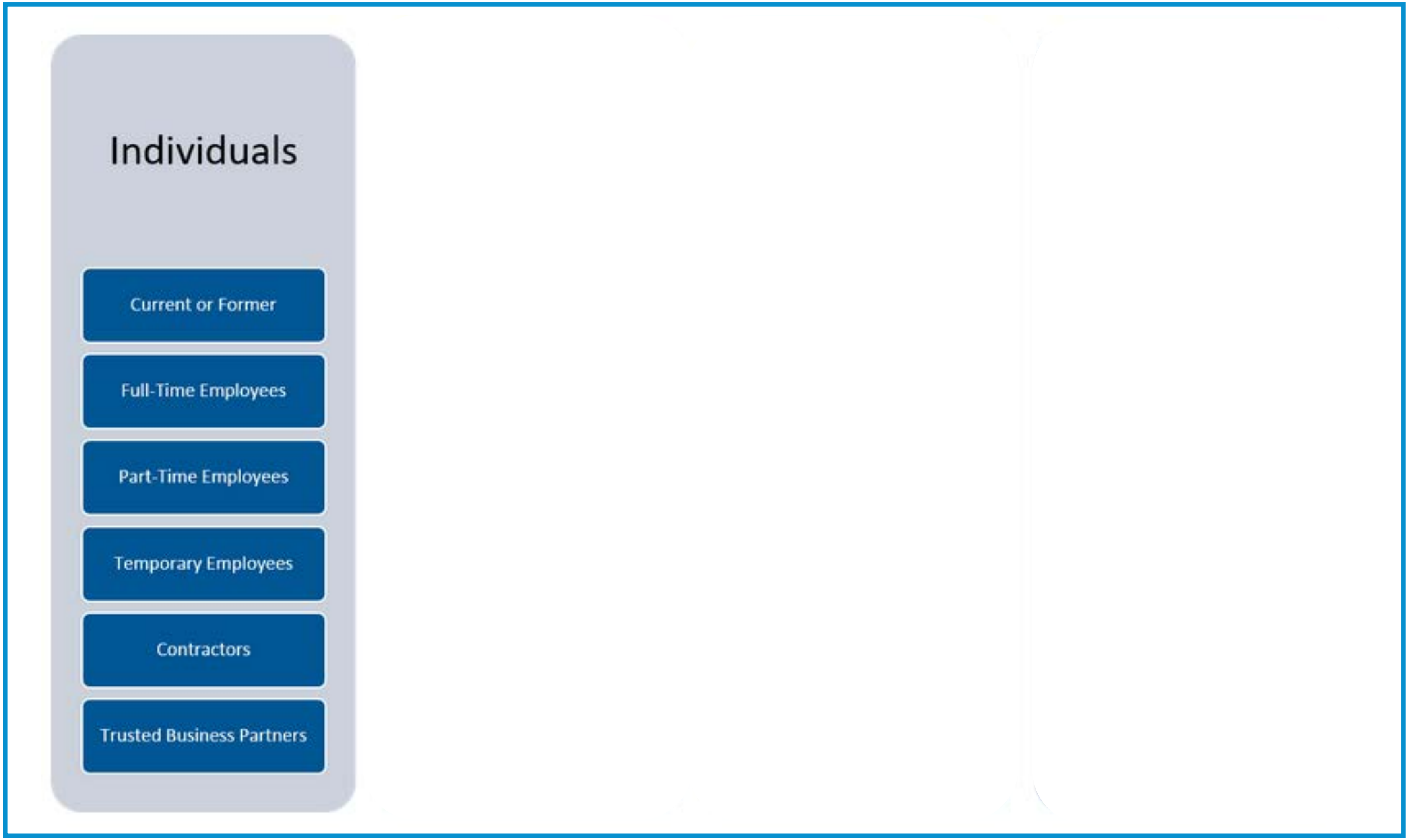
```
Splunk Query Name: Last 30 Days - Possible Theft of IP

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'
```

CERT’s 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

Current or Former

Full-Time Employees

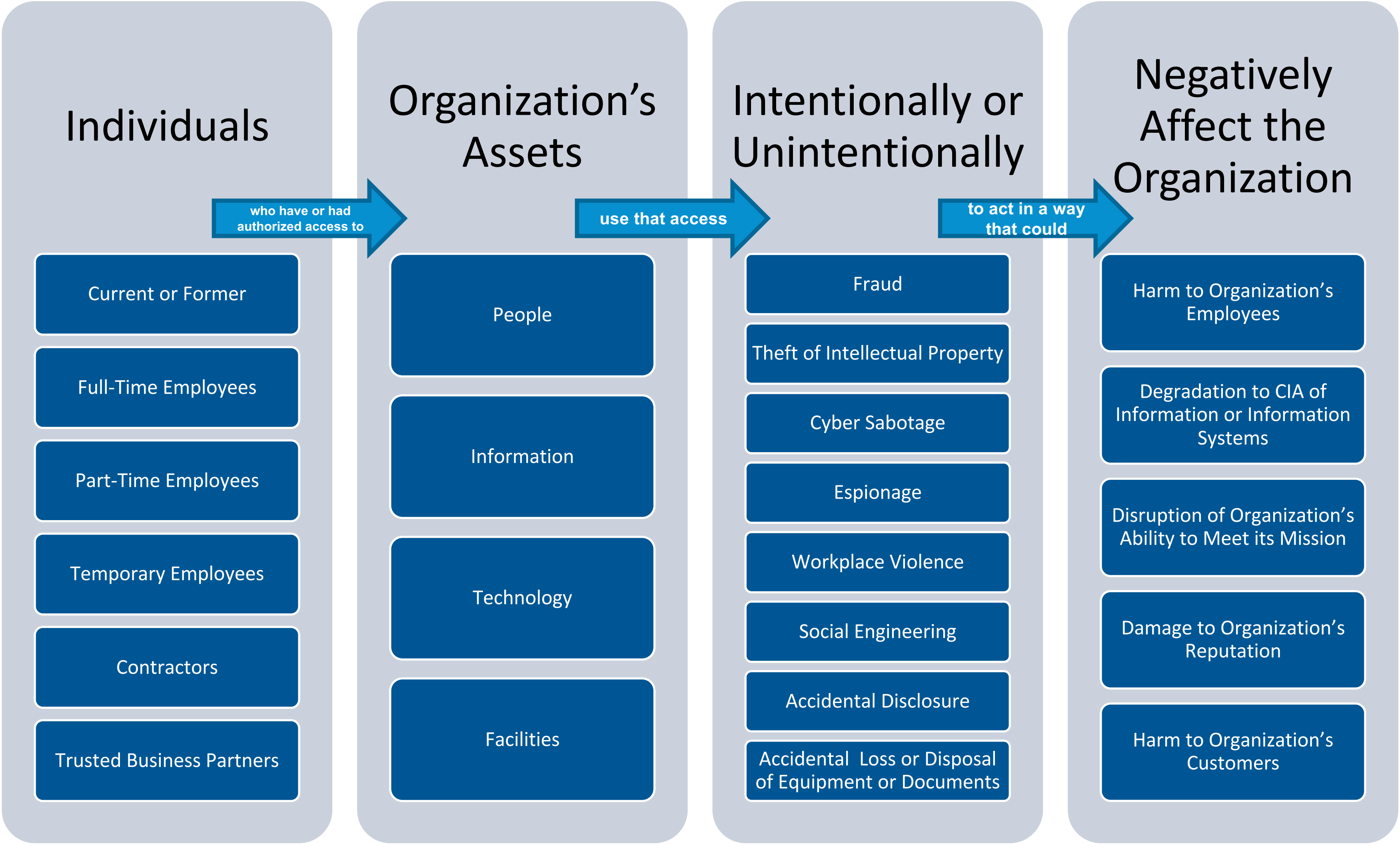
Part-Time Employees

Temporary Employees

Contractors

Trusted Business Partners

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

The Insider Threat

There is not one “type” of insider threat

- Threat is to an organization’s critical assets
  - People
  - Information
  - Technology
  - Facilities
- Based on the motive(s) of the insider
- Impact is to Confidentiality, Availability, Integrity

