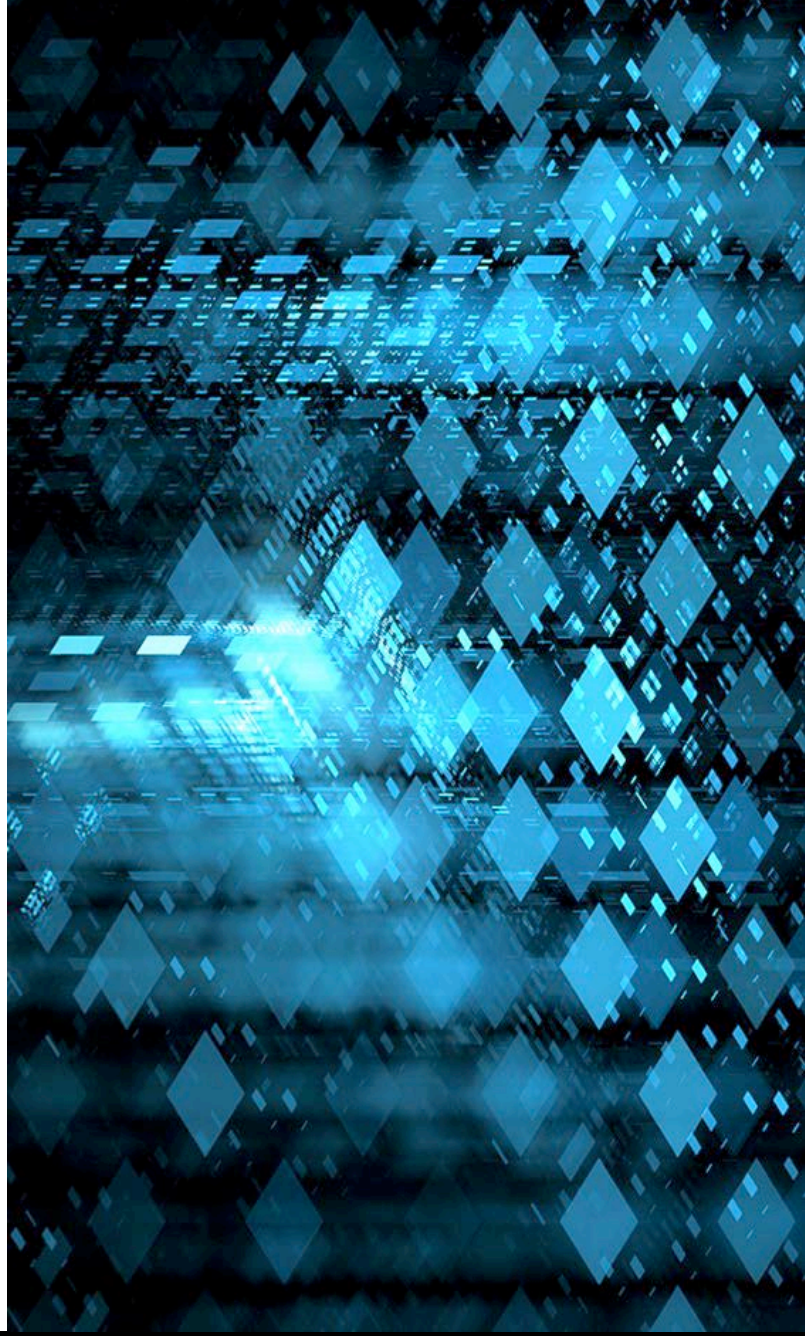
Insider Threat Overview: Preventing, Detecting and Responding to Insider Threats



Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Notices

This material is based upon work funded and supported by the Independent Agency 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 sponsored by the United States Department of Defense.

DM17-0926

Course Introduction

ACTUAL CASE
Federal employee sabotages employer's computers…

Disables account access, installs viruses & remote administration tools, runs personal website on federal computers, and deletes confidential personnel files

ACTUAL CASE
Employees create fraudulent drivers licenses that are used to commit $250,000 in fraud…

In addition, licenses are created for illegal immigrants who could not obtain them legally for $250-$500 per license.

Purpose of This Course

Through presentation of data, case examples, and best practices this course will

- Help you understand the threat posed by insiders
- Introduce you to insider threat terminology and concepts
- Help you be prepared to take steps to assess and mitigate the risk of insider threats

Intended Audience

The course intended audience includes but is not limited to

- Executive Leadership
- Current or potential Insider Threat Program Managers
- Insider Threat Program team members
- Employees within other areas of an organization that interact and support an Insider Threat Program team (e.g., IT, Information Security, Human Resources, Physical Security, Legal, Software Engineering, “Data Owners”)
- Non-executive employees that have access to classified information (general awareness).
- Others who want to learn about Insider Threat issues

Course Objectives

Upon completion of this course, participants will be able to:

- State the CERT National Insider Threat Center definition of an insider
- Define other basic insider threat terminology
- Differentiate between types of insider threat activities
- Recognize both technical and behavioral indicators of insider threat
- Identify best practices for detection, mitigation, and response to insider threats
- Explain why detecting and responding to insider threats can not rely only on technical indicators and solutions

Agenda

Course Introduction

Module 1: Introduction to the CERT National Insider Threat Center

Module 2: What is Insider Threat?

Module 3: Insider Threat Sabotage

Module 4: Insider Theft of Intellectual Property

Module 5: Insider Threat Fraud

Module 6: Unintentional Insider Threat

Module 7: Insider Threat Prevention, Detection, and Mitigation Strategies

Course Conclusion

Resources

Module 1: Introduction to the CERT National Insider Threat Center

What Is CERT?

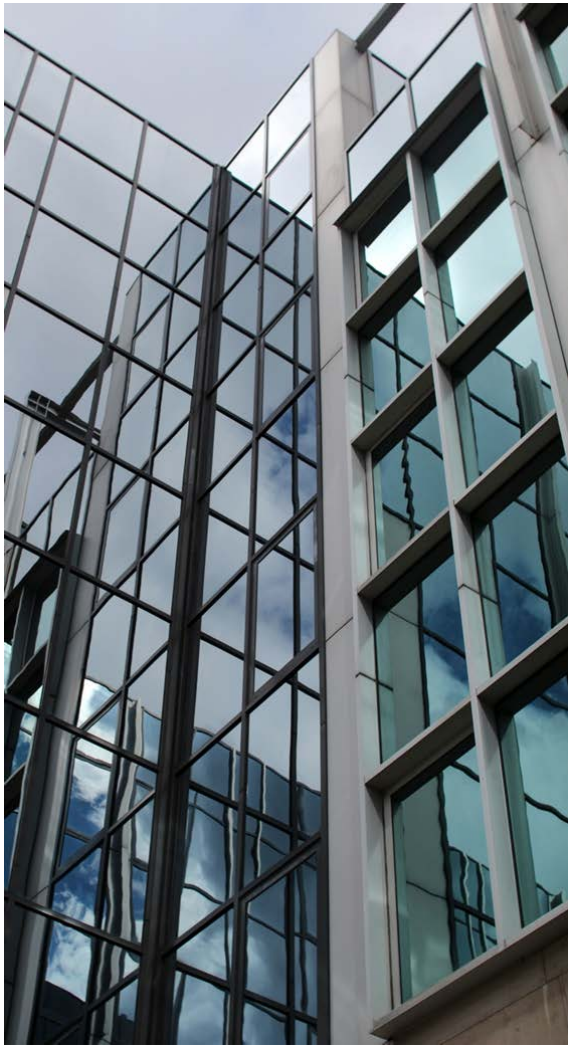
Center of Internet security expertise

Established in 1988 by the US Department of Defense on the heels of the Morris worm that created havoc on the ARPANET, the precursor to what is the Internet today

Located in the Software Engineering Institute (SEI)

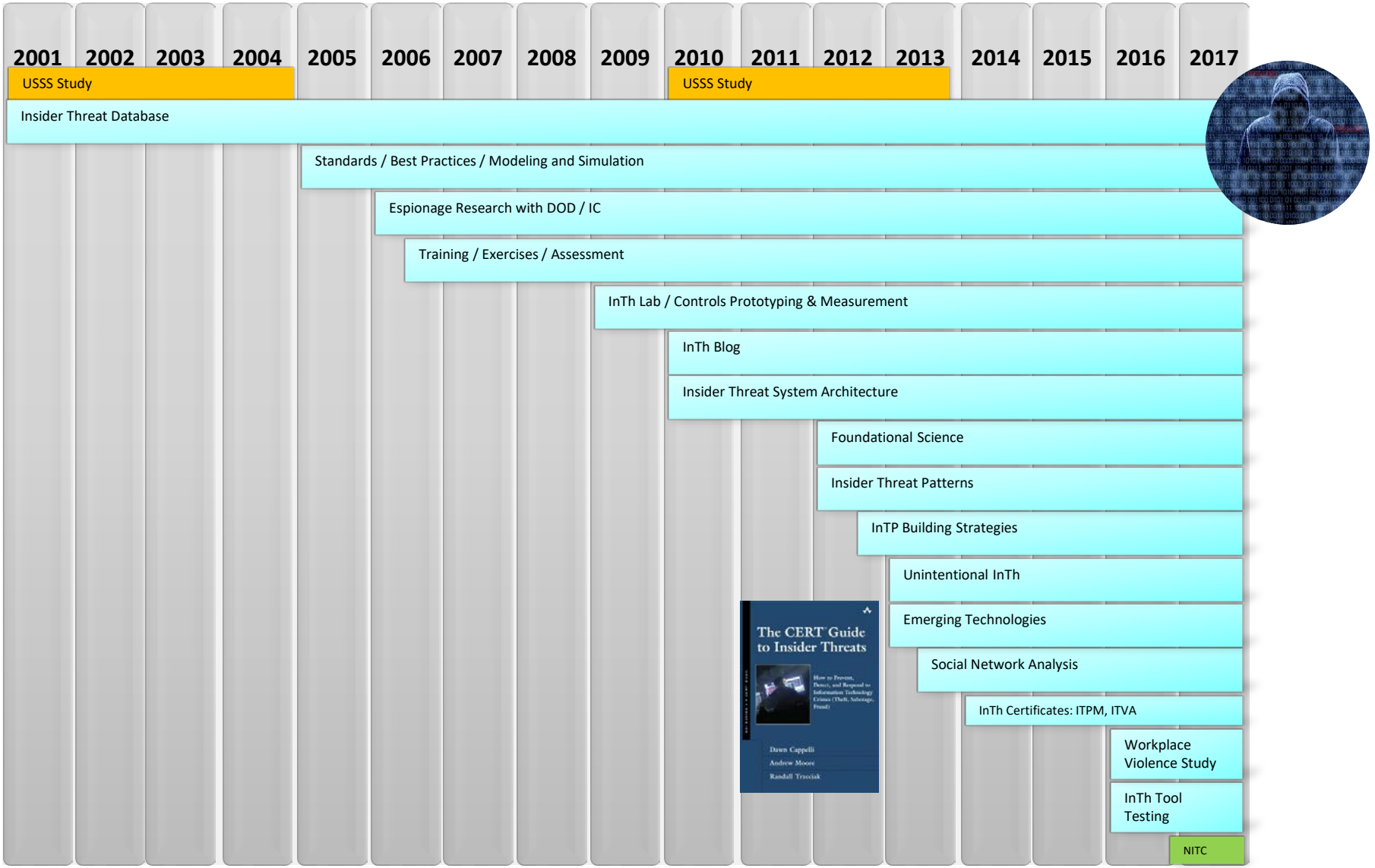
- Federally Funded Research & Development Center (FFRDC)
- Operated by Carnegie Mellon University (Pittsburgh, Pennsylvania)

The CERT National Insider Threat Center



- The CERT National Insider Threat Center (NITC) focuses on providing insider threat expertise across sectors.
- 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

NITC Timeline



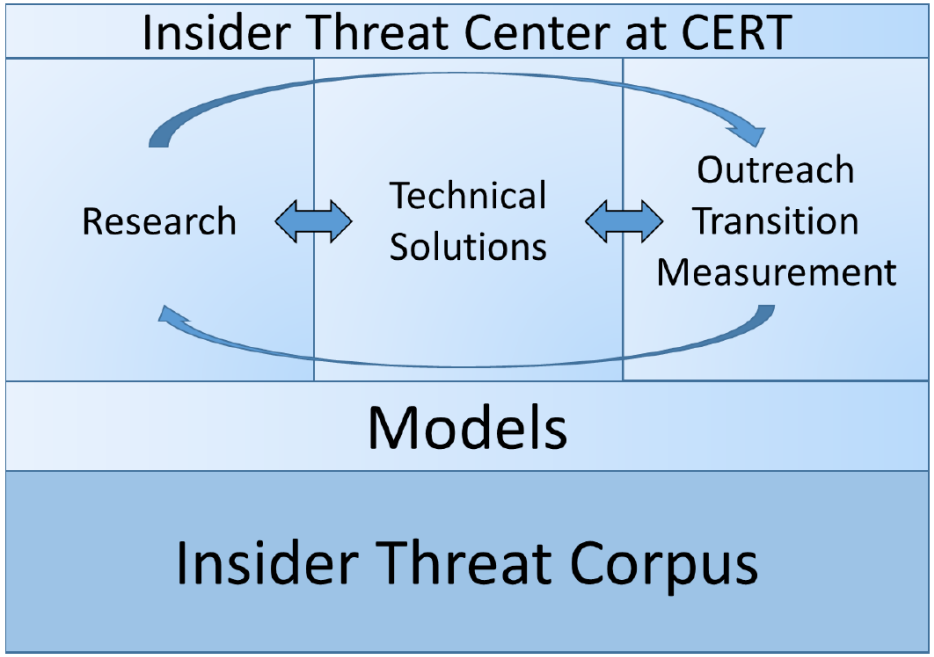
NITC Case Collection Approach

Ongoing collection	Cases from 1996 to the present that primarily occurred in the U.S. are coded in the NITC Incident Corpus
Sources	Court documents, interviews, media reports, social media, investigators' notes
Big picture approach	Examine technical, psychological, and organizational aspects of the problem
Objective	Analyze actual cases to develop information for prevention & early detection

Homeland Security

NITC Incident Corpus

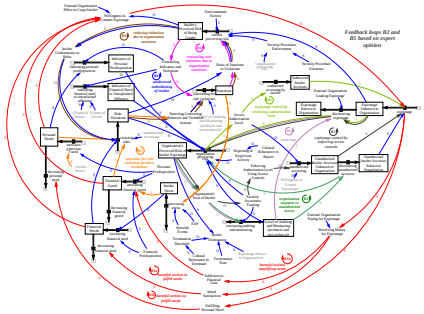
- Database of over 1600 insider threat incidents
  - Includes interviews of actual offenders
- Coded to allow analysis of technical actions & behaviors observables
- Development of technical controls to baseline and detect anomalous actions
- Research into areas of
  - Sentiment analysis
  - Workplace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



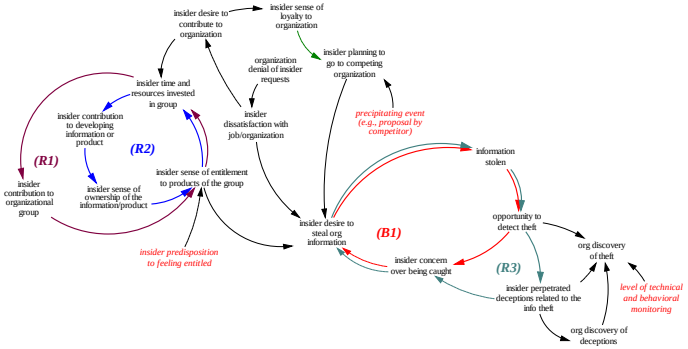
NITC Methodology

Collect, code, and empirically analyze incidents

Develop Causal Models



Deriving Candidate Controls and Indicators



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 Insider Threat Modeling Approach

Objectives

- Communicate the multi-disciplinary nature of the problem.
  - Problem and mitigation requires analysis of policies, practices, technologies over time
  - Need to consider behavioral, technical, and organizational issues
- Develop innovative training materials.
- Help organizations understand how to work across departments to mitigate the insider threat risk.
  - May require mental model shift or culture change
- Case Types / Crime Profiles
  - IT Sabotage
  - Theft of Intellectual Property
  - Fraud
  - National security espionage

Collaborations (Past, Current, Future)

Organizations	Focus Areas
Domain experts	• Psychology (Secret Service, FBI, DoD, CERT 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

Trust and Confidentiality

NITC never reveals or discusses the identity of

- organizations or insiders in our databases
- sponsors / customers unless they give us permission

Module 1 Conclusion

The NITC

- bases its models and profiles of Insider Threat on empirical analysis
- continues to maintain the largest corpora of actual insider threat incidents
- focuses on socio-technical indicators and mitigations for detection, prevention, and response to insider threat activity

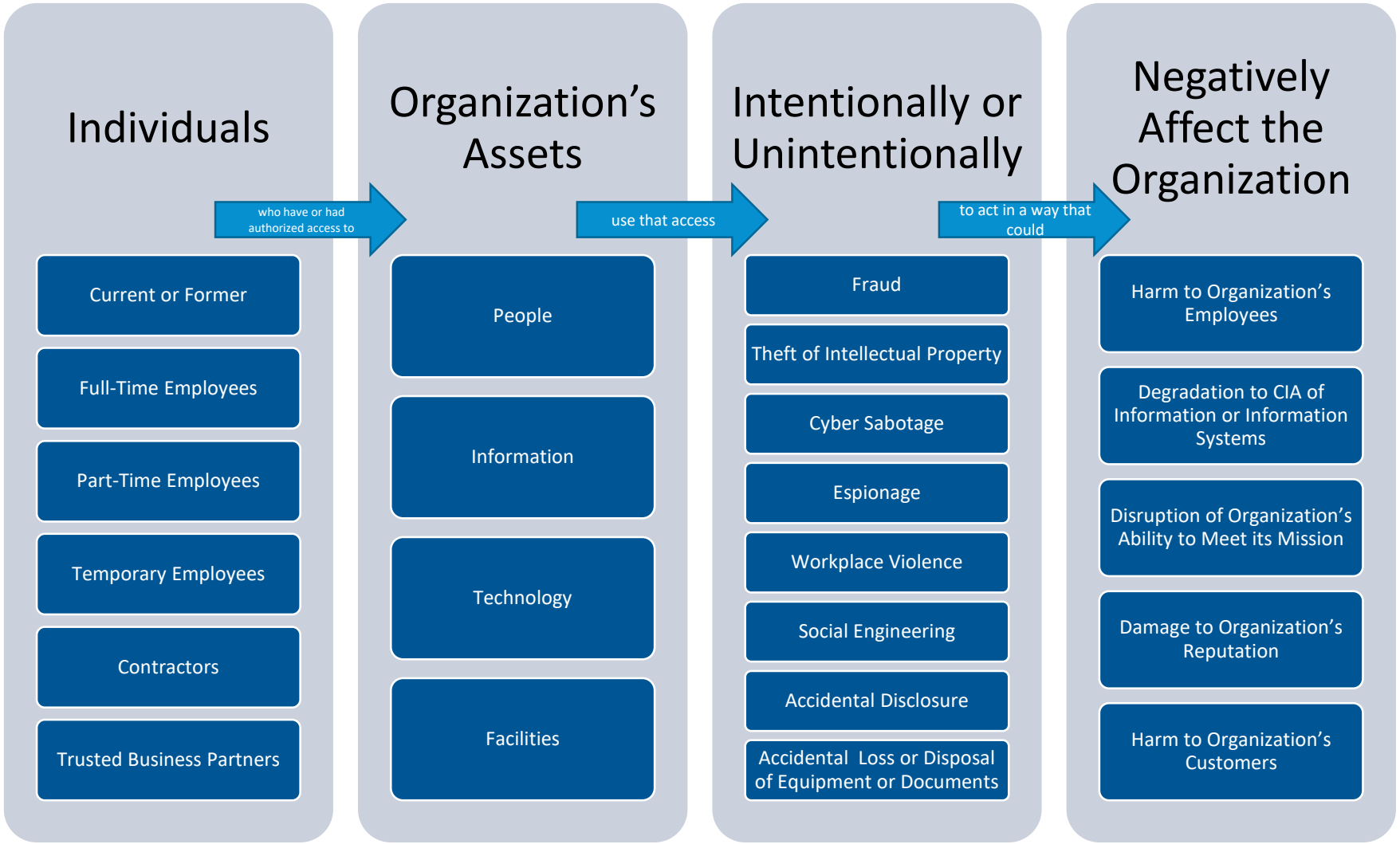
Module 2: What is Insider Threat?

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?

What / Who is an Insider Threat?



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

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

Just think about the following:

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

Insider Threat Issue -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, for example:

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

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
Foreign allegiances	US organizations operating branches outside the US with the majority of employees who are not US citizens

How Serious is Insider Threat?

