Five Best Practices to Combat the Insider Threat

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

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.

DM18-0619

Agenda

8:00: **Overview of the National Insider Threat Center**

8:15: **Our Research**

8:30: **What is the Insider Threat?**

8:45: **3 Insider Threat Models**

9:00: **5 Best Practices**

Five Best Practices to Combat the Insider Threat

Ms. Carrie Gardner

Cyber Security Engineer,

CERT National Insider Threat Center

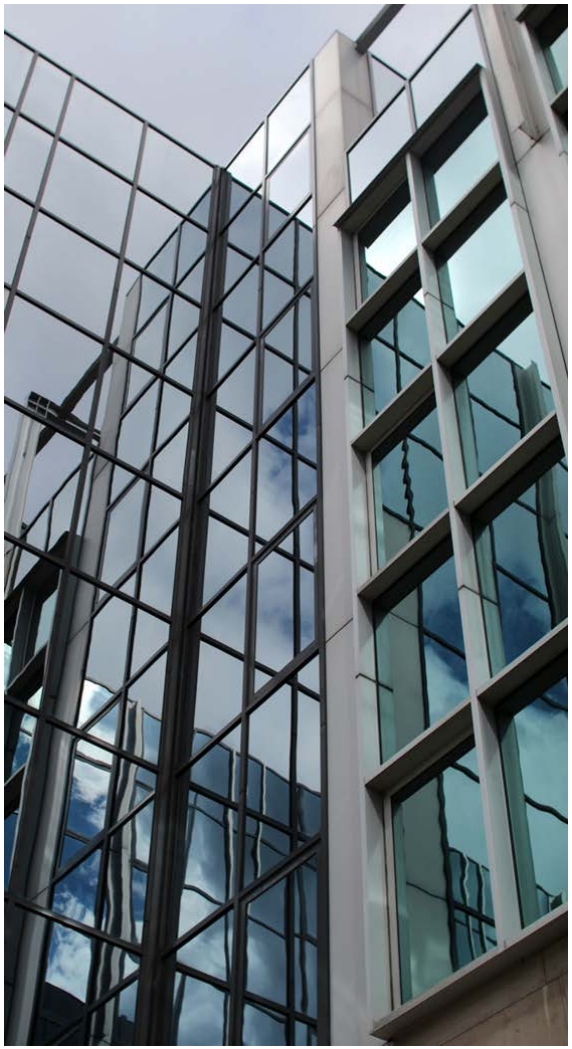
Established as a DoD FFRDC at Carnegie Mellon University in 1984

Only DoD R&D center focused on software and cybersecurity

Offices in Pittsburgh, Arlington, and Los Angeles

About 600 staff (~400 tech staff)

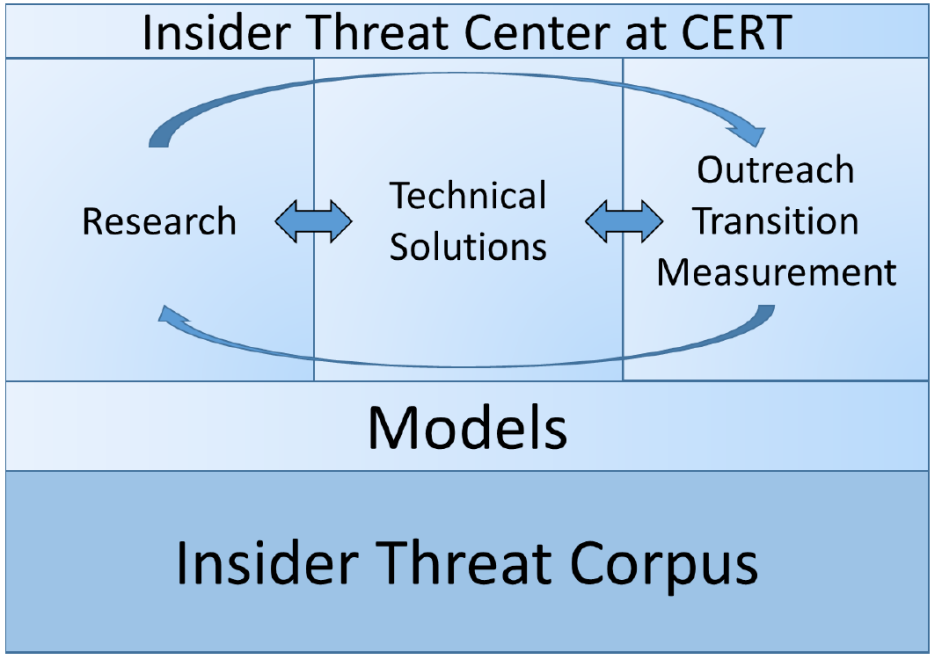
The CERT Division's National Insider Threat Center



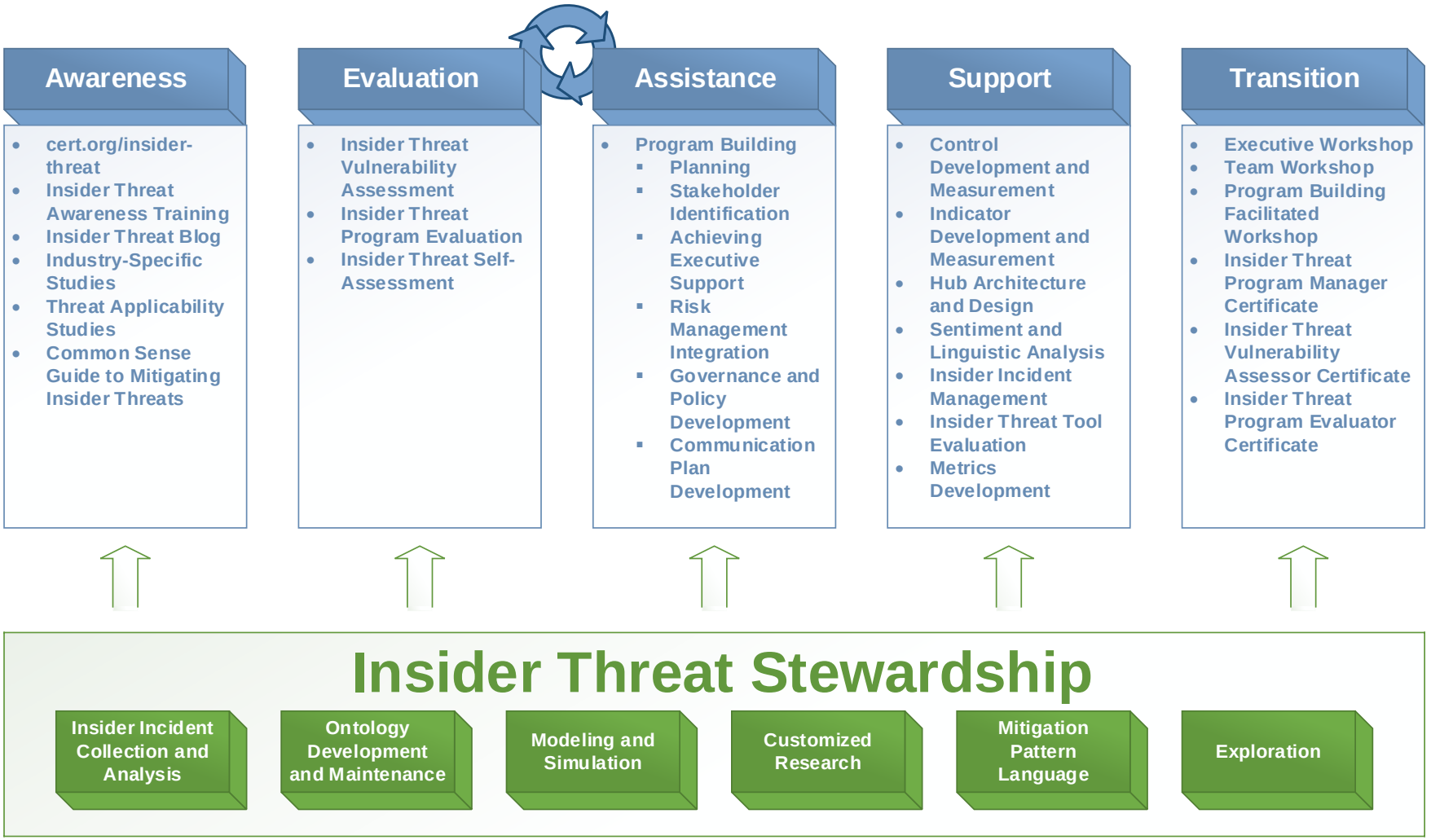
- Center of insider threat expertise
- Began working in this area in 2001 with the U.S. Secret Service
- Mission: enable effective insider threat mitigation, incident management practices, and develop capabilities for deterring, detecting, and responding to evolving cyber and physical threats
- Action 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
  - Text analysis
  - Workplace violence
  - Typing heuristics
  - Biometrics



Our Insider Threat Portfolio



Other NITC Services

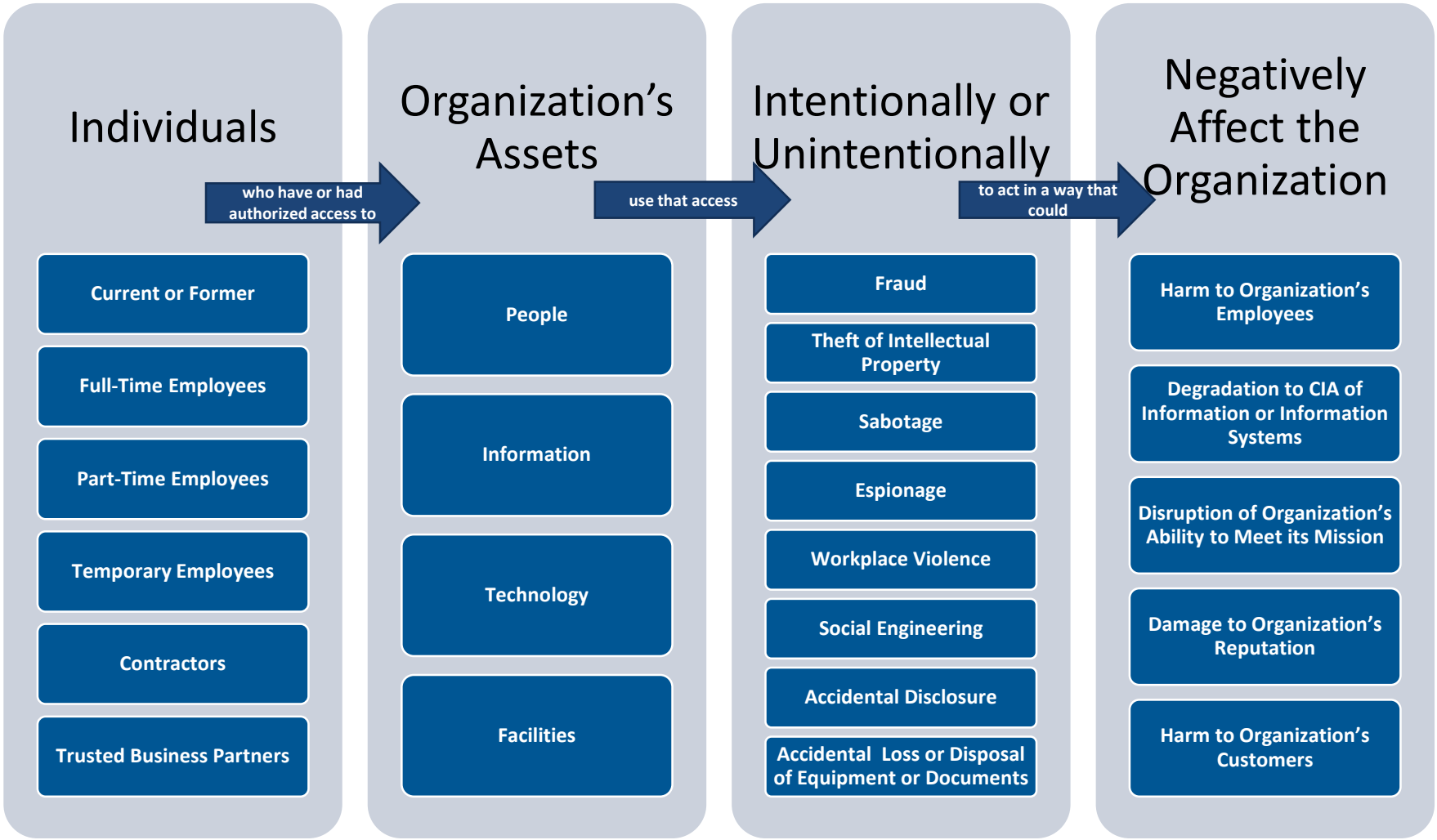
- Building an Insider Threat Program
  - Insider Threat Program Manager Certificate (ITPM-C)
  - Insider Threat Analyst Training
- Insider Threat Vulnerability Assessment
  - Insider Threat Vulnerability Assessor Certificate (ITVA-C)
  - Insider Threat Vulnerability Assessment License
- Evaluating an Insider Threat Program
  - Insider Threat Program Evaluator Certificate (ITPE-C)
- Insider Threat Analyst Training Course
- Insider Threat Control/Indicator Development / Deployment / Measurement
- Insider Threat Data Analytics Hub Development / Deployment
- Customized Insider Threat Research
  - Insider Threat Tool Evaluation Criteria Development

What is the Insider Threat?