Cyber attack = Cyber Impact

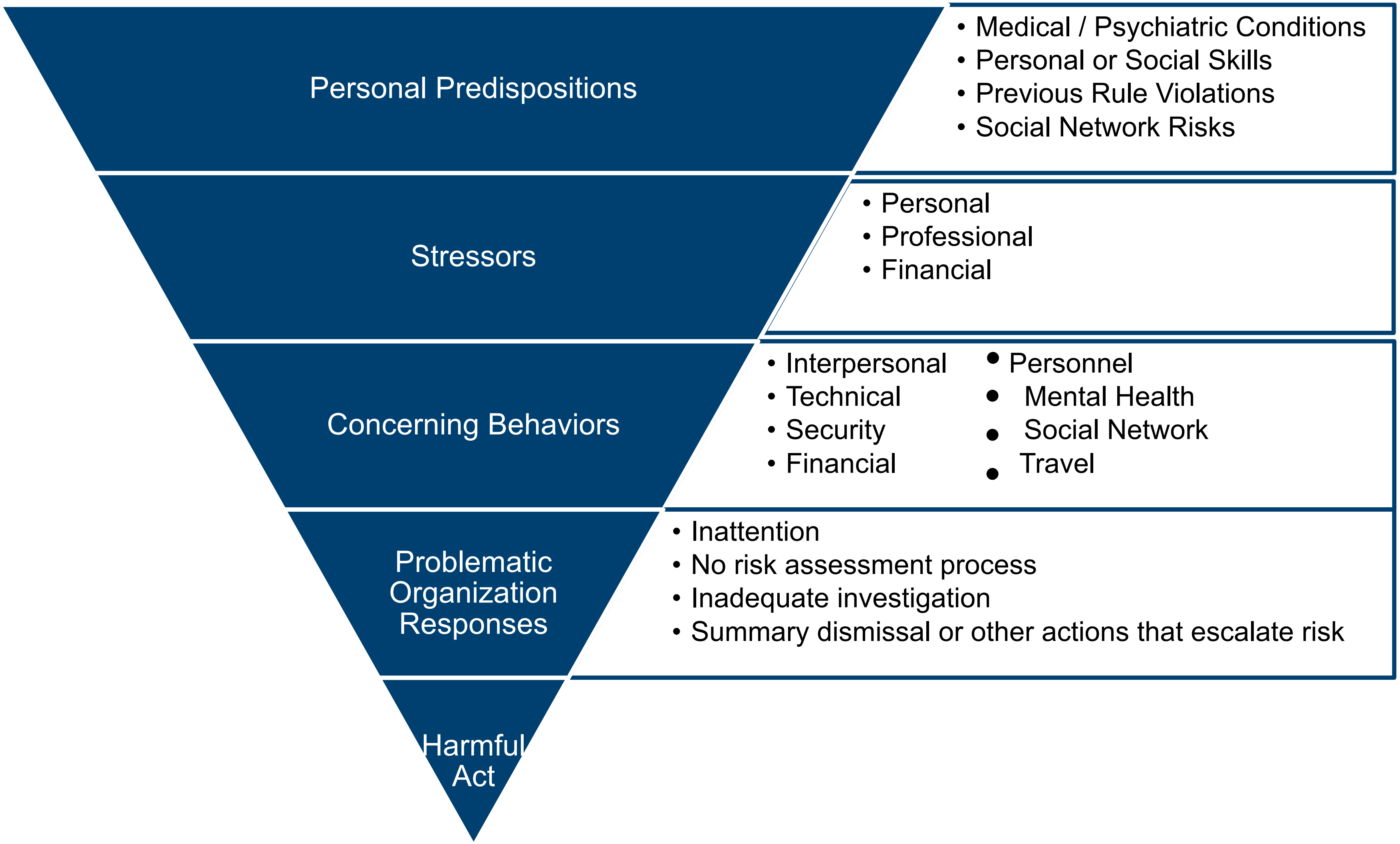
Kinetic attack = Kinetic Impact

Cyber attack = Kinetic Impact

Kinetic attack = Cyber Impact

Types of Malicious Insider Incidents

CERT’s Critical Path to Insider Risk



Personal Predispositions

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

Stressors

- Personal
- Professional
- Financial

Concerning Behaviors

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

Problematic Organization Responses

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

Harmful Act

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

TRUE STORY*: IT Sabotage*

911 services disrupted for 4 major cities

Disgruntled former employee arrested and convicted for this deliberate act of sabotage.

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.

TRUE STORY: *Fraud*

An undercover agent who claims to be on the “No Fly list” buys a fake drivers license from a ring of DMV employees...

The identity theft ring consisted of 7 employees who sold more than 200 fake licenses for more than $1 Million.

Insider Incidents in Tax Organizations-1

A clerk at a government entity exceeded their authorized access to the organization's database to investigate the parent of their grandchild. The insider, without any need-to-know, accessed the individual's account on 4 occasions. A government audit detected the incident. The insider was arrested and convicted.

An insider working for a government entity committed an act of Theft of IP by stealing customer PII in order to fill out fraudulent tax returns. The insider filled out more than 120 fraudulent forms and received about $300,000 from the tax returns. It is suspected that the insider had been accessing customer information and filing out the fraudulent tax returns for over 3 years.

Insider Incidents in Tax Organizations-2

An insider was employed by a state agency for 7 years and had access to customer information including customer names, addresses, dates of birth, and Social Security Numbers (SSNs). The insider would obtain the information and format it into a sheet then email to other outsiders. The outsiders would use the stolen PII to file fraudulent tax returns and would pay the insider to steal more customer information.

The insider stole PII of more than 3,000 customers, mostly those of teenagers.

The outsiders used all of the PII and filed federal income tax returns that claimed over $7.5 million in fraudulent refunds.

The insider plead guilty and was sentenced to more than 80 months imprisonment, 3 years supervised release, and over $3,000,000 ($3 Million) in restitution.