2017 U.S. State of Cybercrime Survey -1

CSO Magazine, USSS,

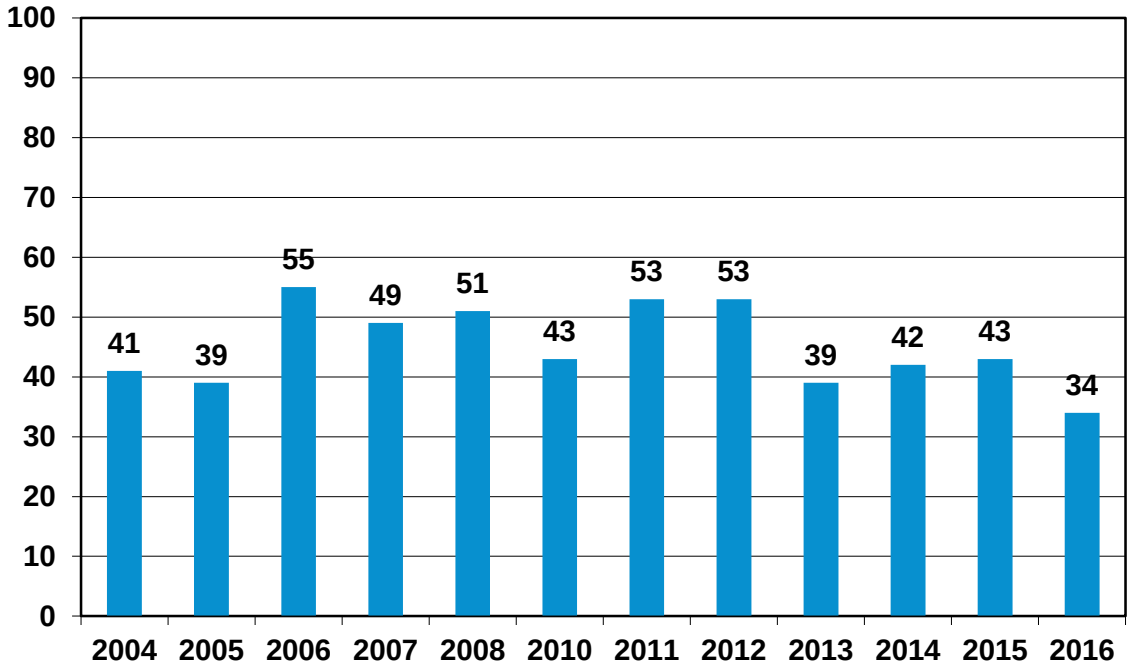
CERT Division, & Forcepoint

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.

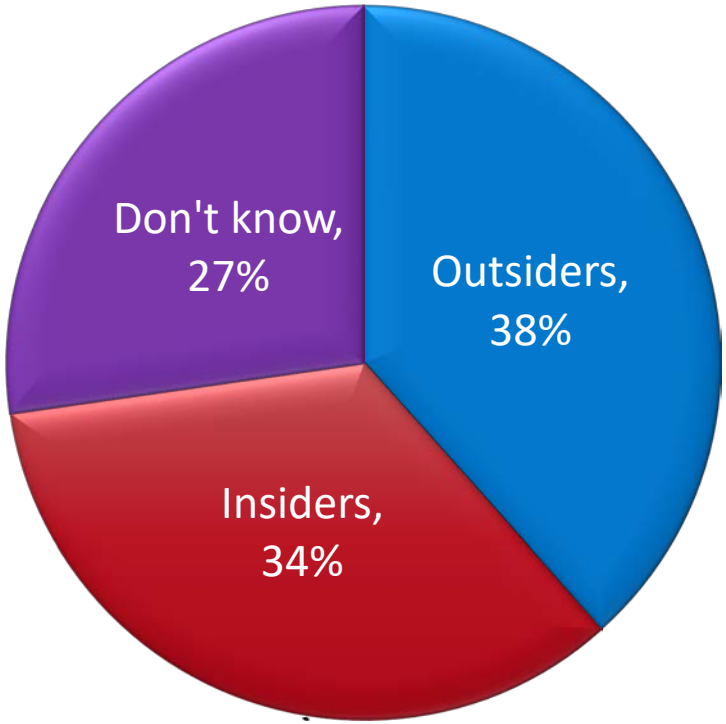
Insiders made up the highest percentage of the following incidents:

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

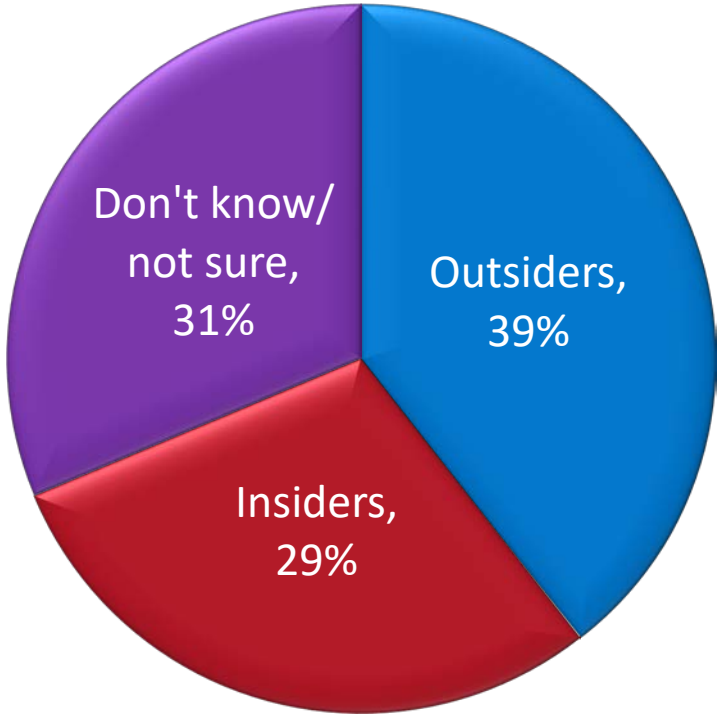
What percentage of the cyber security events (the past 12 months) are known or suspected to have been caused by



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

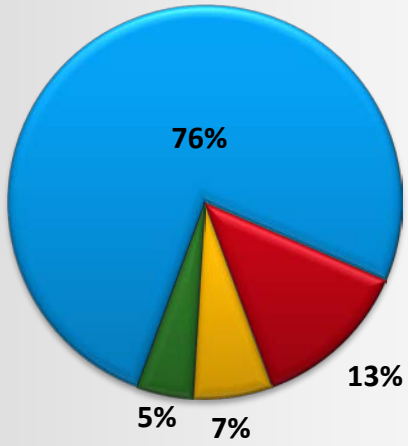
In general, cybercrimes were more costly or damaging to your organization when caused by



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)

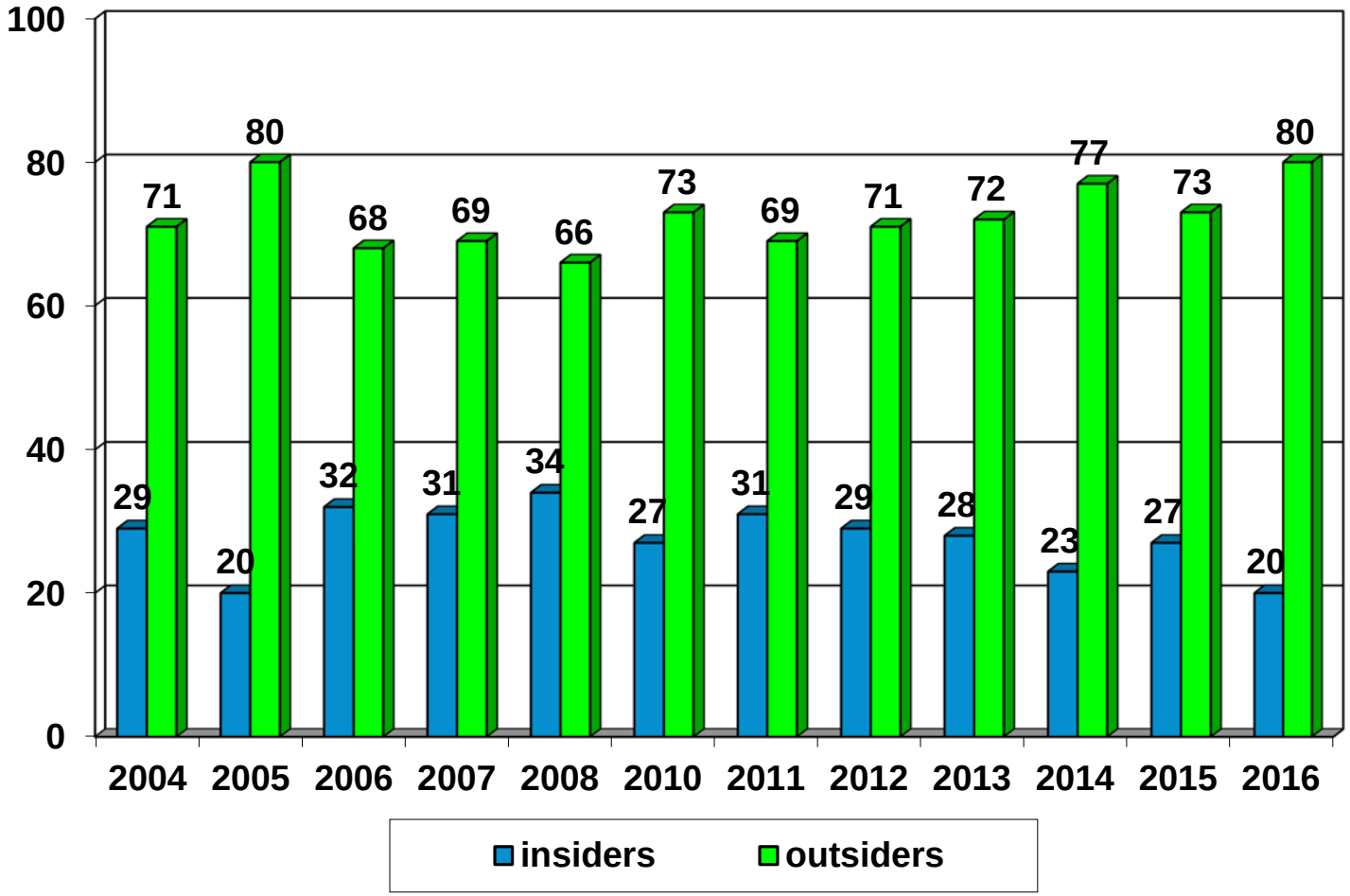
Reason(s) cybercrimes were not referred for legal action

	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

Types of Insider Threat Activities

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 which 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

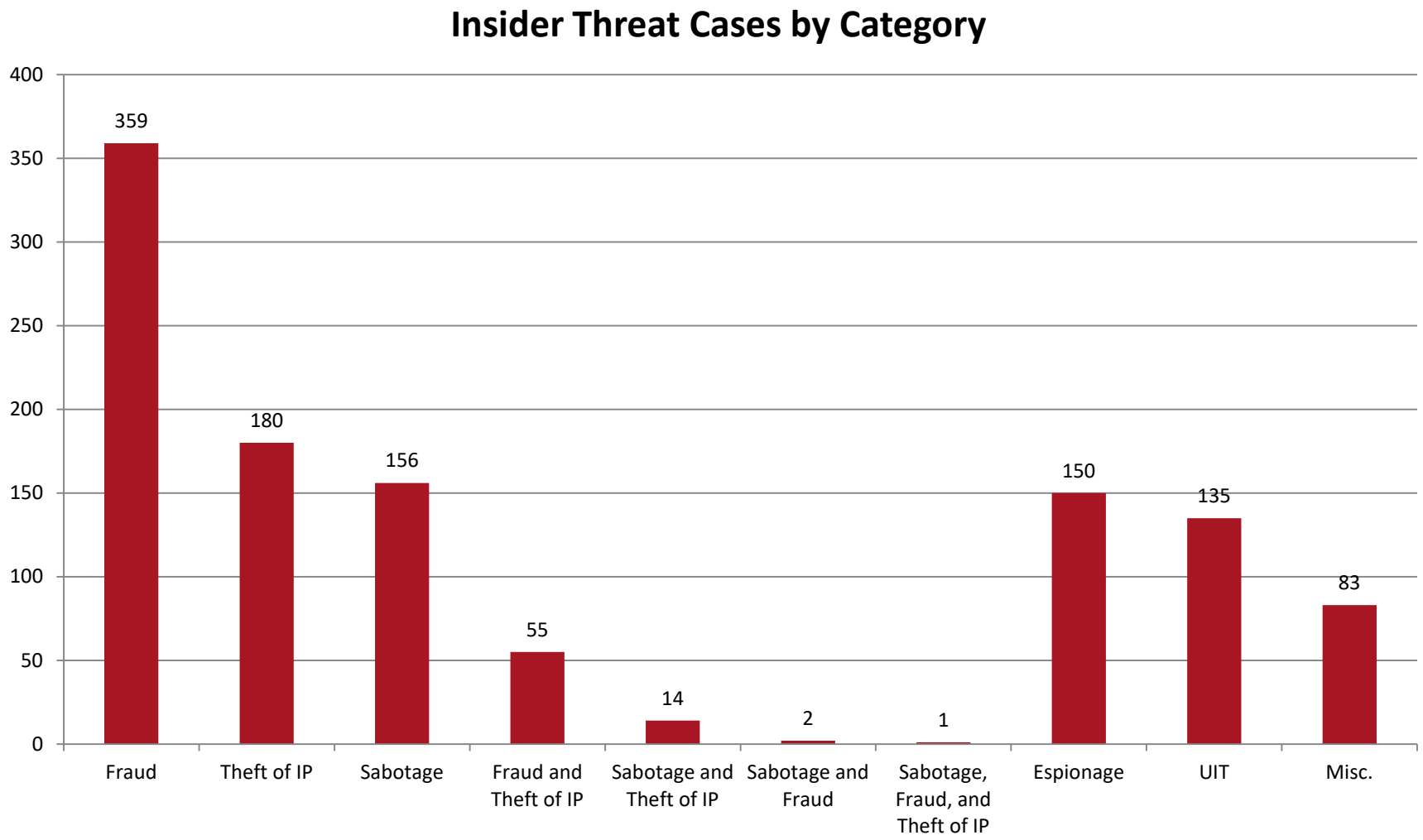
- The act of communicating, delivering or transmitting information pertaining to the national defense of the United States to any foreign government or faction, with intent or reason to believe that is to be used to the injury of the United States or to the advantage of a foreign nation

Miscellaneous

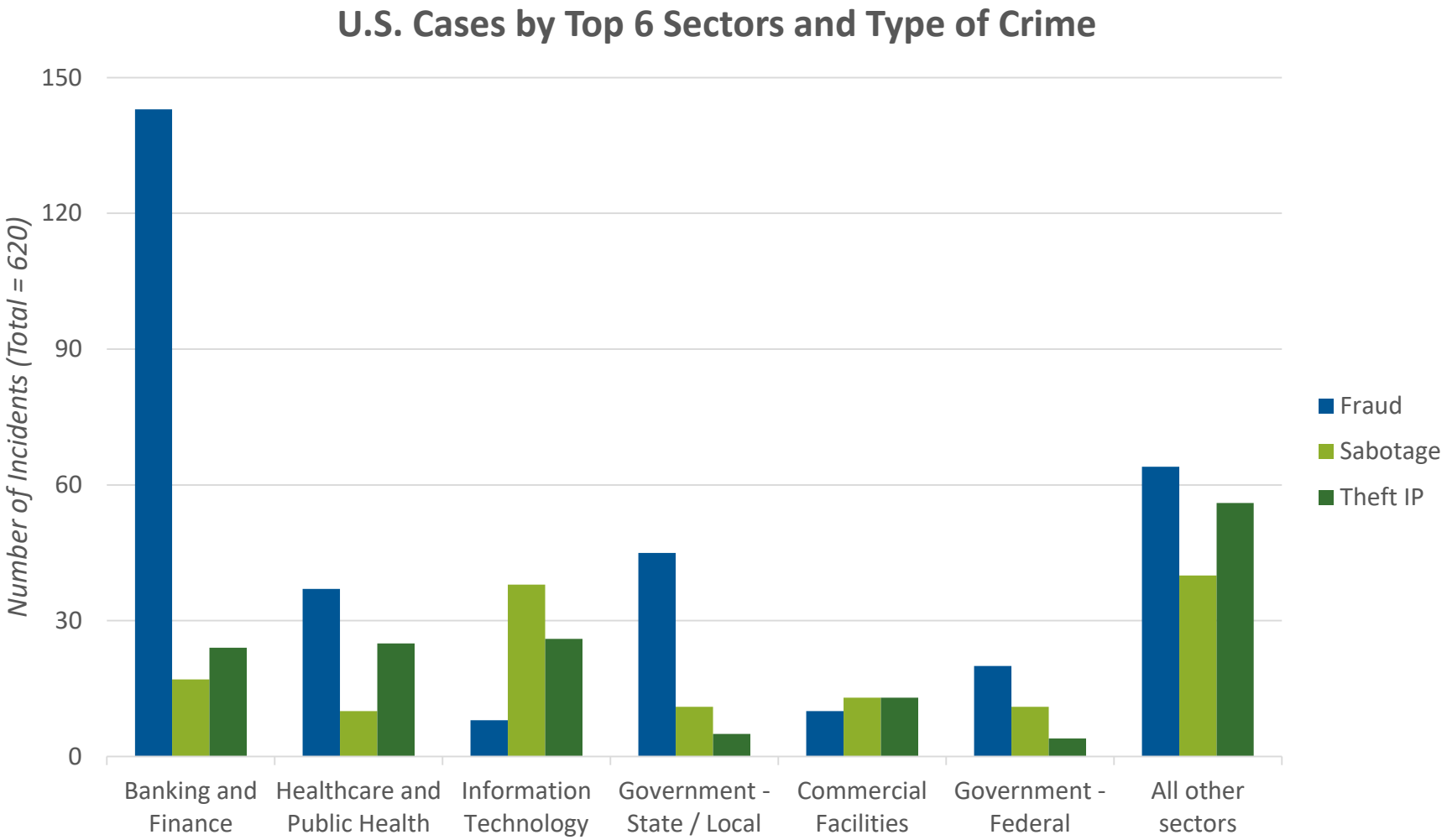
- Unauthorized disclosure of information insider believed should be in the public domain
- Query of database to find address of person – information provided to acquaintance who physically harmed individual
- Query of high-profile individuals to access personal information
- Unauthorized access to co-worker's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

