



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

Course Introduction

Notices

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

CERT® and CERT Coordination Center® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-0486

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.





COULD THIS HAPPEN TO YOU?

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 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 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 Insider Threat Center

Notices

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

CERT® and CERT Coordination Center® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-0486

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)

What Is the CERT Insider Threat Center?

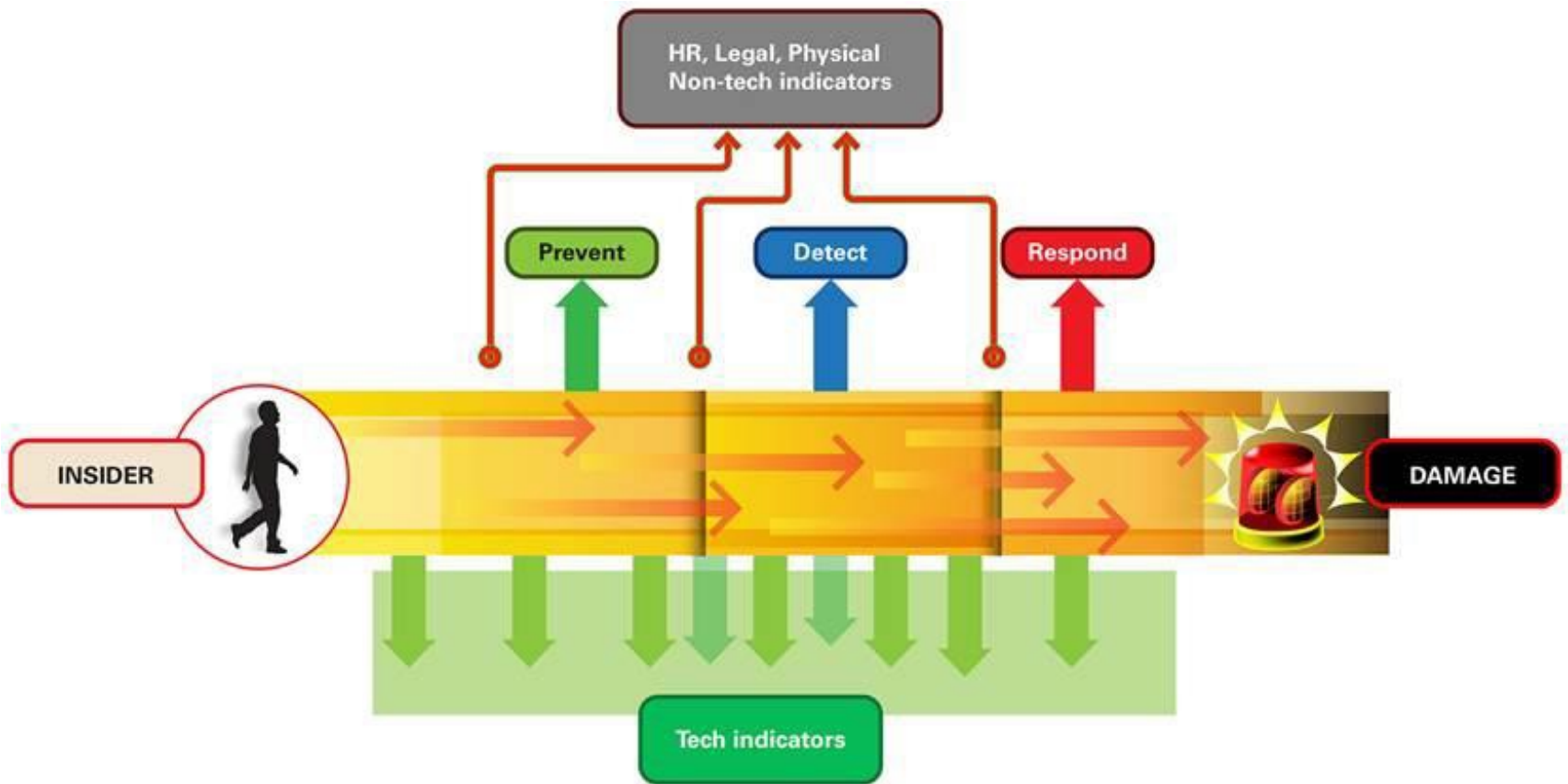
Center of insider threat expertise

Began working in this area in 2001
with the U.S. Secret Service



Our mission: *The CERT Insider Threat Center conducts empirical research and analysis to develop and transition socio-technical solutions to combat insider cyber threats.*

CERT Insider Threat Center Objective



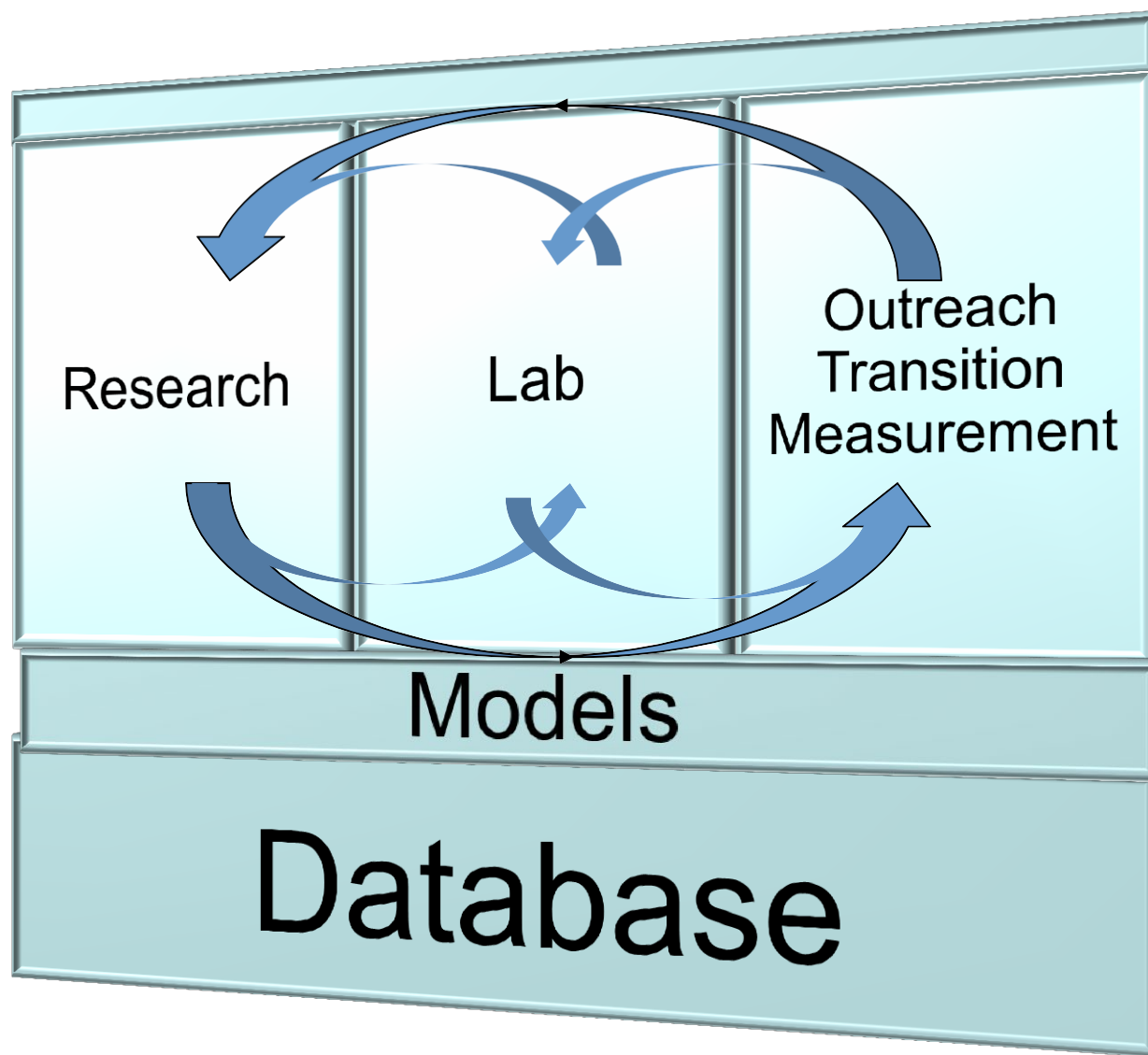
Opportunities for prevention, detection, and response for an insider attack

CERT Insider Threat Center Case Collection Approach

Ongoing collection	Cases from 1996 – present that occurred in the U.S. are coded in the CERT database
Sources	Court documents, interviews, 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