Summary of Insider Incidents

	IT Sabotage	Fraud	Theft of Intellectual Property
Current or former Employee?	Former	Current	Current (within 30 days of resignation)
Type of position	Technical (e.g., sys admins, programmers, DBAs)	Non-technical (e.g., data entry, customer service) or their managers	Technical (e.g., scientists, programmers, engineers) or sales
Gender	Male	Fairly equally split between male and female	Male
Target	Network, systems, or data	PII or Customer Information	IP (trade secrets) or Customer Information
Access Used	Unauthorized	Authorized	Authorized
When	Outside normal working hours	During normal working hours	During normal working hours
Where	Remote access	At work	At Work

Insider Fraud: A Closer Look

Insider Fraud Study

Funded by U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T)

Conducted by the CERT Insider Threat Center in collaboration with the U.S. Secret Service (USSS)

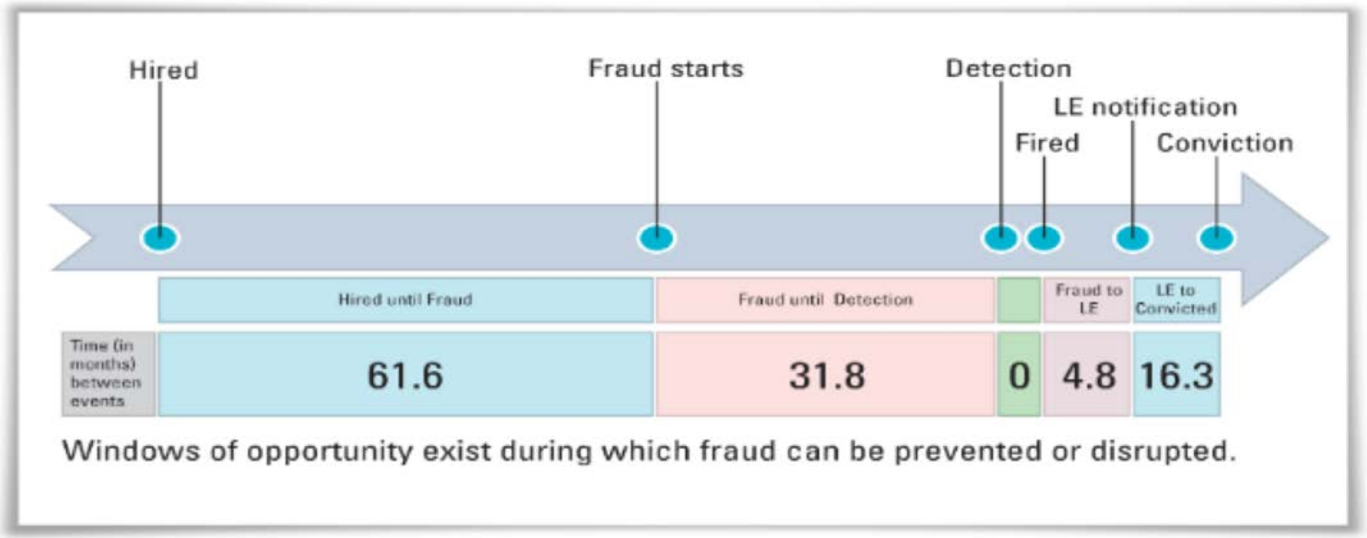
Full report: “Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector” (http://www.sei.cmu.edu/library/abstracts/reports/12sr004.cfm)

Booklet: “Insider Fraud in Financial Services” (http://www.sei.cmu.edu/library/abstracts/brochures/12sr004-brochure.cfm)

INSIDER FRAUD IN FINANCIAL SERVICES

Low and Slow

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



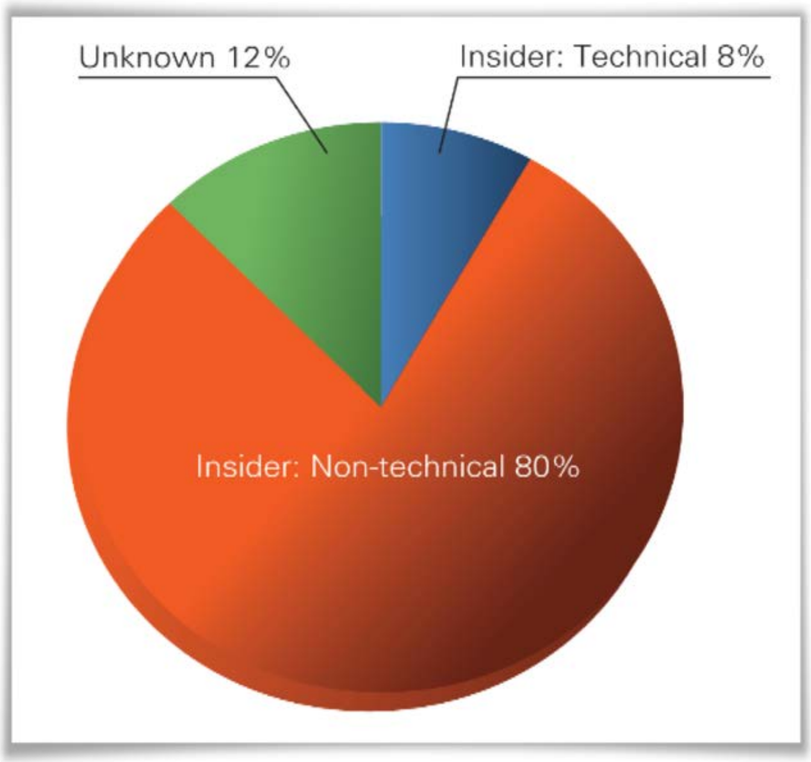
	Hired until Fraud	Fraud until Detection		Fraud to LE	LE to Convicted
Time (in months) between events	61.6	31.8	0	4.8	16.3

Windows of opportunity exist during which fraud can be prevented or disrupted.

There are, on average, over 5 years between a subject’s hiring and the start of the fraud. There are 32 months between the beginning of the fraud and its detection.

Low-Tech

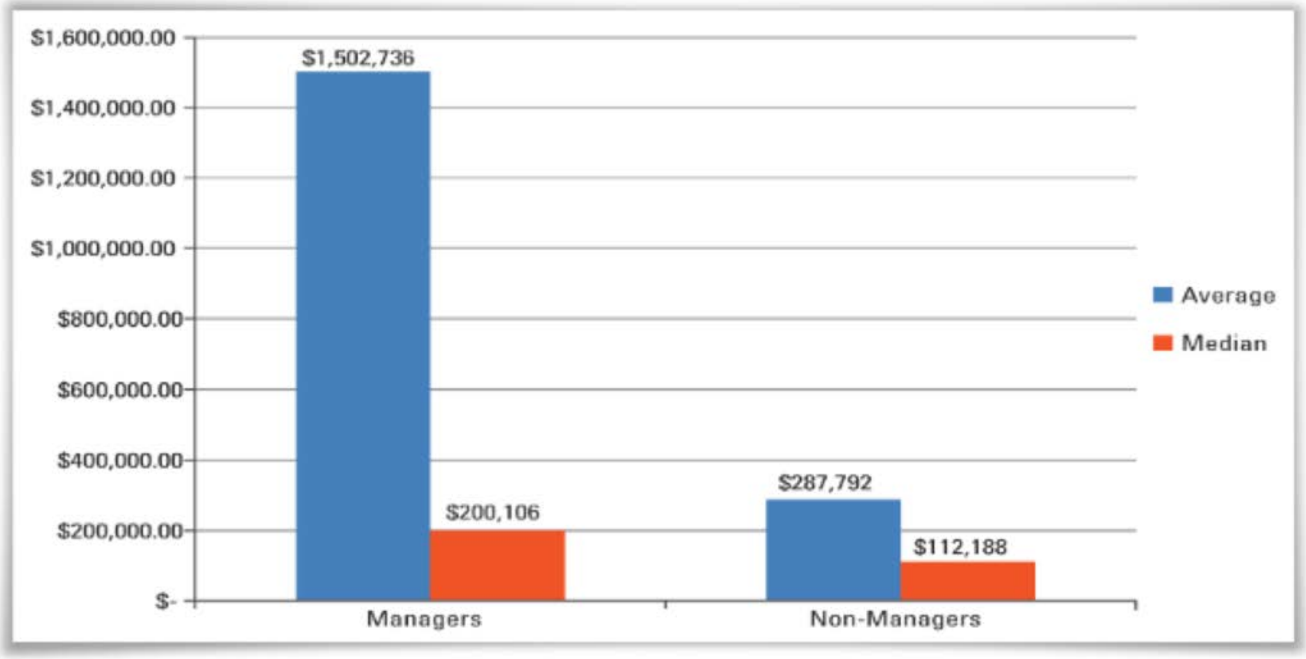
Insiders’ means were not very technically sophisticated.