This course does not cover National Security Insider Espionage

CERT's Insider Threat Incident Corpus

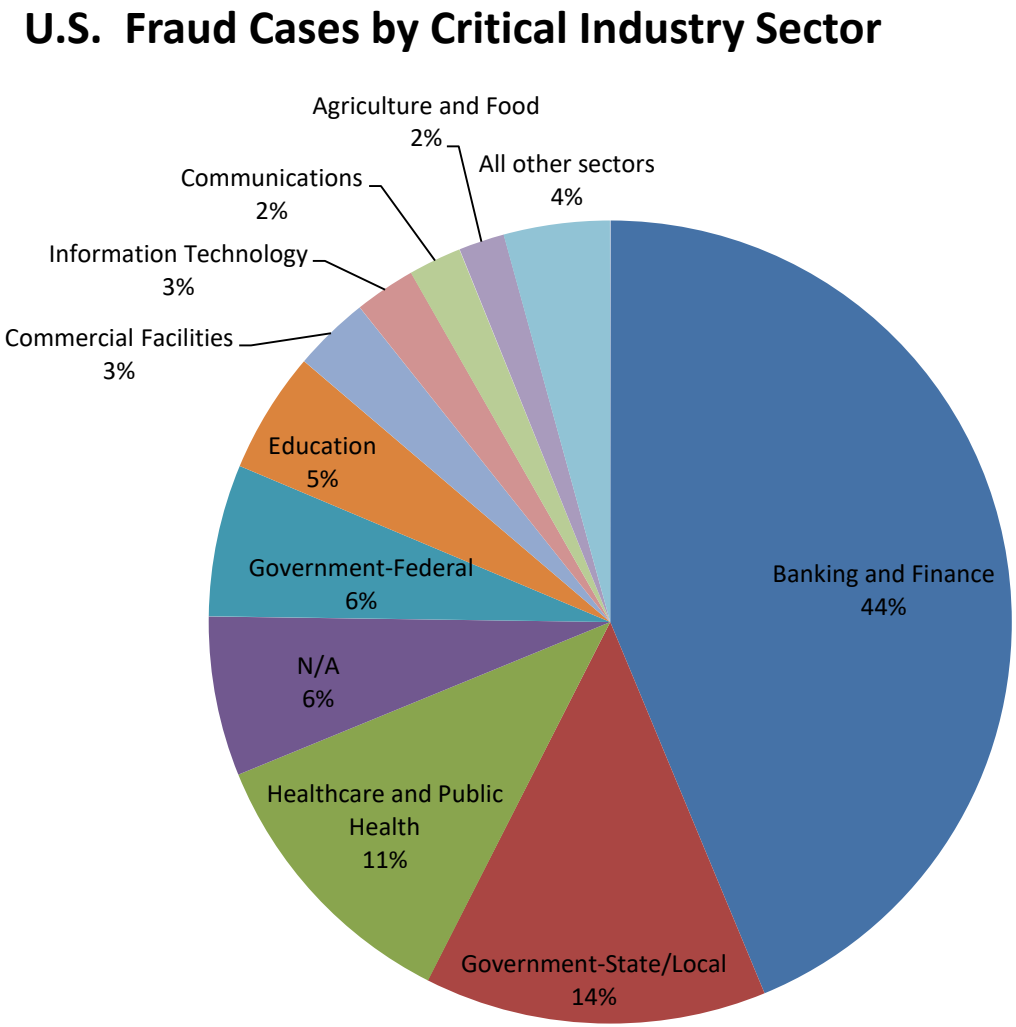


Critical Infrastructure Sectors



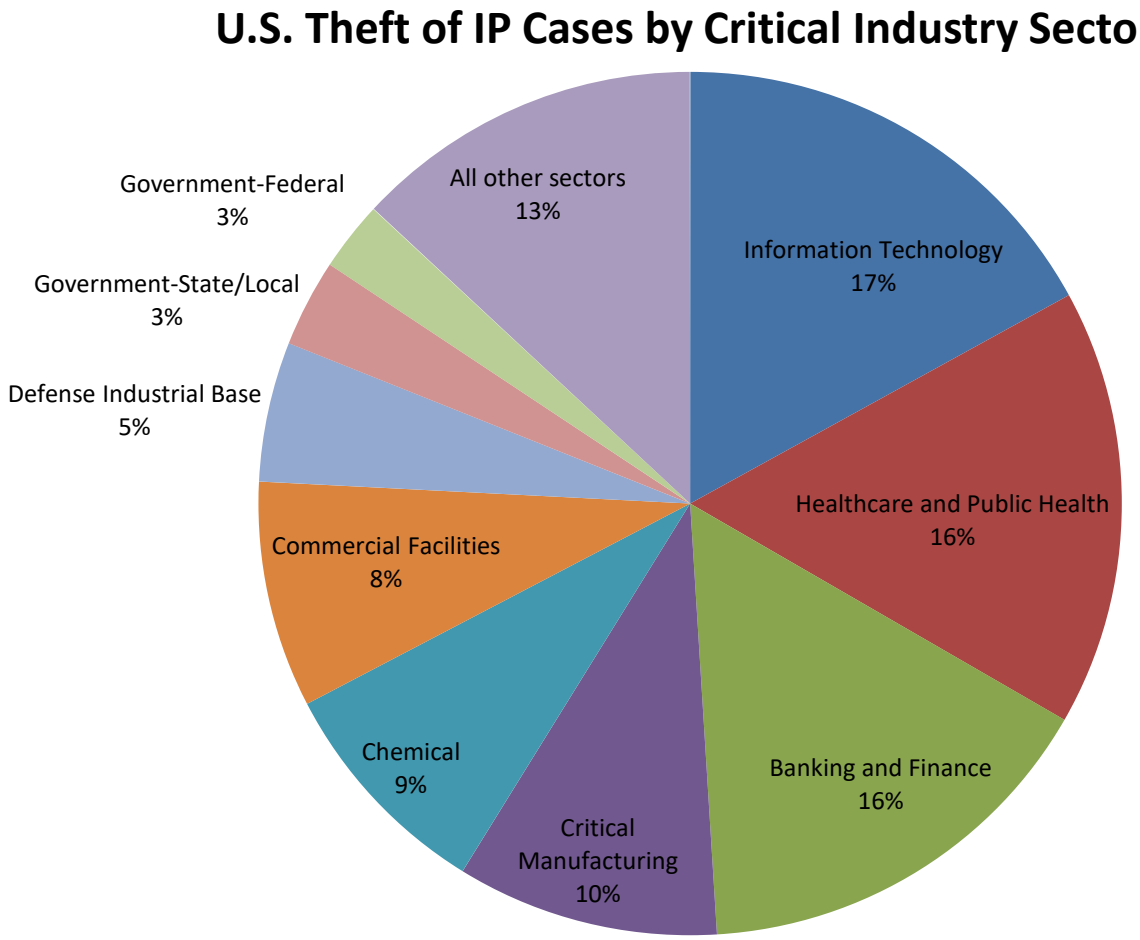
Note: Does not include incidents that involve multiple case types or espionage.

Critical Infrastructure Sectors - Fraud



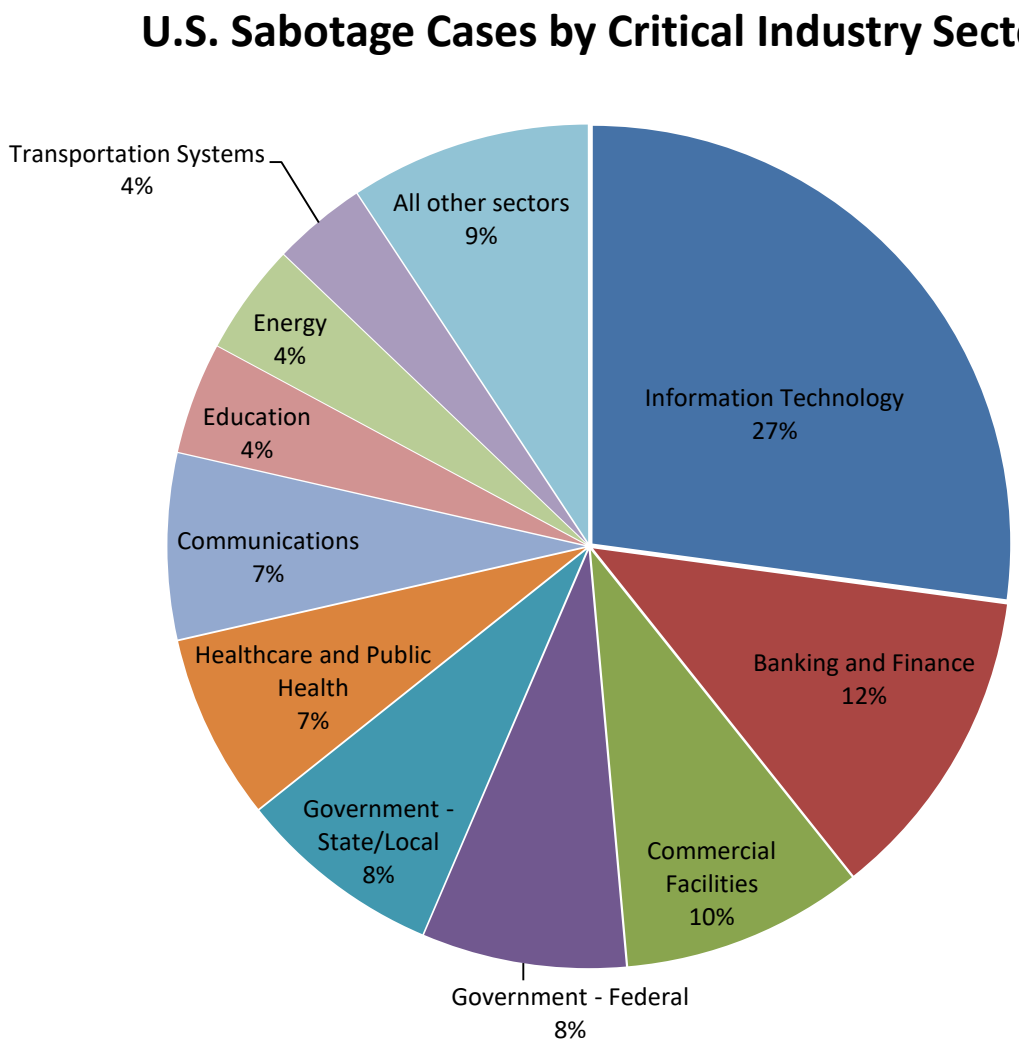
*** This does not include espionage cases involving classified information*

Critical Infrastructure Sectors – Theft of IP



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

Critical Infrastructure Sectors - Sabotage



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

Module 2 Conclusion

Insiders can be current or former employees, contractor, sub-contractors, or other trusted business partners.

The NITC identifies five basic types of insider threat activities, each has its own profile.

- Fraud
- Theft of Intellectual Property
- IT Sabotage
- National Security Espionage
- Unintentional Insider Threat

There is also a miscellaneous category for threats that do not fit the other profiles.

Insider threat controls can also provide protection from outsiders.

Module 3: Insider Threat Sabotage

TRUE STORY: *IT Sabotage*

SCADA sabotage releases 800,000 liters raw sewage

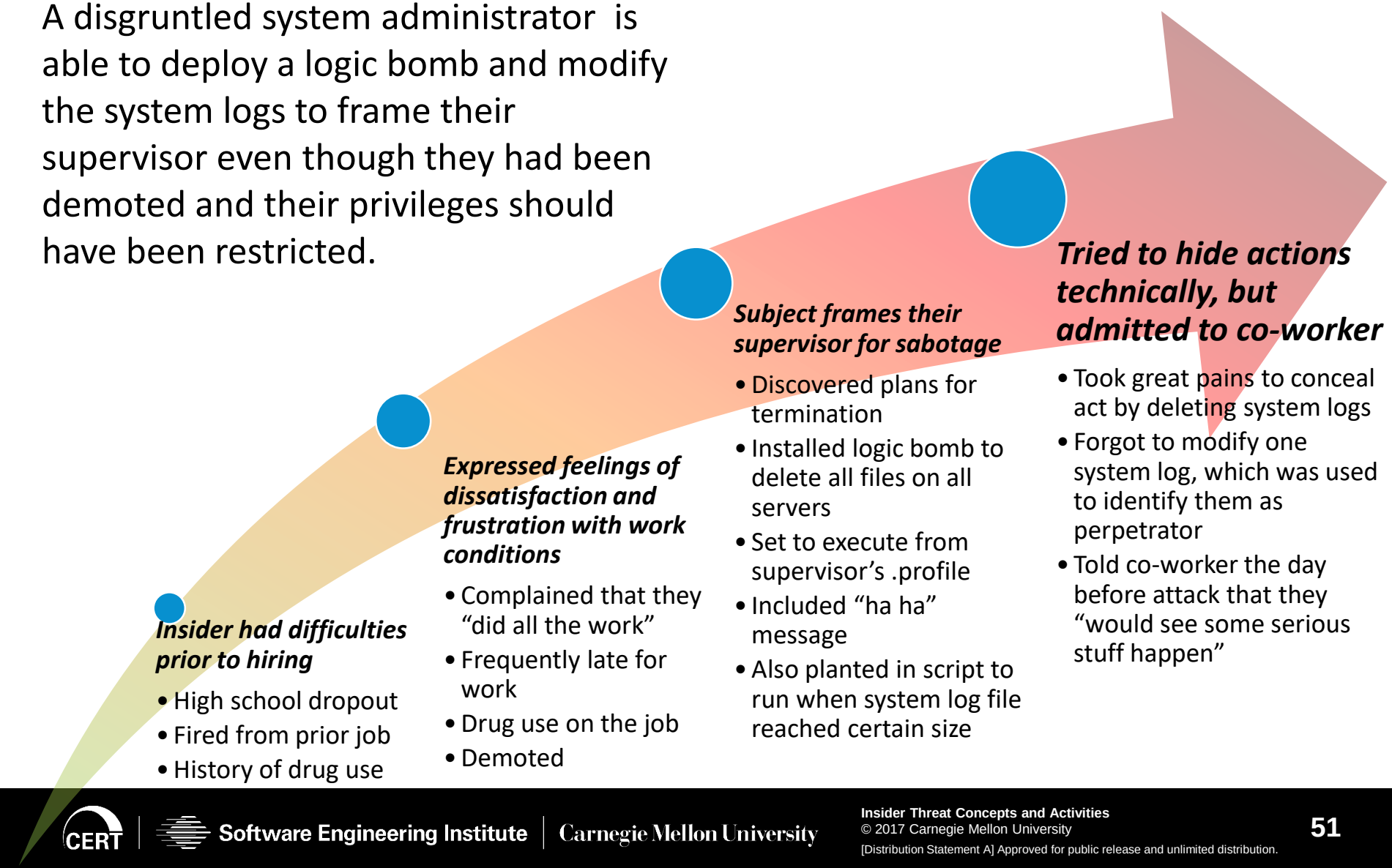
TRUE STORY:

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"

Other Cases of IT Sabotage

A subcontractor at an energy management facility breaks the glass enclosing the emergency power button, then shuts down computers that regulate the exchange of electricity between power grids, even though their own employer had disabled their access to their own facility following a dispute.

- Impact: Internal power outage; Shutdown of electricity between the power grids in the US.

Former employee of auto dealer modified vehicle control system after being laid off

- Searched for known customers and sent out unwarranted signals to vehicle control devices…disabled ignitions and set off alarms

System administrator at a manufacturing plant, passed over for promotion, deployed “logic bomb” prior to resigning, deleting critical software required to run operation

- Financial damage $10M; Forced to lay off 80 employees

Who were the Saboteurs?

Insider Demographics	
Position	System administrators, database administrators, other technical positions with current or pending termination
Tenure	Typically 2 years or less / 5 years or more
Age Range	Two-thirds of insiders were between 21 and 40
Gender	Over 90% of saboteurs were male
Marital Status	Fairly evenly split married versus single

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

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.

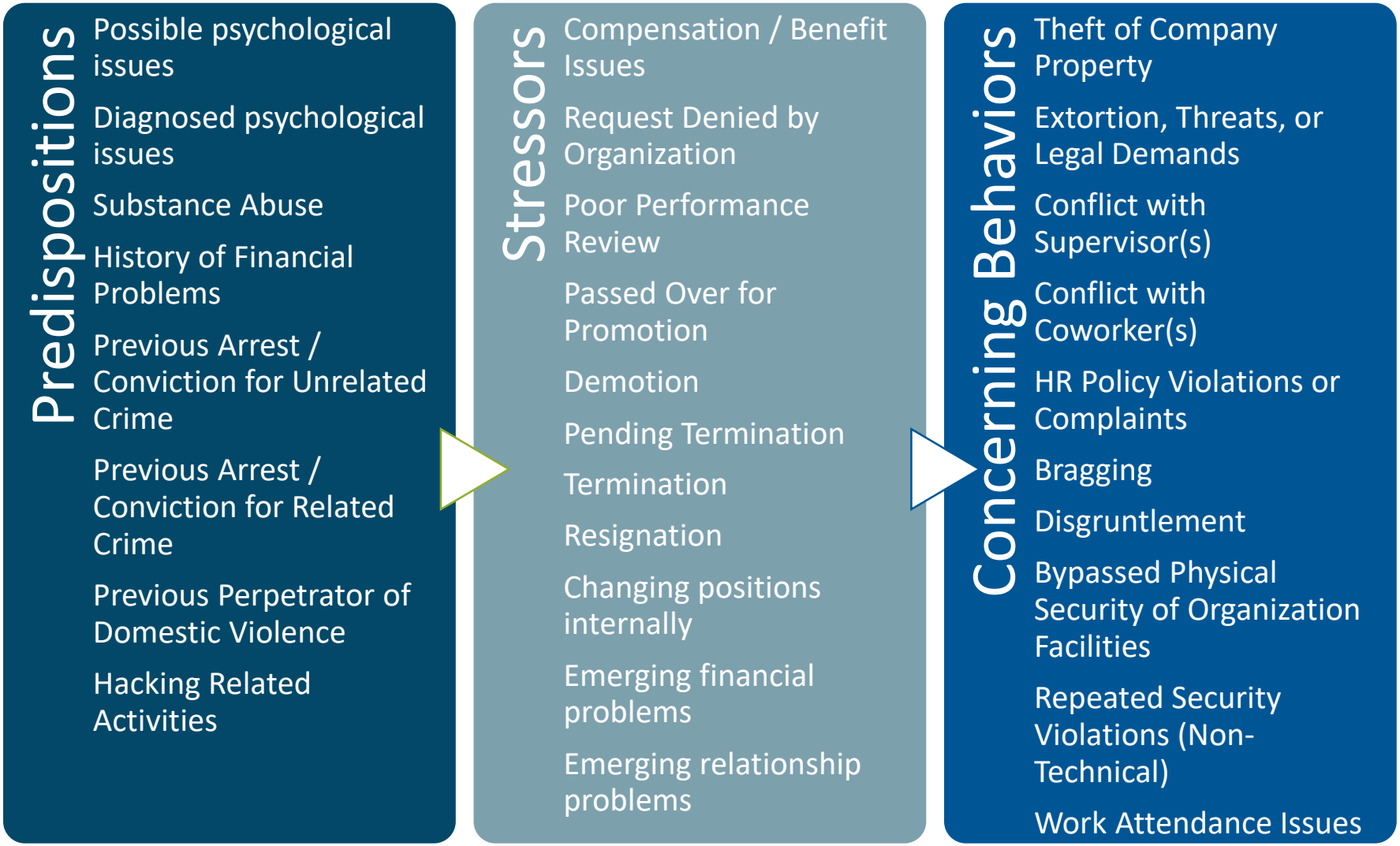
The majority of saboteurs attacked after pending or completed termination.

In many cases, organizations failed to detect technical precursors.

Lack of physical and electronic access controls facilitated IT sabotage.

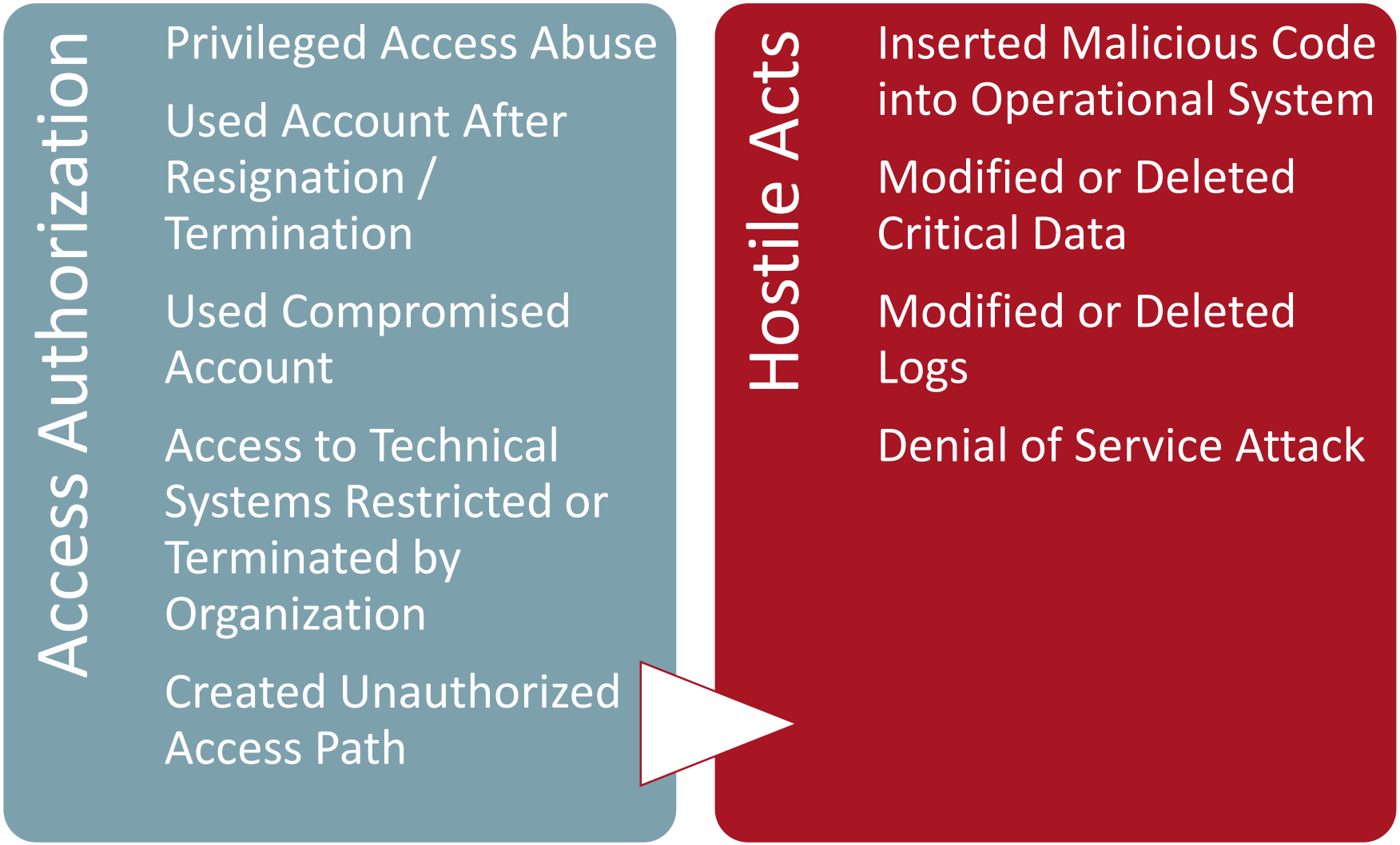
IT Sabotage Potential Behavioral Precursors

IT Sabotage Behavioral Precursors



IT Sabotage Potential Technical Precursors

IT Sabotage Technical Precursors



Unknown Access Paths Observed in Cases

- Planted logic bomb while still employed
- Created backdoors before termination or after being notified of termination
- Installed modem for access following termination
- Changed all passwords right before resignation
- Disabled anti-virus on desktop & tested virus
- Network probing
- Installed remote network administration tool
- Downloaded and installed malicious code and tools (e.g., rootkit, password cracker or virus)
- Disabled system logs & removed history files

Undetected Sabotage Precursors

Technical

- Failure to create backups as required
- Unauthorized access of customers' systems
- Unauthorized use of coworkers' unattended machines
- System access following termination
- Access of web sites prohibited by acceptable use policy
- Use of backdoor accounts
- Enabled remote access on coworker's workstations

Behavioral

- Failure to document systems or software as required
- Sharing passwords with others & demanding passwords from subordinates
- Refusal to return laptop upon termination
- Refusal to swipe badge to record physical access

Module 3 Conclusion

Insider Threat Sabotage

- usually involves the most technical or sophisticated types of attacks
- is usually committed by more technical staff such as systems and network administrators, database administrators, or similar types of staff
- is usually done for revenge or in response to perceived wrongs or unmet expectations
- is often performed by employees who have had previous observed events where they were clearly disgruntled
- can potentially be identified and mitigated by identifying the technical and behavioral precursors and acting on them
- can also be prevented by ensuring good information assurance practices are in place along with good human resource and physical security policies and practices

Module 4: Insider Theft of Intellectual Property

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.