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.

Scope of the Insider Threat



Insider Threats Can Be Cyber or Physical

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

Physical attack = Physical Impact

Cyber attack = Physical Impact

Physical attack = Cyber Impact

Insider Threat Issues -1

Insiders pose a substantial threat by virtue of their knowledge of, and access to, their employers' systems and/or databases.

Insiders can bypass existing physical and electronic security measures through ***legitimate*** measures.

Insider Threat Issues -2

Think about the following questions.

- Has your organization been victim of an insider attack?
- Can you ***confidently*** say you have ***not*** been the victim of an insider attack?

Insider Threat Issues -3

Many organizations feel they have to choose between protection from outsiders versus insiders.

Keep in mind that once an outsider gets in, there is a good chance they will perform the same types of malicious acts as malicious insiders.

- Plant malicious code or logic bomb
- Create backdoor account
- Exfiltrate intellectual property or other proprietary information

Insider negligence or malfeasance could aid outsiders getting in.

- Therefore, insider threat controls can also provide protection from outsiders.

The Expanding Complexity of “Insiders”

Area	Description
Willing or unintentional collusion with outsiders	Insiders recruited by, working for, or used by outsiders, including organized crime and foreign organizations or governments
Business partners	Difficulty in controlling/monitoring access to your information and systems by “trusted” business partners
Mergers & acquisitions	Heightened risk of insider threat in organizations being merged into acquiring organization
Cultural differences	Difficulty in recognizing behavioral indicators exhibited by insiders working for US organizations who are not US citizens

How Serious are Insider Threats?

2017 U.S. State of Cybercrime Survey -1

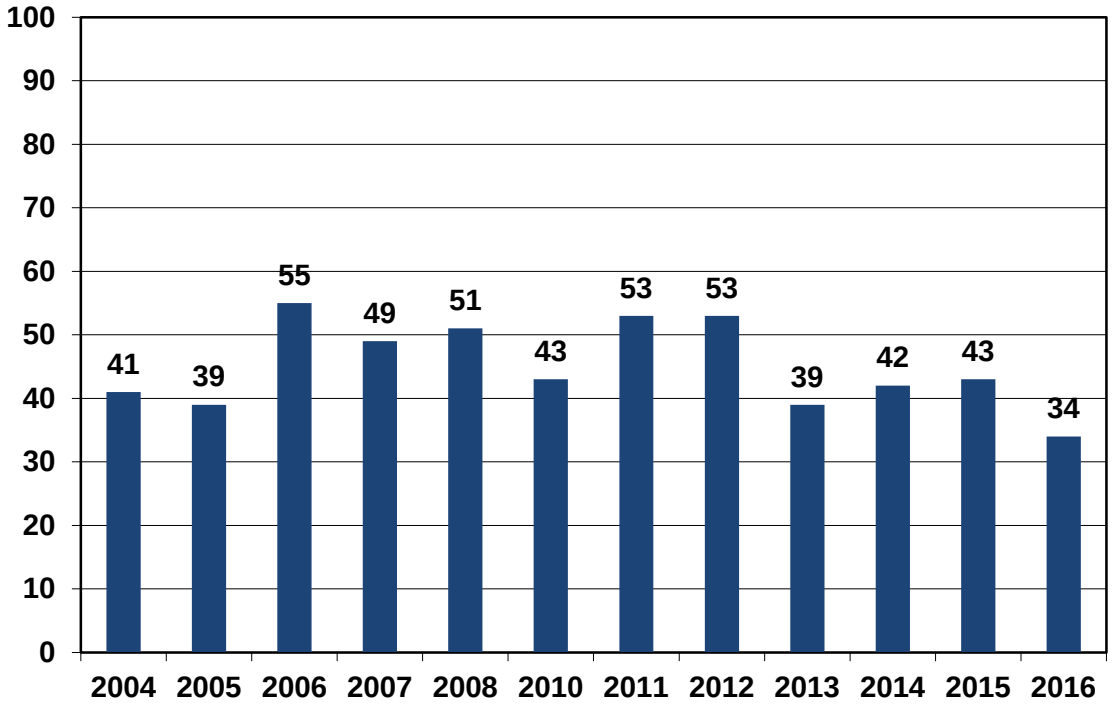
CSO Magazine, USSS, CERT Division, & Forcepoint

510 respondents

41% of organizations have 500 or more employees

59% of organizations have less than 500 employees

Percentage of Participants Who Experienced an Insider Incident



Source: 2017 U.S. State of Cybercrime Survey, in partnership with Forcepoint, CSO, U.S. Secret Service, and CERT Division of Software Engineering Institute at Carnegie Mellon University

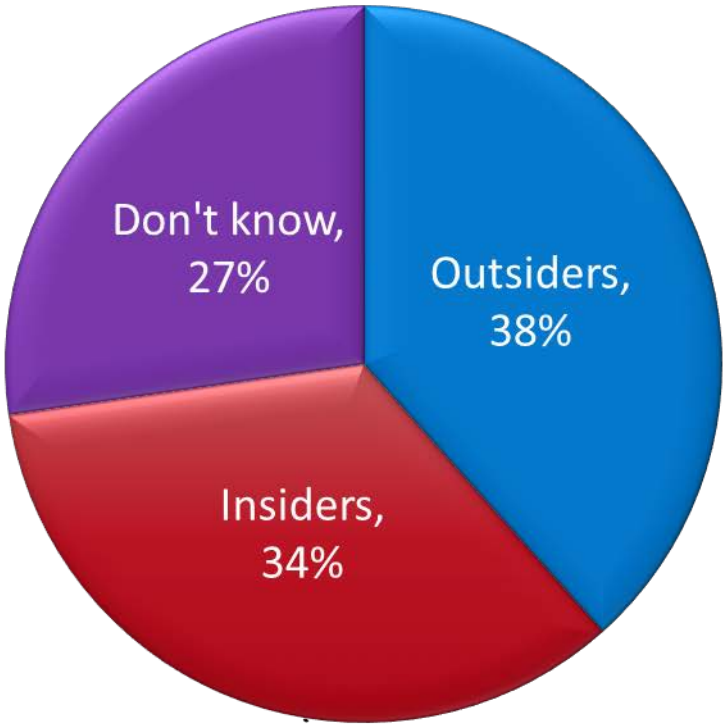
2017 U.S. State of Cybercrime Survey -2

29% of respondents	Incidents caused by insiders were more costly or damaging.
Insiders made up the highest percentage of the following incidents:	
Private or sensitive information unintentionally exposed Private or sensitive information intentionally exposed	45% 35%
Customer records compromised or stolen	40%
Employee records compromised or stolen	38%
Confidential records compromised or stolen	33%

Source: 2017 U.S. State of Cybercrime Survey, in partnership with Forcepoint, CSO, U.S. Secret Service, and CERT Division of Software Engineering Institute at Carnegie Mellon University

2017 U.S. State of Cybercrime Survey -3

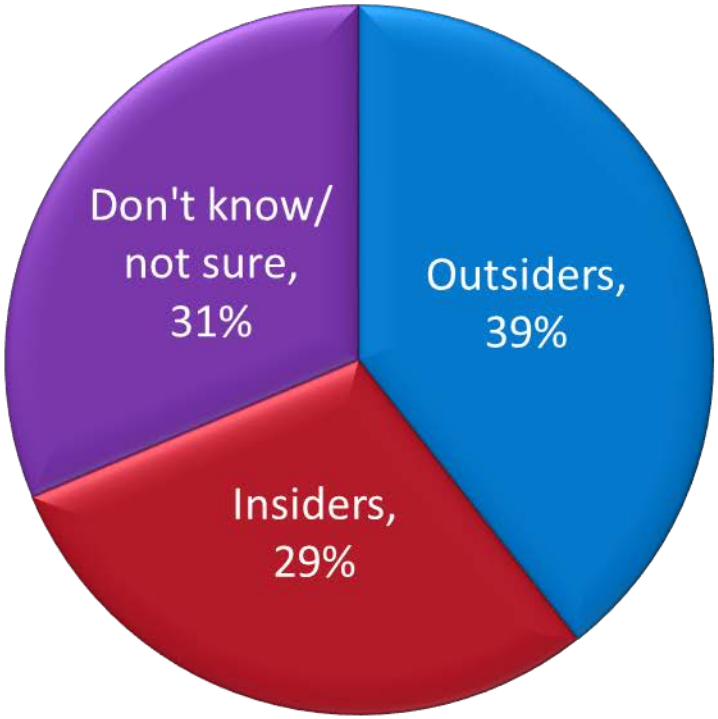
What percentage of the cyber security events (the past 12 months) are known or suspected to have been caused by



Source: 2017 U.S. State of Cybercrime Survey, in partnership with Forcepoint, CSO, U.S. Secret Service, and CERT Division of Software Engineering Institute at Carnegie Mellon University

2017 U.S. State of Cybercrime Survey -4

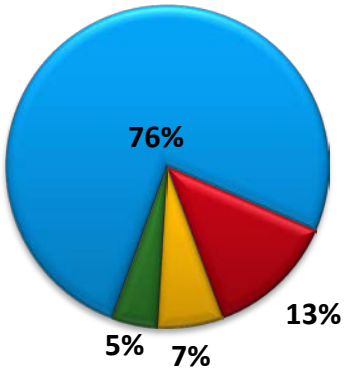
In general, cybercrimes were more costly or damaging to your organization when caused by



Source: 2017 U.S. State of Cybercrime Survey, in partnership with Forcepoint, CSO, U.S. Secret Service, and CERT Division of Software Engineering Institute at Carnegie Mellon University