Non-technical subjects were responsible for 65 (81 percent) incidents. Seven were external attackers, but their methods were also non-technical.

Managers vs. Non-Managers

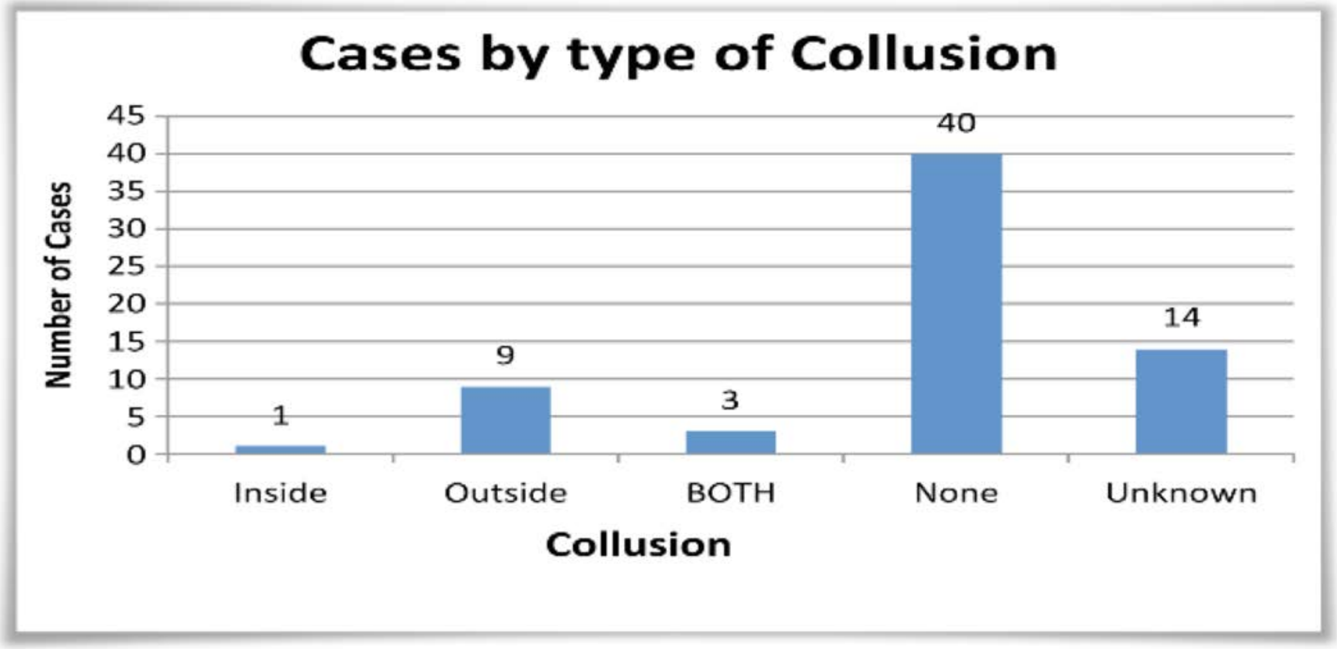
Fraud by managers differs substantially from fraud by non-managers by damage and duration.



Of 61 subjects, 31 (51 percent) were managers, VPs, bank officers, or supervisors. The median results show that managers consistently caused more actual damage ($200,106) than non-managers ($112,188).

Collusion

Most cases do not involve collusion.



There was not a significant number of cases involving collusion, but those that did occur generally involved external collusion (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.

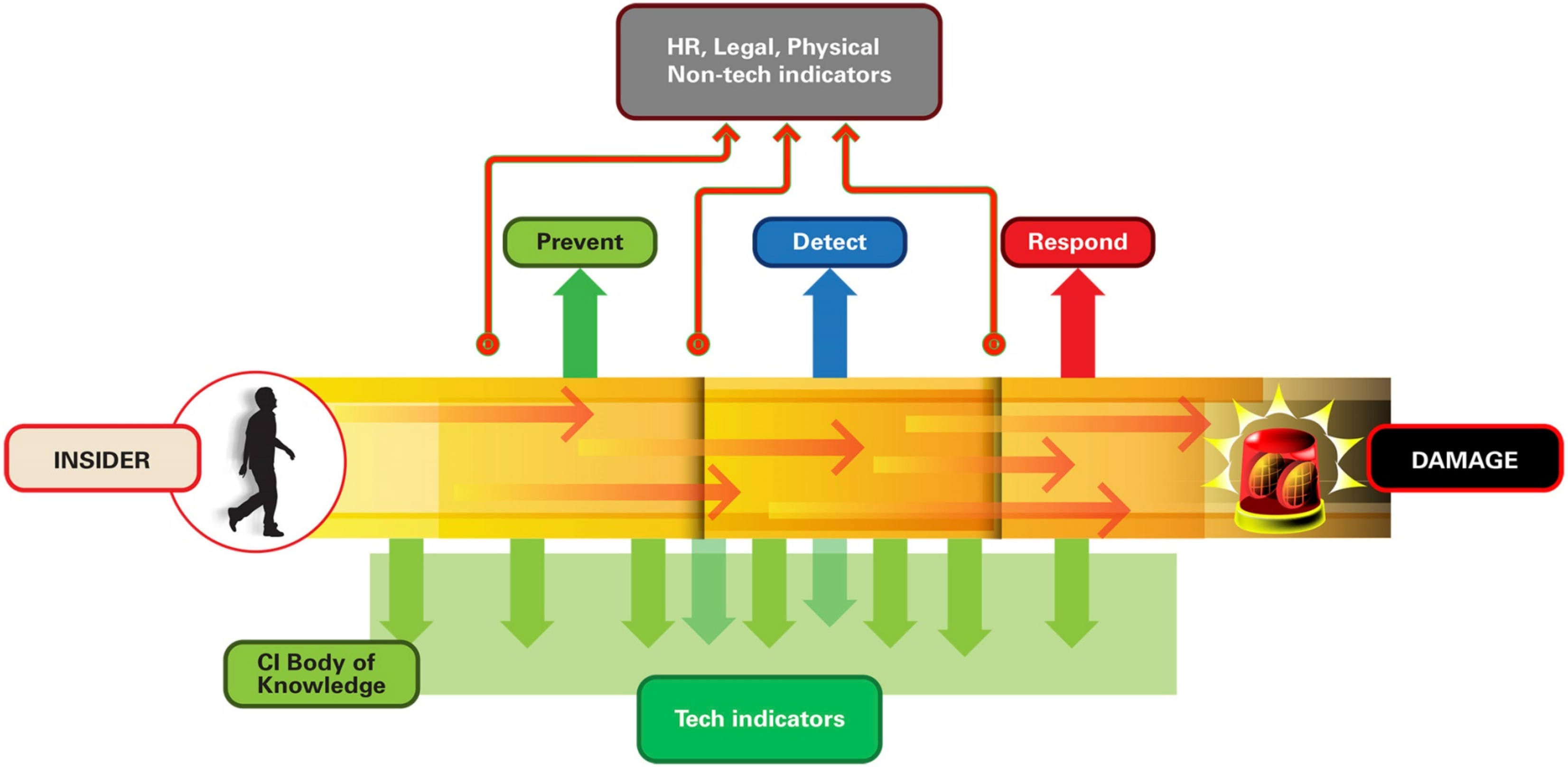
The most common way attacks were detected was through routine or impromptu audits.