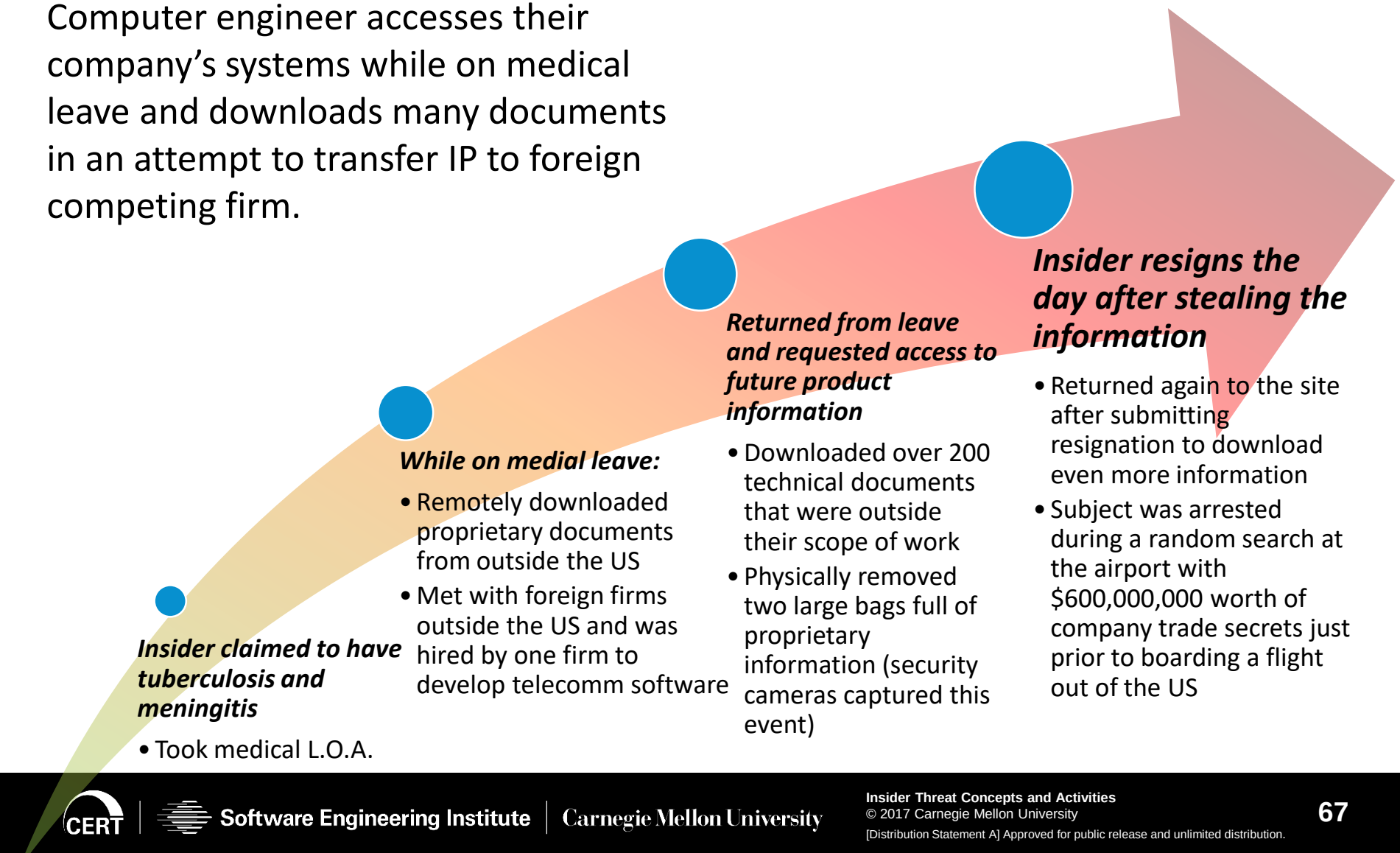
TRUE STORY: *Theft of IP*

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

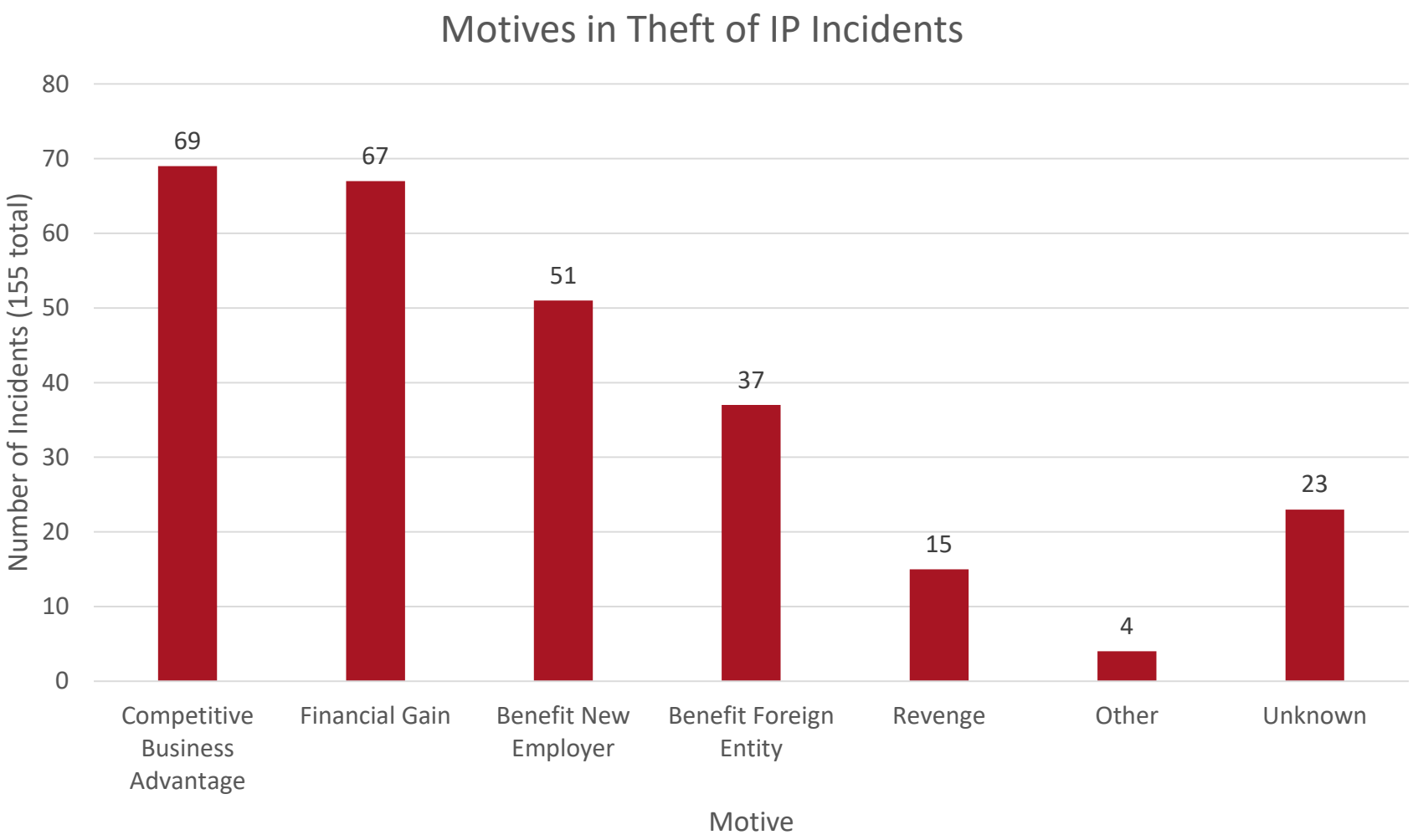
Who committed Theft of IP?

Insider Demographics	
Position	Current employees working as scientists, engineers, programmers, sales people
Tenure	Typically 5 years or more with victim organization
Age Range	Approximately 85% were male
Gender	Approximately 85% were male
Marital Status	Typically married
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

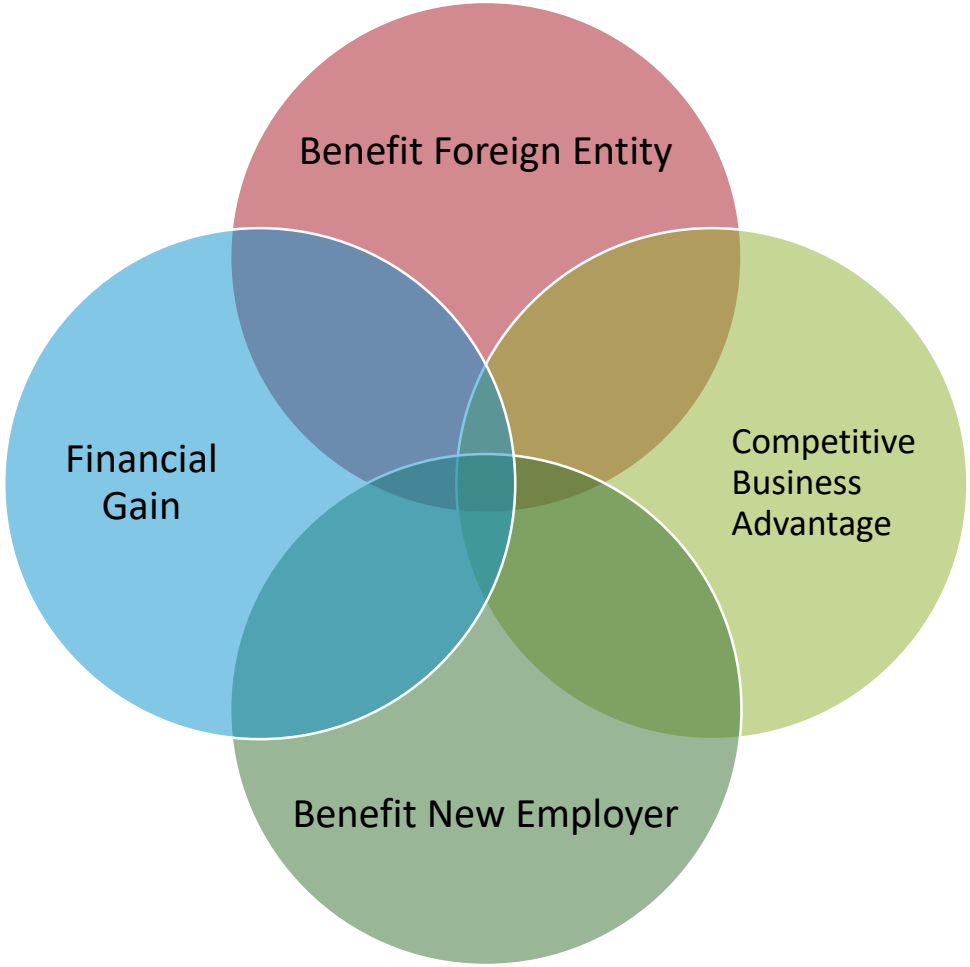
Theft of IP Precursors and Observations

- Mergers & Acquisitions
- Insider Promoted
- 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

Motives for Theft of IP



Theft of IP for Foreign Government or Organization

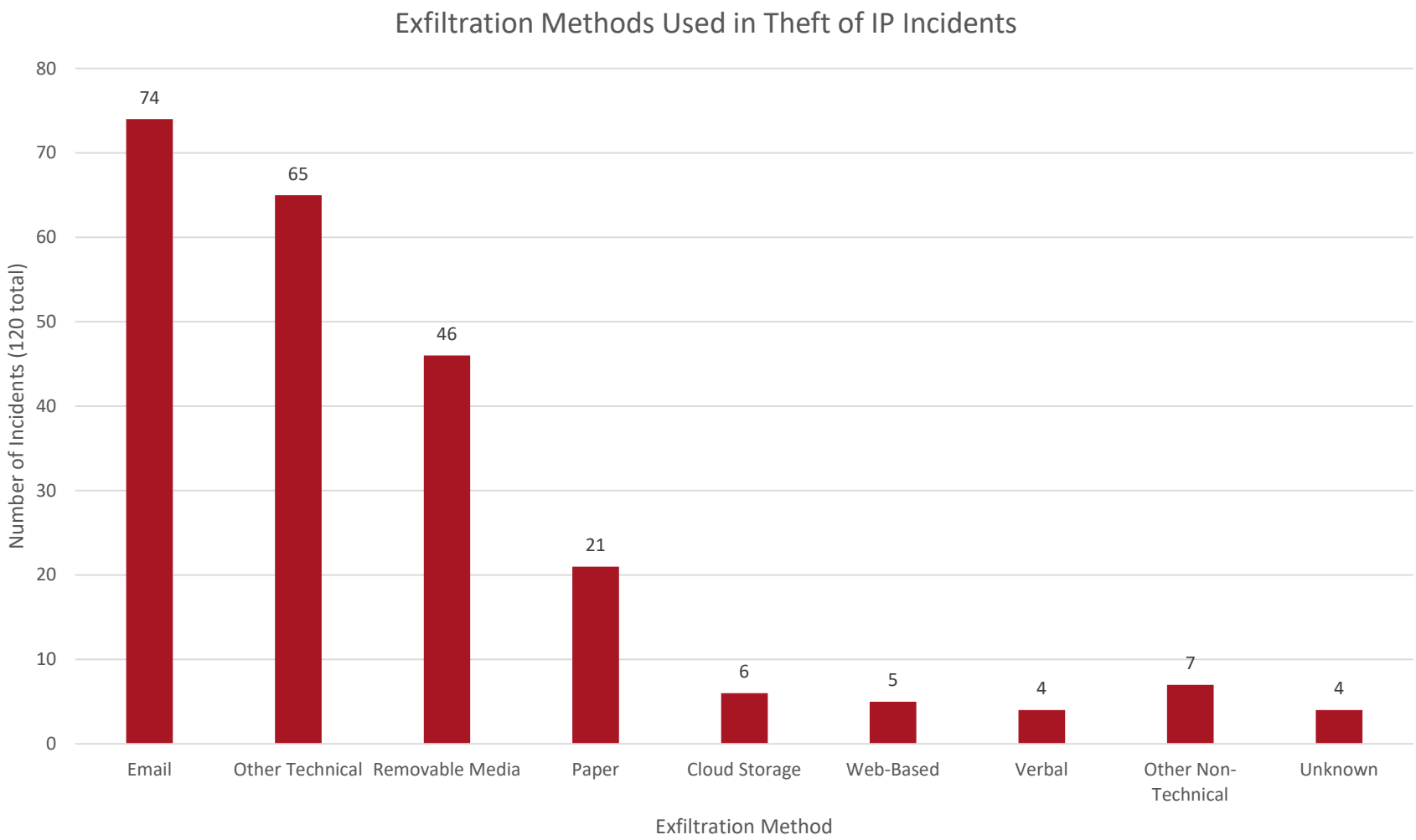


Theft of IP incidents often had converging motives.

Approximately one-quarter of theft of IP incidents were for the benefit of a foreign government or organization.

These insiders were also motivated by financial gain, benefit of new employers (i.e., foreign employers), and competitive business advantage.

Common Methods of Exfiltration



Considerations for Mitigation

- Understand the risks posed by privileged access abuse
- Recognize efforts at concealment
- Consider export control and/or travel reporting policies as it is much more difficult to recover IP once it leaves the U.S.
- Establish procedures for use of removable media
- Develop policies on allowable use of personal email
- Consider additional monitoring around resignations, particularly in the event of group resignation
- Establish consistent exit procedures

Module 4 Conclusion

Insider Threat Theft of Intellectual Property

- is usually committed by current staff in the roles of scientists, engineers, programmers, and sales people
- is usually performed during normal working hours using authorized access
- is often quick theft upon resignation
- is often done to gain immediate advantage at a new job, start a new business, or give to a foreign company or government
- Prevention and mitigation strategies can include
  - training on and enforcement of IP agreements and expectations
  - monitoring of IP copied to removable media or printed
  - monitoring of employee around resignation

Module 5: Fraud

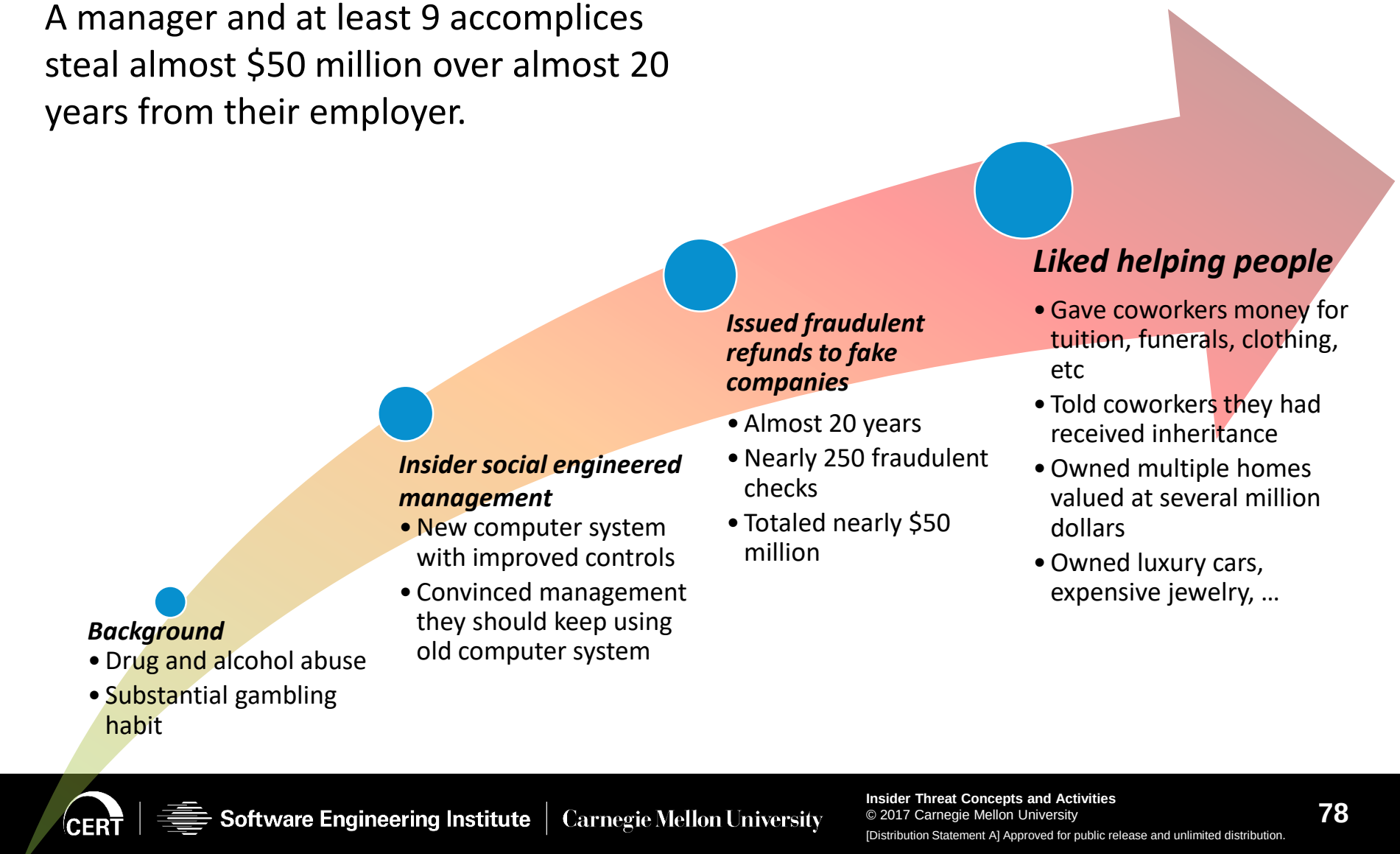
TRUE STORY:

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, …

Other Cases of Fraud

An accounts payable clerk, over a period of 3 years, issued 127 unauthorized checks to themselves and others...