2017 U.S. State of Cybercrime Survey -5

How Insider Incidents Are Handled



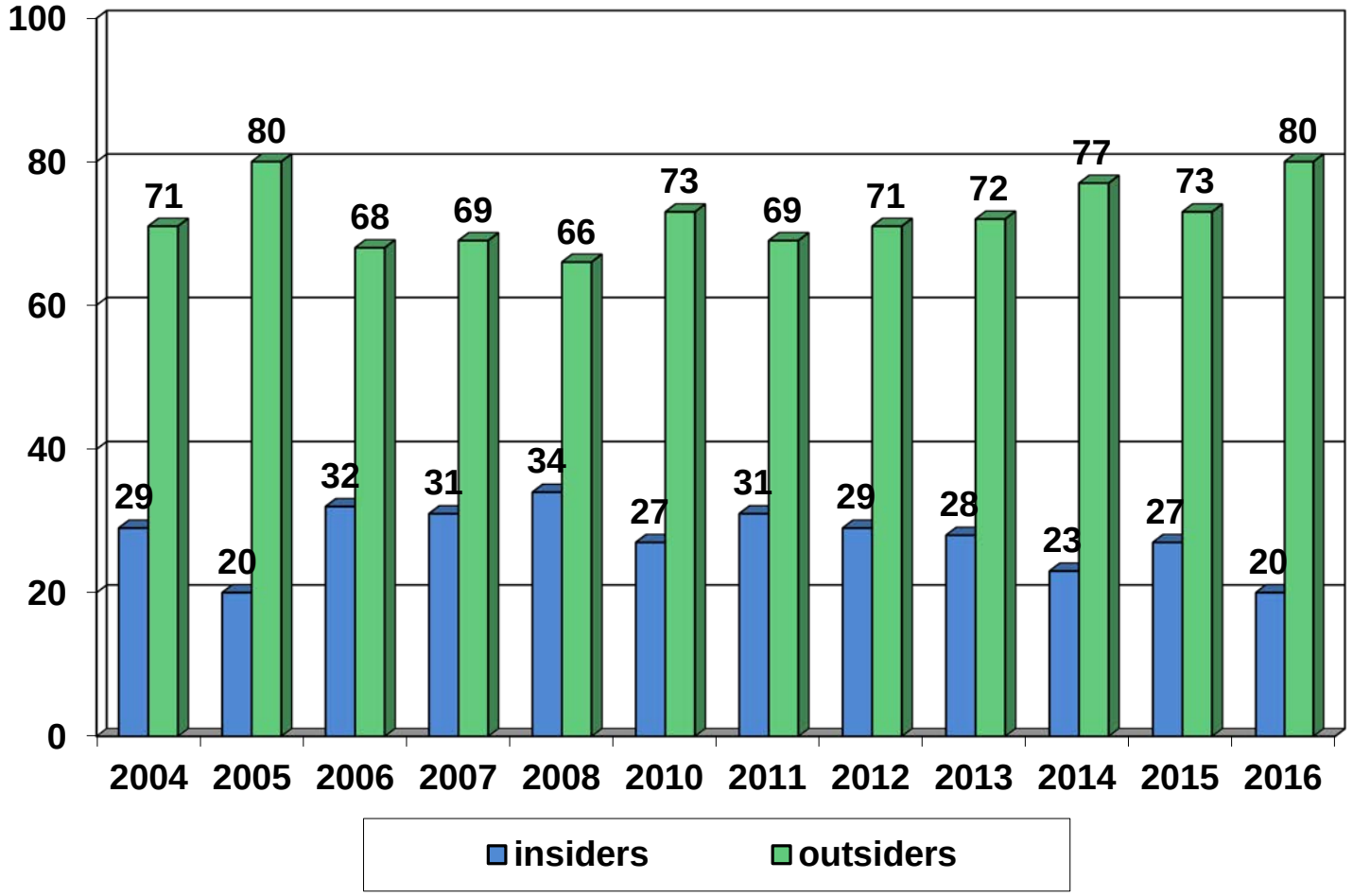
- Internally (without legal action or law enforcement)
- Internally (with legal action)
- Externally (notifying law enforcement)
- Externally (filing a civil action)

Reason(s) cybercrimes were not referred for legal action	2016	2015	2014	2013	2012
Damage level insufficient to warrant prosecution	40%	36%	36%	34%	36%
Could not identify the individual/ individuals responsible for committing the cybercrime	44%	31%	34%	37%	32%
Lack of evidence/not enough information to prosecute	32%	25%	34%	36%	36%
Concerns about negative publicity	7%	8%	13%	12%	9%
Concerns about liability	7%	7%	7%	8%	7%
Concerns that competitors would use incident to their advantage	5%	7%	7%	7%	6%
Unaware that we could report these crimes	5%	7%	6%	6%	5%
Other	8%	5%	6%	8%	12%
Prior negative response from law enforcement	4%	3%	5%	6%	5%
L.E. suggested incident was national security related	3%	3%	2%	3%	4%
Don't know	18%	28%	29%	21%	28%

Source: 2017 U.S. State of Cybercrime Survey, in partnership with Forcepoint, CSO, U.S. Secret Service, and CERT Division of Software Engineering Institute at Carnegie Mellon University

2017 U.S. State of Cybercrime Survey -6

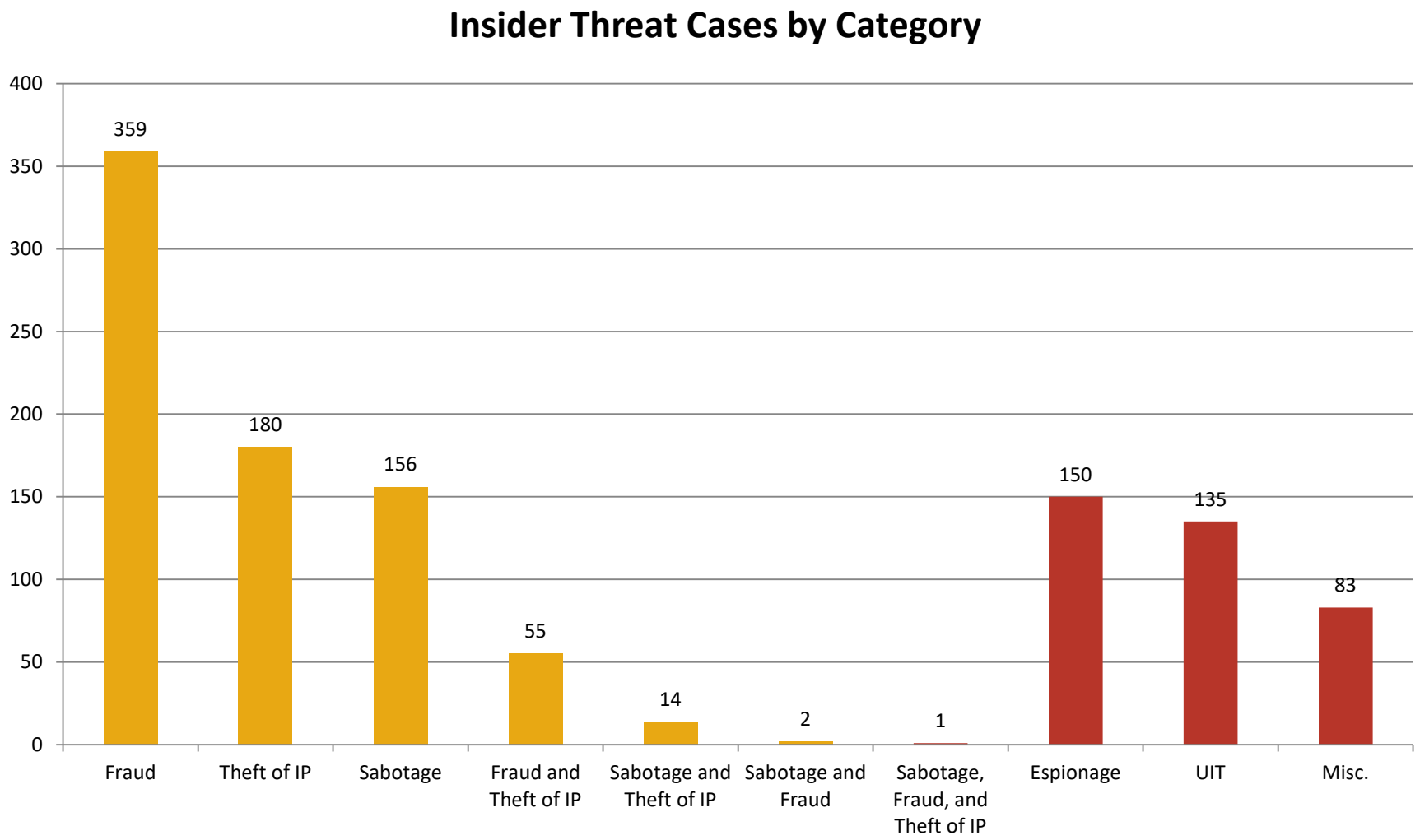
Percentage of insiders versus outsiders



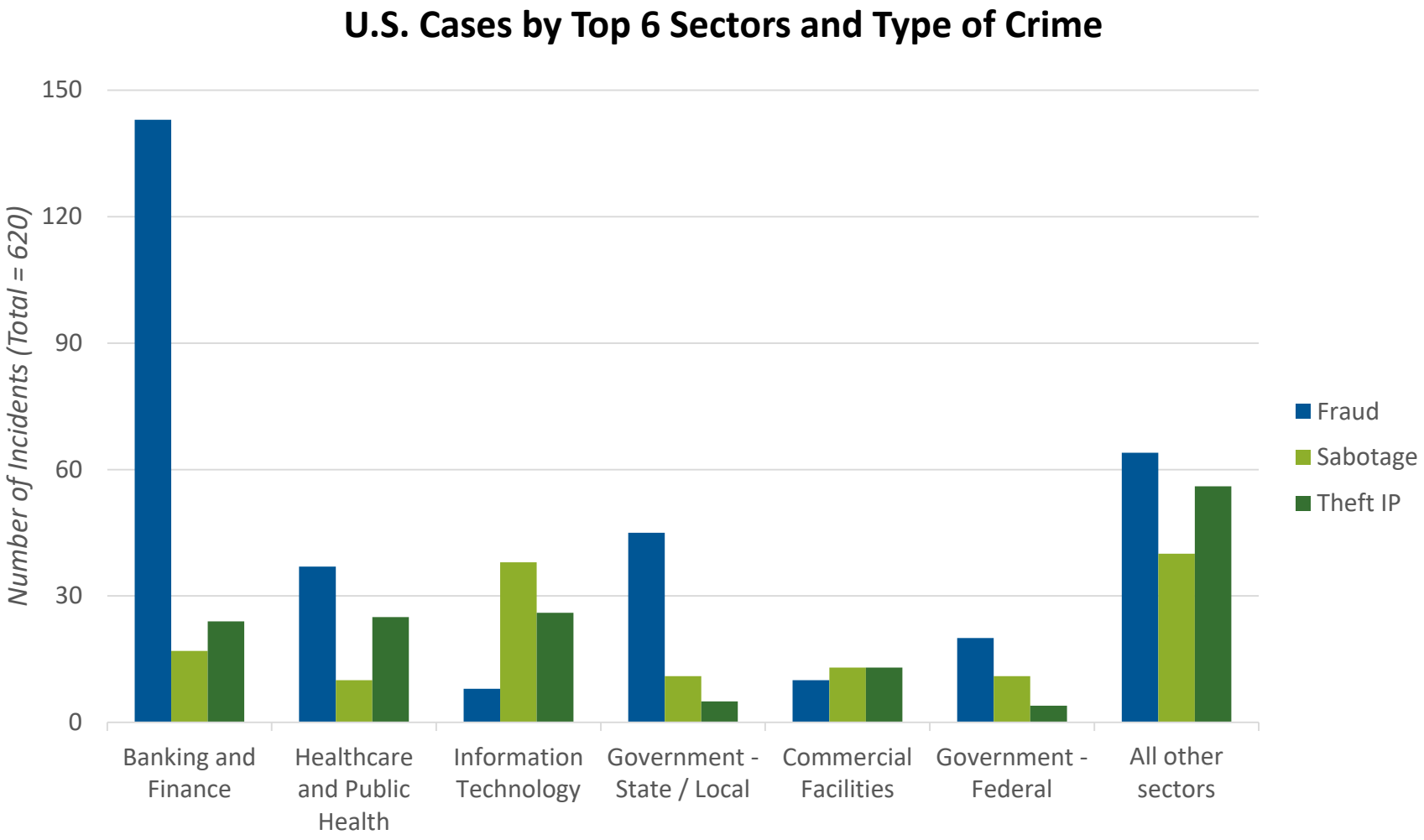
Source: 2017 U.S. State of Cybercrime Survey, in partnership with Forcepoint, CSO, U.S. Secret Service, and CERT Division of Software Engineering Institute at Carnegie Mellon University