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).

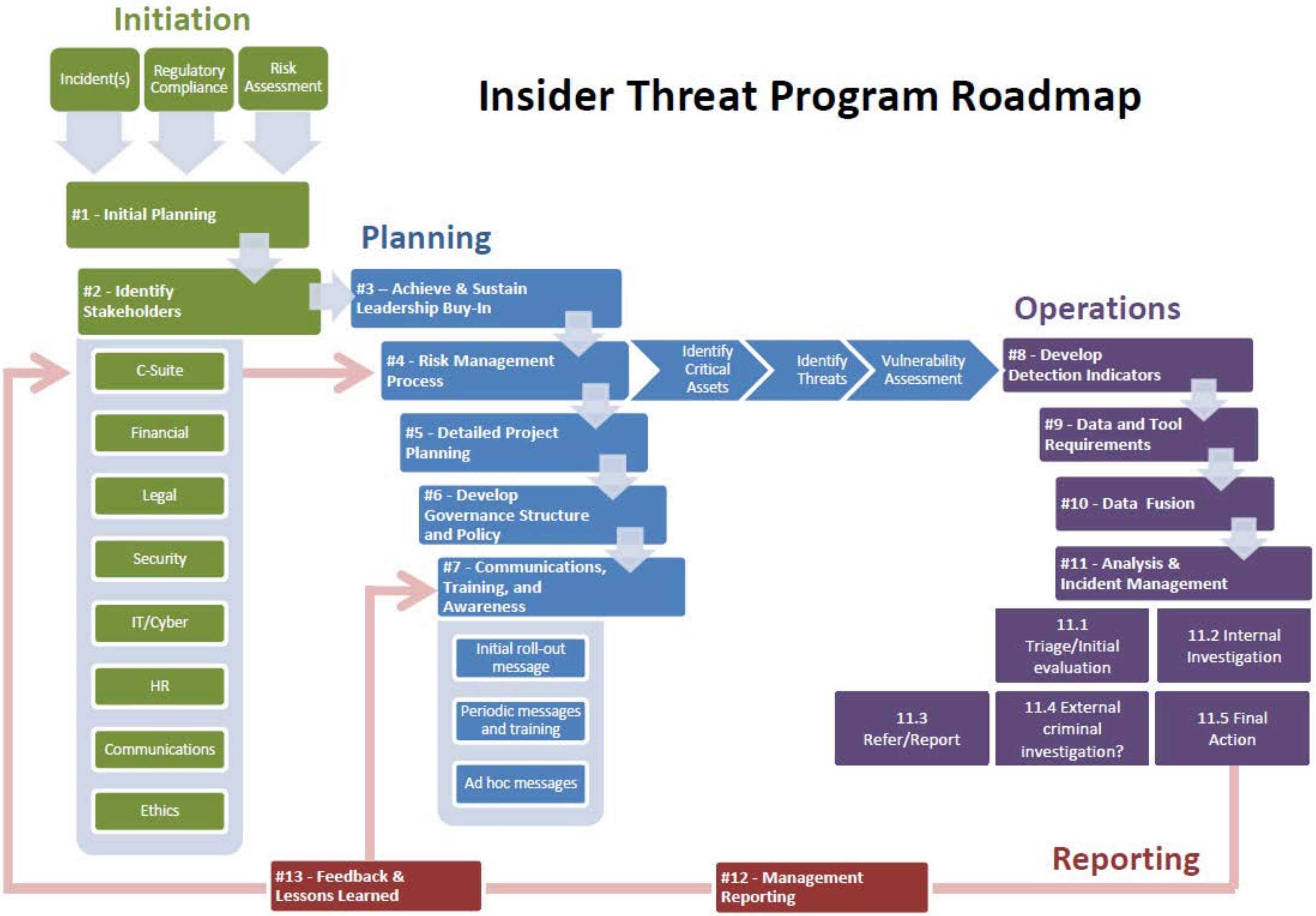
Building an Insider Threat Program

Goal for an Insider Threat Program



Opportunities for prevention, detection, and response for an insider incident

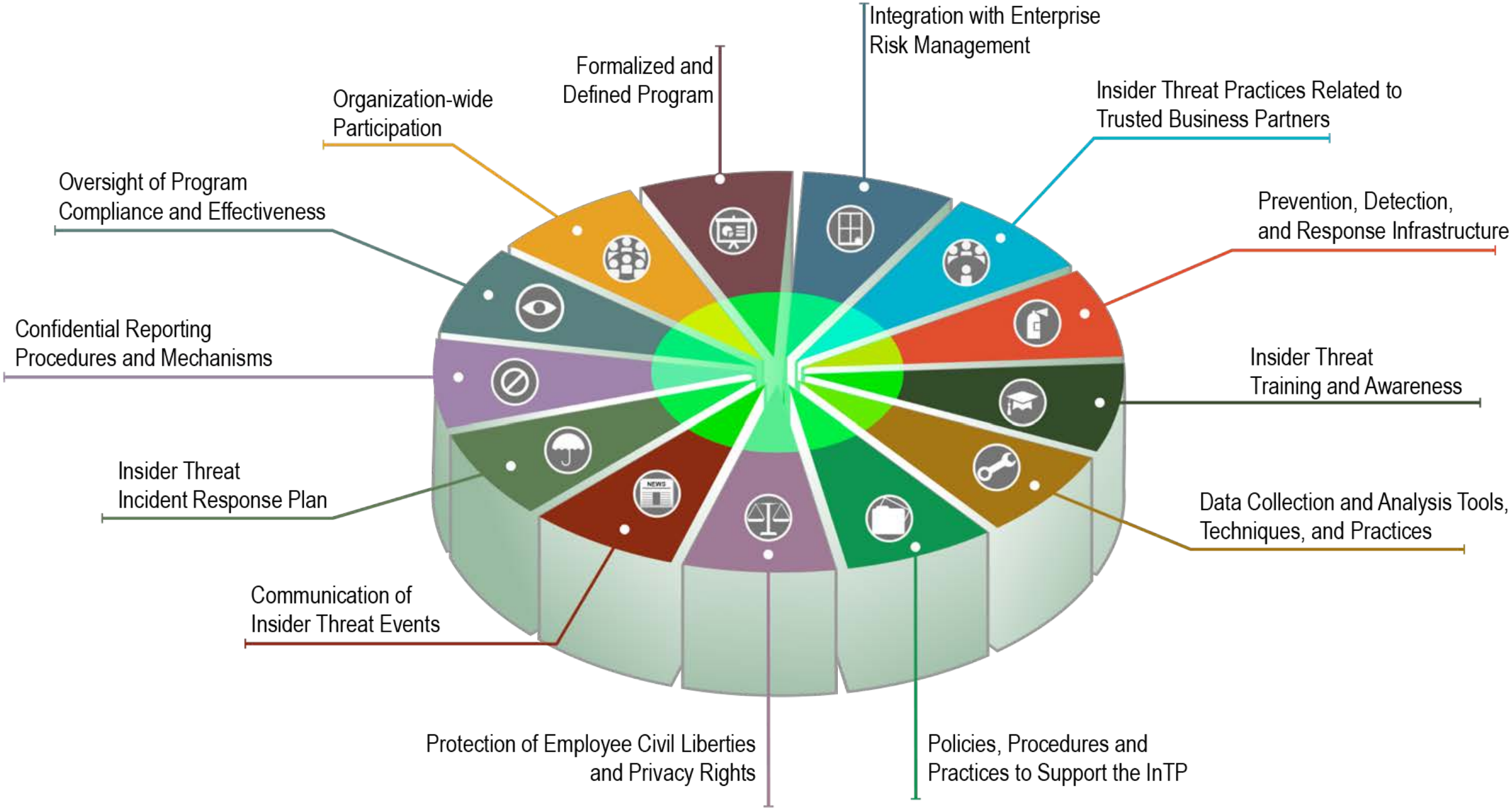
Essential Elements of an Insider Threat Program