- Checks totaled over $875,000

A front desk office coordinator stole PII from hospital...

- Over 1100 victims and over $2.8 M in fraudulent claims

A database administrator at major US Insurance Co. downloaded 60,000 employee records onto removable and solicited bids for sale over the Internet

An office manager for a trucking firm fraudulently puts their spouse on the payroll for weekly payouts, and erases records of payments…

- Over almost a year loss of over $100K

Coordinated Fraud Rings

Stolen Identity Refund Fraud (SIRF) rings are increasingly common. Often, both insiders and outsiders coordinate the tasks necessarily to file false tax returns, from stealing PII to filing the returns to cashing checks.

In one case, at least 10 individuals, about half of whom were insiders, obtained PII from 5 organizations, which included 3 state-level organizations, a call center, and a military hospital.

Additional insiders abused their positions at a check cashing center to cash fraudulently-obtained tax return checks.

The group of insiders and outsiders filed approximately $20 Million in fraudulent tax returns, receiving as much as $7.5 Million before they were discovered and apprehended.

Who were the Fraudsters?

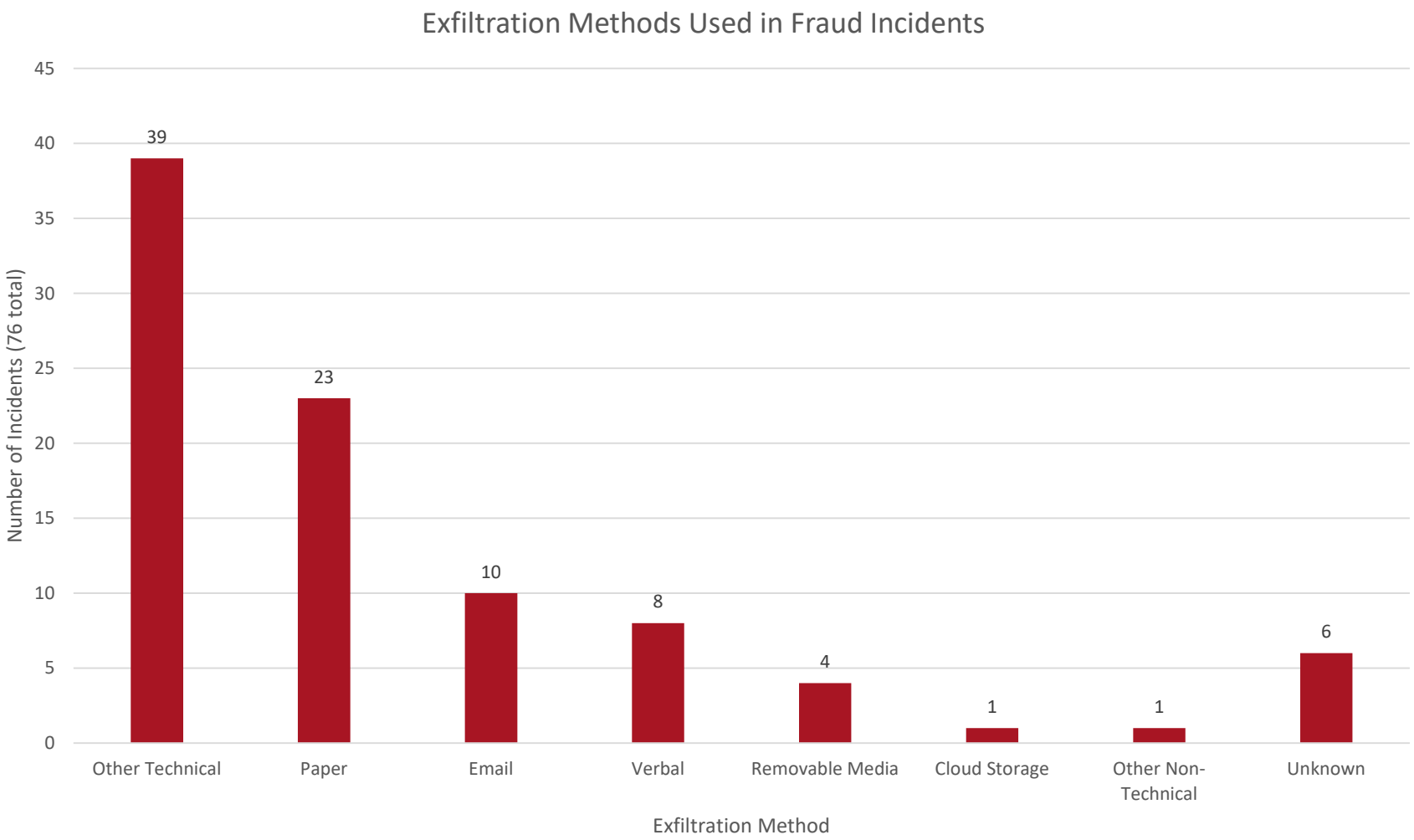
Insider Demographics	
Position	Current employees in nontechnical positions
Tenure	Typically 5 years or more / 1 year or less
Age Range	Two-thirds are between the ages of 21 and 40
Gender	Fairly even split between male and female
Marital Status	Fairly even split between single and married

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

Known Issues

- 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

Common Methods of Exfiltration



Other Technical Aspects – Fraud

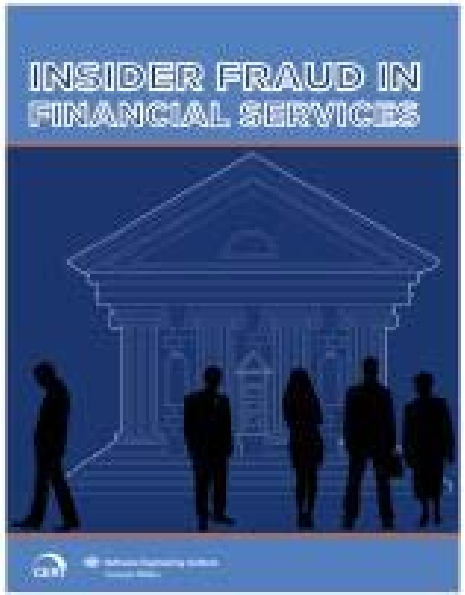
- Privileged Access Abuse
- Created / Used Fraudulent Assets
- Created / Used an Alias
- Modified Critical Data
- Used Compromised Account
- Used Unattended, Unsecured Workstation
- Social Engineering of Employees in Attack

Insider Fraud Study (2012)

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

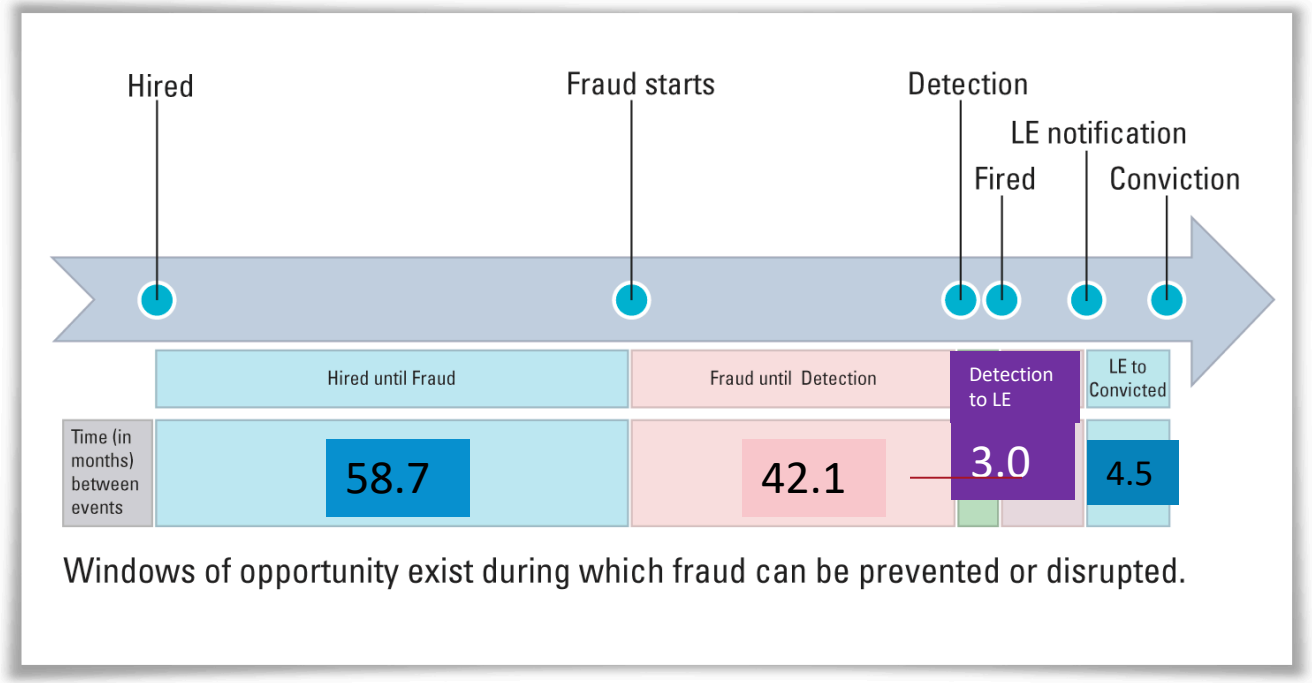
Conducted by the NITC in collaboration with the U.S. Secret Service (USSS)

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)



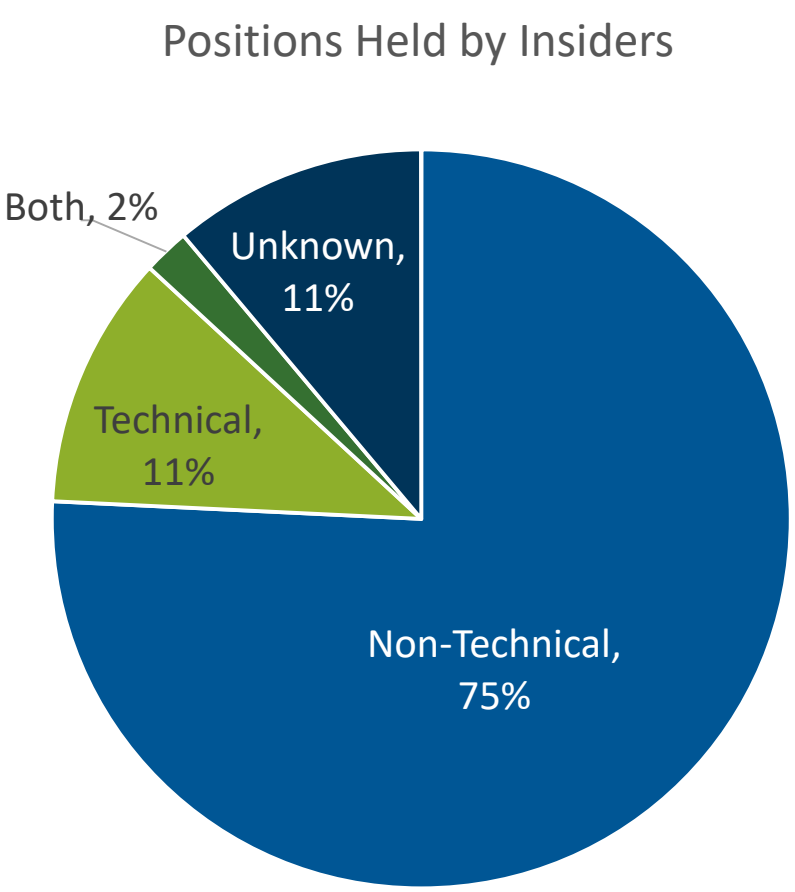
Low and Slow

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.

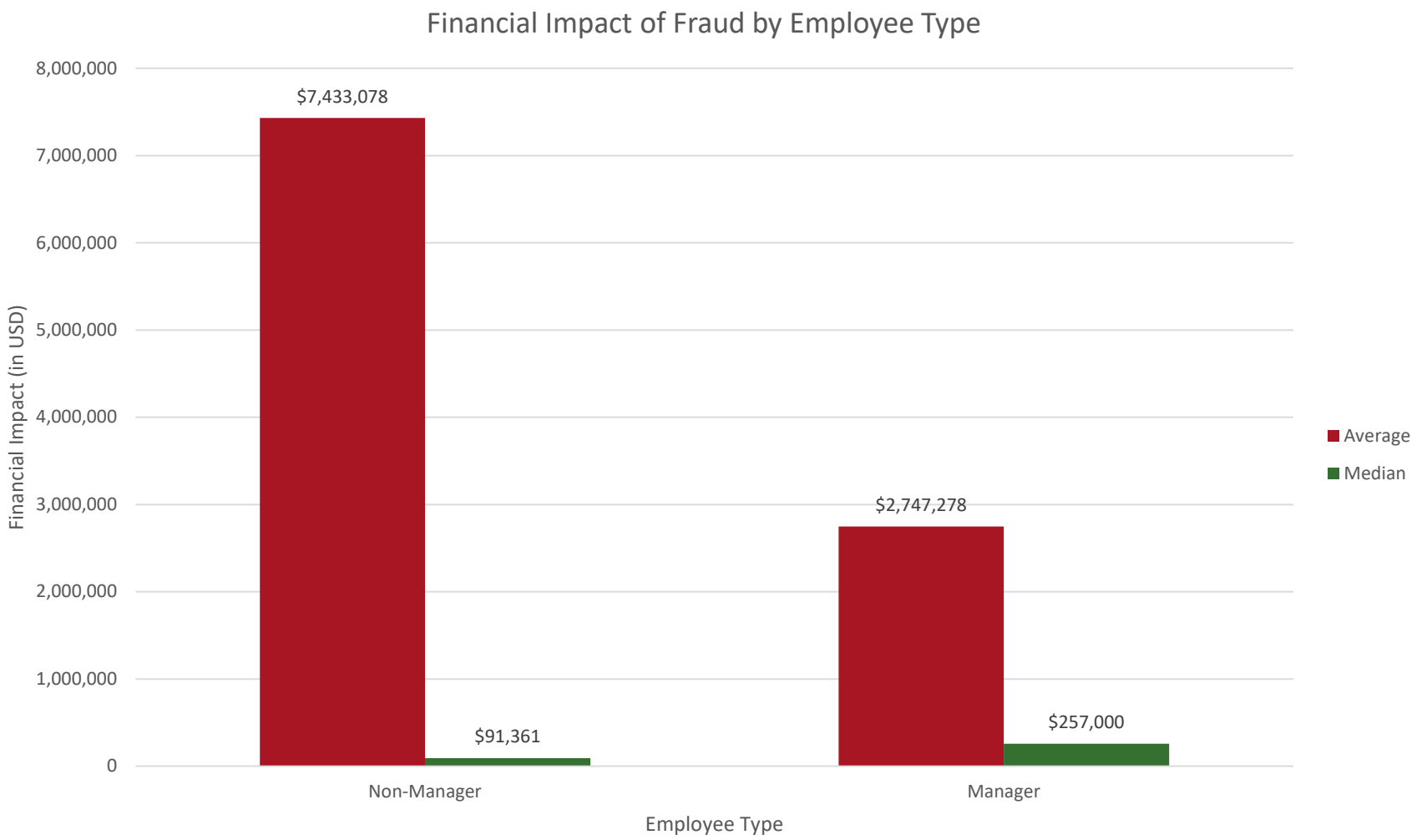
Non-Technical Positions



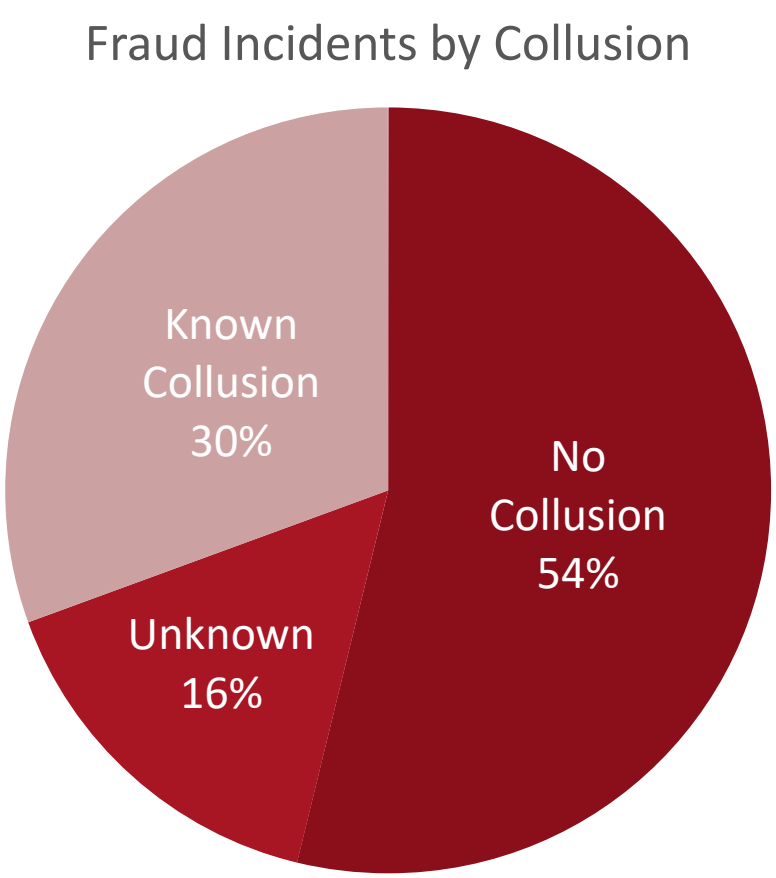
Three-quarters of fraudsters occupied non-technical positions, such as:

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

Fraud by Non-Managers vs. Managers



Fraud and Collusion -1



Most fraud cases do not involve collusion.