CERT Unique Approach to the Problem -1

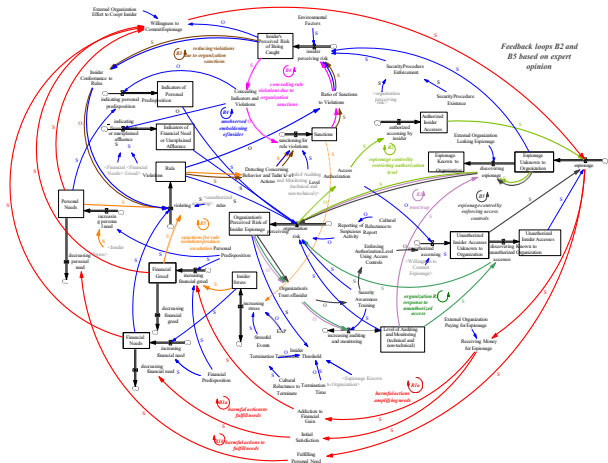


Research Models

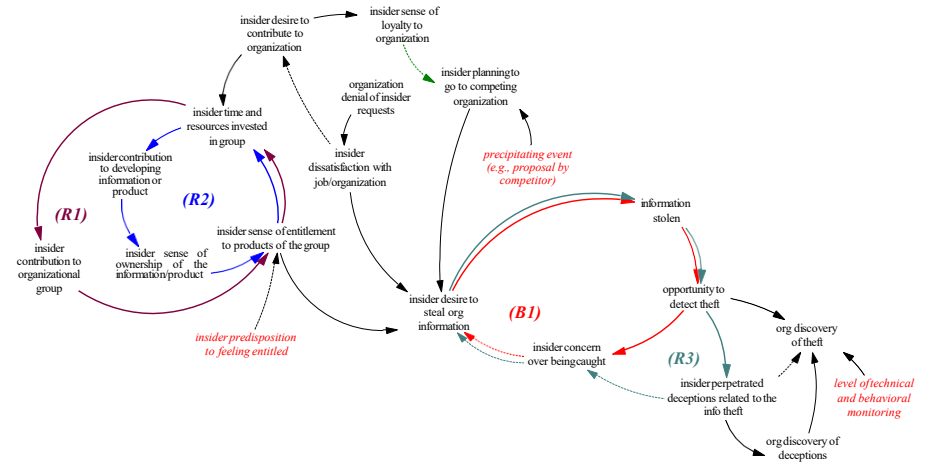


CERT Unique Approach to the Problem -3

Research Models

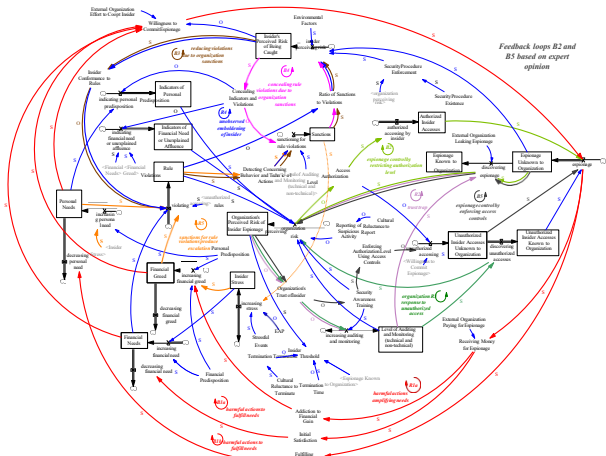


Deriving Candidate Controls and Indicators

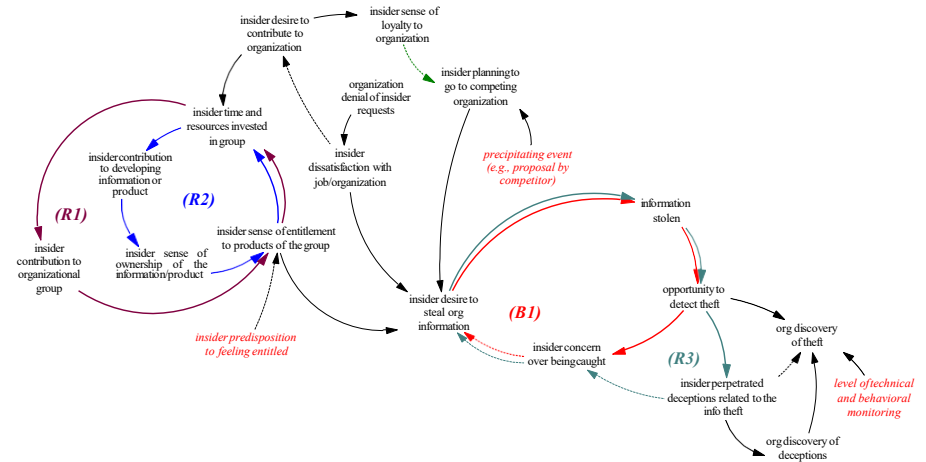


CERT Unique Approach to the Problem -4

Research 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'
```

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

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, culture change

Models (crime profiles)

- IT sabotage
- theft of intellectual property
- employee fraud
- espionage (preliminary)

Trust and Confidentiality

CERT Insider Threat Center *never* reveals or discusses the identity of

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

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

There is not one solution for addressing the insider threat.

- Technology alone may not be the most effective way to prevent and/or detect an incident perpetrated by a trusted insider.

Module 1 Conclusion

The CERT Insider Threat Center

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

Module 2: What is Insider Threat?

Notices

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

CERT® and CERT Coordination Center® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-0486

The CERT Insider Threat Center's Definition

A malicious insider is a current or former employee, contractor, or other business partner who

- *has or had authorized access to an organization's network, system or data and*
- *intentionally exceeded or misused that access in a manner that*
- *negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.*



Another Type of Insider: Unintentional

Current or former employee, contractor, or other business partner who

- *has or had authorized access to an organization's network, system, or data and who, through*
- *through their action/inaction without malicious intent*
- *causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems.*



Separate the “Target” from the “Impact” from the “Actor”

Target

Critical Assets

- People
- Technology
- Information
- Facilities

WHAT

Impact

Confidentiality
Availability
Integrity

HOW

Actor(s)

Employees

- Current
- Former

Contractors

Subcontractors

Suppliers

Trusted Business

Partners

WHO

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?

2014 US State of Cybercrime Survey -1

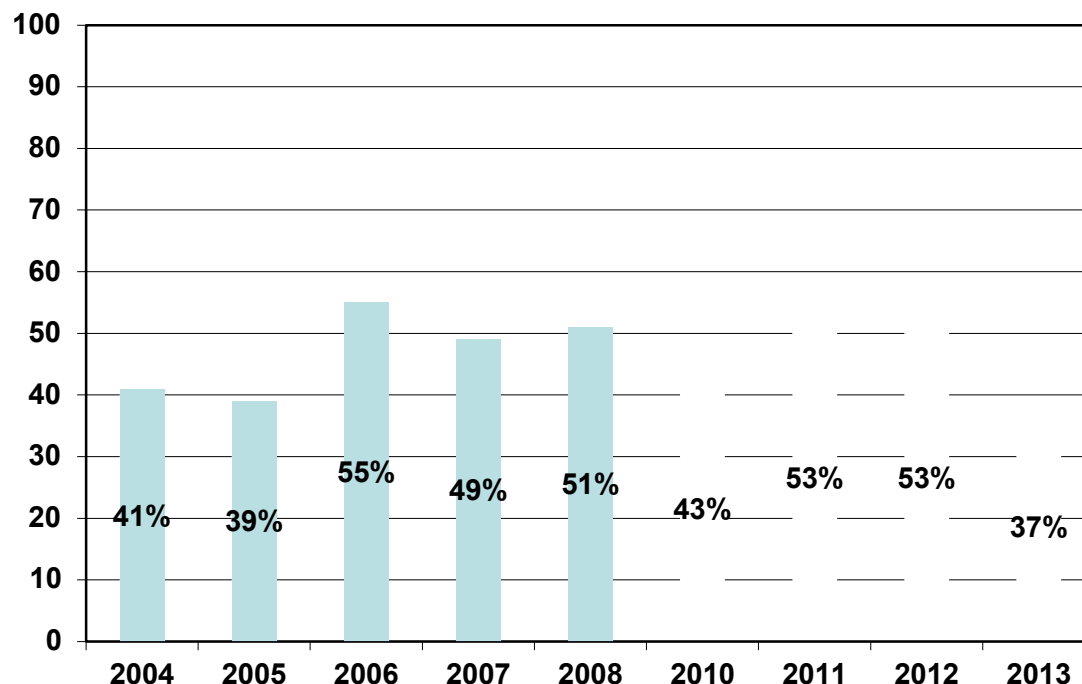
CSO Magazine, USSS, CERT & PWC

557 respondents

Percentage of Participants Who Experienced an Insider Incident

28% of organizations have more than 5000 employees

43% of organizations have less than 500 employees



Source: 2014 US State of Cybercrime Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Price Waterhouse Cooper, April 2014

2014 US State of Cybercrime Survey -2

32 % of respondents	Damage caused by insider attacks more damaging than outsider attacks
---------------------	--

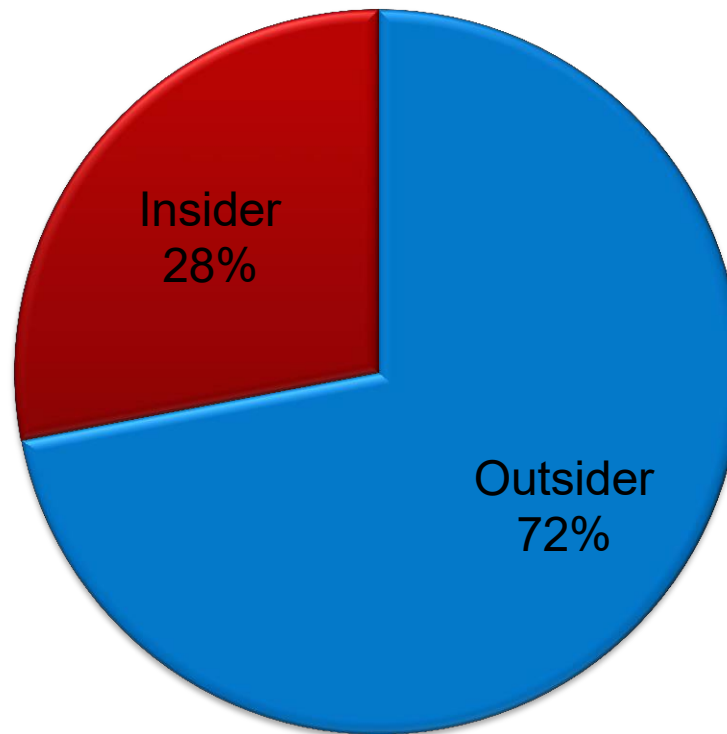
Insiders made up the highest percentage of the following incidents:

Private or sensitive information unintentionally exposed	(82%)
Confidential records compromised or stolen	(76%)
Customer records compromised or stolen	(71%)
Employee records compromised or stolen	(63%)

Source: 2014 US State of Cybercrime Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Price Waterhouse Cooper, April 2014

2014 US State of Cybercrime Survey -3

What percent of the Electronic Crime events are known or suspected to have been caused by:

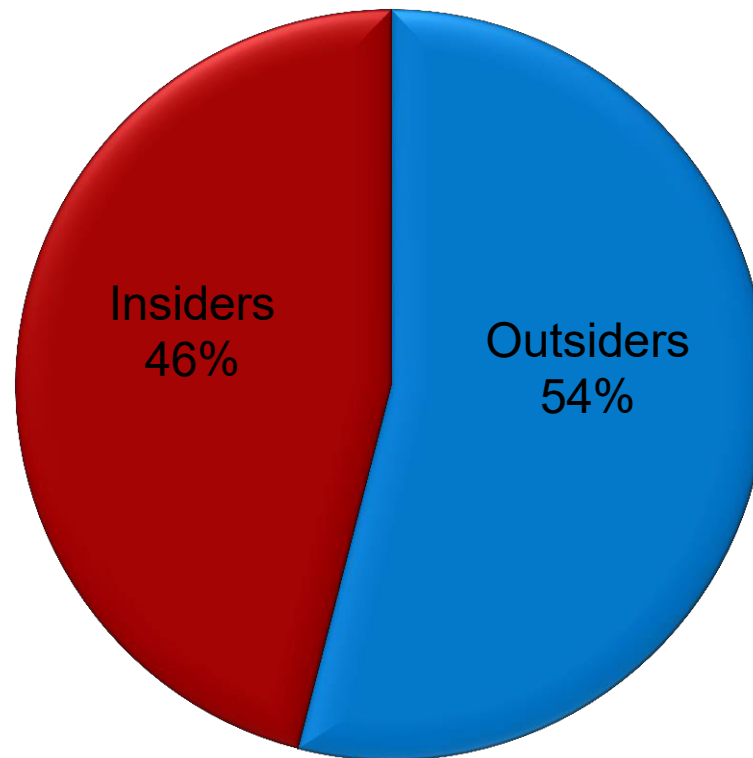


Does not include respondents not aware of which activity was more damaging. Because of this, the number of respondents differed for this question (316).

Source: 2014 US State of Cybercrime Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Price Waterhouse Cooper, April 2014.