NITC Research

NITC Insider Threat Incident Corpus

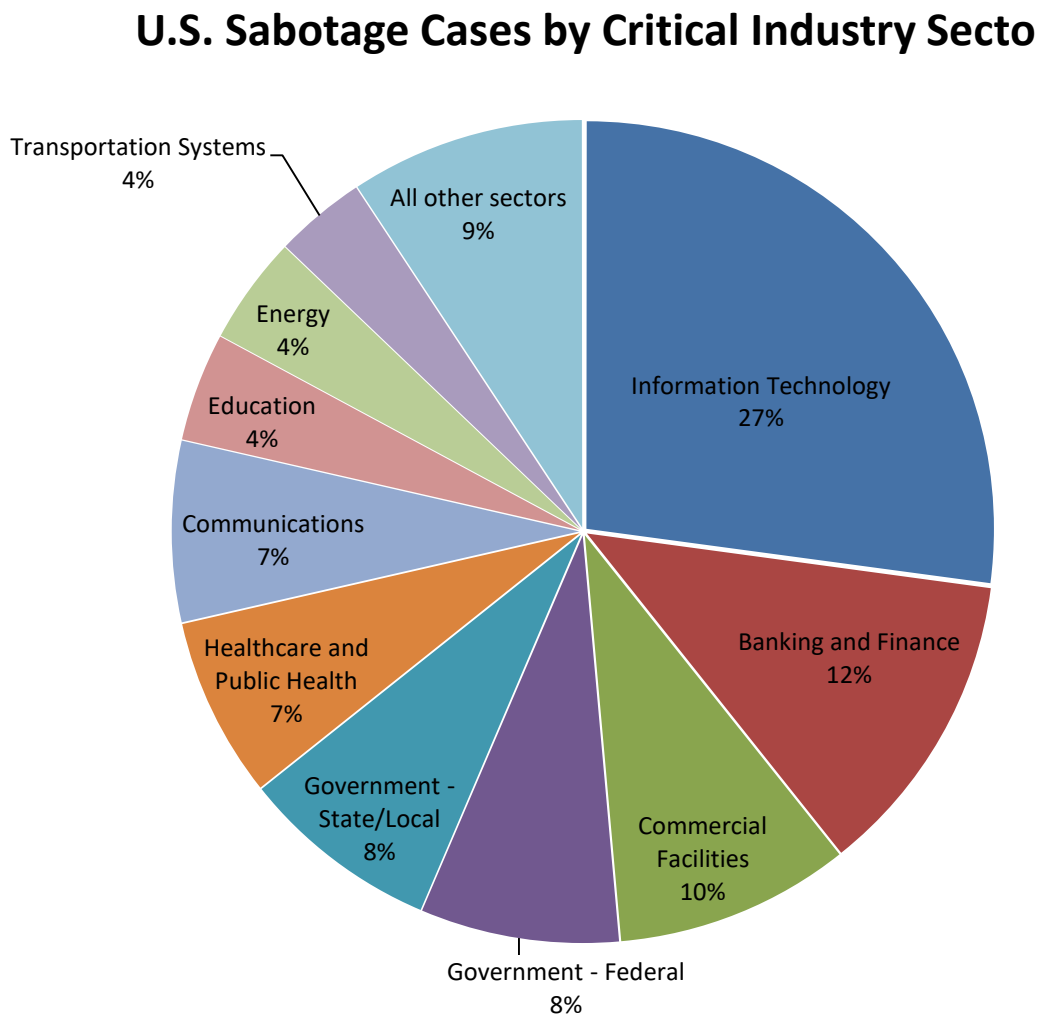


Critical Infrastructure Sectors



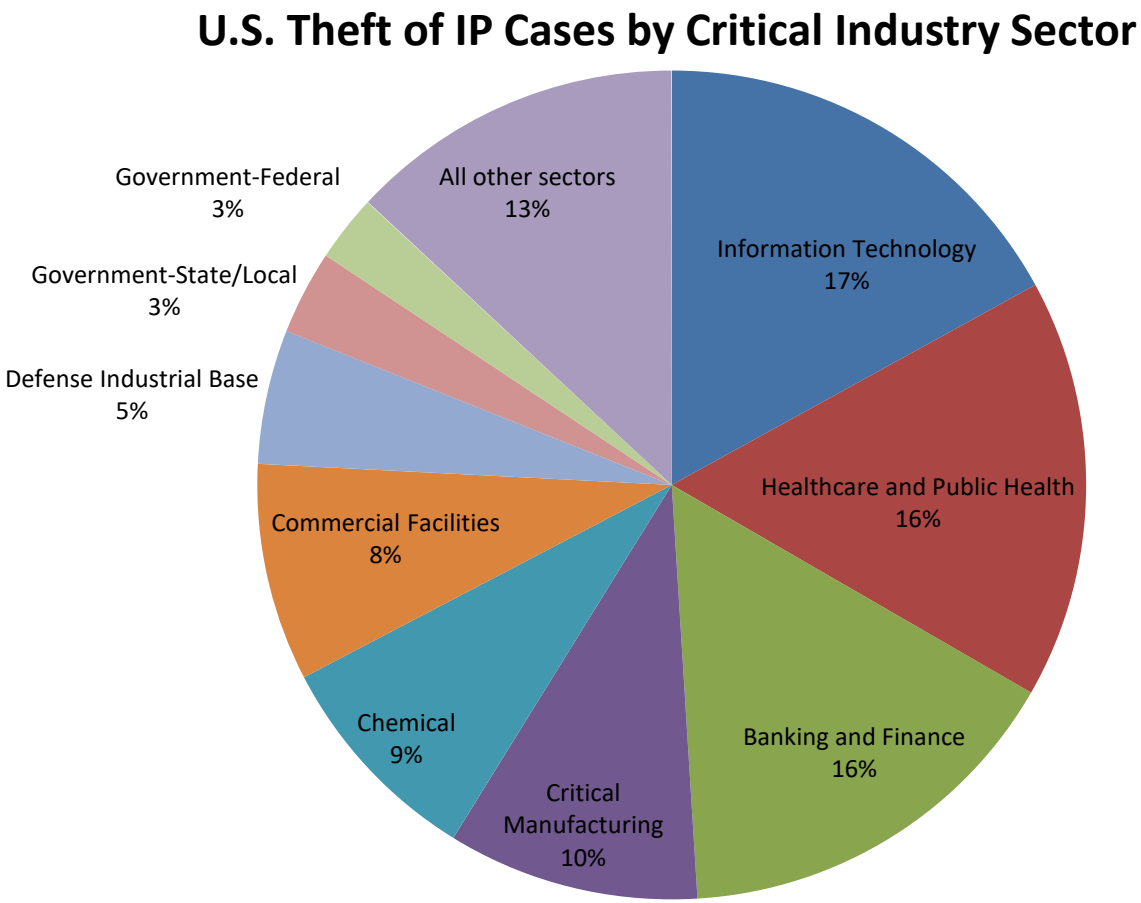
Note: Does not include incidents that involve multiple case types or espionage.

Critical Infrastructure Sectors – Sabotage



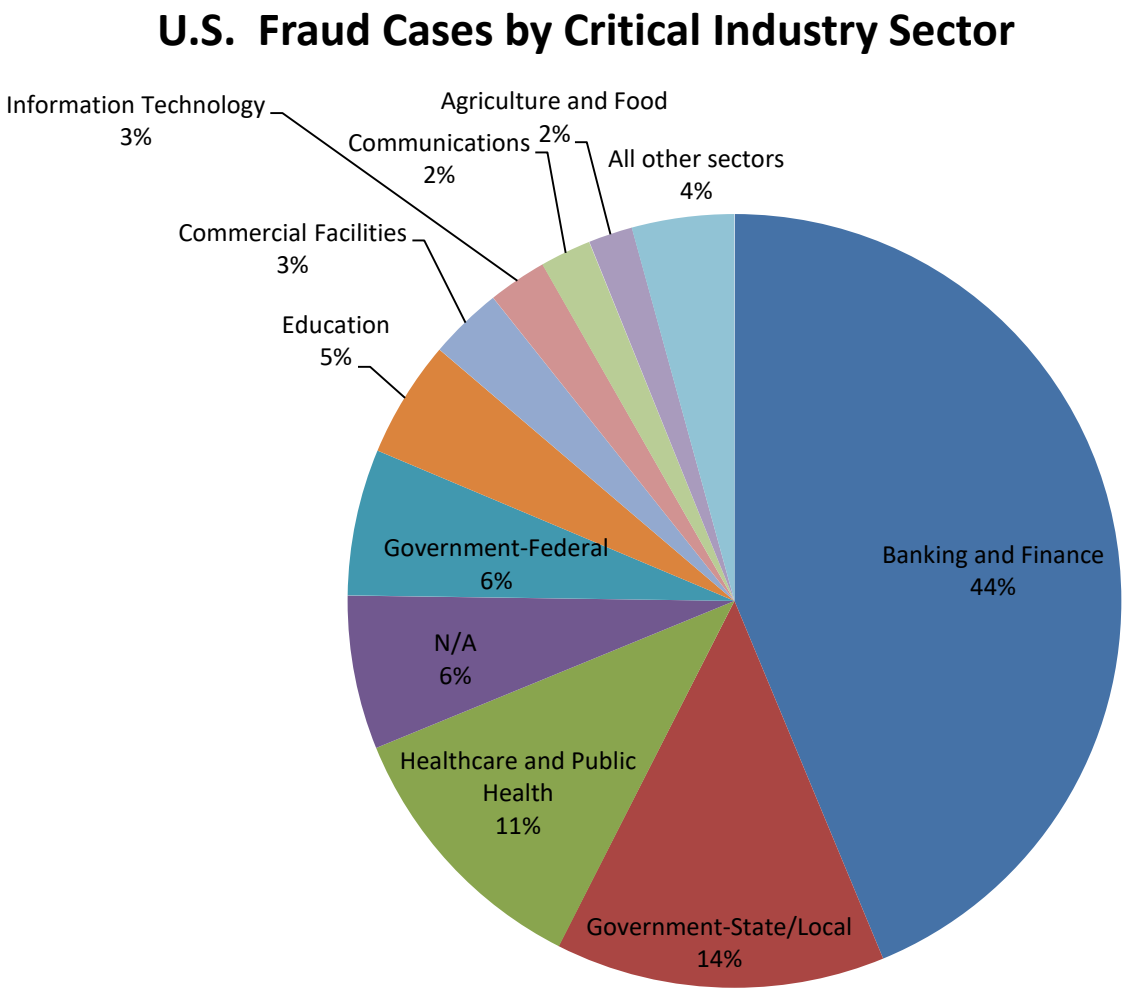
*** This does not include espionage cases involving classified information*

Critical Infrastructure Sectors – Theft of IP



*** This does not include espionage cases involving classified information*

Critical Infrastructure Sectors – Fraud



*** This does not include espionage cases involving classified information*

Insider Threat Model Components

Why is understanding insider threat model components important?

To smartly select proper security controls!

Consider your possible threat scenarios (fraud, theft of IP, sabotage, etc.)