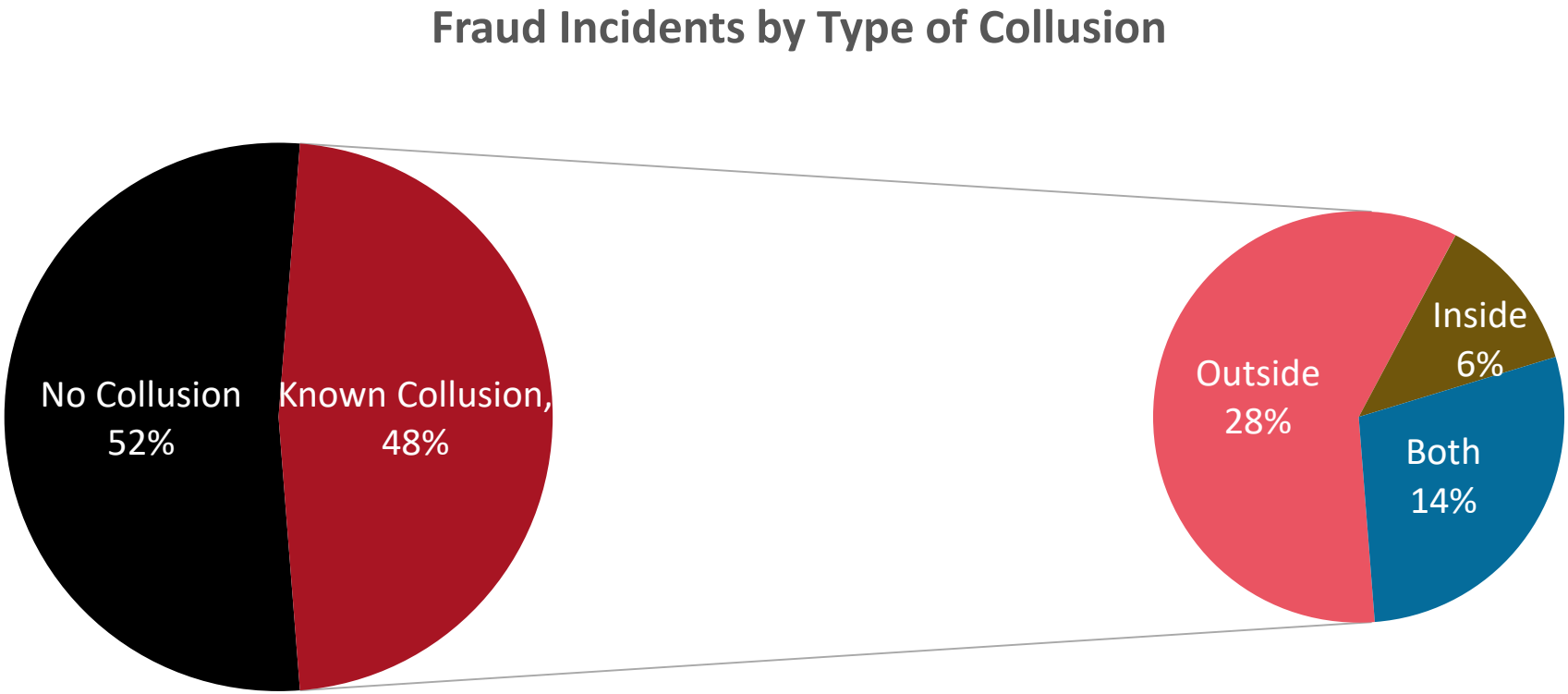
However, it is important to note that:

Approximately 30% 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.

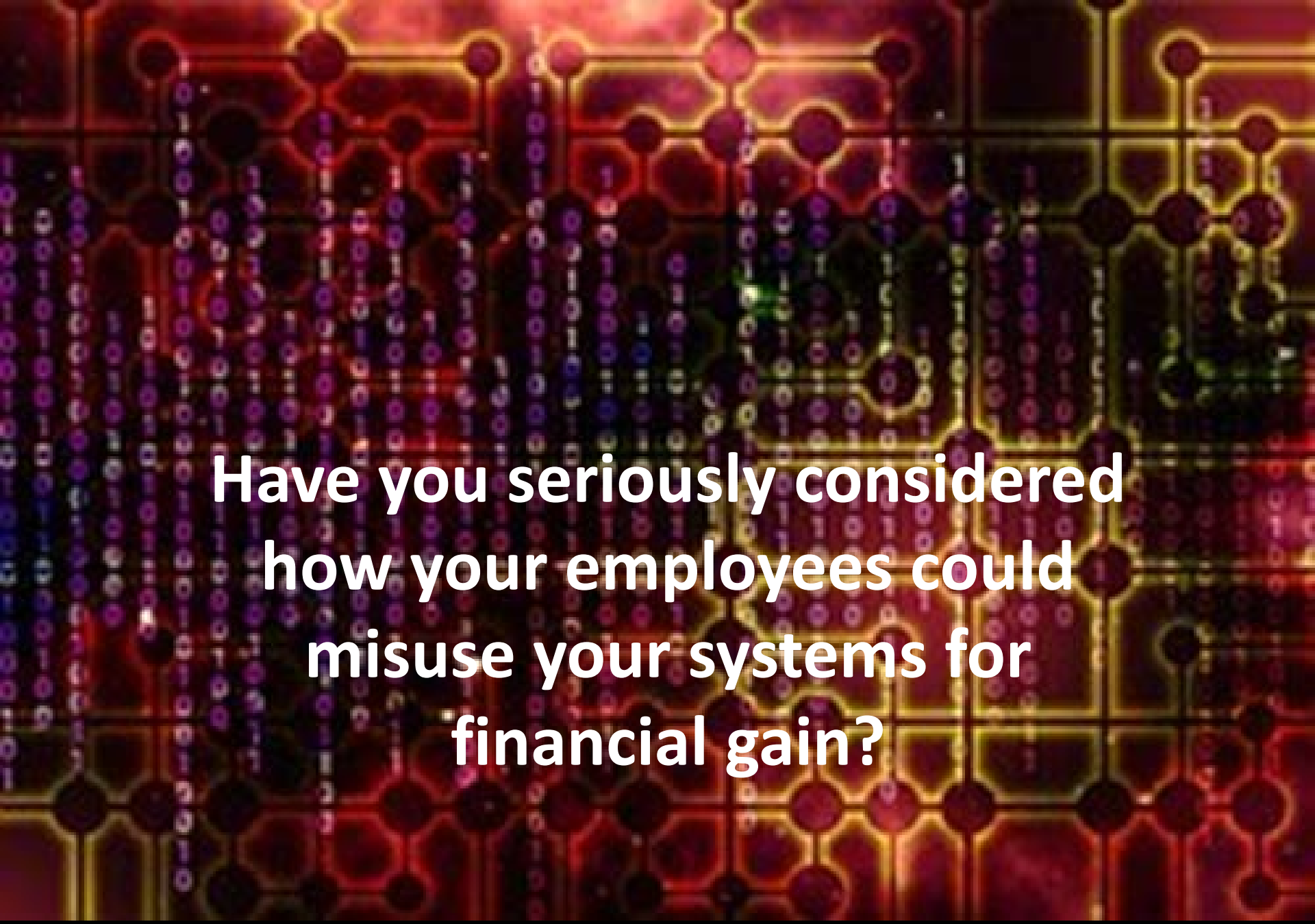
Over half of the insiders were detected by other victim organization employees, though none of the employees were members of the IT staff.

This fact, in conjunction with the mere 6 percent of cases where software and systems were used in detection, seems to indicate that fraud-detection technology was either ineffective or absent.

As expected, most initial responders to the incidents were managers or internal investigators (75 percent).

Countermeasures – Theft to Commit 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 Employee Assistance Program or other recourse for employees experiencing personal or financial problems



Module 5 Conclusion

Insider Threat Fraud

- usually perpetrated by current employees
- is usually committed during normal working hours using authorized access
- is usually focused on theft or modification of PII or customer information
- usually occurs over a long period of time at a low level of activity
- initial model showed acts were committed by low-level staff, but recent Fraud Study funded by DHS showed that managers also perform fraud and their activities usually cause more damage
- detection often resulted from routine or impromptu audits
- Prevention and mitigation strategies can include
  - Clearly document and consistently enforce policies and controls.
  - Log, monitor, and audit employee online actions.
  - Pay special attention to accountants and managers.

Summary of Malicious/Intentional Insider Threats

	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, or 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 Info
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

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

Module 6 – Unintentional Insider Threat

Summary of Cases

Over 130 Cases Collected

- Case had to include either of the following two situations:
  - A non-malicious insider makes a mistake or loses a device.
  - A secondary actor influences a non-malicious insider to take an action that provides the actor access to the assets or at least enables the actor to have a potential impact on them.

Sources of Collected Cases

- Privacy Rights Clearinghouse (PRC) www.privacyrights.org
- Articles from public media

Patterns of Incidents

Four patterns of incidents were identified based on the threat vector.

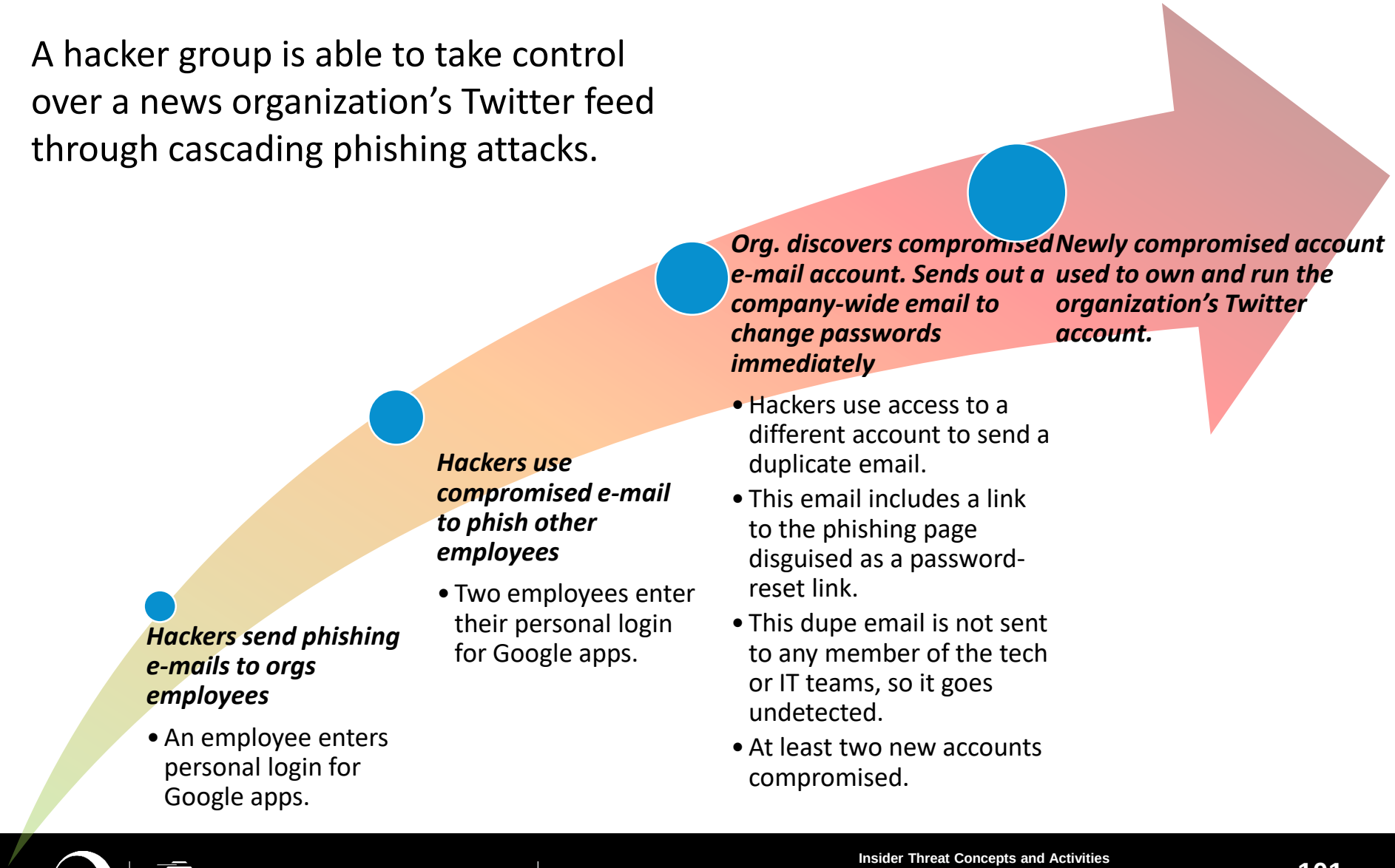
DISC	accidental disclosure (e.g., via the internet)
	sensitive information posted publicly on a website, mishandled, or sent to the wrong party via email, fax, or mail
UIT-HACK	malicious code (e.g., hacking, malware/spyware)
	an outsider's electronic entry acquired through social engineering (e.g., phishing email attack, planted or unauthorized USB drive) and carried out via software, such as malware and spyware
PHYS	improper/accidental disposal of physical records
	lost, discarded, or stolen non-electronic records, such as paper documents
PORT	portable equipment no longer in possession
	lost, discarded, or stolen data storage device, such as a laptop, PDA, smart phone, portable memory device, CD, hard drive, or data tape

TRUE STORY: Example of DISC Threat Vector

Congressman posts travel plans and current location on Facebook while visiting a theater of conflict.

Example for UIT-HACK Threat Vector

A hacker group is able to take control over a news organization's Twitter feed through cascading phishing attacks.



Hackers send phishing e-mails to orgs employees

- An employee enters personal login for Google apps.

Hackers use compromised e-mail to phish other employees

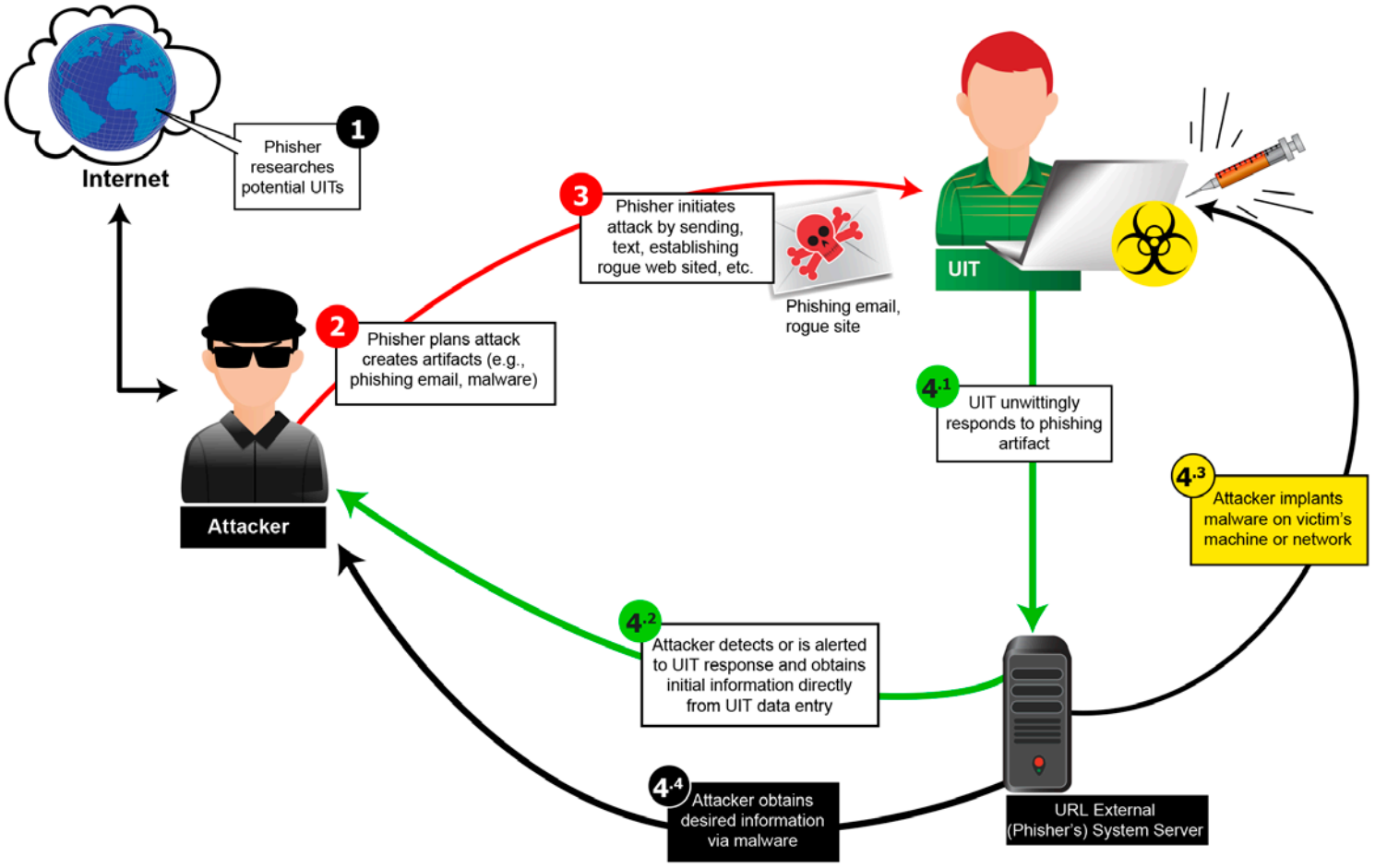
- Two employees enter their personal login for Google apps.

Org. discovers compromised e-mail account. Sends out a company-wide email to change passwords immediately

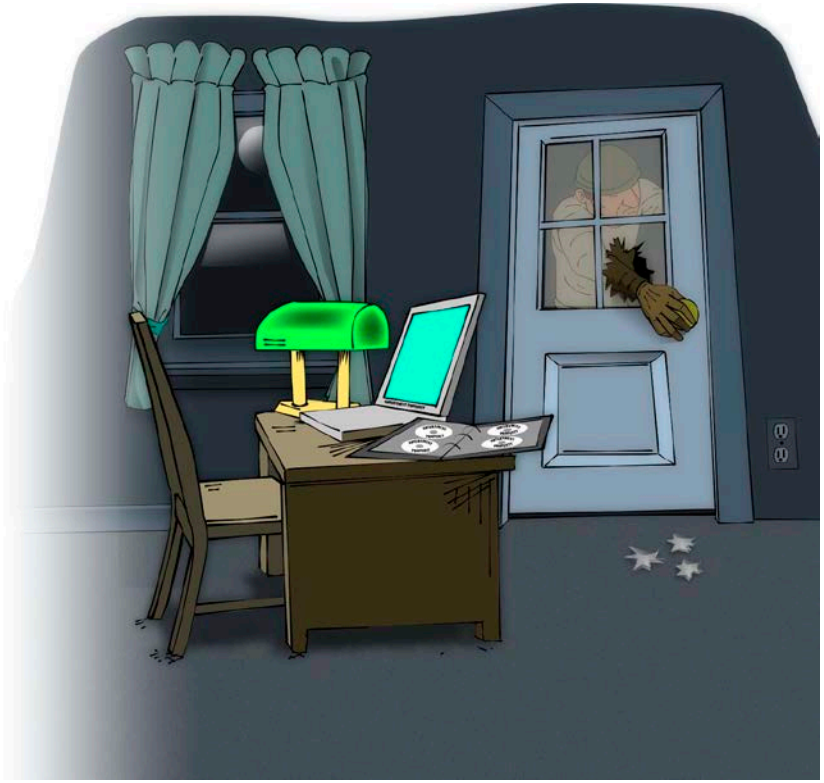
- Hackers use access to a different account to send a duplicate email.
- This email includes a link to the phishing page disguised as a password-reset link.
- This dupe email is not sent to any member of the tech or IT teams, so it goes undetected.
- At least two new accounts compromised.

Newly compromised account used to own and run the organization's Twitter account.

Case Examples – UIT-HACK Threat Vector



TRUE STORY: Example of PORT Threat Vector



A mid-level employee copied millions of personnel records to CDs and stored them, along with a work laptop in their home.

Someone broke into their home, stealing these items.

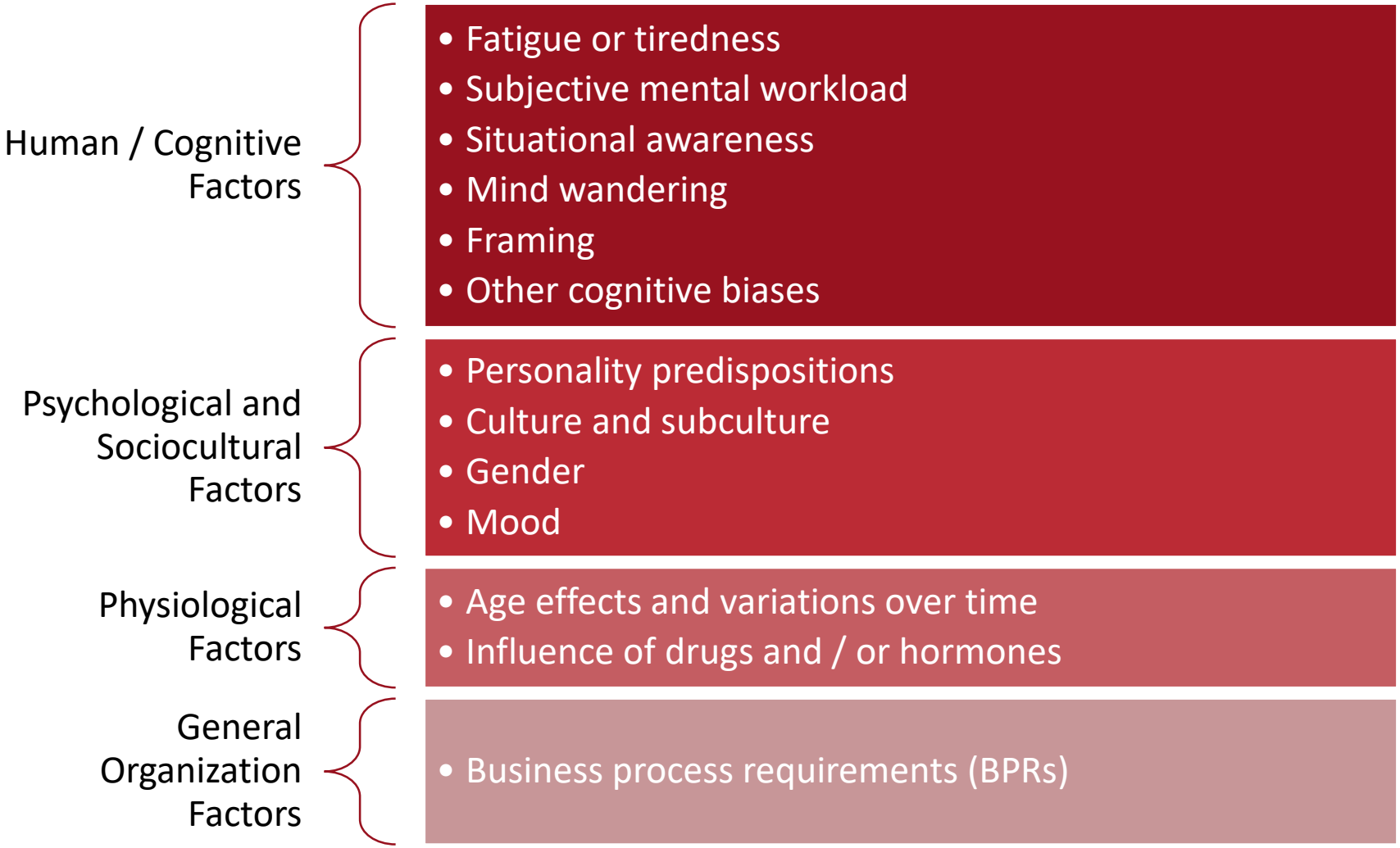
This is one of the largest single breaches ever documented in terms of numbers of individuals affected.