2014 US State of Cybercrime Survey -4

Which Electronic Crimes were more costly or damaging to your organization, those perpetrated by:

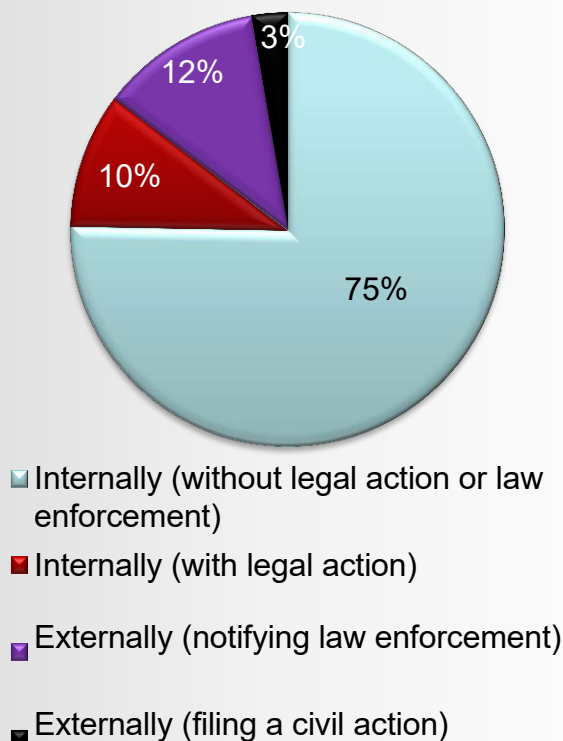


Does not include respondents not aware of which activity was more damaging. Because of this, the number of respondents differed for this question (384).

Source: 2014 US State of Cybercrime Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Price Waterhouse Cooper, April 2014. Does not include respondents not aware of which activity was more damaging.

2014 US State of Cybercrime Survey -5

How Insider Intrusions Are Handled



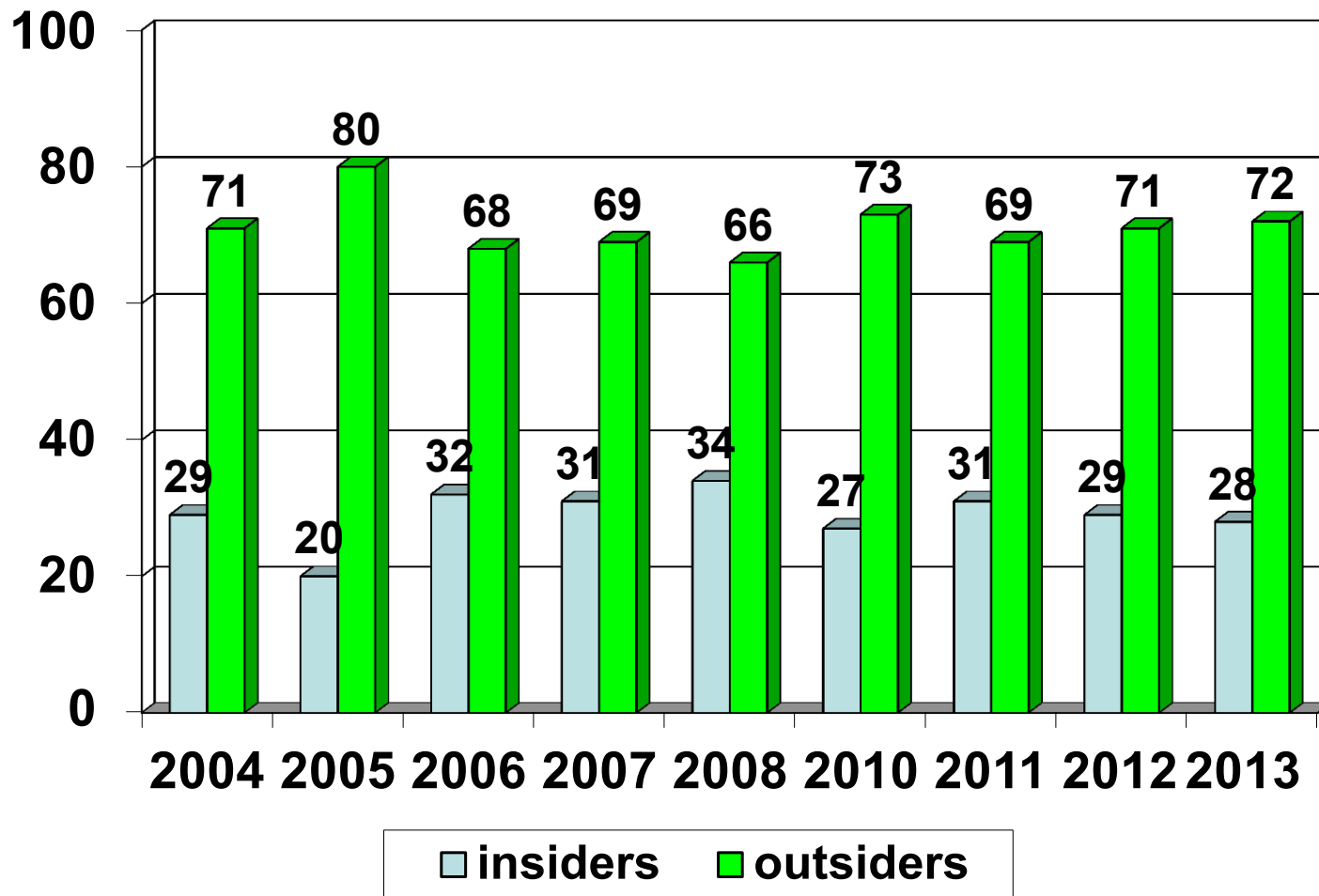
Reason(s) CyberCrimes were not referred for legal action

	2013	2012	2011
Damage level insufficient to warrant prosecution	34%	36%	40%
Lack of evidence/not enough information to prosecute	36%	36%	34%
Could not identify the individual/individuals responsible for committing the eCrime	37%	32%	37%
Concerns about negative publicity	12%	9%	14%
Concerns about liability	8%	7%	9%
Concerns that competitors would use incident to their advantage	7%	6%	7%
Prior negative response from law enforcement	8%	5%	6%
Unaware that we could report these crimes	6%	5%	4%
L.E. suggested incident was national security related	3%	4%	4%
Other	8%	12%	11%
Don't know	21%	28%	20%

Source: 2014 US State of Cybercrime Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Price Waterhouse Cooper, April 2014

2014 US State of Cybercrime Survey -6

Percentage of insiders versus outsiders



Source: 2014 US State of Cybercrime Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Price Waterhouse Cooper, April 2014

An abstract graphic featuring a glowing blue brain in the center, surrounded by binary code (0s and 1s) in a teal color. The word "INSIDER" is written in a stylized, orange, blocky font with a blue outline, positioned to the right of the brain. The background is a dark blue gradient with faint circular patterns.

INSIDER

Types of Insider Activities

Types of Insider Activities -1

Insider 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

Insider 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

Insider 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

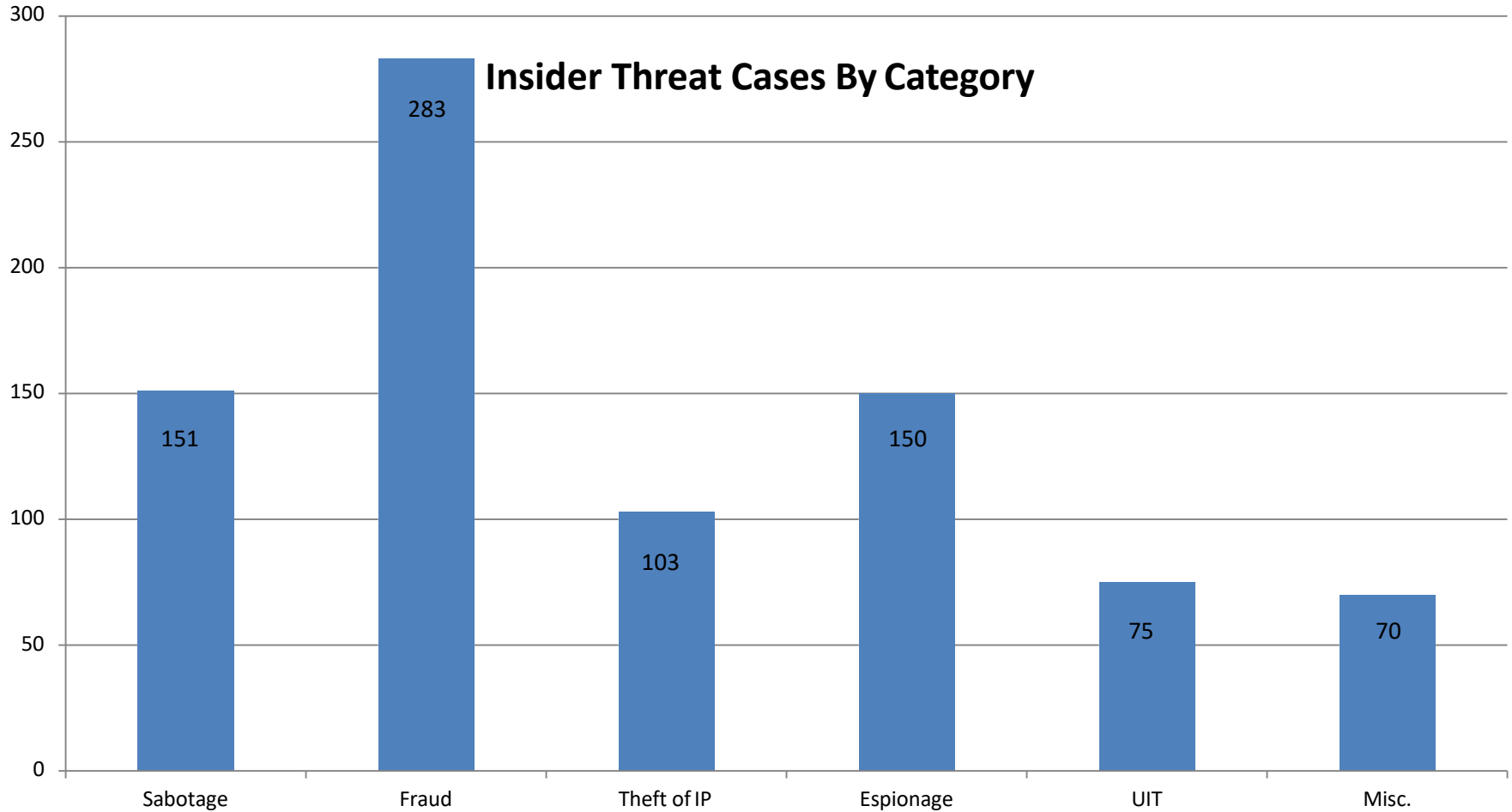
- The act of communicating, delivering or transmitting information pertaining to the national defense of the United States to any foreign government or faction, with intent or reason to believe that is to be used to the injury of the United States or to the advantage of a foreign nation

Miscellaneous

- 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

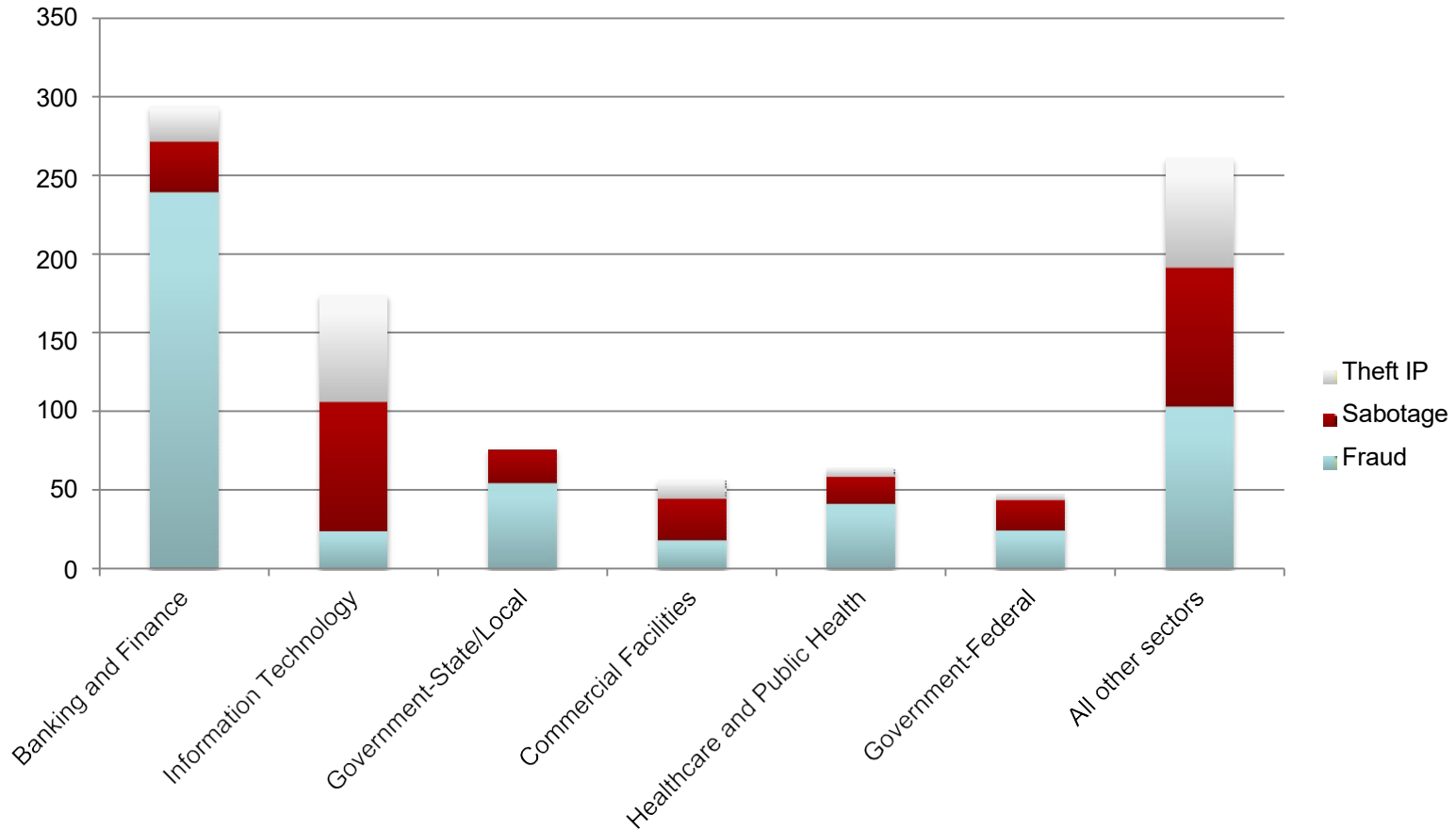
This workshop does not cover National Security Insider Espionage

CERT's Insider Threat Case Database



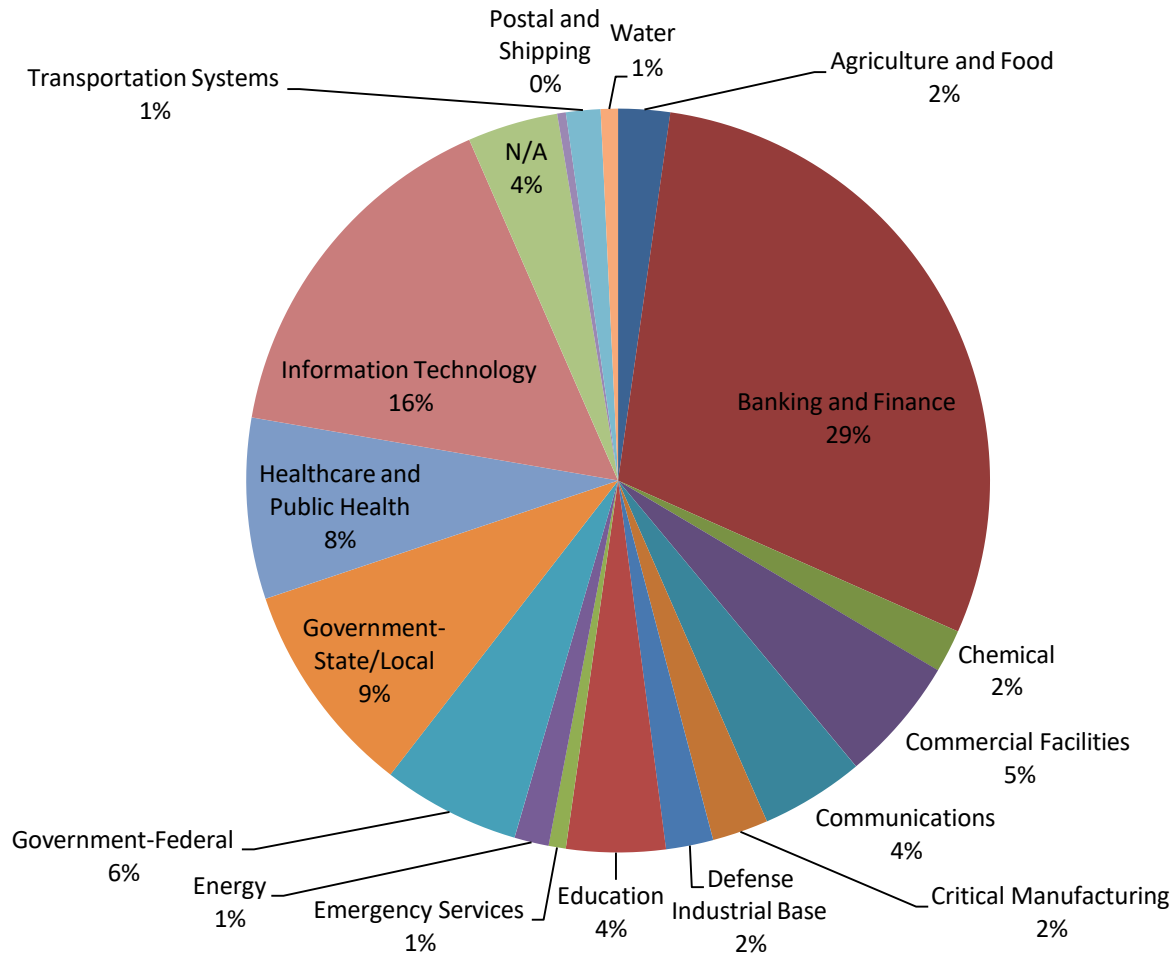
Critical Infrastructure Sectors -1

US Cases by Sectors (Top 6) and Type of Crime



Critical Infrastructure Sectors -2

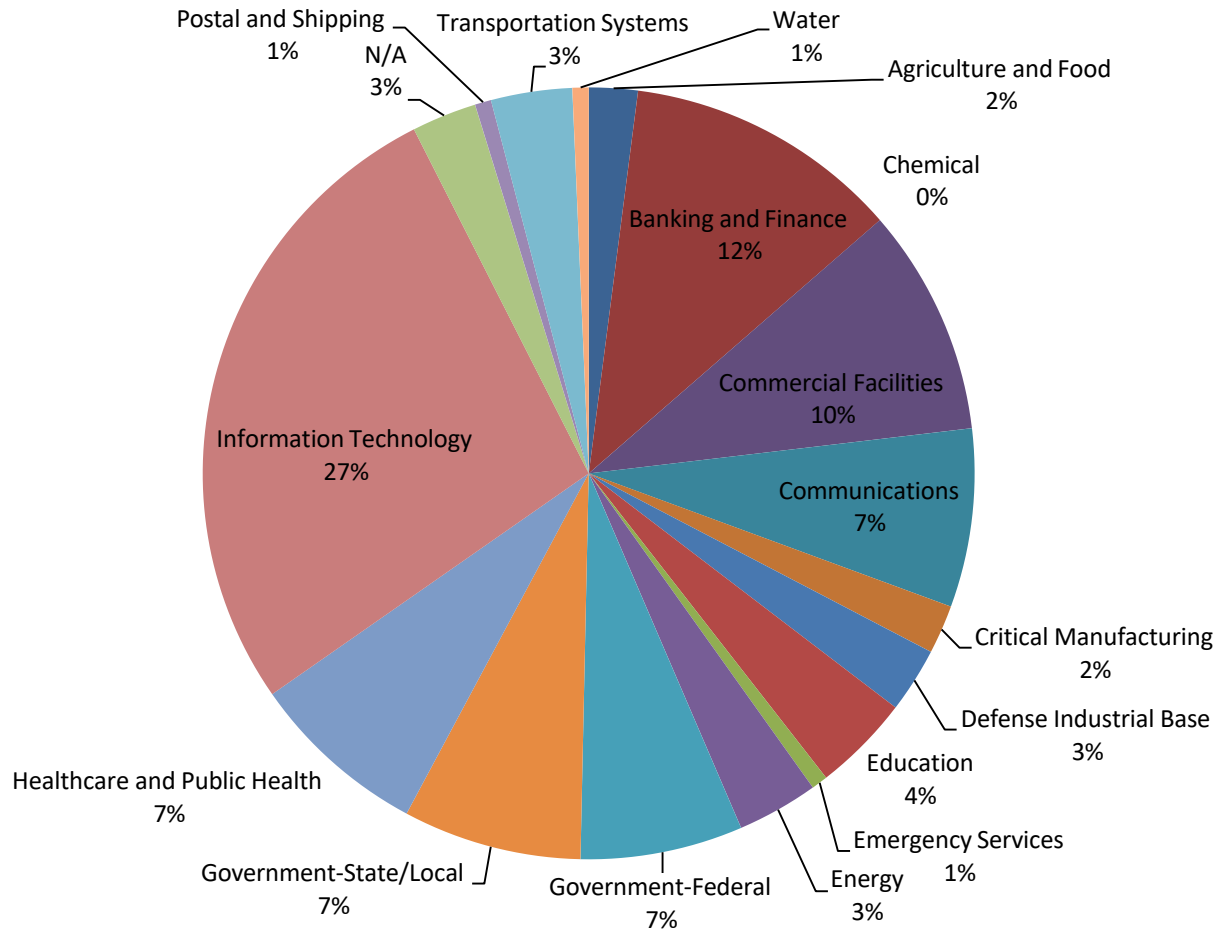
U.S. Cases by Critical Industry Sector



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

Critical Infrastructure Sectors – Sabotage

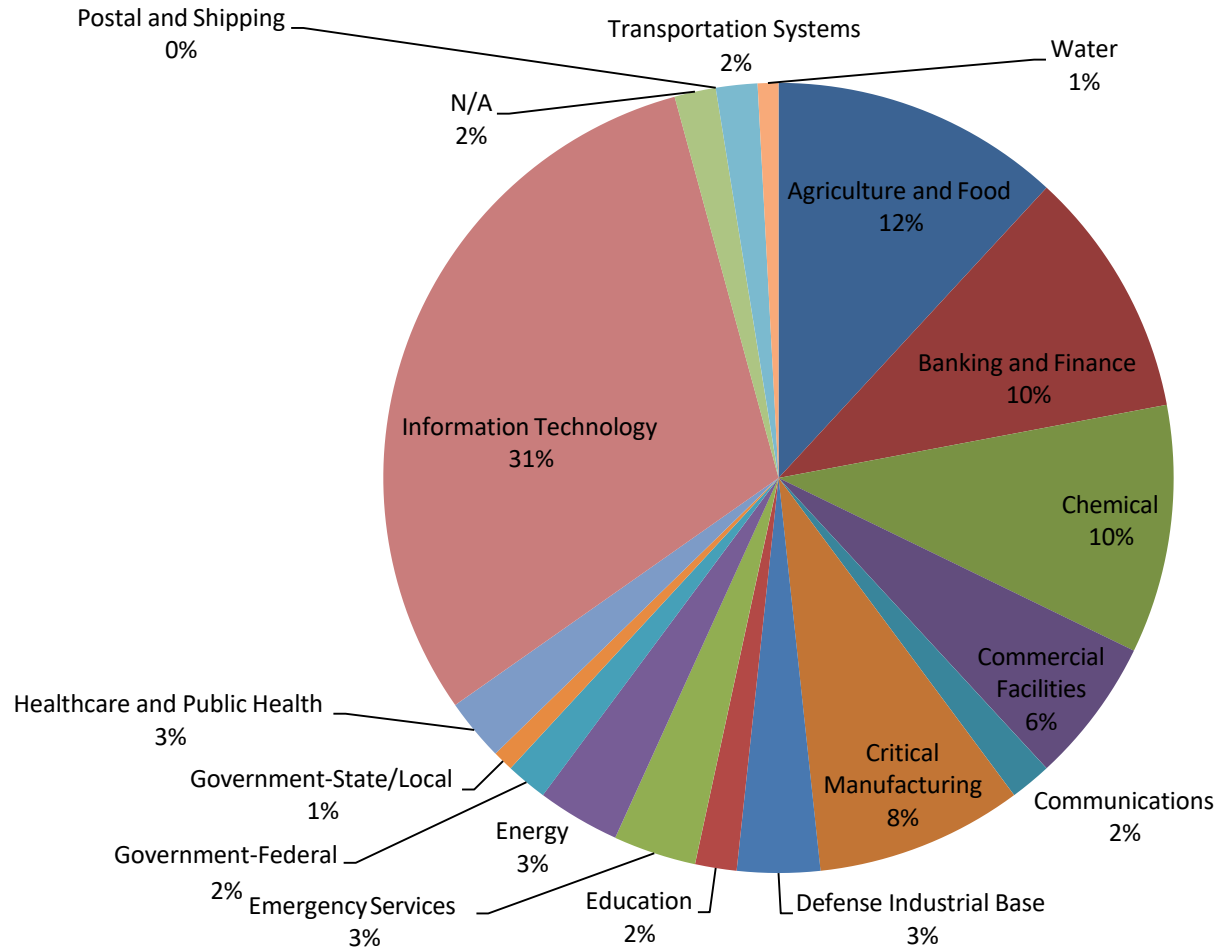
US Sabotage Cases by Critical Industry Sector



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

Critical Infrastructure Sectors – Theft of IP

US IP Theft Cases by Critical Industry Sector



**** 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 CERT Insider Threat Center identifies five basic types of insider threat activities, each has its own profile.

- IT Sabotage
- IT Intellectual Property Theft
- IT Fraud
- 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

Notices

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

CERT® and CERT Coordination Center® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-0486

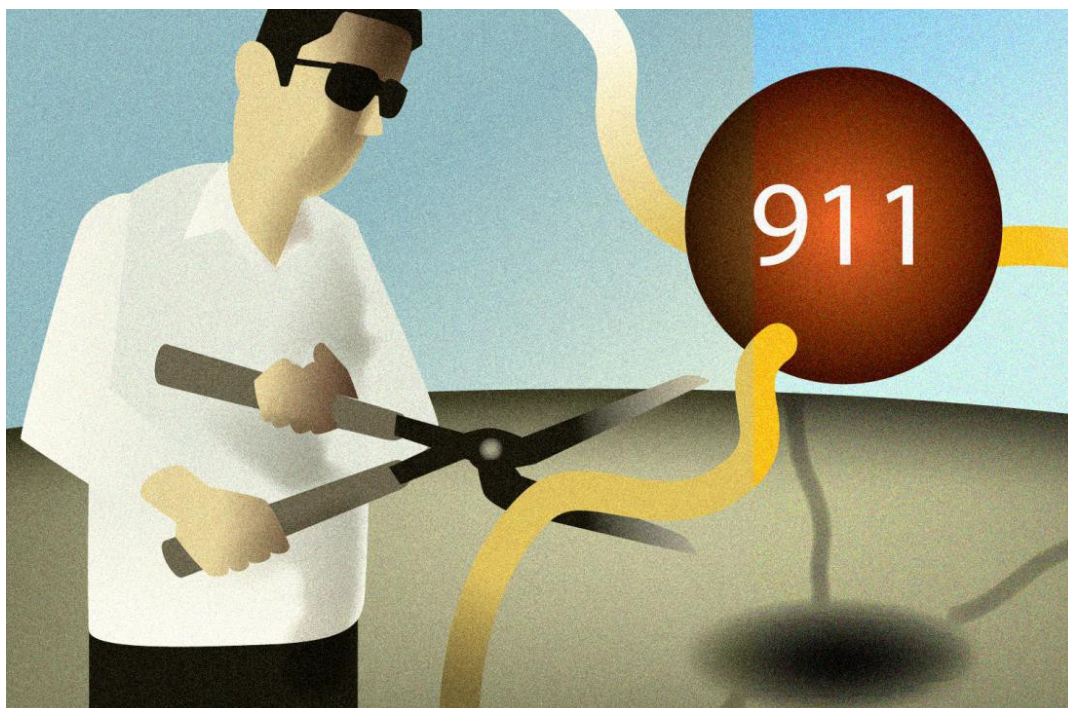
IT Sabotage



TRUE STORY:

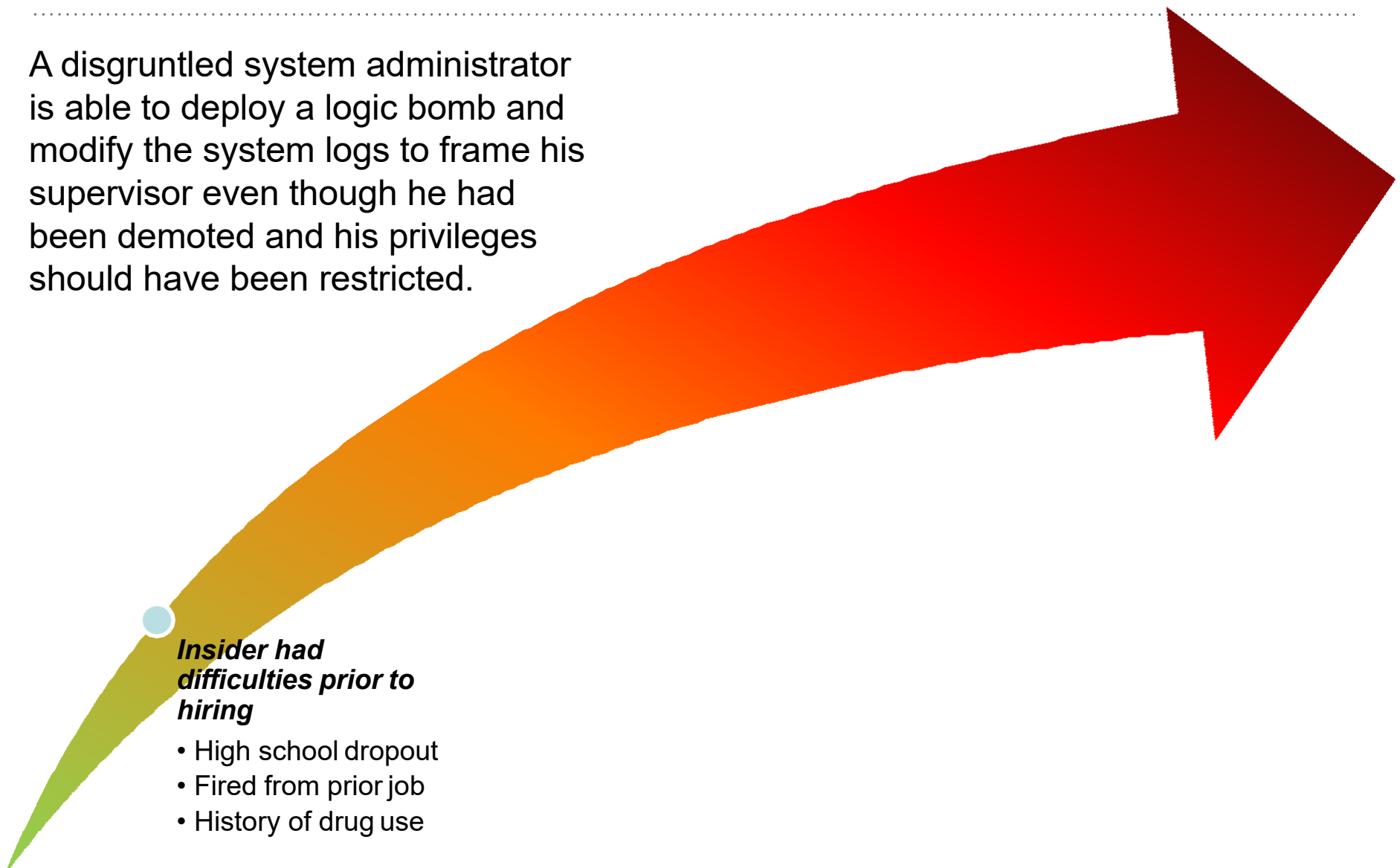