Decompose the threat scenarios into their component parts

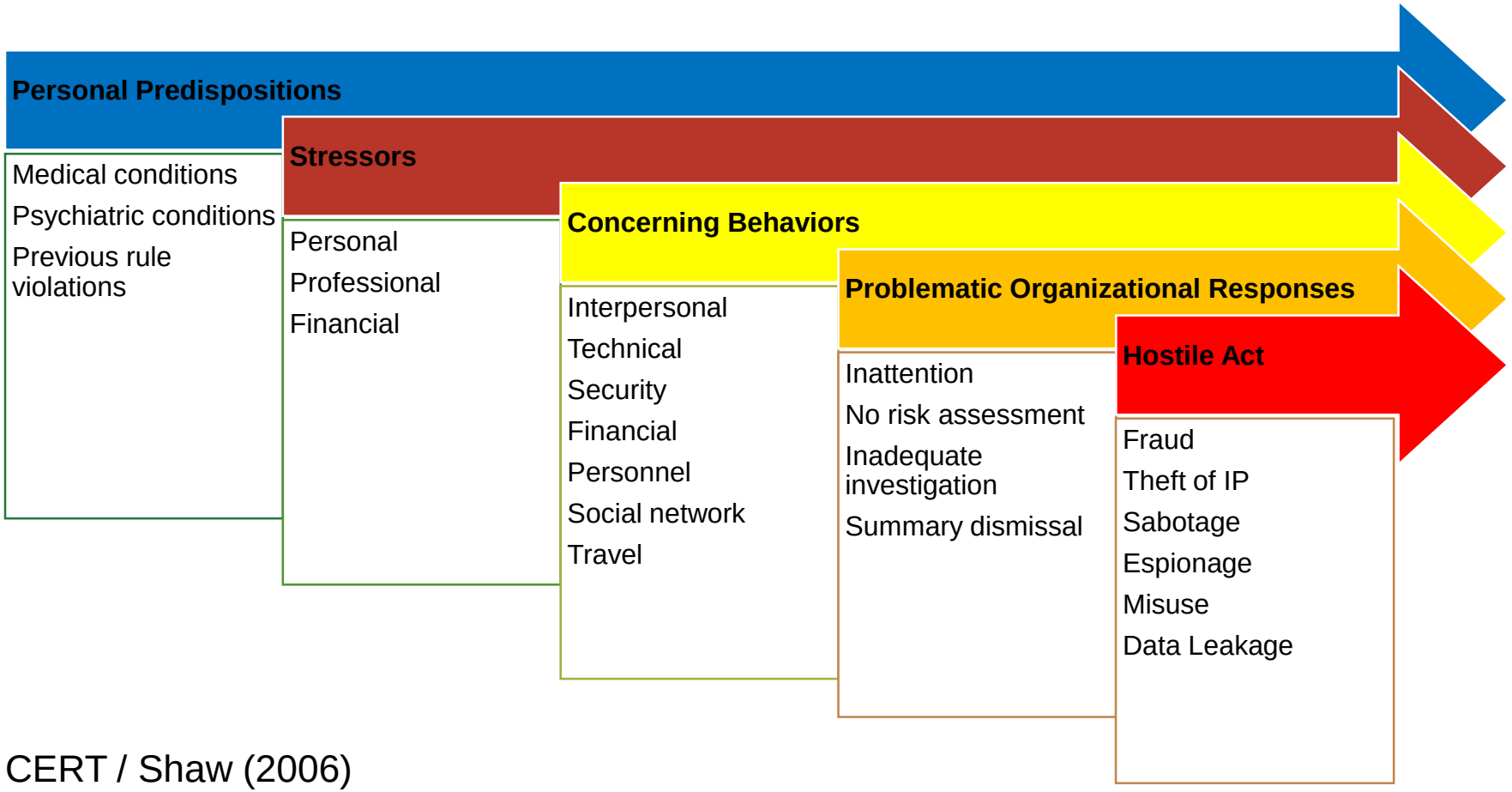
- Models can help here

Map threat scenario components to observables

Map observables to controls

- Select controls of varying functions (preventative, detective, corrective, deterrent, etc.) for a defense-in-depth strategy

Critical Path to Insider Risk



CERT / Shaw (2006)

Types of Insider Activities -1

IT Sabotage

- An insider's use of IT to direct specific harm at an organization or an individual
  - Deletion of information
  - Bringing down systems
  - Web site defacement to embarrass organization

Theft of Intellectual Property

- An insider's use of IT to steal intellectual property from the organization
  - This category includes industrial espionage involving insiders.
    - Proprietary engineering designs, scientific formulas, etc.
    - Proprietary source code
    - Confidential customer information
    - Industrial Espionage

Types of Insider Activities -2

Fraud

- An insider’s use of IT for the unauthorized modification, addition, or deletion of an organization's data (not programs or systems) for personal gain, or theft of information that leads to fraud (identity theft, credit card fraud)
- Theft and sale of confidential information (SSN, credit card numbers, etc.)
- Modification of critical data for pay (driver’s license records, criminal records, welfare status, etc.)

Unintentional Insider Threat

- An insider whose actions or lack of action without malicious intent causes harm or the possibility of harm

Types of Insider Activities -3

National Security Insider Espionage

- The act of communicating, delivering or transmitting information pertaining to the national defense of the United States to any foreign government or faction, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation

Miscellaneous

- Unauthorized disclosure of information insider believed should be in the public domain
- Query of database to find address of person – information provided to acquaintance who physically harmed individual
- Query of high-profile individuals to access personal information
- Unauthorized access to co-worker's emails

3 Most Common Models

IT Sabotage

IP Theft

Fraud

IT Sabotage

TRUE STORY: *IT Sabotage*

SCADA sabotage releases 800,000 liters raw sewage

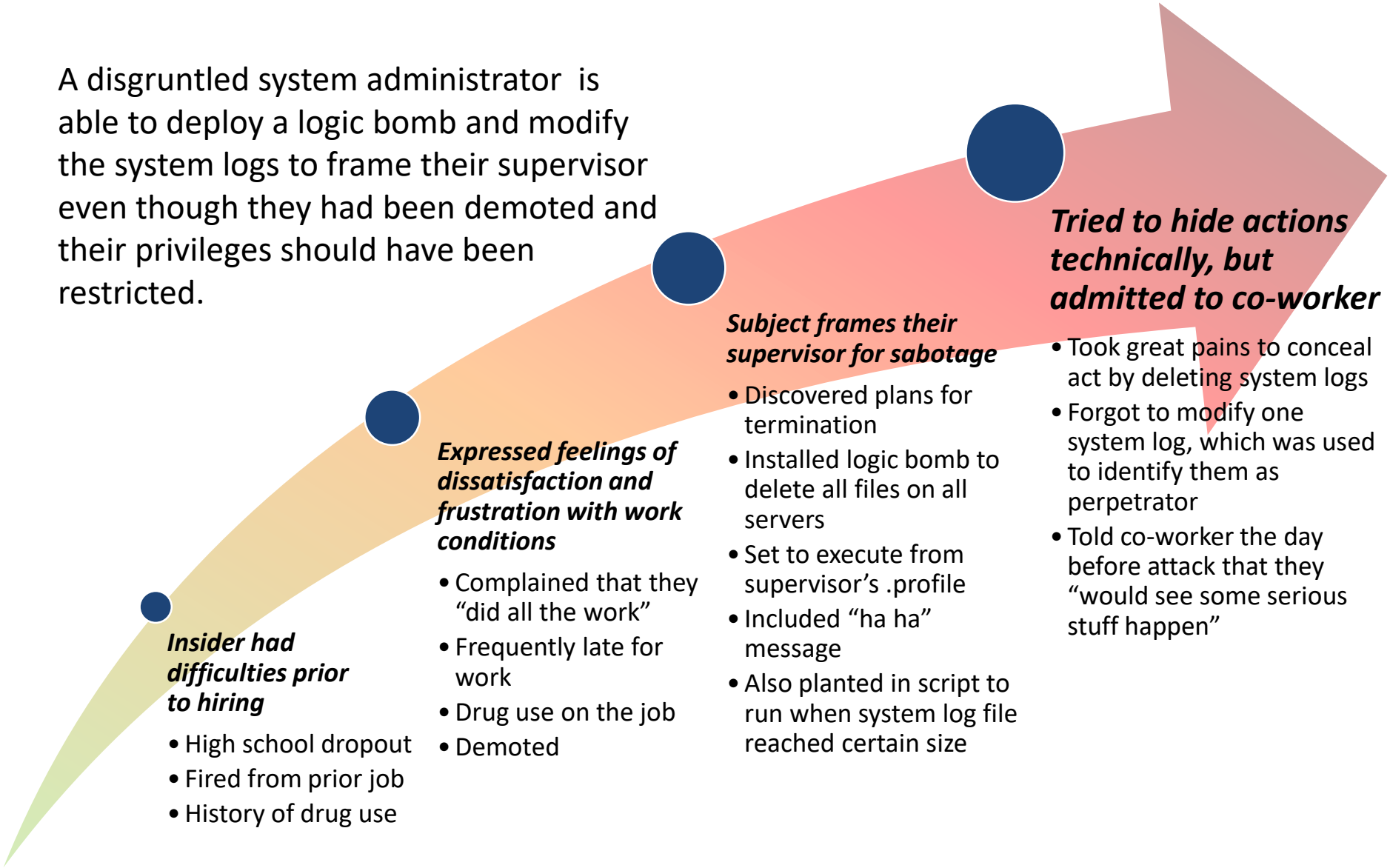
TRUE STORY: *IT Sabotage*

911 services disrupted for 4 major cities

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

Insider IT Sabotage Example

A disgruntled system administrator is able to deploy a logic bomb and modify the system logs to frame their supervisor even though they had been demoted and their privileges should have been restricted.



Insider had difficulties prior to hiring

- High school dropout
- Fired from prior job
- History of drug use

Expressed feelings of dissatisfaction and frustration with work conditions

- Complained that they "did all the work"
- Frequently late for work
- Drug use on the job
- Demoted

Subject frames their supervisor for sabotage

- Discovered plans for termination
- Installed logic bomb to delete all files on all servers
- Set to execute from supervisor's .profile
- Included "ha ha" message
- Also planted in script to run when system log file reached certain size

Tried to hide actions technically, but admitted to co-worker

- Took great pains to conceal act by deleting system logs
- Forgot to modify one system log, which was used to identify them as perpetrator
- Told co-worker the day before attack that they "would see some serious stuff happen"

The IT Sabotage M.O.

Attack Metrics	
Target(s)	Systems, servers, and networks
Method(s)	Malicious code or modification / deletion of code
Location	Typically remotely
Time	Outside of normal working hours
Impact	Average between $800,000 and $1 Million
Average Length	Over 1/3 of incidents took place over 24hrs or less

Observations from Insider Threat IT Sabotage Cases -1

Most insiders had personal predispositions that contributed to their risk of committing malicious acts.

Most insiders' disgruntlement is due to unmet expectations.

In most cases, stressors, including sanctions and precipitating events, contributed to the likelihood of insider IT sabotage.

Behavioral precursors were often observable in insider IT sabotage cases but not appropriately mitigated by the organization.

Observations from Insider Threat IT Sabotage Cases -2

Insiders created or used access paths unknown to management to set up their attack and conceal their identity or actions.

The majority of saboteurs attacked after pending or completed termination.

In many cases, organizations failed to detect technical precursors.

Lack of physical and electronic access controls facilitated IT sabotage.