TRUE STORY: Example of PHYS Threat Vector

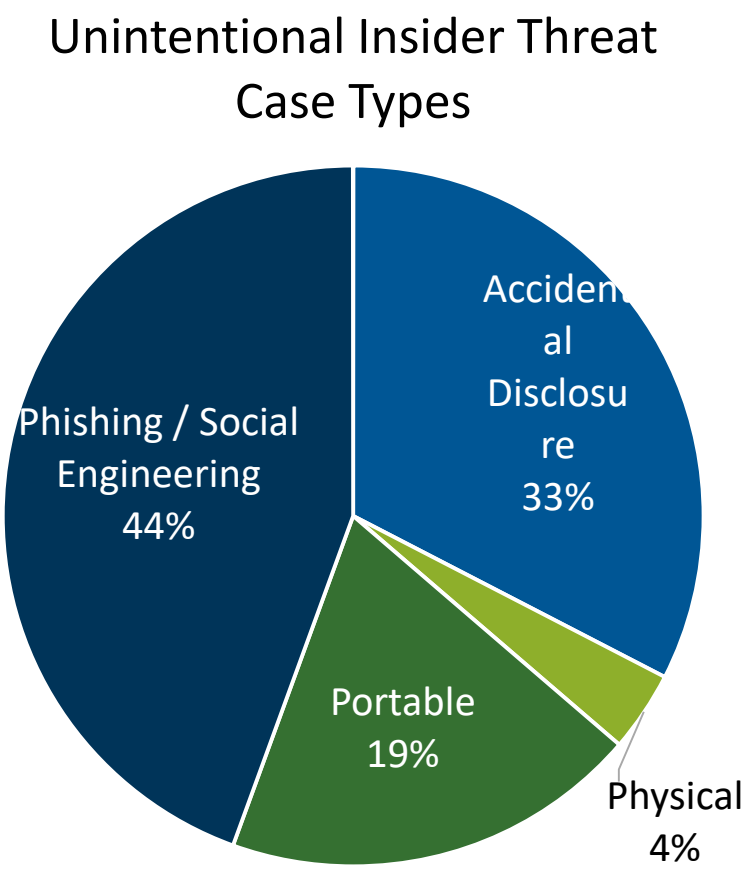
Two cases of 4-6 cards with names, birth dates and Social Security numbers, and salaries of employees who worked for a State government agency in the late 1970s were sold as surplus items.

The purchaser asked $300,000 payment for return as punishment for government laxity. The State threatened a lawsuit to obtain the return of the cards.

Contributing Factors in Risk Perception



Key Takeaways



Half (50%) of Phishing / Social Engineering cases were caused by External Subjects / Hacks.

Over three-quarters (78%) of incidents were the responsibility of the insider.

Mitigation Strategies for Unintentional Insider Threats

Threat Vector		UIT-HACK	DISC	PHYS	PORT
MITIGATION / COUNTERMEASURE	Training to heighten awareness and reduce human error (BP 9, BP 7)	X	X	X	X
	Usability of software and tools to reduce human error	X	X		
	Management practices to reduce likelihood of human error (BP 5, BP 8)	X	X	X	X
	Email safeguards (anti-phishing, anti-malware) (BP 7)	X	X		
	Firewalls	X	X		
	Antivirus/anti-malware protection (BP 19)	X	X		X
	Data encryption on storage devices (BP 13, 19)		X		X
	Password protection on storage devices (BP 10,19)		X		X
	Wireless and Bluetooth safeguards (disable, protect) (BP 13)				X
	Remote memory wipe for lost equipment (BP 13, 19)				X

Module 6 Conclusion

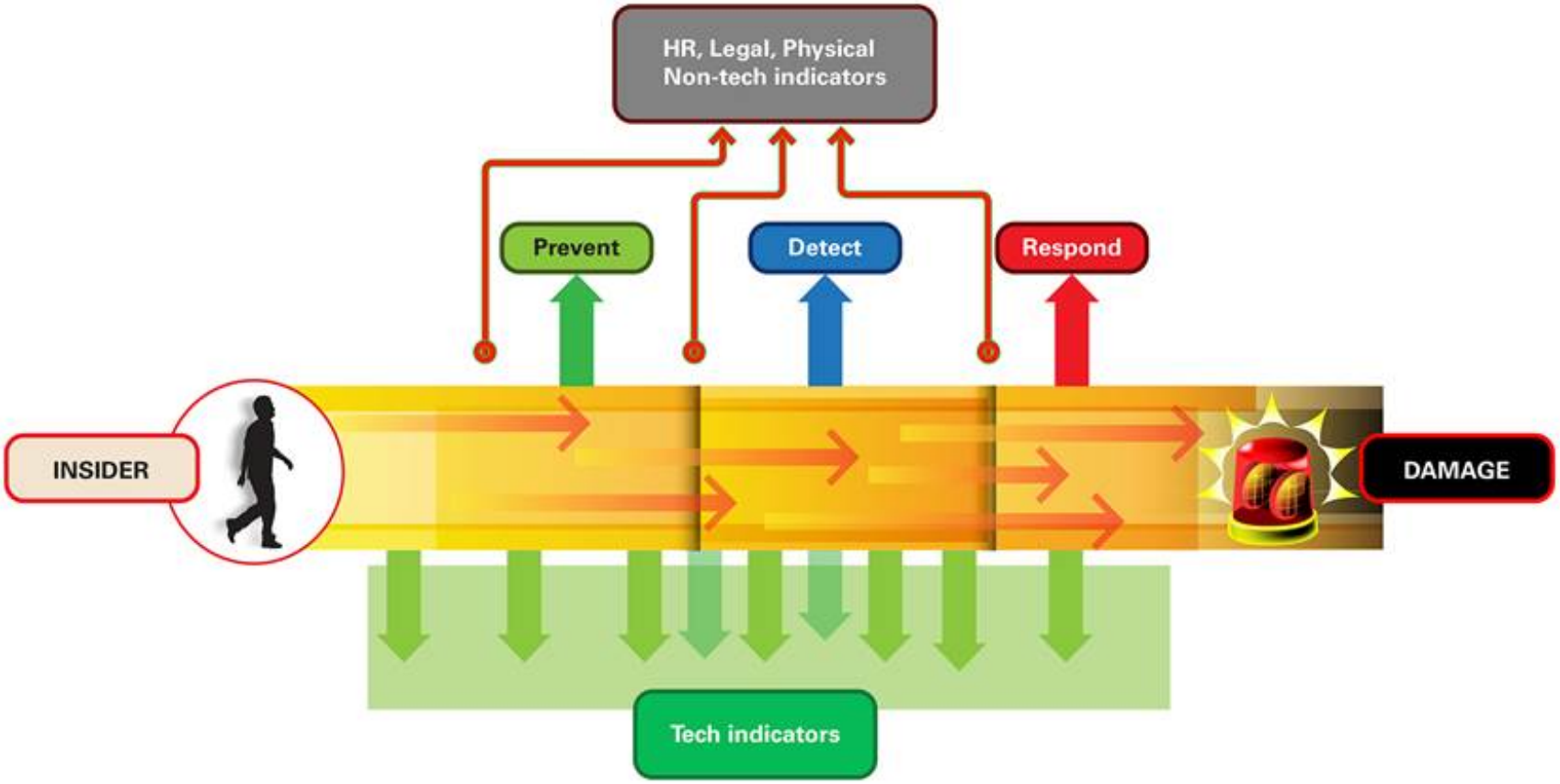
Unintentional Insider Threat:

- Is Human
- Can be prevented, detected, and mitigated
- Will not be eliminated

Many of the same controls used for Malicious Insider Threat are also useful for Unintentional Insider Threat.

Module 7: Insider Threat Prevention, Detection, and Mitigation Strategies

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



Stages of Insider Threat Mitigation

Common Sense Guide to Mitigating Insider Threats

http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=484738

Best Practices for Insider Threat Mitigation -1

Know and protect your critical assets.
Develop a formalized insider threat program.
Clearly document and consistently enforce policies and controls.
Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.
Anticipate and manage negative issues in the work environment.
Consider threats from insiders and business partners in enterprise-wide risk assessments.
Be especially vigilant regarding social media.
Structure management and tasks to minimize unintentional insider stress and mistakes.
Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.
Implement strict password and account management policies and practices.

Best Practices for Insider Threat Mitigation -2

Institute stringent access controls and monitoring policies on privileged users.
Deploy solutions for monitoring employee actions and correlating information from multiple data sources.
Monitor and control remote access from all end points, including mobile devices.
Establish a baseline of normal behavior for both networks and employees.
Enforce separation of duties and least privilege.
Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.
Institutionalize system change controls.
Implement secure backup and recovery processes.
Close the doors to unauthorized data exfiltration.
Develop a comprehensive employee termination procedure.

Technical and Organizational Strategies

Insider Threat Controls

Balance information sharing with information restriction and monitoring.

- Technical Controls
- Management Controls
- Operational Controls

Use traditional controls.

- Account management

Customize traditional controls.

- Monitoring

Add new approaches.

Some Available Controls from CERT

Using Plagiarism Detection Algorithms to Prevent Data Exfiltration in Near Real Time

Detecting and Preventing Data Exfiltration Through Encrypted Web Sessions via Traffic Inspection

Using a SEIM Signature to Detect Potential Precursors to IT Sabotage

Using Centralized Logging to Detect Data Exfiltration Near Insider Termination

More information is available at:
http://www.cert.org/insider-threat/research/controls-and-indicators.cfm

Insider Threat Technical Issues

Use technical balancing where possible.

- Identify critical proprietary information / files.
- Consider digital rights management.
- Consider encryption.
- Log access to critical proprietary information / files.
- Consider host-based monitoring, including laptops.
- Consider data leakage protection tools for detection of exfiltration of critical information.

Account management is a critical issue.

Consider change controls for operating system scripts, mission critical systems, and executables that should not change frequently.

Carefully design a code review strategy.

Our Suggestion

Continuous Logging (Trust)

Targeted Monitoring (Enforce)

Real-time Alerting (Verify)

Application to your Organization -1

Many organizations are able to log the majority of online activity

BUT

Many organizations do not have the resources, including software, hardware, and people, to consistently audit and monitor all online transactions

Application to your Organization -2

The challenge to organizations is to use a combination of technical and non-technical potential indicators of malicious activity to identify individuals who may be more at risk of committing an insider crime

and then

Apply the auditing and monitoring strategies outlined in this presentation

Application to your Organization -3

The good news is that most of the monitoring solutions suggested in this presentation can be implemented using existing tools, technologies, and staff

But it does require new processes for communication between HR, IT, Information Security, Legal, Physical Security, management, … regarding employee issues

- Employees on the HR radar
- Employees who are about to be terminated, have resigned, have been laid off, …

It Is Important to Remember…

Policies and procedures must be in place and enforced.

Policies and procedures should outline:

- Who handles incidents perpetrated by insiders.
- How are these incidents reported and tracked.
- At what stage and via what process is HR, IT, legal, and law enforcement contacted or involved in the handling of such incidents.

Determine who is authorized to work with human resources or any other group established to handle insider problems.

- Whoever has been identified to handle and track these types of events, should work with HR when a problem is suspected.
- While working with HR, IT should also be involved to monitor online activity.

Management or management policy should outline when and how legal and law enforcement is involved.

Insider Threat Organizational Requirements

Organizational

- Work together as a unit.
- Know critical assets.
- Know who has authorized access to an organization's network, system or data.
- Develop policies and procedures regarding insider problems and who will handle them and how.
- Understand how legal, privacy, and policy issues impact the organization.

- Know your actors.
  - Employees
  - Contractors
  - Subcontractors
  - Suppliers
  - Trusted Business Partners
- Plan awareness training for all your actors.
  - Determine who needs to know what.

Final Thoughts

Caveats:

- For malicious insider activities and mitigations, we only have data on criminals
  - Our findings / recommendations could result in a high false positive rate
- These monitoring techniques are not a guarantee
  - In the event of a missed insider attack, these methods will be tremendously beneficial for incident response and forensic analysis teams
- Consider legal, privacy, and policy issues before implementing any employee monitoring program

Food for thought:

- Which of the monitoring techniques we've presented might also be effective in detecting external intruders if they manage to gain access?
- Could these controls be effective against both insiders and outsiders?

Module 7 Conclusion

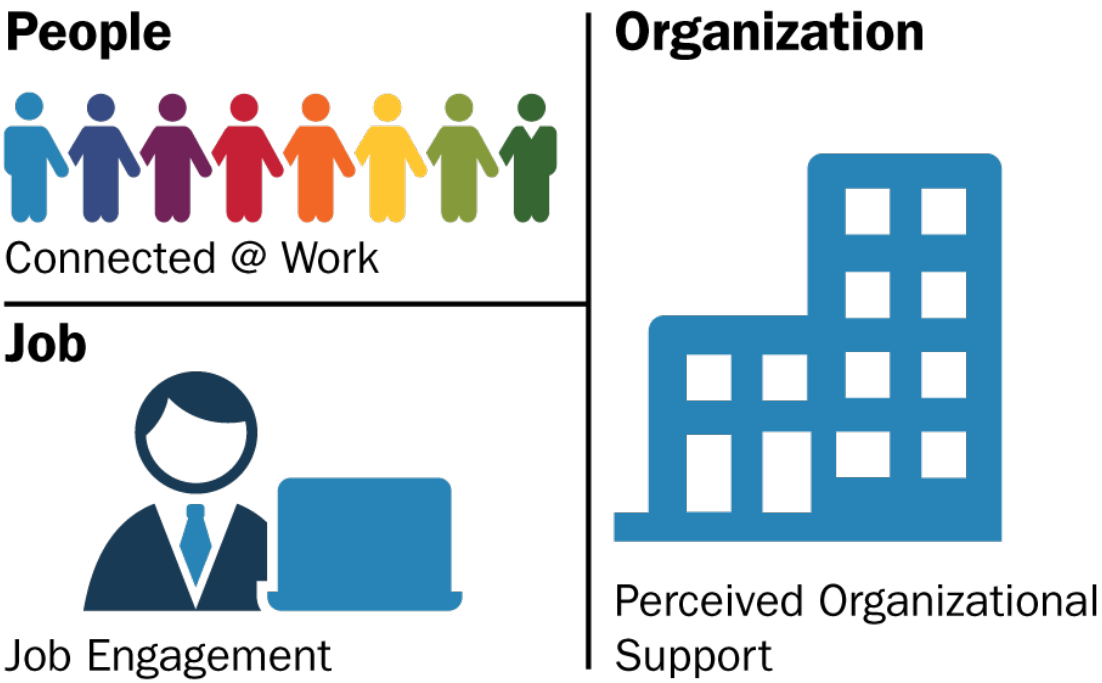
Organizations need both technical and organizational solutions for effective prevention, detection, and response to insider threat activity.

Monitoring of both technical and organizational indicators is the only way to successful identify potential insider threats and risks.

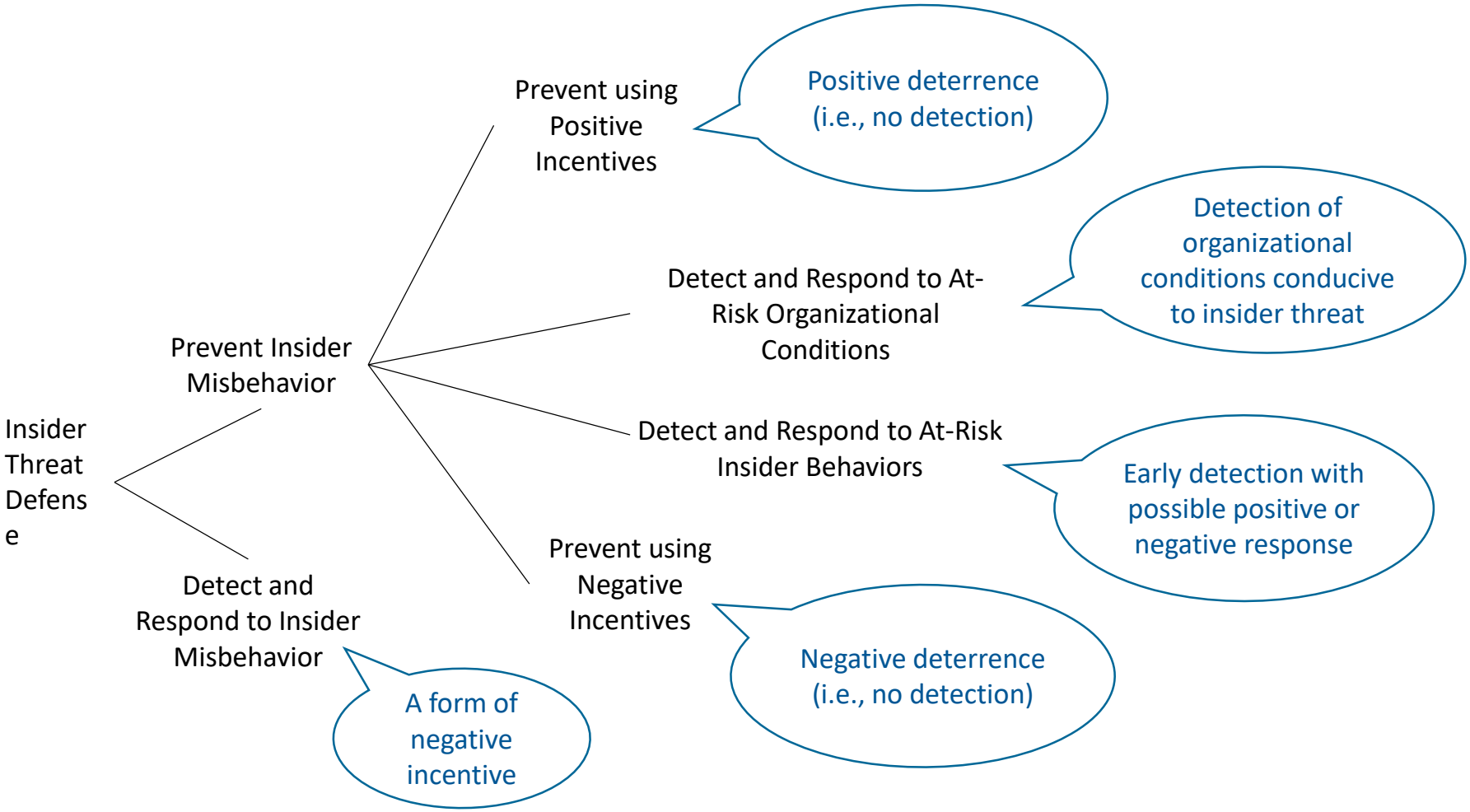
Controls and processes that are part of a successful information assurance program will also be part of a successful insider threat program.