911 services disrupted for 4 major cities

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



Insider IT Sabotage Example -1

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



Insider had difficulties prior to hiring

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

Insider IT Sabotage Example -2

A disgruntled system administrator is able to deploy a logic bomb and modify the system logs to frame his supervisor even though he had been demoted and his 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 “he did all the work”
- Frequently late for work
- Drug use on the job
- Demoted

Insider IT Sabotage Example -3

A disgruntled system administrator is able to deploy a logic bomb and modify the system logs to frame his supervisor even though he had been demoted and his 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 “he did all the work”
- Frequently late for work
- Drug use on the job
- Demoted

Subject frames his supervisor for sabotage

- Discovered plans to fire him
- 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

Insider IT Sabotage Example -4

A disgruntled system administrator is able to deploy a logic bomb and modify the system logs to frame his supervisor even though he had been demoted and his 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 “he did all the work”
- Frequently late for work
- Drug use on the job
- Demoted

Subject frames his supervisor for sabotage

- Discovered plans to fire him
- 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 him as perpetrator
- Told co-worker the day before attack that “he 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 his own employer had disabled his 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?

Positions: system administrators, database administrators, other technical positions

Age: 17 – 60

Gender: mostly males

Variety of racial and ethnic backgrounds

Marital status: fairly evenly split married versus single

Observations from Insider Threat IT Sabotage Cases -1

- 1. Most insiders had personal predispositions that contributed to their risk of committing malicious acts.*
- 2. Most insiders' disgruntlement is due to unmet expectations.*
- 3. In most cases, stressors, including sanctions and precipitating events, contributed to the likelihood of insider IT sabotage.*
- 4. Behavioral precursors were often observable in insider IT sabotage cases but ignored by the organization.*

Observations from Insider Threat IT Sabotage Cases -2

5. *Insiders created or used access paths unknown to management to set up their attack and conceal their identity or actions. The majority attacked after termination.*
6. *In many cases, organizations failed to detect technical precursors.*
7. *Lack of physical and electronic access controls facilitated IT sabotage.*



IT Sabotage Potential Behavioral Precursors

IT Sabotage Potential Behavioral Precursors

Personal predispositions

Serious mental health disorders

Personality problems

Social skills and decision making

History of rule violation



Unmet Expectations Observed in Cases

Salary/bonus

Promotion

Freedom of on line actions

Work ethic

Project requirements - deadlines, milestones

Overestimated abilities

Access to information following termination

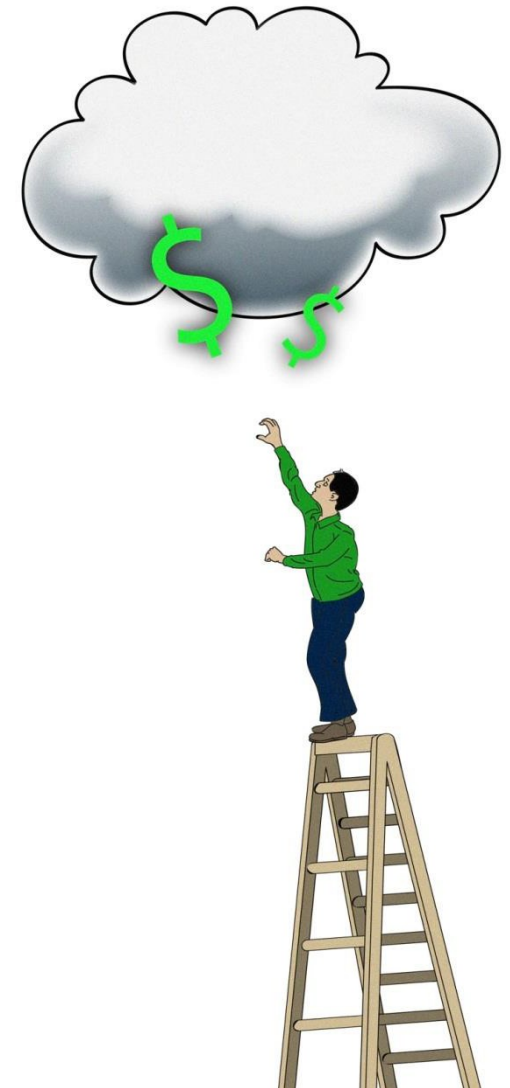
Use of company resources

Job dissatisfaction

Supervisor demands

Coworker relations

Responsibilities



Behavioral Precursors Observed in Cases

Drug use

Conflicts (coworkers, supervisor)

Aggressive or violent behavior

Web surfing, chat rooms at work

Mood swings

Bizarre behavior

Used organization's computers for personal business

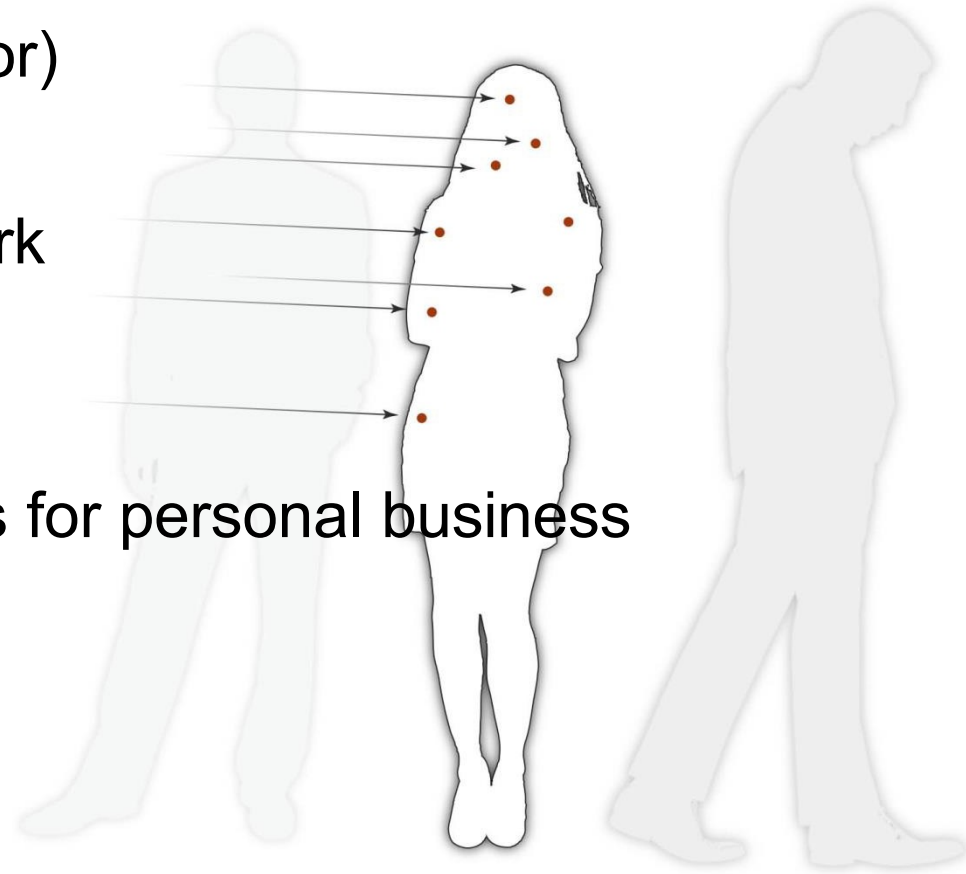
Poor performance

EEO complaint

Absence/tardiness

Sexual harassment

Poor hygiene



Stressors / Sanctions Observed in Cases

Termination

- gross insubordination
- violation of company rules
- poor performance