Insider Threat Program Roadmap
Initiation
Incident(s)
Regulatory Compliance
Risk Assessment
#1 - Initial Planning
#2 - Identify Stakeholders
C-Suite
Financial
Legal
Security
IT/Cyber
HR
Communications
Ethics
Planning
#3 – Achieve & Sustain Leadership Buy-In
#4 - Risk Management Process
Identify Critical Assets
Identify Threats
Vulnerability Assessment
#5 - Detailed Project Planning
#6 - Develop Governance Structure and Policy
#7 - Communications, Training, and Awareness
Initial roll-out message
Periodic messages and training
Ad hoc messages
Operations
#8 - Develop Detection Indicators
#9 - Data and Tool Requirements
#10 - Data Fusion
#11 - Analysis & Incident Management
11.1 Triage/Initial evaluation
11.2 Internal Investigation
11.3 Refer/Report
11.4 External criminal investigation?
11.5 Final Action
Reporting
#12 - Management Reporting
#13 - Feedback & Lessons Learned

Source:

https://www.insaonline.org/insider-threat-roadmap/

CERT Insider Threat Center Key Components of an Insider Threat Program


Integration with Enterprise Risk Management
Insider Threat Practices Related to Trusted Business Partners
Prevention, Detection, and Response Infrastructure
Insider Threat Training and Awareness
Data Collection and Analysis Tools, Techniques, and Practices
Policies, Procedures and Practices to Support the InTP
Protection of Employee Civil Liberties and Privacy Rights
Communication of Insider Threat Events
Insider Threat Incident Response Plan
Confidential Reporting Procedures and Mechanisms
Oversight of Program Compliance and Effectiveness
Organization-wide Participation
Formalized and Defined Program
NEWS

Observables
(Potential Indicators?)

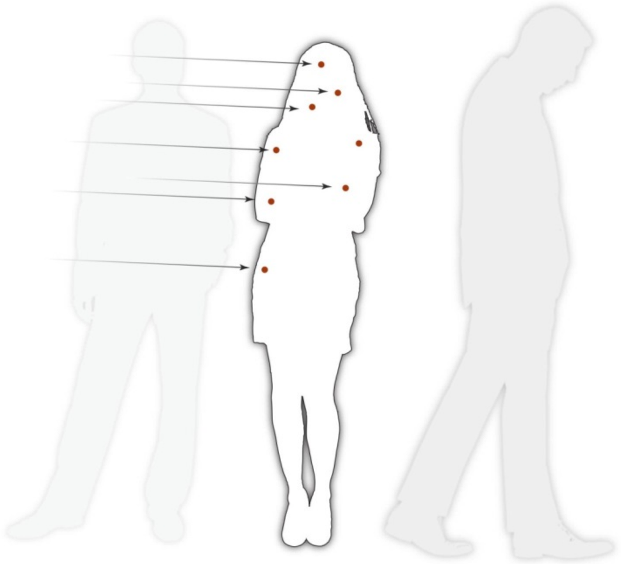
Insider Motives Observed in Cases

- Financial Gain
- Ideology
- Revenge
- Recognition
- Curiosity
- Excitement
- Benefit a Foreign Entity
- Gain a Competitive Business Advantage
- Start a New Business
- Benefit a New Employer

Unmet Expectations Observed in Cases

- Salary/bonus
- Promotion
- Freedom of online actions
- Workload
- Overestimated abilities
- Supervisor demands
- Coworker relations
- Job engagement
- Perceived organizational support
- Connectedness at work

Behavioral Precursors Observed in Cases



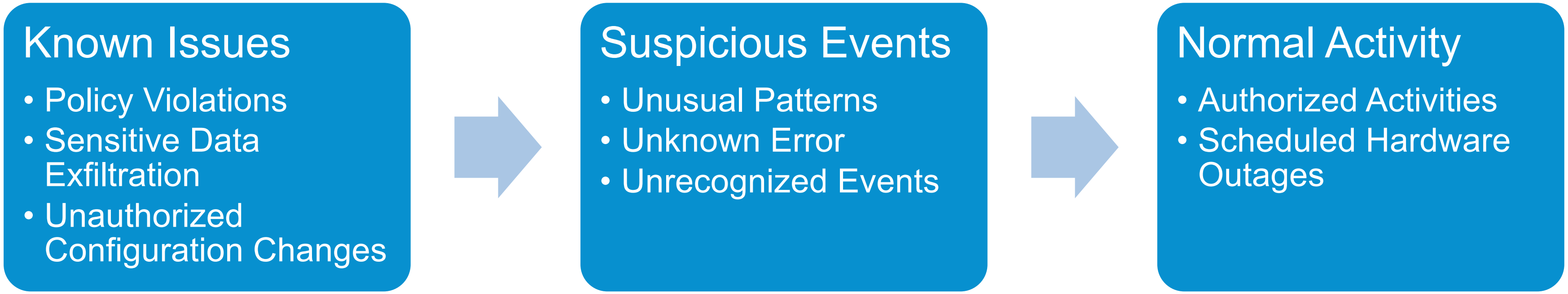
- Drug use
- Conflicts (coworkers, supervisor)
- Aggressive or violent behavior
- Mood swings
- Using organization’s computers for personal business
- Poor performance
- Absence/tardiness
- Sexual harassment

Technical Precursors Observed in Cases

- Downloading and using tools such as rootkits, password sniffers, or password crackers
- Disabling automated backups
- Disabling logging / deleting log files
- Failure to document systems or software as required
- Unauthorized access of customers' systems
- Unauthorized use of coworkers' machines left logged in
- Sharing passwords with others & demanding passwords from subordinates
- System access following termination
- Network probing / data hoarding
- Failing to swipe badge to record physical access
- Access of web sites prohibited by acceptable use policy
- Failure to return IT equipment upon termination
- Creation and use of backdoor accounts

Anomaly Detection

A Phased Approach to Insider Threat Anomaly Detection



Known Issues

- Policy Violations
- Sensitive Data Exfiltration
- Unauthorized Configuration Changes

Suspicious Events

- Unusual Patterns
- Unknown Error
- Unrecognized Events

Normal Activity

- Authorized Activities
- Scheduled Hardware Outages

Baselining

Establish “normal behavior” across bins.