Positive Incentives and Insider Threat

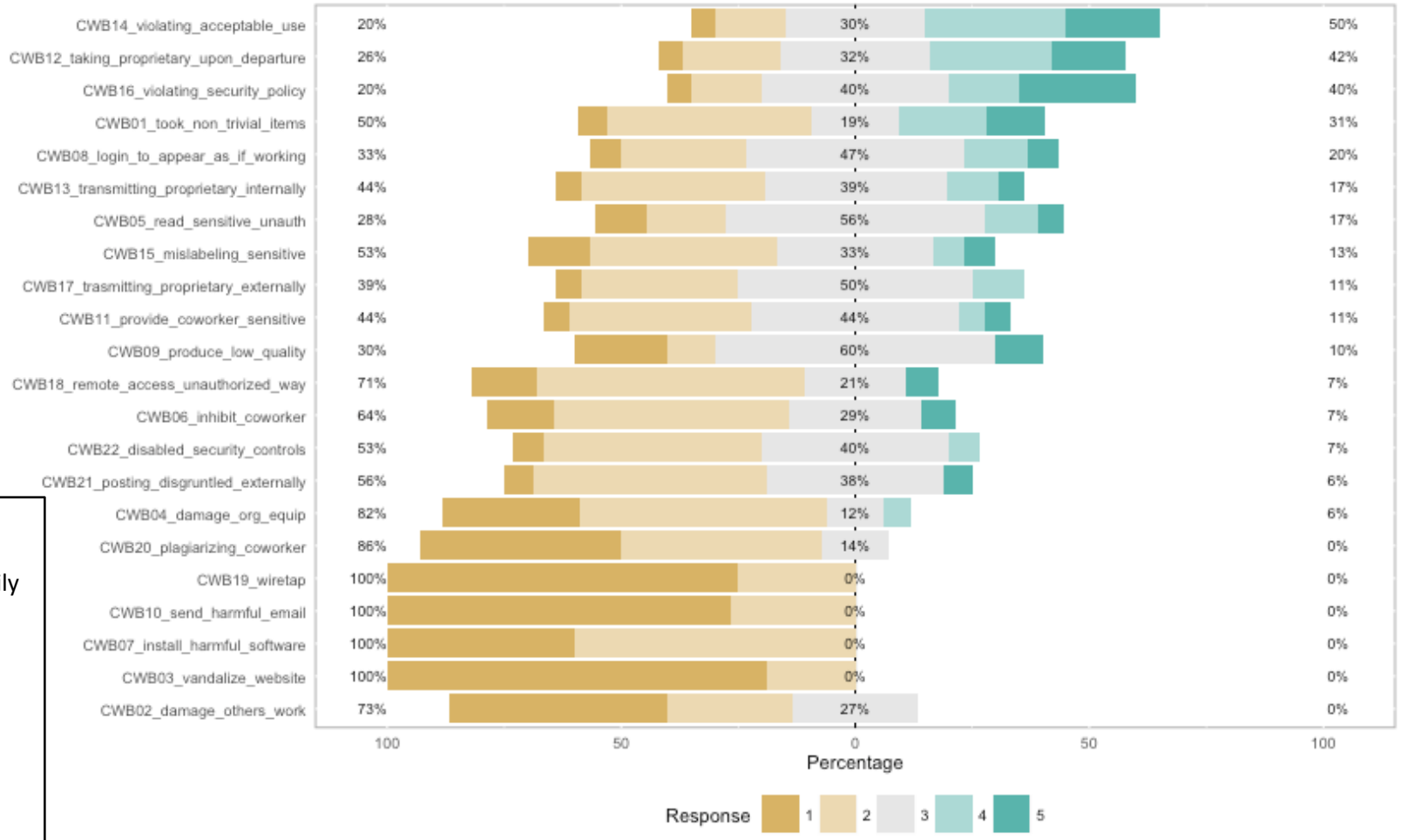
Three Dimensions of Employee-Organization Alignment



Research Context



Descriptive Stats: Counterproductive Work Behaviors



Frequency Rating

5: All the time
- At least once daily

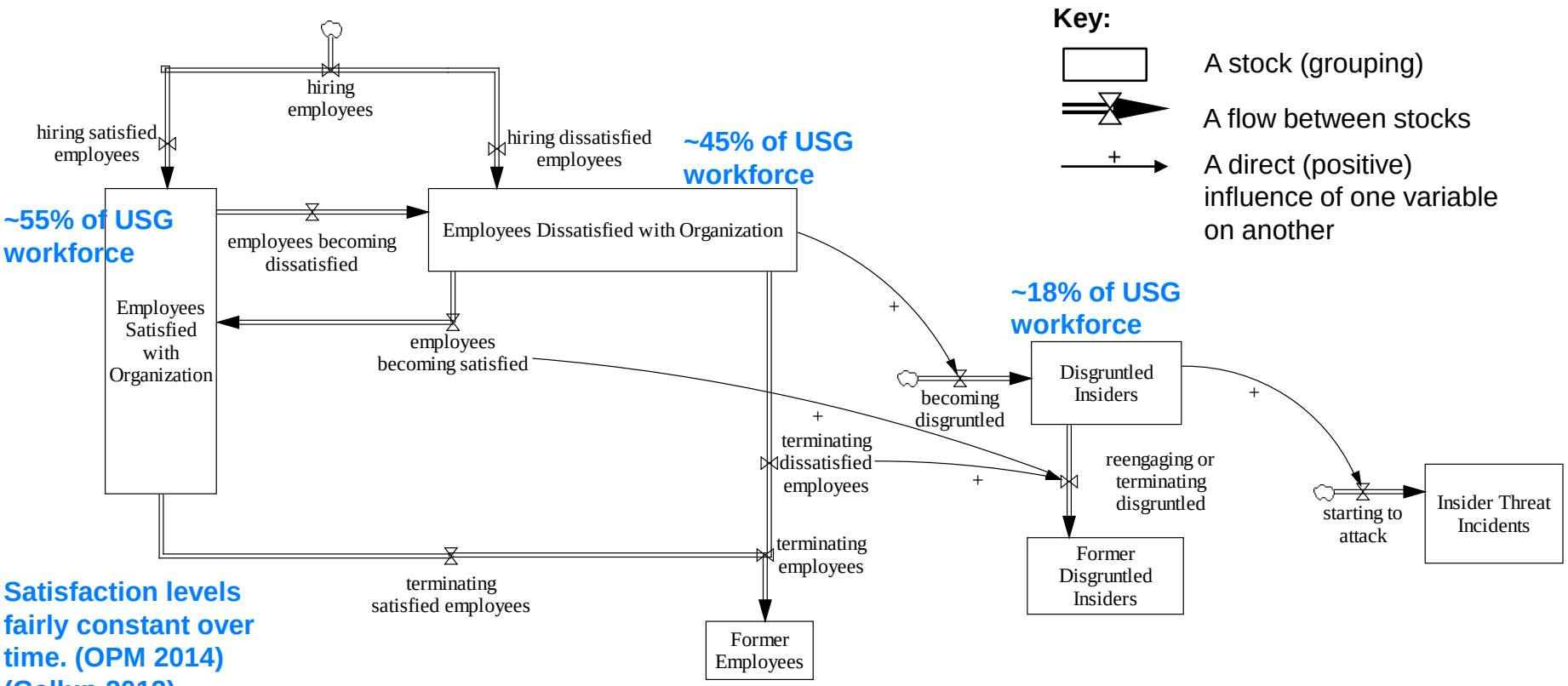
4: Often
- At least once a week

3: Sometimes
- At least every other month

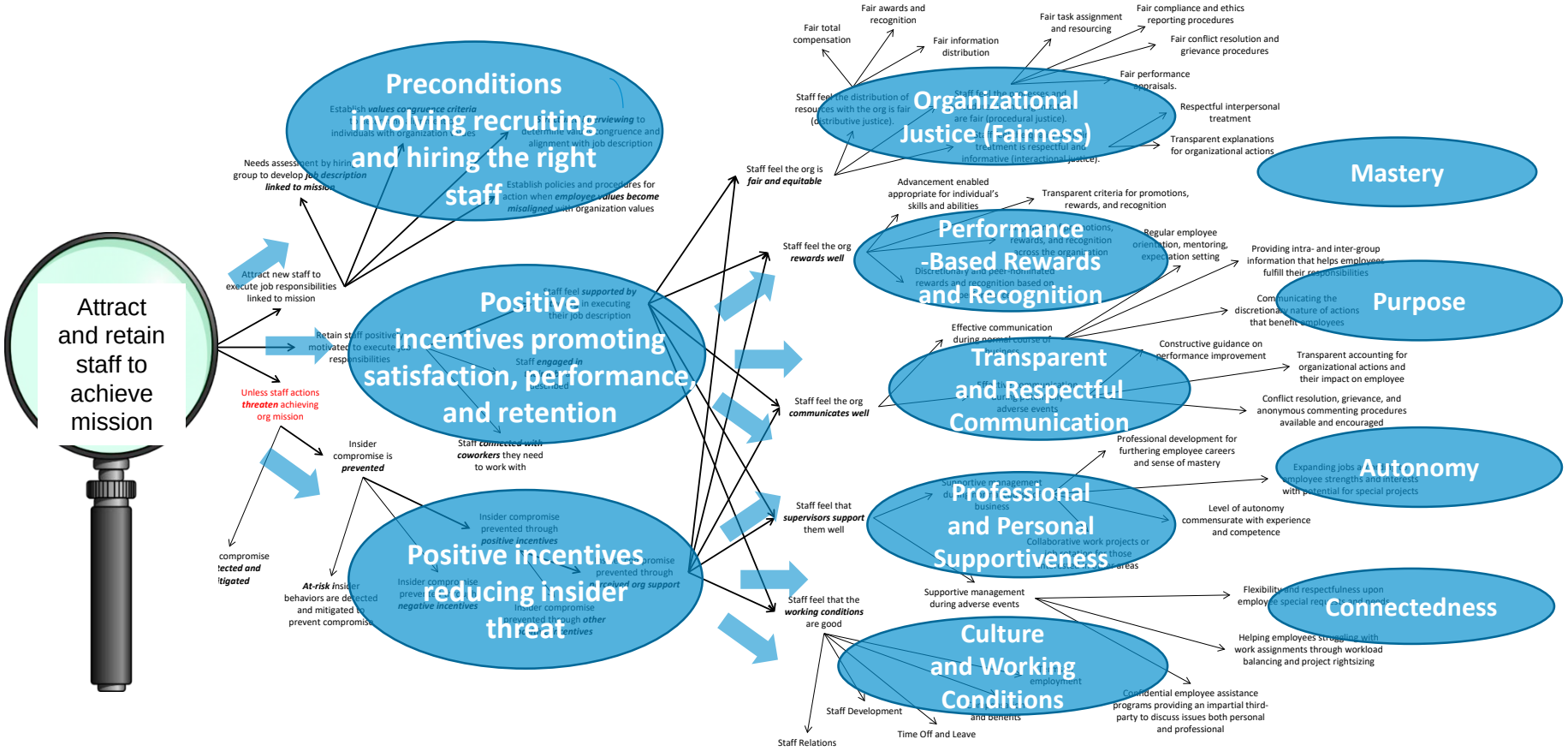
2: Occasionally
- At least once a year

1: Never

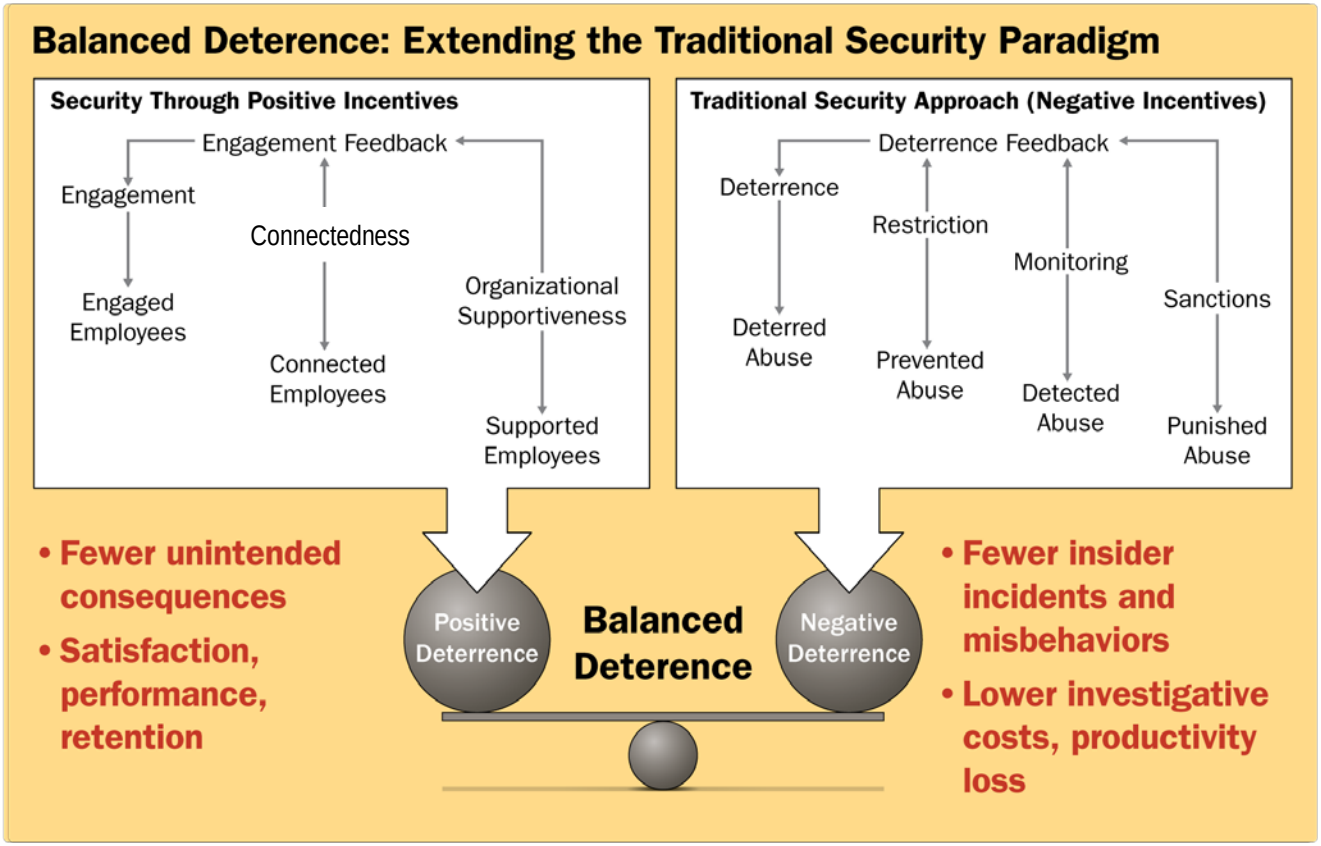
Emerging Physics of Job Satisfaction, Disgruntled Insider Threat



Positive Incentive-Based Principles and Practice Areas



Vision: Extending the Traditional Security Paradigm



Course Conclusion

Insider Threat Mitigation

Need to balance information sharing with information restriction and monitoring

- Technical Controls
- Management Controls
- Operational Controls

Traditional Controls

- Many insider attacks could be prevented by traditional controls (e.g. account management)
- Other insider attacks could be prevented by customizations to traditional controls (e.g. monitoring)
- Some insider attacks may require new approaches altogether

Short Term

Form an insider threat team that includes HR, Legal, IT, Information Security, Data Owners, Management, Security.

Create policies that cross organizational boundaries – work with legal counsel.

Consistently enforce the policies.

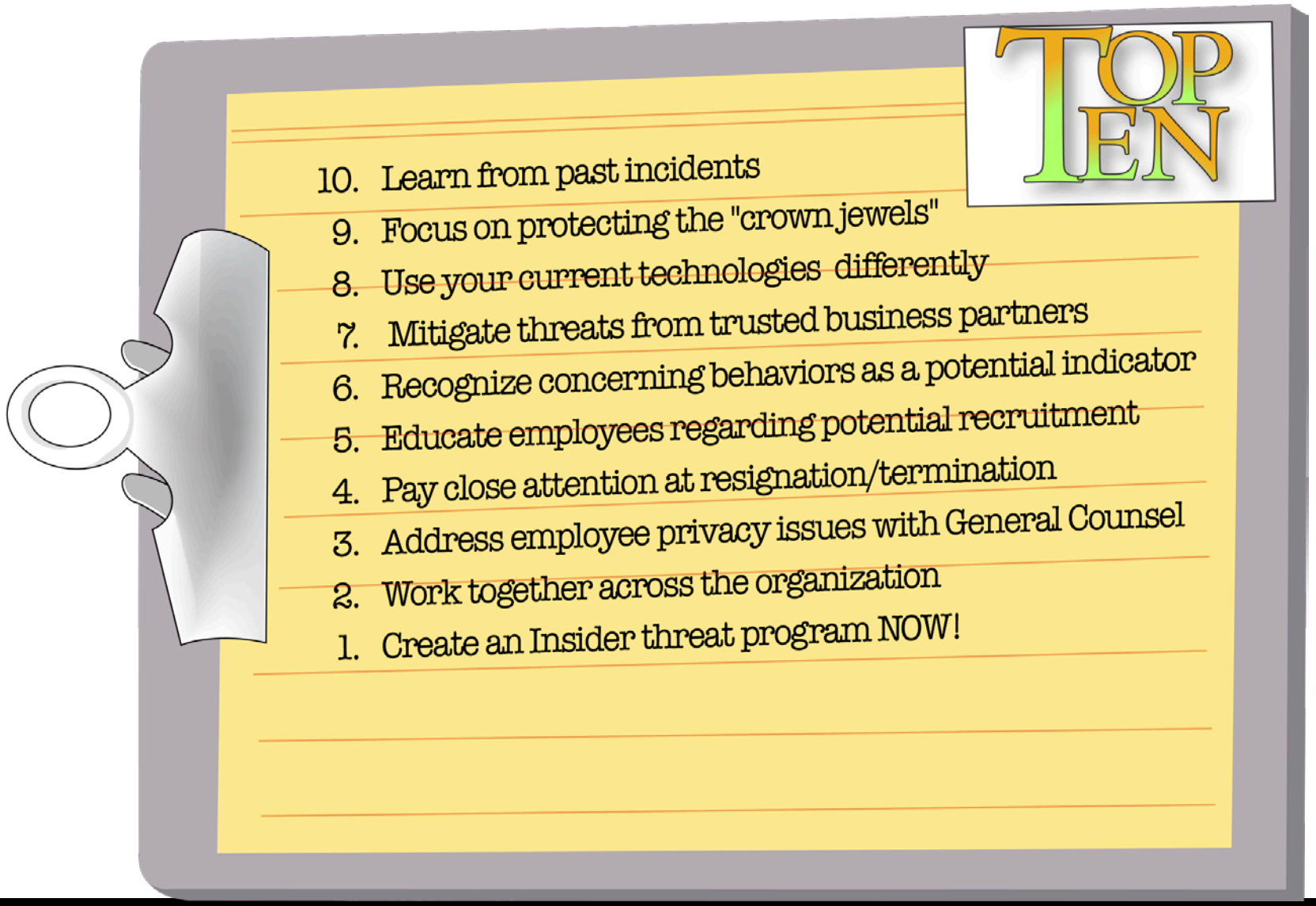
Develop processes and implement controls that enforce communication across departments.

Long Term

Automated detection mechanism

- Unified rules engine configured with insider threat indicators and risk thresholds
- Data mining system that correlates unstructured data contained in logs, browsing information, email, internal documents, performance reviews, physical access, etc.
- Intelligent reasoning system that can make a decision about whether to flag a user as being a risk to the organization

The CERT Top 10 List for Winning the Battle Against Insider Threats



Resources

NITC Resource Highlights

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 Control/Indicator Development / Deployment

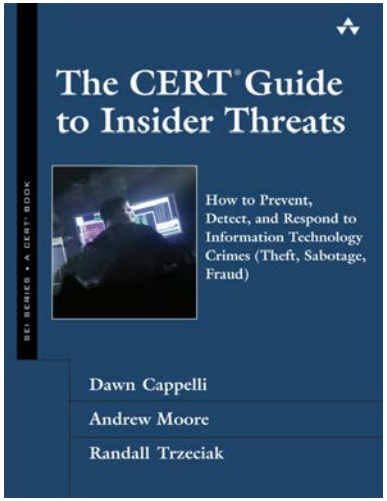
Insider Threat Data Analytics Hub Development / Deployment

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

NTIC Publications and References



Collins, M., Theis, M., Trzeciak, R. F., Strozer, J., Clark, J., Costa, D., Cassidy, T., Albrethsen, M., & Moore, A. P. (2016). Common Sense Guide to Mitigating Insider Threats (5th Ed.). Pittsburgh: Software Engineering Institute.

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.

Moore, Andrew; Savinda, Jeff; Monaco, Elizabeth; Moyes, Jamie; Rousseau, Denise; Perl, Samuel; Cowley, Jennifer; Collins, Matthew; Cassidy, Tracy; VanHoudnos, Nathan; Buttles-Valdez, Palma; Bauer, Daniel; & Parshall, Allison. The Critical Role of Positive Incentives for Reducing Insider Threats. CMU/SEI-2016-TR-014. Software Engineering Institute, Carnegie Mellon University. 2016.

Many more at: https://www.cert.org/insider-threat/publications/index.cfm

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/