- not being a team player
- close to Christmas
- false information on background check
- discussion about termination of employment

Passed over for promotion

Demotion

- due to poor performance
- due to project completion

Sanctions

- reprimands for work-related issues
- reprimands for aggressive and malicious behavior
- suspension for excessive absenteeism

Transfer between departments

Supervisor

- new supervisor hired
- disagreement with supervisor

Access changed

Financial

- disagreement over salary & compensation
- bonuses lower than expected
- failure of offering of severance package

Death in family

Divorce

Explosive disagreement with colleagues

Termination of subcontractor contract

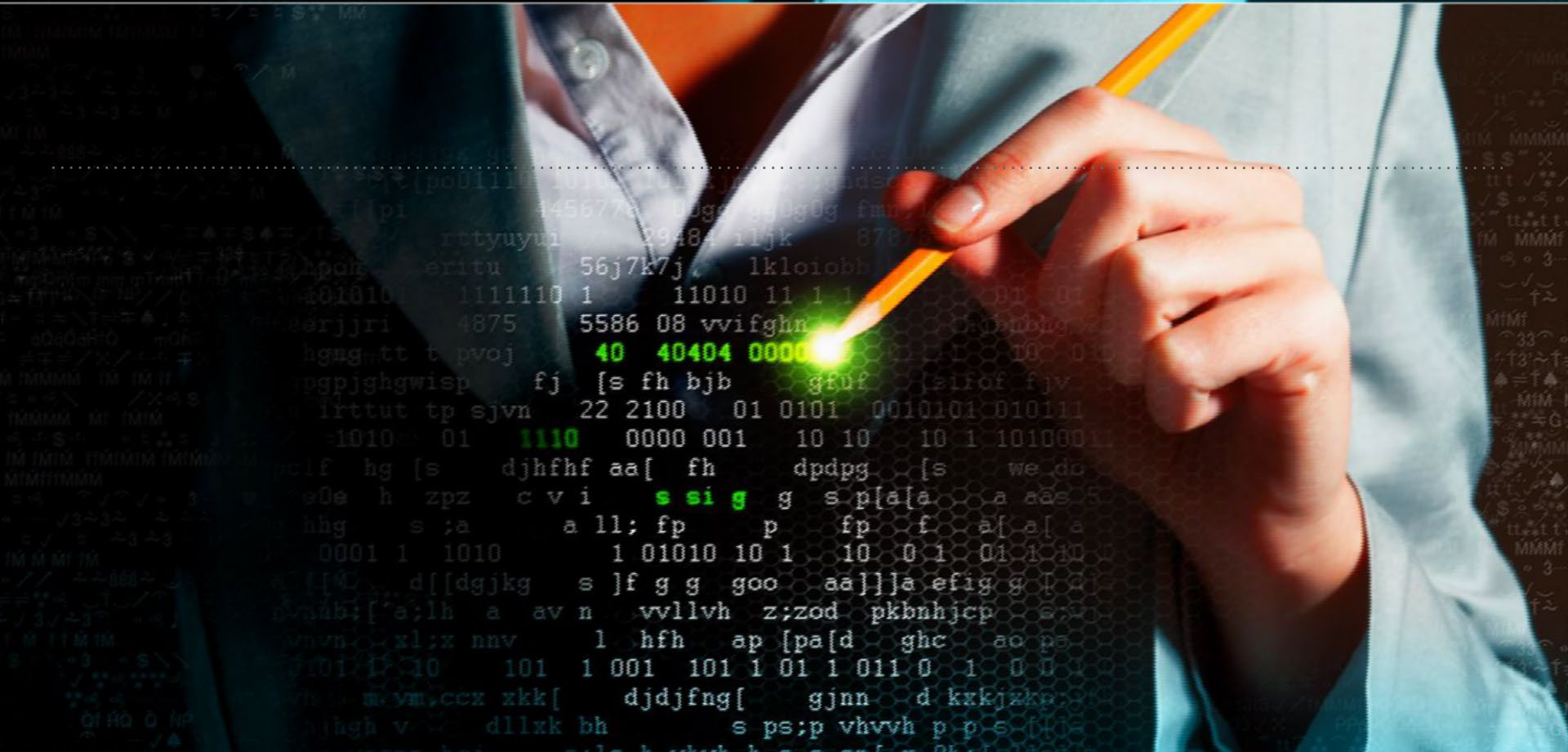
Termination of partnership because of money

Co-workers overriding decisions

Responsibilities removed from projects

Outsourcing of project

Suspension of Internet access



IT Sabotage Potential 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 and tested virus

Network probing

Installed remote network administration tool

Downloaded and installed malicious code and tools (e.g., password cracker or virus)

Disabled of system logs and removal of history files



Technical Precursors Undetected in Cases

Downloading and use of “hacker tools” such as rootkits, password sniffers, or password crackers

Failure to create backups as required

Failure to document systems or software as required

Unauthorized access of customers’ systems

Unauthorized use of coworkers’ machines left logged in

Sharing passwords with others & demanding passwords from subordinates

System access following termination

Refusal to swipe badge to record physical access

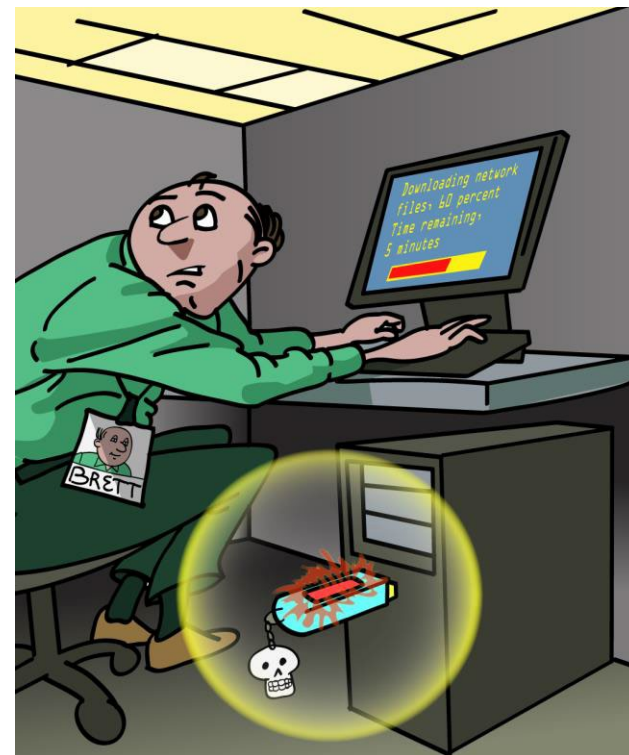
Access of web sites prohibited by acceptable use policy

Refusal to return laptop upon termination

Use of backdoor accounts

Use of organization’s system for game playing, violating acceptable use policy

Set up every new computer so he could access it remotely



Behavioral vs. Technical Indicators:

One month prior to attack:

- Nearly half of the saboteurs had the first observed event at which the insider clearly became disgruntled.
- Only three had engaged in the first observed technical event that clearly enabled the attack.

One week prior to attack:

- 11 of 14 saboteurs had first event where they became disgruntled.
- Only 6 had engaged in the first observed technical event that clearly enabled the attack.

This would suggest that detecting a potential insider threat's disgruntlement would be much more effective in preventing attacks than simply monitoring for technical activity that may indicate a malicious event.



How do you handle privileged technical employees and contractors who are “on the HR radar”?

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 noticing the technical and behavioral precursors and acting on it
- 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

.....

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

CERT® and CERT Coordination Center® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-0486

Theft of Intellectual Property



TRUE STORY:

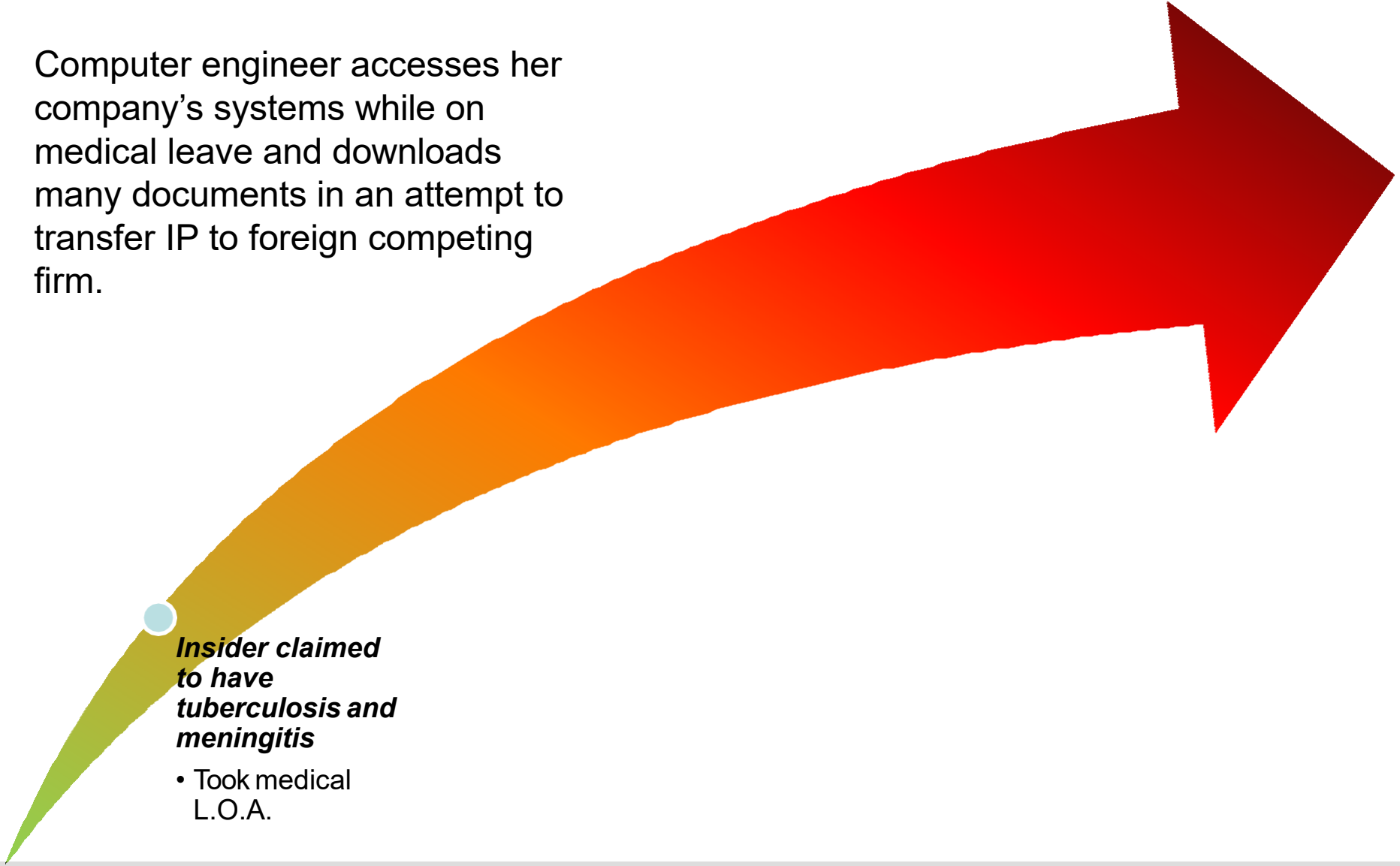
Research scientist downloads 38,000 documents containing his company's trade secrets before going to work for a competitor...

Information was valued at \$400 Million



Insider Theft of IP Example -1

Computer engineer accesses her 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.

Insider Theft of IP Example -2

Computer engineer accesses her 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 medical 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

Insider Theft of IP Example -3

Computer engineer accesses her 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 medical 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 her scope of work