Mapping IT Sabotage Model Components to Observables

Model Component	Associated Observables
Personal Predispositions	Co-worker conflicts
	History of policy / rule violations
	Aggressive, angry or violent behavior
Unmet Expectations	Being passed over for a promotion
	Being demoted or transferred
	Issues with supervisor
	Disagreement over salary and compensation
Behavioral Precursors	Co-worker or supervisor conflicts
	Sudden decline in work performance or attendance
	Aggressive, violent, or angry behavior
	Substance abuse

Model Component	Associated Observables
Technical Precursors	Creating backdoor, shared, non-attributable, or unauthorized accounts
	Disabling or attempting to disable security controls
	Downloading and installing malicious code and / or hacking tools
Concealment	Using backdoor, shared, non-attributable, or unauthorized accounts
	Modifying or deleting logs or backups
	Failing to record physical access
Hostile Act	Modification / deletion of critical data
	Denial of service attack
	Physical attack to equipment
	Inserting malicious code into system

Mapping IT Sabotage Observables to Controls - 1

Observable	Associated Control	Control Type
Co-worker conflicts	Human Resource Management System	Detective
	Anonymous / Confidential Reporting System	Detective
History of policy / rule violations	Human Resource Management System	Detective
	Background Checks	Detective
Aggressive, angry or violent behavior	Anonymous / Confidential Reporting System	Detective
Being passed over for a promotion	Human Resource Management System	Detective
Being demoted or transferred	Human Resource Management System	Detective
Issues with supervisor	Human Resource Management System	Detective
Disagreement over salary and compensation	Human Resource Management System	Detective

Mapping IT Sabotage Observables to Controls - 2

Observable	Associated Control	Control Type
Sudden decline in work performance or attendance	Employee Performance Management System	Detective
	Sanctions	Corrective
Aggressive, violent, or angry behavior	Anonymous / Confidential Reporting System	Detective
Substance abuse	Human Resource Management System	Detective
Creating backdoor, shared, non-attributable, or unauthorized accounts	Host-based audit logs	Detective
Tampering with, disabling, or attempting to disable security controls	Host-based audit logs	Detective
Downloading and installing malicious code and / or hacking tools	Application blacklisting / whitelisting	Preventative
	Host-based audit logs	Detective

Mapping IT Sabotage Observables to Controls - 3

Observable	Associated Control	Control Type
Using backdoor, shared, non-attributable, or unauthorized accounts	Host-based audit logs	Detective
	Authentication server logs	Detective
Modifying or deleting logs or backups	Host-based audit logs	Detective
Failing to record physical access	Badging system logs	Detective
Modification / deletion of critical data	Change and configuration management systems	Detective
	Backup systems	Recovery
Denial of service attack	Server logs	Detective
Physical attack to equipment	Locks	Preventative
	Cameras	Detective
Insertion of malicious code into operational system	Change and configuration management systems	Detective

IP Theft

TRUE STORY: *Theft of IP*

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

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

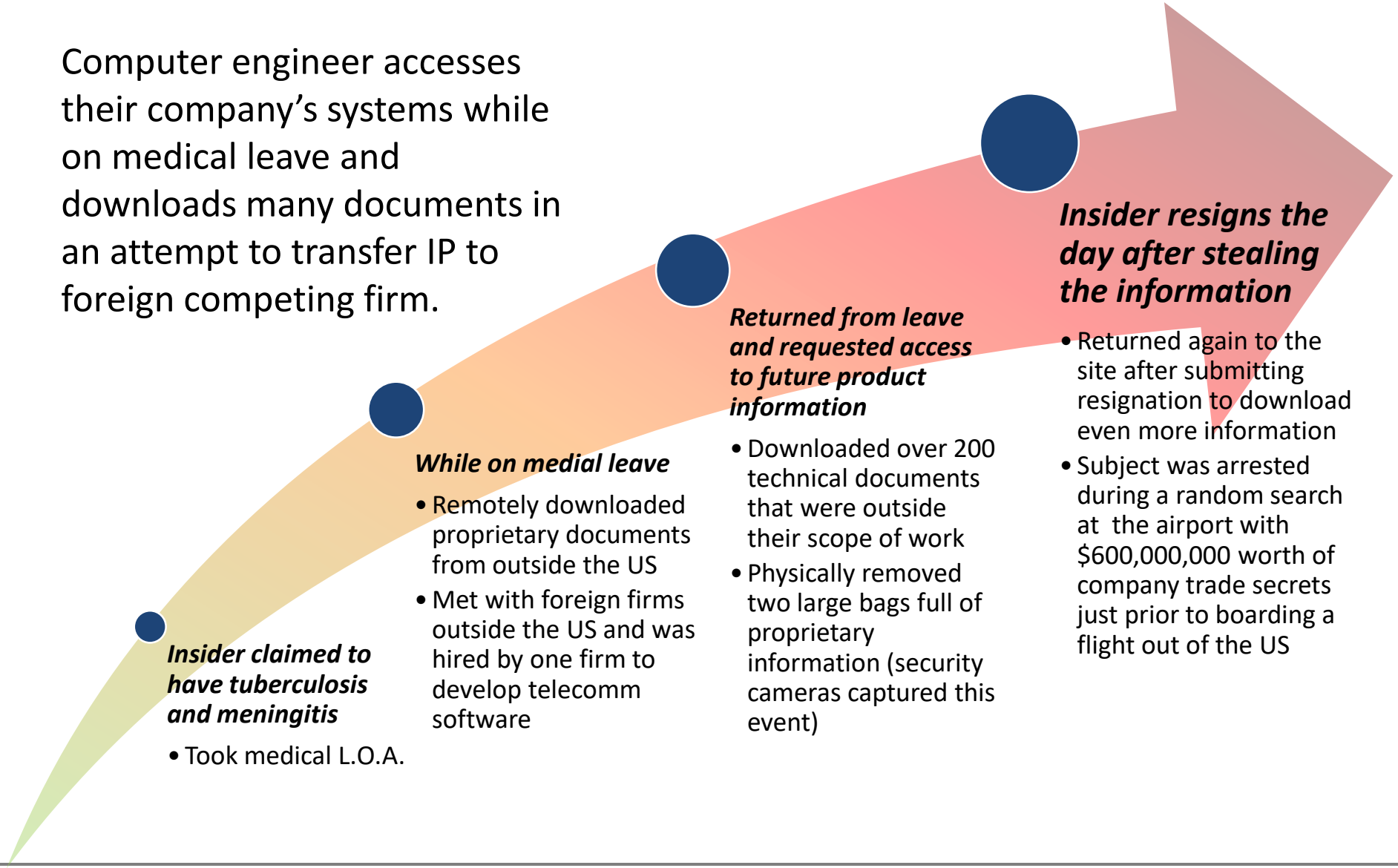
TRUE STORY: *Theft of IP*

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

Information was valued at $400 Million.

Insider Theft of IP Example

Computer engineer accesses their company's systems while on medical leave and downloads many documents in an attempt to transfer IP to foreign competing firm.



Insider claimed to have tuberculosis and meningitis

- Took medical L.O.A.

While on medial leave

- Remotely downloaded proprietary documents from outside the US
- Met with foreign firms outside the US and was hired by one firm to develop telecomm software

Returned from leave and requested access to future product information

- Downloaded over 200 technical documents that were outside their scope of work
- Physically removed two large bags full of proprietary information (security cameras captured this event)

Insider resigns the day after stealing the information

- Returned again to the site after submitting resignation to download even more information
- Subject was arrested during a random search at the airport with $600,000,000 worth of company trade secrets just prior to boarding a flight out of the US

The IP Theft M.O.

Attack Metrics	
Target(s)	Trade secrets, Source code, Internal information, Customer information, Product information
Method(s)	Authorized access but unauthorized downloads
Location	On-site, but occasionally remotely
Time	During normal working hours
Average Length	15.3 months
Impact	Average impact between $9 Million and $30 Million

Theft of IP Precursors and Observations

Mergers & Acquisitions

Insider Demoted

Insider Terminated

Insider Resigned

Group Resignation

Insider Forms New Competing Business

Insider Planning with / Went to Work for a Competitor

Insider Seeking New Employment

Unauthorized Downloads

HR Violations or Complaints

Suspicious Foreign Travel and/or Contacts

Insider Recruits / Attempts to Recruit Other Insiders

Mapping IP Theft Model Components to Observables

Model Component	Associated Observables
Personal Predispositions	History of policy / rule violations
	Sense of entitlement
Stress / Life Event	Mergers & Acquisitions
	Demotion
	Termination
	Competitor Proposal
Behavioral Precursors	Sense of Entitlement
	Insider Forms New Competing Business

Model Component	Associated Observables
Behavioral Precursors cnt.	Insider Planning with / went to work for a Competitor
	Insider Seeks New Employment
	HR Violations
Technical Precursors	Unauthorized downloads
Hostile Act	Theft of data

Mapping IT Sabotage Observables to Controls - 1

Observable	Associated Control	Control Type
History of policy / rule violations	Human Resource Management System	Detective
	Background Checks	Detective
Sense of entitlement	Human Resource Management System	Detective
Being passed over for a promotion	Human Resource Management System	Detective
Being demoted or transferred	Human Resource Management System	Detective
Issues with supervisor	Human Resource Management System	Detective
Disagreement over salary and compensation	Human Resource Management System	Detective

Mapping IT Sabotage Observables to Controls - 2

Observable	Associated Control	Control Type
Sudden decline in work performance or attendance	Employee Performance Management System	Detective
	Sanctions	Corrective
Aggressive, violent, or angry behavior	Anonymous / Confidential Reporting System	Detective
Substance abuse	Human Resource Management System	Detective
Creating backdoor, shared, non-attributable, or unauthorized accounts	Host-based audit logs	Detective
Tampering with, disabling, or attempting to disable security controls	Host-based audit logs	Detective
Downloading and installing malicious code and / or hacking tools	Application blacklisting / whitelisting	Preventative
	Host-based audit logs	Detective

Mapping IT Sabotage Observables to Controls - 3

Observable	Associated Control	Control Type
Using backdoor, shared, non-attributable, or unauthorized accounts	Host-based audit logs	Detective
	Authentication server logs	Detective
Modifying or deleting logs or backups	Host-based audit logs	Detective
Failing to record physical access	Badging system logs	Detective
Modification / deletion of critical data	Change and configuration management systems	Detective
	Backup systems	Recovery
Denial of service attack	Server logs	Detective
Physical attack to equipment	Locks	Preventative
	Cameras	Detective
Insertion of malicious code into operational system	Change and configuration management systems	Detective

Fraud

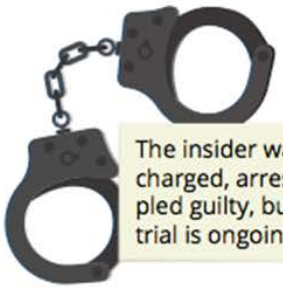
ACTUAL CASE
Employee steals money from cash drawer through No-Sale After Void Scheme…

The insider was a full-time employee of the victim organization, a postal service.

Over the course of about 2 years, the insider engaged in the practice of unlawfully and knowingly converting victim organization funds for personal use through a "No-Sale After Void" scheme.

The insider intentionally voided cash transaction sales of victim organization stamps to customers so that the system would not account for funds paid by customers for stamps.

The insider then performed a "No Sale" transaction which caused the cash drawer to open, whereupon the insider took the cash paid by the customers for personal use.



The insider was charged, arrested, and pled guilty, but the trial is ongoing.