- User-Based
  - Compare each user to himself or herself.
- Role-Based
  - Compare users in the same roles against each other.
- Pattern-Based
  - Compare common patterns to previous occurrences of the pattern.
- Threshold-Based
  - Compare the average number of activities/events.

Indicator Development

Indicators

Technical

- Technical actions that could do your organization harm

Behavioral

- Common precursors to insider activity

Temporality and sequence

- 30-day rule

Context is key

- Stimulus
- Job role

Qualities of effective indicators

- Weighting
- Specificity

Technical Data

Security Device Reporting Analysis

Operations analysts within the SOC typically monitor consoles where large amounts of information are collected from the security ‘sensors’ and devices.

This set of information includes

- IDS alerts
- IPS alerts
- Antivirus alerts
- Firewall logs
- Proxy logs
- Network flow records
- Packet capture and session recreation information
- Correlated events from security event managers
- External (global) threat and architecture information

Hub Tools – UAM / UBA

User Activity Monitoring (UAM): **“**UAM refers to the technical capability to observe and record the actions and activities of an individual, at any time, on any device accessing … information in order to detect insider threats and support authorized investigations.” –NITTF Guide

Often serves as the starting point and core of an insider threat analysis hub.

User Behavioral Analytics (UBA): “cybersecurity process about detection of insider threats, targeted attacks, and financial fraud. UBA solutions look at patterns of human behavior, and then apply algorithms and statistical analysis to detect meaningful anomalies from those patterns—anomalies that indicate potential threats. Instead of tracking devices or security events, UBA tracks a system's users.” - Gartner

https://www.gartner.com/doc/2831117/market-guide-user-behavior-analytics

Behavioral Data

Behavioral Data Sources

Human Resources Management System Data

Help Desk Trouble Ticket System Logs

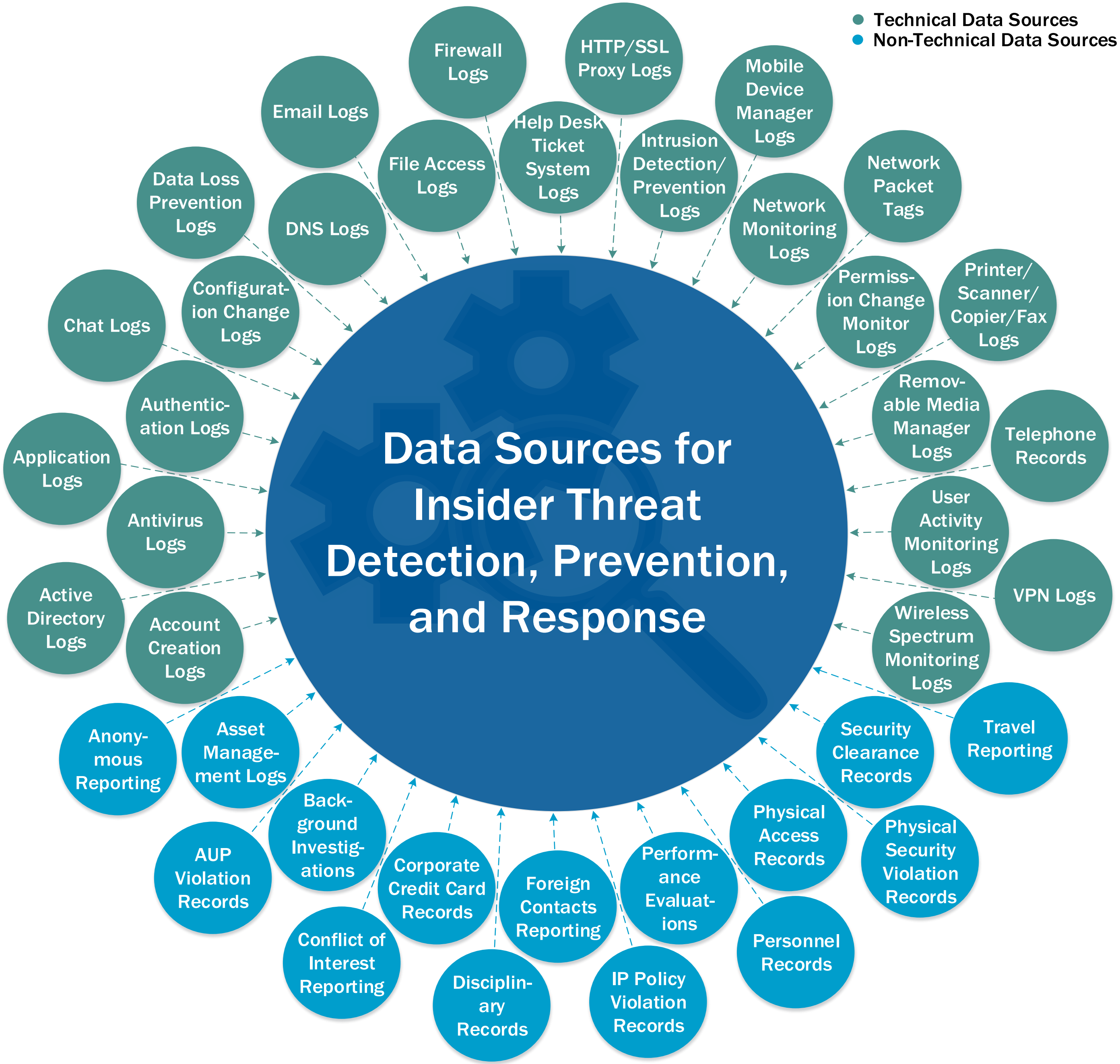
Physical Access Logs

Phone Logs

Personnel Security Systems

Foreign Travel and Reporting Systems

Financial Systems



● Technical Data Sources

● Non-Technical Data Sources

Data Sources for Insider Threat Detection, Prevention, and Response

- Email Logs
- Firewall Logs
- HTTP/SSL Proxy Logs
- Mobile Device Manager Logs
- Network Packet Tags
- Data Loss Prevention Logs
- DNS Logs
- File Access Logs
- Help Desk Ticket System Logs
- Intrusion Detection/ Prevention Logs
- Network Monitoring Logs
- Printer/ Scanner/ Copier/Fax Logs
- Chat Logs
- Configuration Change Logs
- Permission Change Monitor Logs
- Authentication Logs
- Removable Media Manager Logs
- Telephone Records
- Application Logs
- Antivirus Logs
- User Activity Monitoring Logs
- VPN Logs
- Active Directory Logs
- Account Creation Logs
- Wireless Spectrum Monitoring Logs
- Anonymous Reporting
- Asset Management Logs
- Security Clearance Records
- Travel Reporting
- AUP Violation Records
- Background Investigations
- Corporate Credit Card Records
- Foreign Contacts Reporting
- Performance Evaluations
- Physical Access Records
- Physical Security Violation Records
- Conflict of Interest Reporting
- Disciplinary Records
- IP Policy Violation Records
- Personnel Records