- Physically removed two large bags full of proprietary information (security cameras captured this event)

Insider Theft of IP Example -4

Computer engineer accesses her 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 medical 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 her 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

Other Cases of Theft of IP

A technical operations associate at a pharmaceutical company downloads 65 GB of information, including 1300 confidential and proprietary documents, intending to start a competing company, in a foreign country...

- Organization spent over \$500M in development costs

Theft of Intellectual Property

Who did it?

- Current employees
- Scientists, engineers, programmers, sales people
- Mostly males
- Average age: 39

What was stolen?

- Trade secrets
- Internal organization information
- Proprietary software/source code
- Business plans, proposals, strategic plans, etc.
- Customer information
- Product information (designs, formulas, etc.)

Dynamics of the Crime -1

How did they steal it?

- During normal working hours
- Using authorized access

Methods of Theft (in order of prevalence)

- Copied/downloaded information
- Emailed information
- Accessed former employer's system
- Compromised account
- Many other methods

Most were quick theft upon resignation

- Most within 30 days of resignation

Dynamics of the Crime -2

Stole information to

- Take to a new job
- Start a new business
- Give to a foreign company or government organization

Known issues / motivation

- Disagreement over ownership of intellectual property
- Financial compensation issues
- Relocation issues
- Hostile work environment
- Mergers & acquisitions
- Company attempting to obtain venture capital
- Problems with supervisor
- Passed over for promotion
- Layoffs

Subclasses of IP Thieves

The Entitled Independent

- Approximately half of the theft of IP cases
- A dissatisfied insider acting primarily alone to steal information to take to a new job or to his own side business

The Ambitious Leader

- Approximately half of the theft of IP cases
- A leader who recruits insiders to steal information for some larger purpose

Theft of IP for Foreign Government or Organization

Approximately one third of the insider theft of IP cases were for the benefit of a foreign government or organization.

All of these cases fit the Ambitious Leader model.

It is much more difficult to recover IP once it leaves the U.S.

Common Methods of Exfiltration

25 cases (50%) involved removing data directly from a host

- Removable Media – 80% of the cases
- Email – over 50% of the cases
- Remote Network Access – over 25% of the cases
- Laptops – 20% of the cases
- Physical – less than 10% of the cases

Considerations for Mitigation

Recognize efforts at concealment

Decide upon proper use of removable media

Decide upon proper use of personal email

Pay close attention around a resignation

Establish consistent exit procedures



Do you check for stolen information when employees, contractors, subcontractors, and other trusted business partners with access to critical information leave?

Module 4 Conclusion

Insider Threat Intellectual Property Theft

- 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
- has two subclasses of thieves based on the CERT Insider Threat Center model:
 - the entitled independent
 - the ambitious leader
- 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

.....

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

CERT® and CERT Coordination Center® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-0486

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 -1

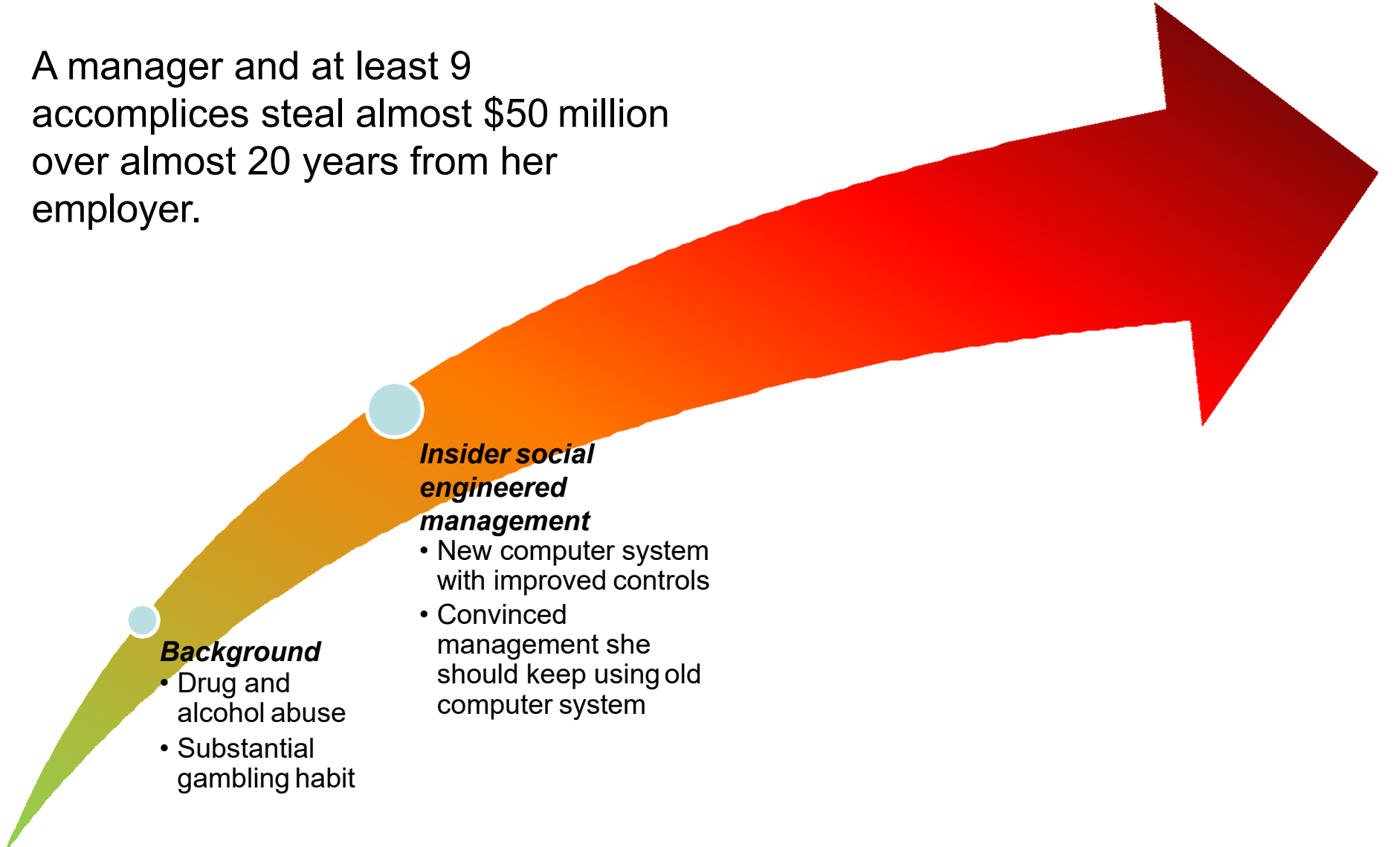
A manager and at least 9 accomplices steal almost \$50 million over almost 20 years from her employer.

Background

- Drug and alcohol abuse
- Substantial gambling habit

Insider Fraud Example -2