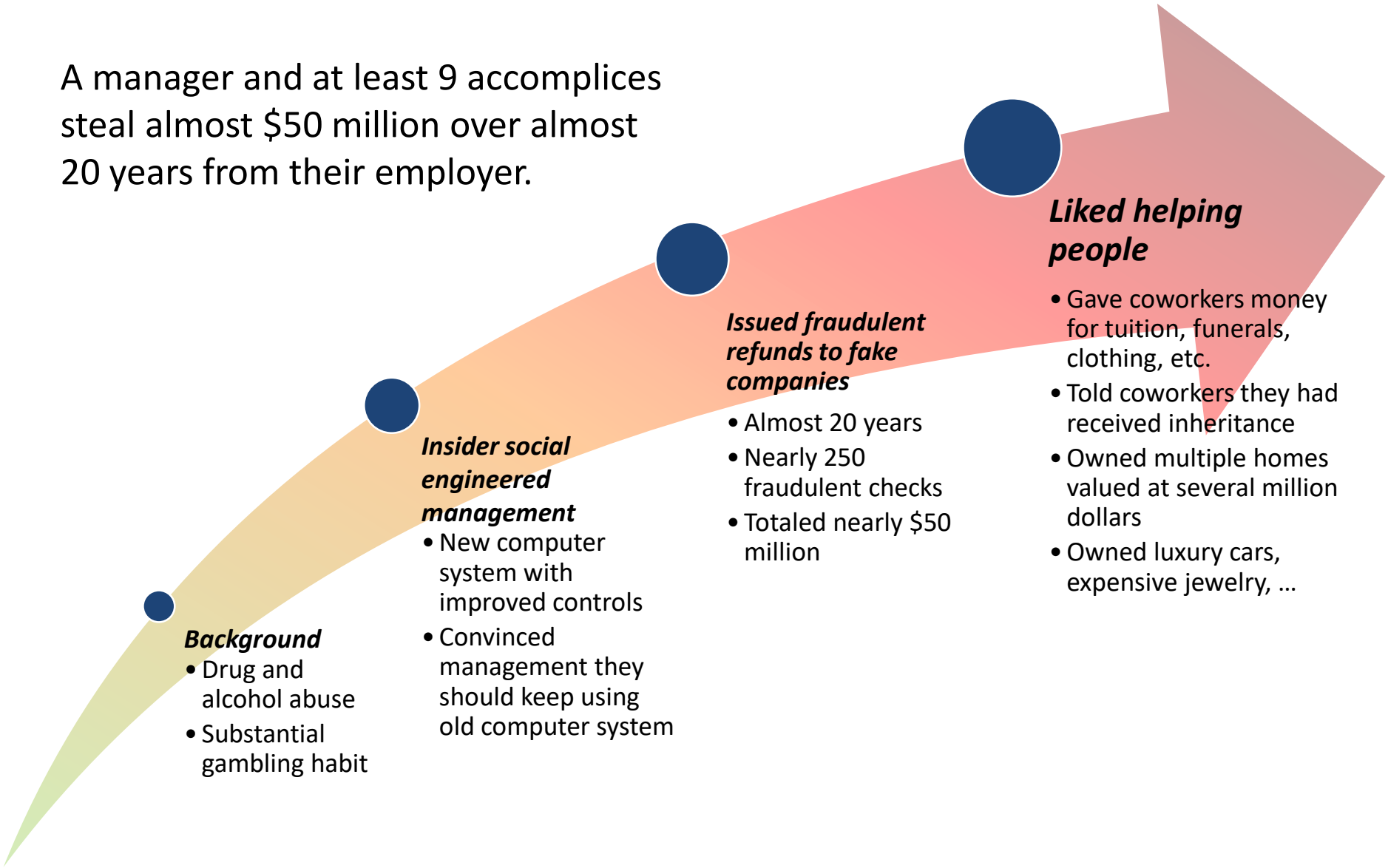
TRUE STORY: *Fraud*

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 Fraud Example

A manager and at least 9 accomplices steal almost $50 million over almost 20 years from their 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, …

The Fraud M.O.

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	21.9 months
Impact	Average between $4.5 Million and $6 Million

Mapping Fraud Model Components to Observables

Model Component	Associated Observables
Personal Predispositions	History of financial difficulties
	Substance abuse
	Previous arrests/convictions
	Gambling problems
Stress / Life Event	Emerging financial difficulties
	Mergers and acquisitions
Behavioral Precursors	Unexplained wealth
	Financial conflict of interest

Model Component	Associated Observables
Technical Precursors	Privileged Access Abuse
	Created / used fraudulent assets
	Created / used an alias
	Modified critical data
	Used compromised account
	Used unattended, unsecured workstation
Hostile Act	Theft of data

Mapping IT Sabotage Observables to Controls - 1

Observable	Associated Control	Control Type
History of Financial Difficulties	Credit Check	Detective
	Background Check	Detective
Substance Abuse	Drug Screen	Detective
	Background Check	Detective
	Human Resource Management System	
Previous Arrest/Conviction	Background Check	Detective
Gambling Problems	Background Check	Detective
Emerging Financial Difficulties	Credit Check	Detective
Mergers and Acquisitions	HR	Detective
Unexplained Wealth	Credit Check	Detective

Mapping IT Sabotage Observables to Controls - 2

Observable	Associated Control	Control Type
Financial Conflict of Interest	Anonymous / Confidential Reporting	Detective
	Sanctions	Corrective
Privileged Access Abuse	Host-based Audit Logs	Detective
	Anonymous / Confidential Reporting	Detective
Creating backdoor, shared, non-attributable, or unauthorized accounts	Host-based audit logs	Detective
Tampering with, disabling, or attempting to disable security controls	Host-based audit logs	Detective
Downloading and installing malicious code and / or hacking tools	Application blacklisting / whitelisting	Preventative
	Host-based audit logs	Detective

Mapping IT Sabotage Observables to Controls - 3

Observable	Associated Control	Control Type
Using backdoor, shared, non-attributable, or unauthorized accounts	Host-based audit logs	Detective
	Authentication server logs	Detective
Modifying or deleting logs or backups	Host-based audit logs	Detective
Failing to record physical access	Badging system logs	Detective
Modification / deletion of critical data	Change and configuration management systems	Detective
	Backup systems	Recovery
Denial of service attack	Server logs	Detective
Physical attack to equipment	Locks	Preventative
	Cameras	Detective
Insertion of malicious code into operational system	Change and configuration management systems	Detective

Fraud Precursors and Observables

Falsified or omitted information

Family medical problems

Substance abuse

Gambling problems

Previous arrests / convictions

Recruitment by / of outsiders or other insiders

History of or emerging financial difficulties

Unexplained wealth

Financial conflict of interest / Employee side business

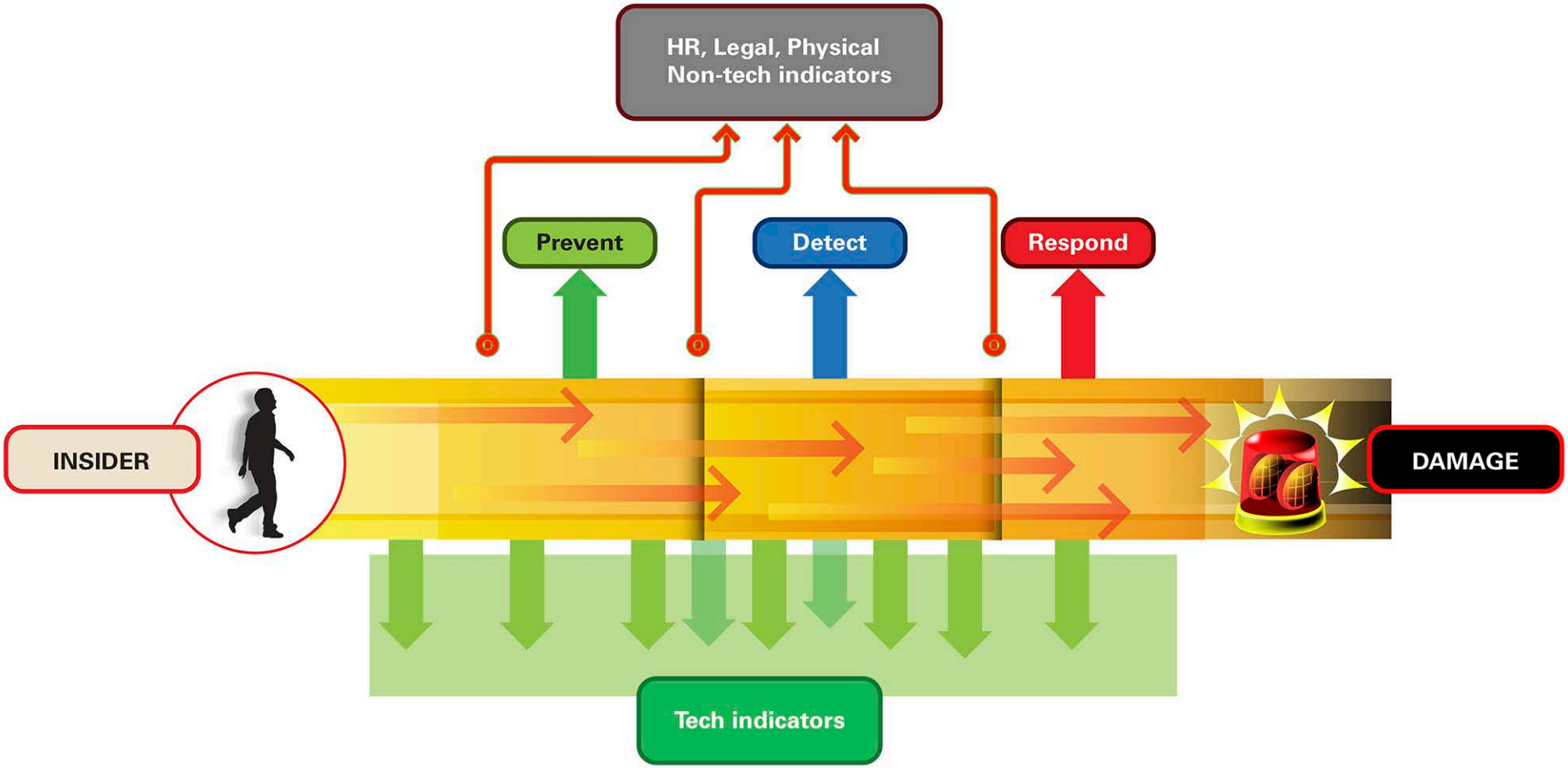
Mergers and acquisitions

Summary of Insider Incidents

	IT Sabotage	IP Theft	Fraud
Current or former Employee?	Former	Current (within 30 days of resignation)	Current
Type of position	Technical (e.g., sys admins, programmers, DBAs)	Technical (e.g., scientists, programmers, engineers) or sales	Non-technical (e.g., data entry, customer service) or their managers
Target	Network, systems, or data	IP (trade secrets) or Customer Information	PII 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

Mitigating the Insider Threat

Mitigating Insider Threat



Opportunities for Prevention, Detection, and Response for an Insider Attack

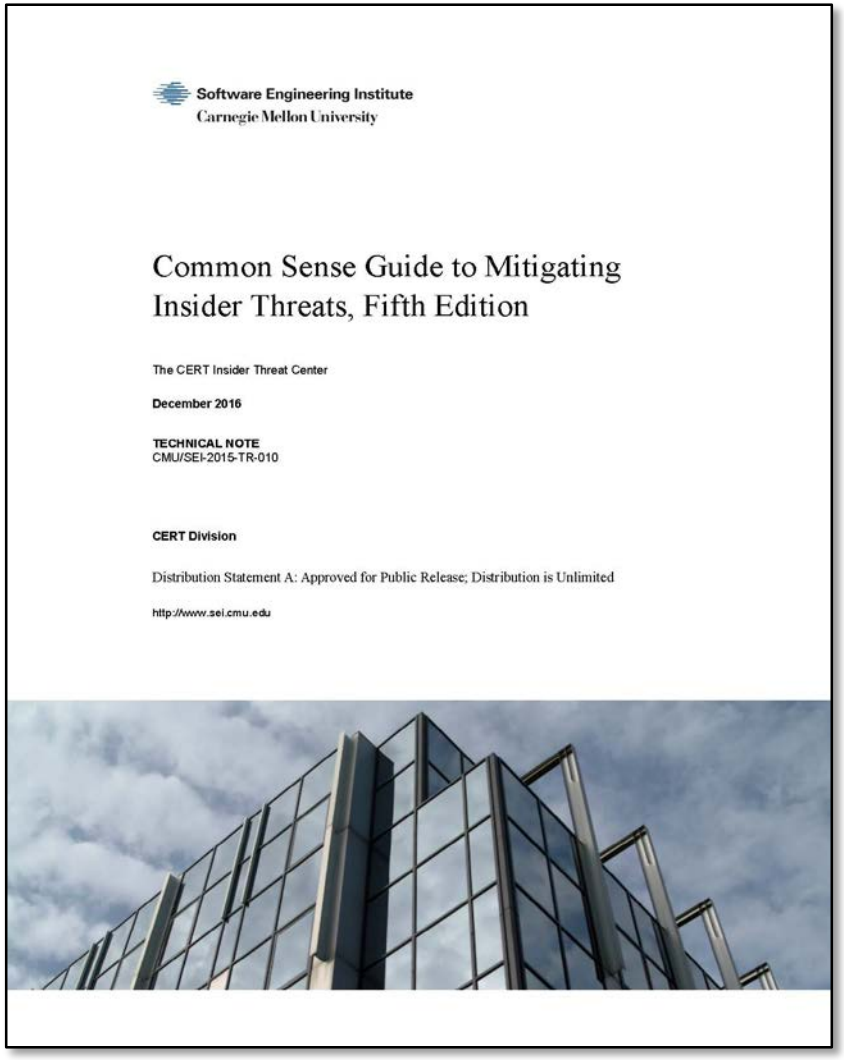
The Three Pillars of a Robust Strategy

Accurately Measure Trust

Right-Size Permissions

Conduct Effective Monitoring

Common Sense Guide (CSG), v5



Software Engineering Institute
Carnegie Mellon University

Common Sense Guide to Mitigating Insider Threats, Fifth Edition

The CERT Insider Threat Center

December 2016

TECHNICAL NOTE
CMU/SEI-2015-TR-010

CERT Division

Distribution Statement A: Approved for Public Release; Distribution is Unlimited

http://www.sei.cmu.edu

Common Sense Guide, v5

Recommendations are designed to aid in the development of detection, prevention, and response to aid in the mitigation of the insider threat

Recommendations are geared towards six groups

1. Human Resources
2. Legal
3. Physical Security
4. Data Owners
5. Information Technology
6. Software Engineering

CSG, new editions from v4

- Includes **fraud, IT sabotage, IP (intellectual property) theft, and espionage**
- New addition of **Unintentional Insider Threat**:
  - has or had authorized access to an organization's network, system, or data and
  - had no malicious intent associated with his or her action (or inaction) that caused harm or substantially increased the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems.
- Workplace violence is mentioned and may be included in next edition following continuing research
- Maps to security best practices in NIST controls, NITTF, Minimum Standards, CERT-RMM and ISO 27002

CSG, v5

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.