Best Practices for the Mitigation of Insider Threats

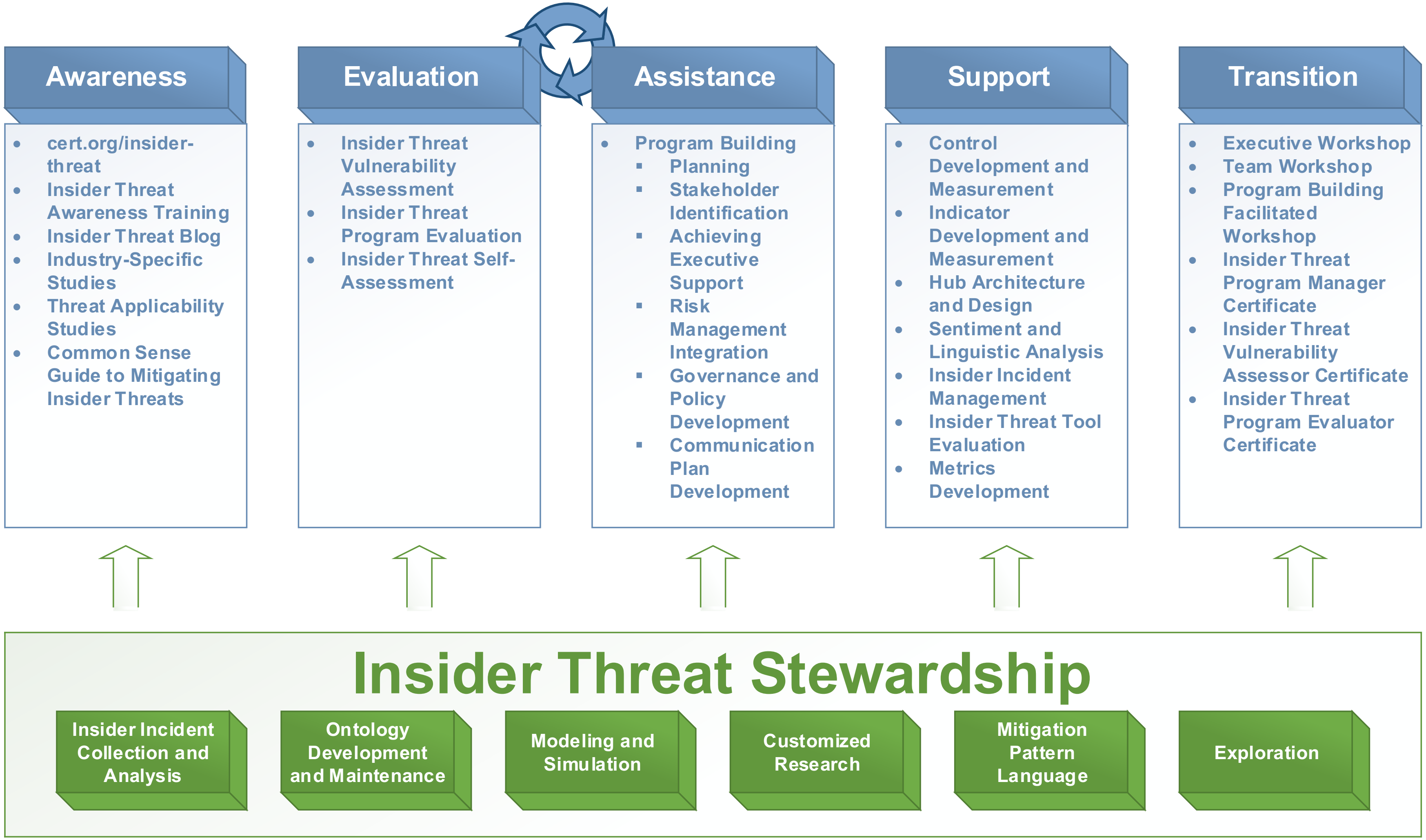
Recommended Best Practices for Insider Threat Mitigation

1 - Know and protect your critical assets.	11 - Institute stringent access controls and monitoring policies on privileged users.
2 - Develop a formalized insider threat program.	12 - Deploy solutions for monitoring employee actions and correlating information from multiple data sources.
3 - Clearly document and consistently enforce policies and controls.	13 - Monitor and control remote access from all endpoints, including mobile devices.
4 - Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.	14 - Establish a baseline of normal behavior for both networks and employees
5 - Anticipate and manage negative issues in the work environment.	15 - Enforce separation of duties and least privilege.
6 - Consider threats from insiders and business partners in enterprise-wide risk assessments.	16 - Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.
7 - Be especially vigilant regarding social media.	17 - Institutionalize system change controls.
8 - Structure management and tasks to minimize unintentional insider stress and mistakes.	18 - Implement secure backup and recovery processes.
9 - Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.	19 - Close the doors to unauthorized data exfiltration.
10 - Implement strict password and account management policies and practices.	20 - Develop a comprehensive employee termination procedure.

http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=484738 or search “cert common sense guide insider threat”

Wrap Up

Our Insider Threat Portfolio



Awareness

- cert.org/insider-threat
- Insider Threat Awareness Training
- Insider Threat Blog
- Industry-Specific Studies
- Threat Applicability Studies
- Common Sense Guide to Mitigating Insider Threats

Evaluation

- Insider Threat Vulnerability Assessment
- Insider Threat Program Evaluation
- Insider Threat Self-Assessment

Assistance

- Program Building
  - Planning
  - Stakeholder Identification
  - Achieving Executive Support
  - Risk Management Integration
  - Governance and Policy Development
  - Communication Plan Development

Support

- Control Development and Measurement
- Indicator Development and Measurement
- Hub Architecture and Design
- Sentiment and Linguistic Analysis
- Insider Incident Management
- Insider Threat Tool Evaluation
- Metrics Development

Transition

- Executive Workshop
- Team Workshop
- Program Building Facilitated Workshop
- Insider Threat Program Manager Certificate
- Insider Threat Vulnerability Assessor Certificate
- Insider Threat Program Evaluator Certificate

Insider Threat Stewardship

- Insider Incident Collection and Analysis
- Ontology Development and Maintenance
- Modeling and Simulation
- Customized Research
- Mitigation Pattern Language
- Exploration

Other CERT Insider Threat Center Services

- Building an Insider Threat Program
  - Insider Threat Program Manager Certificate (ITPM-C)
- Insider Threat Vulnerability Assessment
  - Insider Threat Vulnerability Assessor Certificate (ITVA-C)
- Evaluating an Insider Threat Program
  - Insider Threat Program Evaluator Certificate (ITPE-C)
- Insider Threat Analyst Training Course
- Insider Threat Control/Indicator Development / Deployment
- Insider Threat Data Analytics Hub Development / Deployment
- Insider Threat Training (1/2 day, 1 day, and 2 day interactive workshops)
- Customized Insider Threat Research
  - Ontology Development and Maintenance
  - Sentiment / Linguistic Analysis
  - Insider Threat Tool Evaluation Criteria Development

For More Information

Insider Threat Center website
http://www.cert.org/insider-threat/

Insider Threat Center Email:
insider-threat-feedback@cert.org

Insider Threat Blog
http://www.cert.org/blogs/insider-threat/

Point of Contact

Insider Threat Technical Manager
Randall F. Trzeciak
CERT Program
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-3890
+1 412 268-7040 – Phone
rft@cert.org – Email

http://www.cert.org/insider_threat/