A manager and at least 9 accomplices steal almost \$50 million over almost 20 years from her employer.



Background

- Drug and alcohol abuse
- Substantial gambling habit

Insider social engineered management

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

Insider Fraud Example -3

A manager and at least 9 accomplices steal almost \$50 million over almost 20 years from her employer.

Background

- Drug and alcohol abuse
- Substantial gambling habit

Insider social engineered management

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

Issued fraudulent refunds to fake companies

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

Insider Fraud Example -4

A manager and at least 9 accomplices steal almost \$50 million over almost 20 years from her employer.

Background

- Drug and alcohol abuse
- Substantial gambling habit

Insider social engineered management

- New computer system with improved controls
- Convinced management she 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 she 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 herself 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 her husband on the payroll for weekly payouts, and erases records of payments...

- Over almost a year loss of over \$100K

Insider Fraud

Who did it?

- Current employees
- “Low level” positions
- Gender: fairly equal split
- Average age: 33

What was stolen/modified?

- Personally Identifiable Information (PII)
- Customer Information (CI)

How did they steal/modify it?

- During normal working hours
- Using authorized access

Dynamics of the Crime

Most attacks were long, ongoing schemes

Crimes involved outsider collusion over half the time

Crimes were outsider induced about 1/3 of time

Crimes involved insider collusion about 1/3 of time

Insider acted alone about 1/3 of time

Known Issues

Family medical problems

Substance abuse

Physical threat of outsiders

Financial difficulties

Financial compensation issues

Hostile work environment

Problems with supervisor

Layoffs

Technical Aspects – Theft to Commit Fraud

Electronically

- Downloaded to home
- Looked up and used immediately
- Copied
- Phone/fax
- Email
- Malicious code

Physically

- Printouts
- Handwritten

Remaining unknown

Countermeasures – Theft to Commit Fraud

Train managers on social networking issues

Provide Employee Assistance Program or other recourse for employees experiencing personal or financial problems

Log, monitor, and audit for unusually large queries, downloads, print jobs, emails

Consider data leakage protection tools

Do not overlook physical access controls

Change passwords for all accounts upon termination, including EXTERNAL accounts!

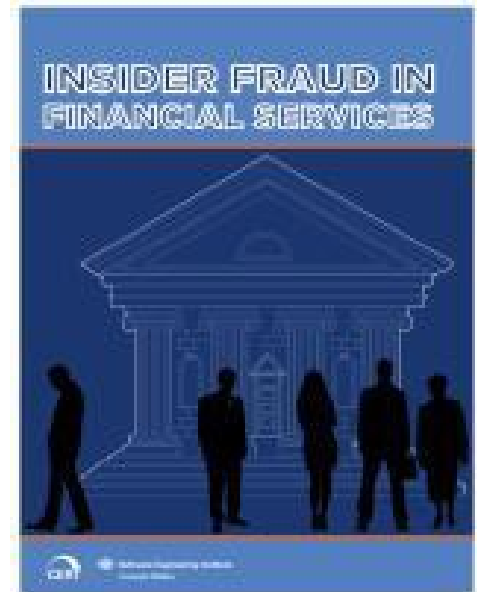
Insider Fraud Study (2012)

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

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

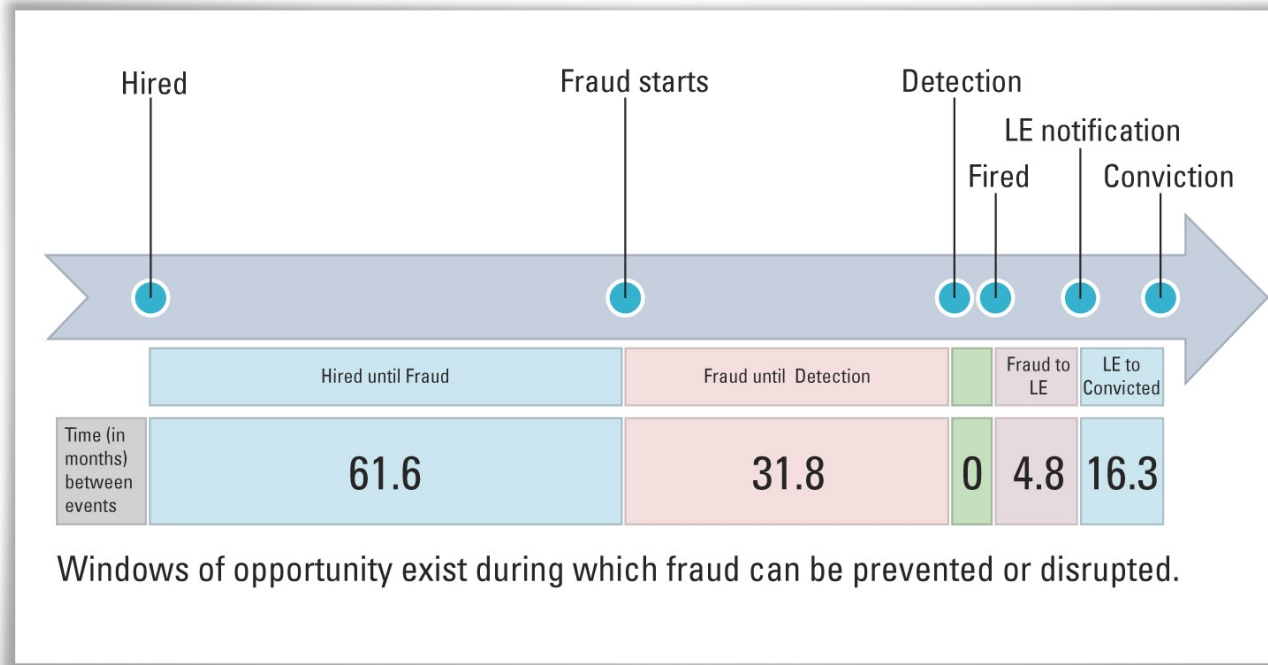
Full report: “Insider Threat Study: Illicit Cyber Activity
Involving Fraud in the U.S. Financial Services Sector”
(<http://www.sei.cmu.edu/library/abstracts/reports/12sr004.cfm>)

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



Low and Slow

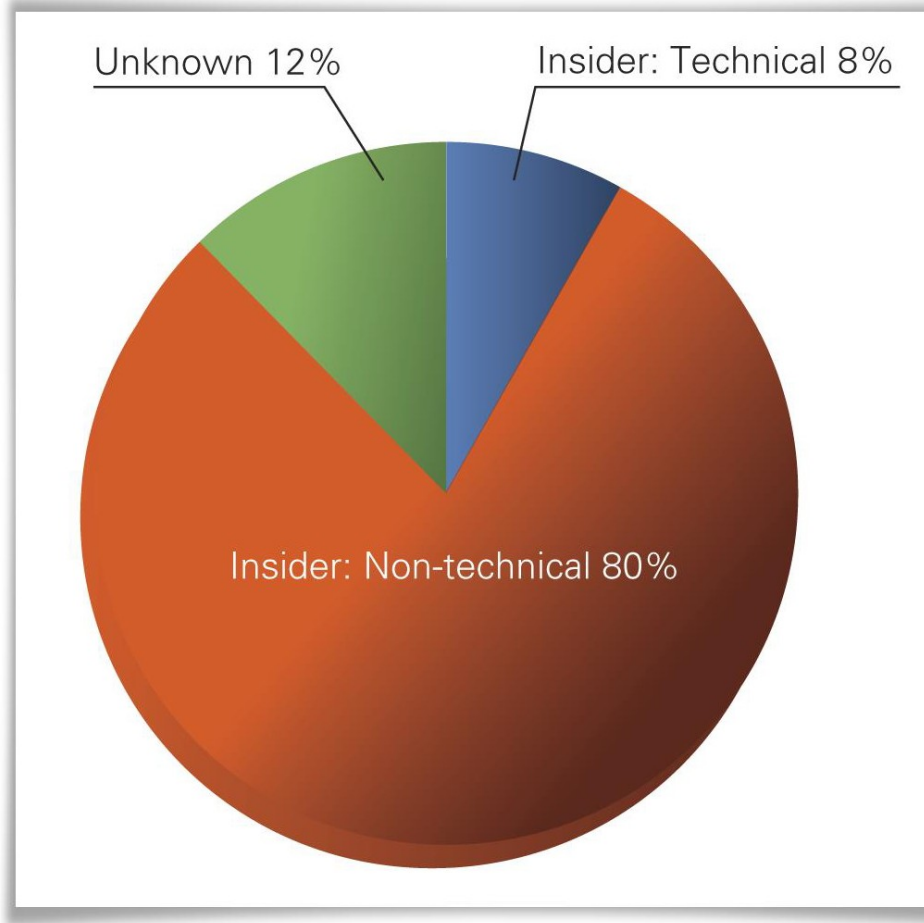
Criminals who executed a “low and slow” approach accomplished more damage and escaped detection for longer.



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

Low-Tech

Insiders' means were not very technically sophisticated.



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

Managers vs. Non-Managers

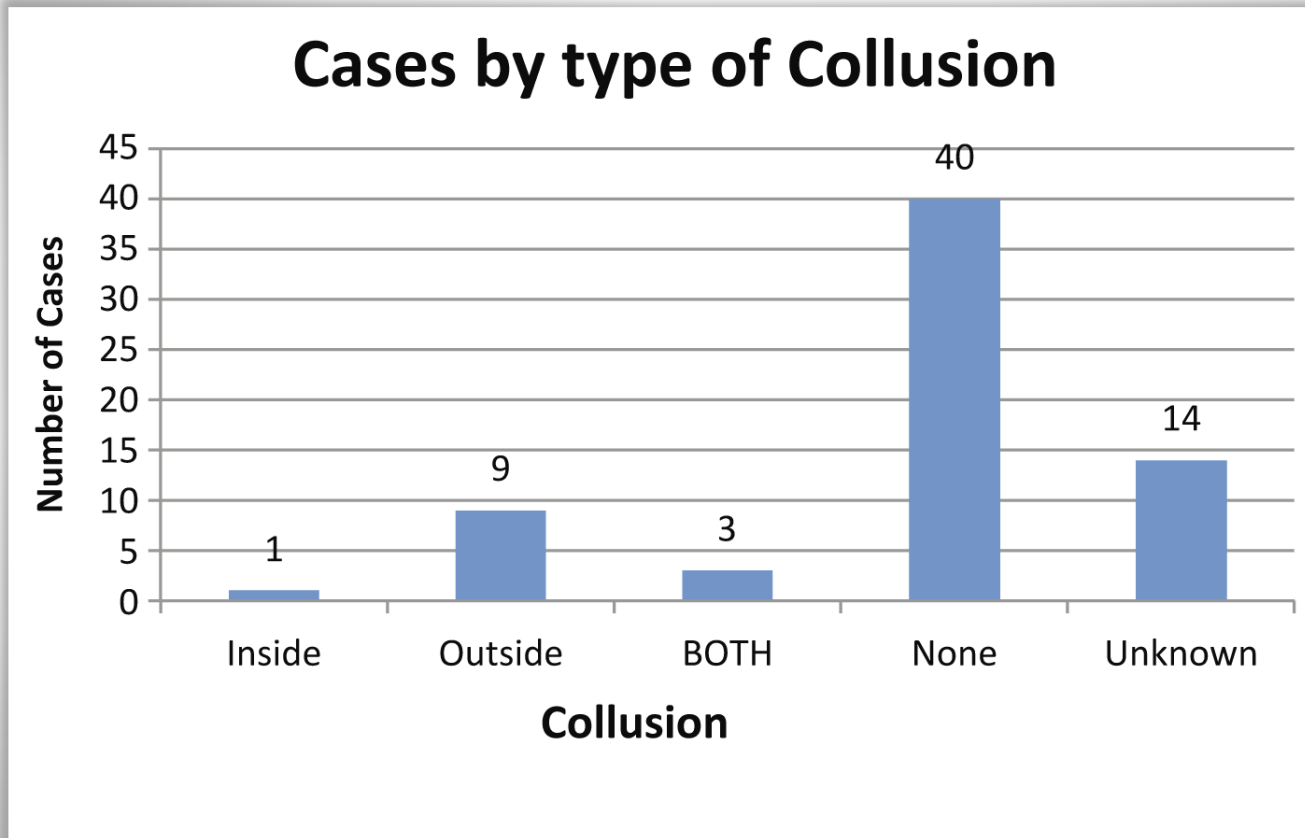
Fraud by managers differs substantially from fraud by non-managers by damage and duration.



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

Collusion

Most cases do not involve collusion.



There was not a significant number of cases involving collusion, but those that did occur generally involved external collusion (i.e., a bank insider colluding with an external party to facilitate the crime).