CERT's Common Sense Guide to Mitigating Insider Threats, Fifth Edition
http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=484738

CSG, v5

For each best practice, we note

- Challenges to implementation
- Quick wins & high impact solutions
- Corresponding security standards
- Relevant responsible unit
- Employee privacy considerations

CSG, Benefits

Executives and Decision Makers

- Provides familiarity with requirements and scope of InTh programs

Insider Threat program Managers

- Learn best practices and how to best engage them for insider threat prevention, detection, and response
- Way to effectively communicate with decision makers
- Utilize to build InTh program

Security Practitioners

- Gain understanding of best practices
- Ensure staff are following and fully implementing BPs

5 Best Practices for Small – Medium Sized Orgs

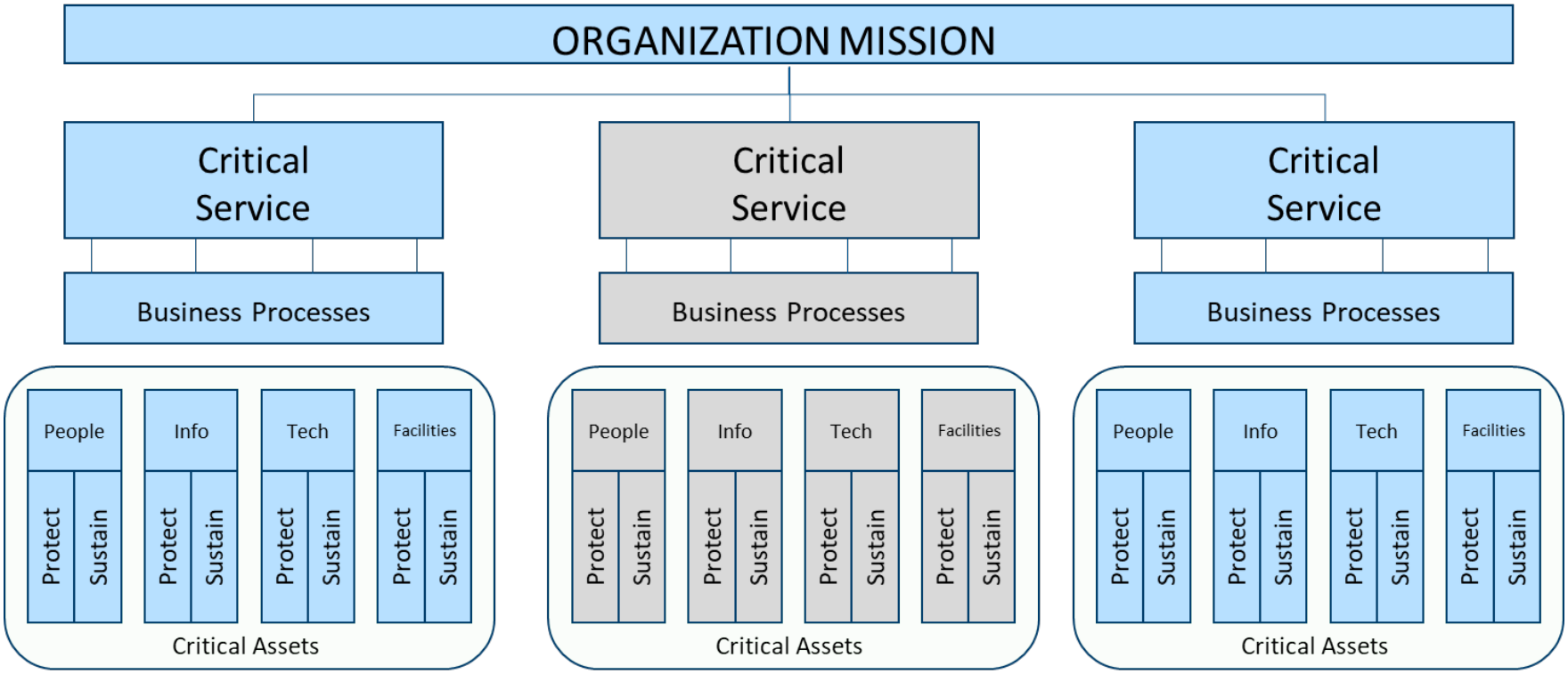
1 - Know and protect your critical assets.	11 - Institute stringent access controls and monitoring policies on privileged users.
2 - Develop a formalized insider threat program.	12 - Deploy solutions for monitoring employee actions and correlating information from multiple data sources.
3 - Clearly document 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.

CERT's Common Sense Guide to Mitigating Insider Threats, Fifth Edition
http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=484738

Best Practice 1

Know and protect your critical assets

Identifying Critical Assets



Identifying Critical Assets

Don’t guess! Get the right people involved

- Enterprise risk management
- Business process owners
- Executive leadership team
- Board of directors

Prioritize threats relative to potential impacts / priorities of your organization

- What’s more important: your organization’s reputation, or its intellectual property?
  - Who makes this call?

Best Practice 3

Clearly document, and consistently enforce policies and controls

Policies and Procedures for Insider Threat Mitigation

Reminder

Don’t forget your administrative controls!

- Policies, **procedures, documentation codify “normal” behavior - important for anomaly detection**

Exemplars

IT Acceptable Use Policy

Intellectual Property Policy

Data Handling and Classification Policy

Change Control and Configuration Management Policy

Employee Onboarding Procedures

Incident Response Plan

Disciplinary Action Procedures

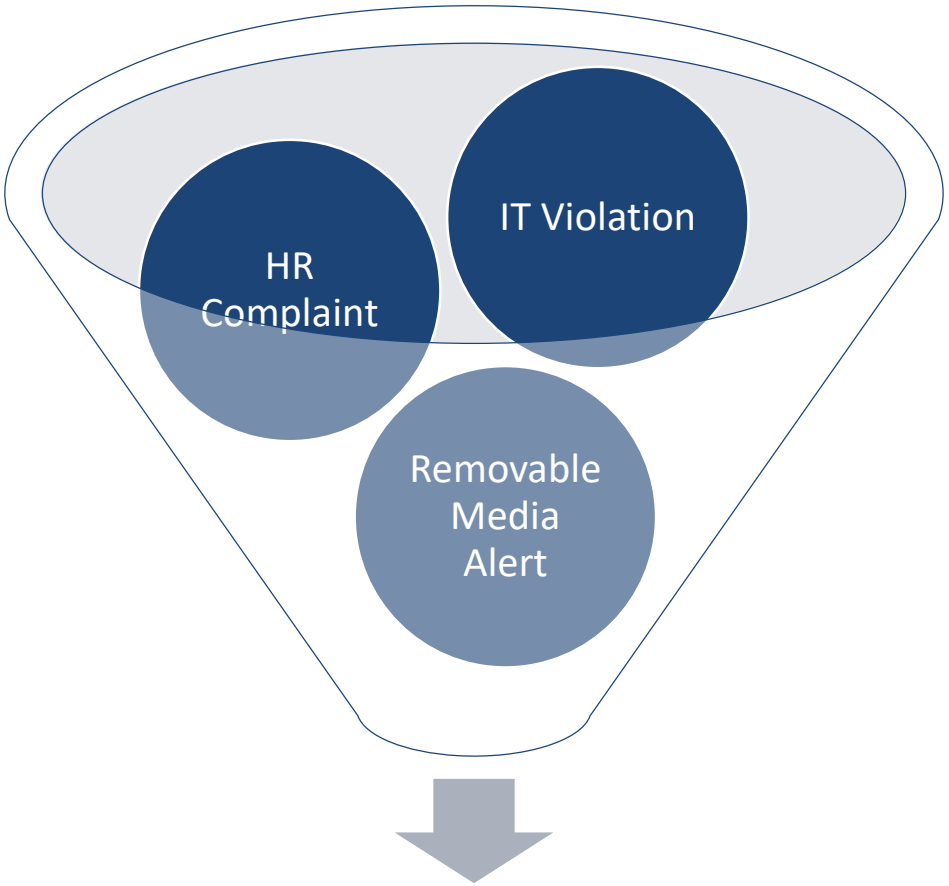
Employee Separation Handling

Trusted Business Partner Agreements

Best Practice 4

Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.

Monitor & Respond



Policies and Procedures for Insider Threat Mitigation

Acceptable Use Policy

Intellectual Property Policy

Data Handling and Classification Policy

Change Control and Configuration Management

Employee Onboarding

Incident Response Plan

Disciplinary Action

Employee Separation Handling

Trusted Business Partner Agreements

Best Practice 11

Institute stringent access controls and monitoring policies on privileged users

Best Practice 18

Implement secure backup and recovery processes

Refine and Refresh

Insider Threats are Dynamic

The threat landscape changes

- **Disruptive technologies**
- Organization-level events
  - Mergers, acquisitions, reductions in force, etc.
- Current events
- The workforce changes

Your organization's appetite for risk changes

Stuff breaks

- "Why isn't that data in the SIEM anymore?"

… So Your Mitigation Strategy Must Be Dynamic

Implement periodic:

- Re-assessments of the highest priority insider threats to your organization's critical assets
- Tests designed to measure the effectiveness of the deployed insider threat controls
- Improvements to deployed controls based on testing and feedback from insider threat program stakeholders

Final Thoughts

- Insider Threat Models vary – and so do the related components and mitigation strategies!
- 5 Best Practices for Small-Medium Sized Organizations
  1. Know Your Critical Assets
  2. Clearly Document and Consistently Enforce Policies and Controls
  3. Beginning with the Hiring Process, Monitor and Respond to Suspicious or Disruptive Behavior
  4. Insitute Stringent Access Controls and Monitoring Policies on Privileged Users
  5. Implement Secure Backup and Recovery Processes
- Your security posture should build-in a continuous evaluation improvement process

For More Information

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

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

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

Thank you!

Questions?

Contact Information

Carrie Gardner
Cyber Security Engineer
CERT National Insider Threat Center (NITC)
Telephone: +1 412.268.7903
Email: cgardner@cert.edu, cgardner@sei.cmu.edu

Website: http://www.cert.org/insider-threat/

National Insider Threat Services

Workshops

Insider Threat Analyst (new course!)

Insider Threat Program Evaluator

Insider Threat Program Manager

Insider Threat Vulnerability Assessor

Assessments

Insider Threat Program Evaluation (ITPE)

Insider Threat Vulnerability Assessment (ITVA)