Audits, Complaints, and Suspensions

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.

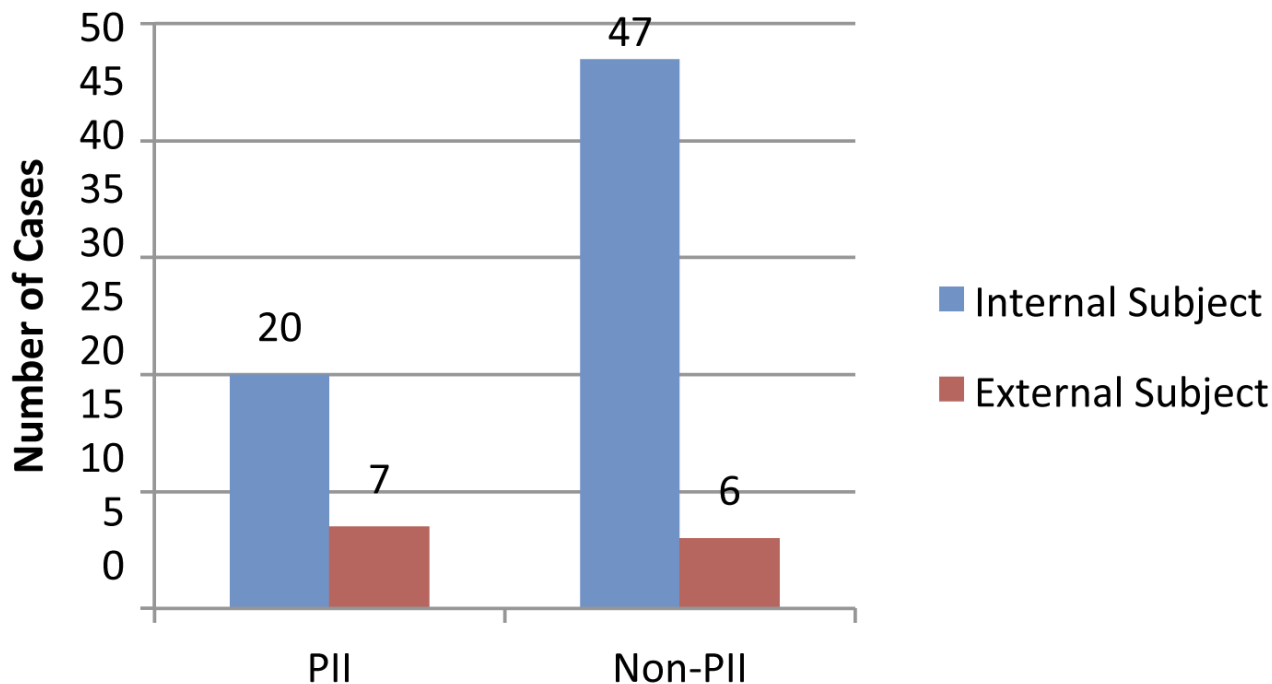
Over half of the insiders were detected by other victim organization employees, though none of the employees were members of the IT staff.

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).

Personally Identifiable Information

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



Of the 80 cases, 34 percent involved PII and 66 percent did not. The external cases were evenly split between PII cases and non-PII cases.



Have you seriously considered how your employees could misuse your systems for financial gain?

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
 - use of data loss prevention tools and policies
 - providing assistance to employees with personal or financial problems
 - monitoring for large, unusual downloads, print jobs, emails

Module 6: Unintentional Insider Threat

Notices

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

CERT® and CERT Coordination Center® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-0486

Summary of 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**

Unintentional Insider Threat



Purpose

Unintentional Insider Threat is a new, but essential area of work, for CERT.

Our Objective is to:

- Provide an understanding of how insider threat activities can include "non" or "un" intentional actions
- Offer mitigation strategies that work for Unintentional Insider Threats

CERT Insider Threat Definition – Review

A current or former employee, contractor, or business partner who meets the following criteria:

- has or had authorized access to an organization's network, system, or data
- has intentionally exceeded or intentionally used that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems

CERT Unintentional Insider Threat Definition

An unintentional insider threat (UIT) is

- a current or former employee, contractor, or business partner
- who has or had authorized access to an organization's network, system, or data and who,
- through action or inaction without malicious intent,
- causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems.

Individual

- has ACCESS.
- does not intend to harm the organization.
- causes actions that result in (potential or actual) harm to the organization.

Summary of Cases

Over 75 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
- CERT database of insider threat cases. This database includes more than 800 insider threat cases, with information derived from court documents, investigator notes, news stories, and business and research partners.
- 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 (UIT-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

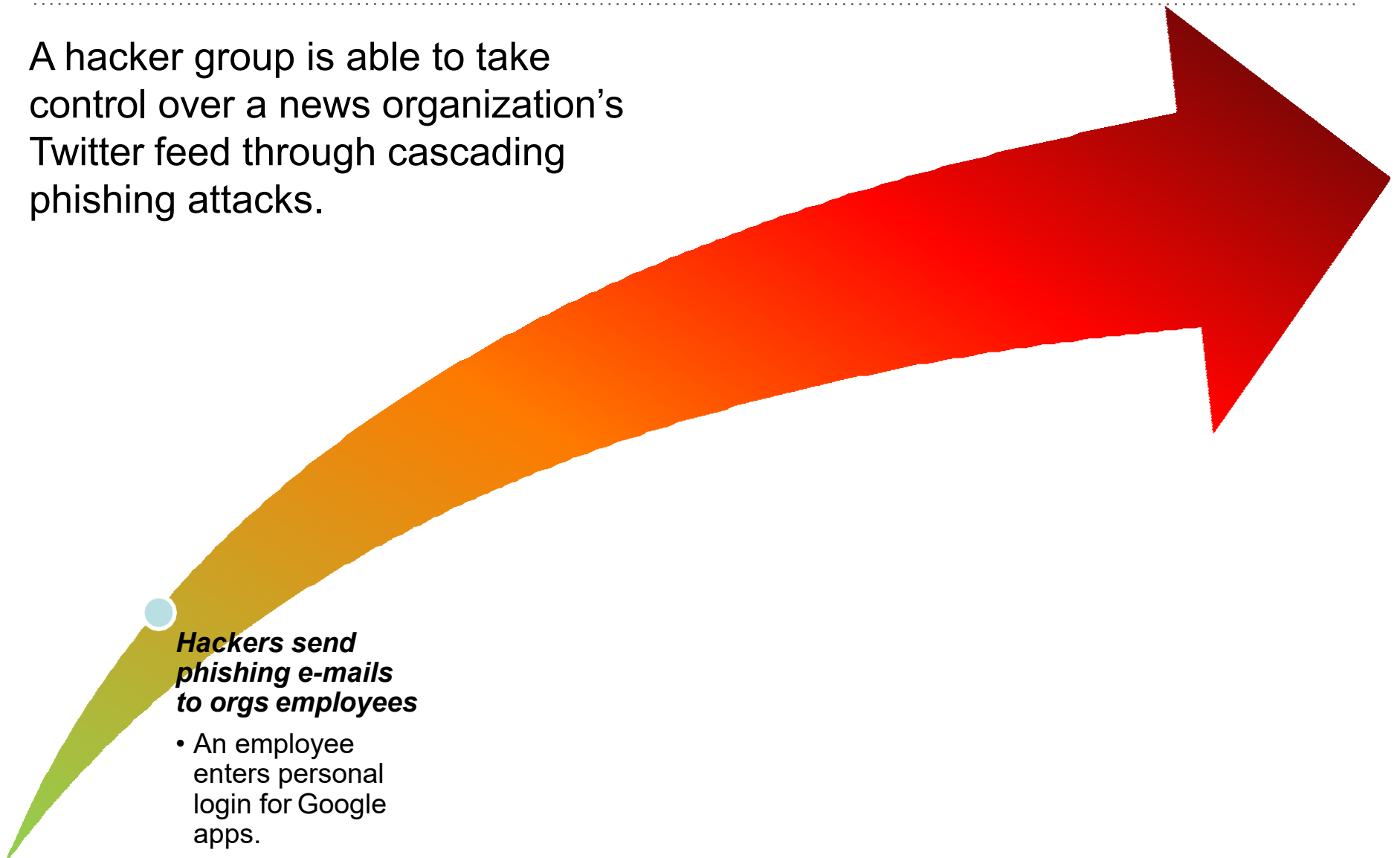
TRUE STORY: Example of DISC Threat Vector

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



UIT-HACK Threat Vector Example -1

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

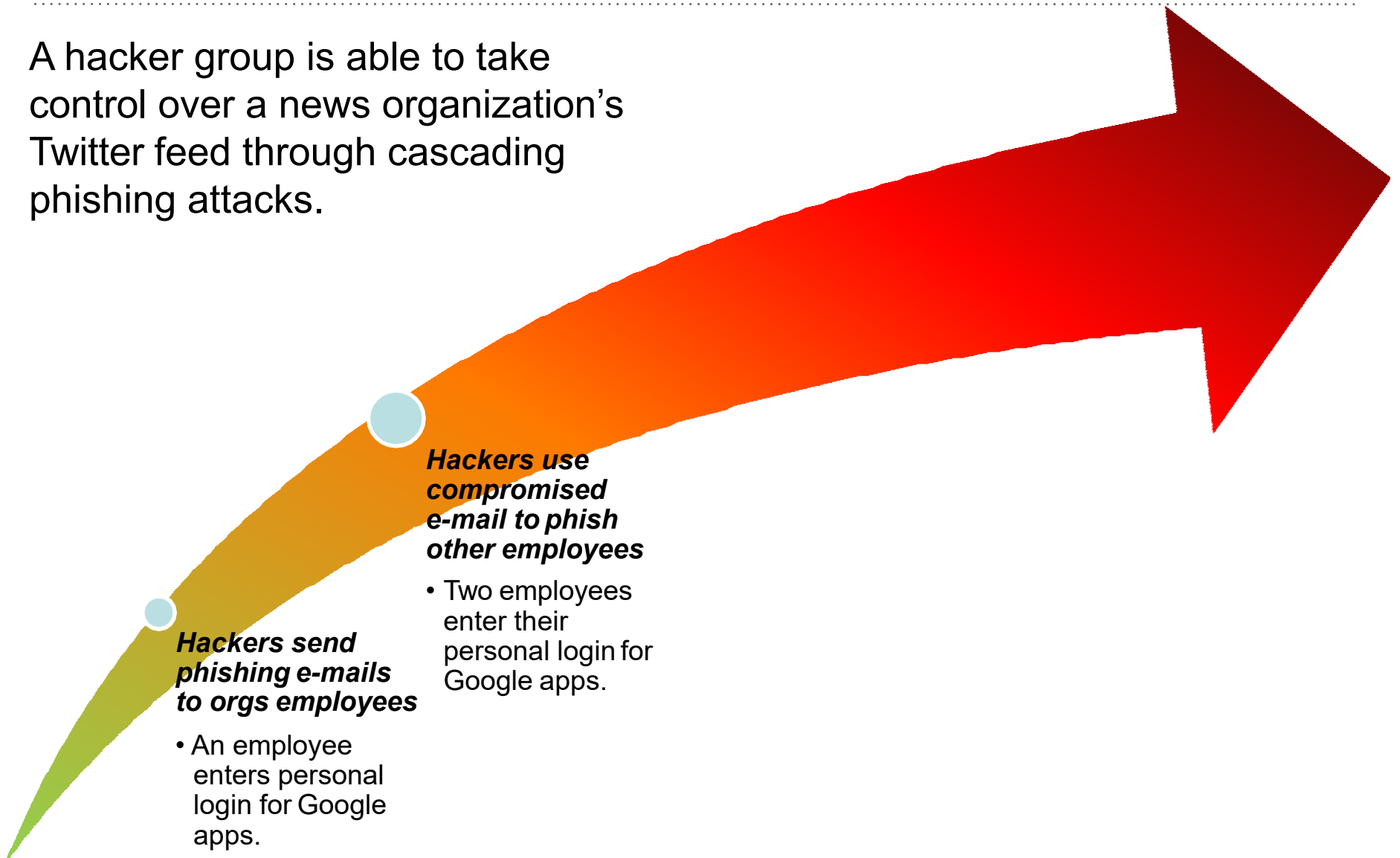


Hackers send phishing e-mails to orgs employees

- An employee enters personal login for Google apps.

UIT-HACK Threat Vector Example -2

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.

UIT-HACK Threat Vector Example -3

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.

UIT-HACK Threat Vector Example -4

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

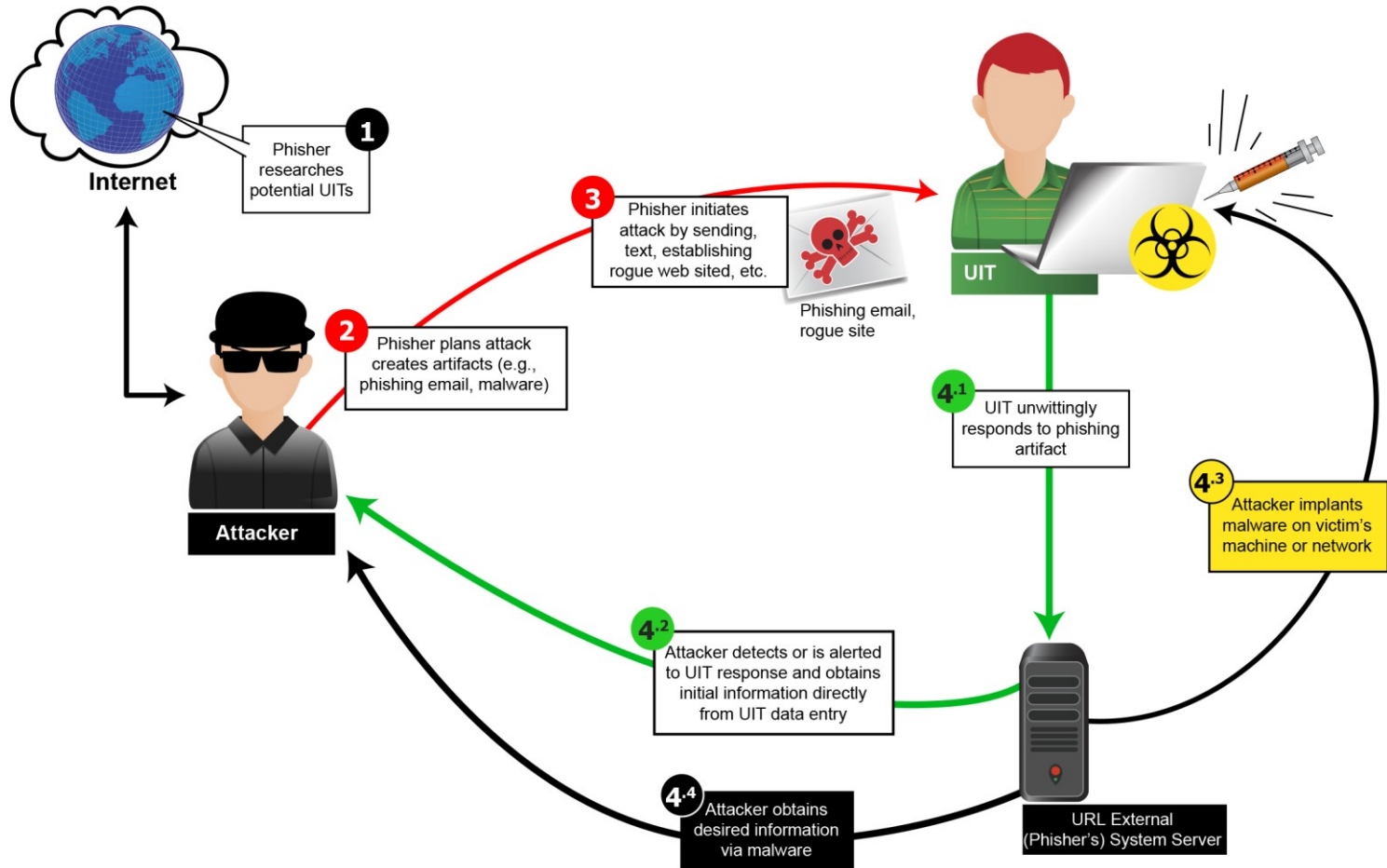
- Two employees enter their personal login for Google apps.

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 his home.

Someone broke into his 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.



UIT Contributing Factors in Cases

- Human Error
- Fatigue
- Subjective mental workload
- Situation awareness
- Mind wandering
- Risk perception and risky decision making
- Human limitation and biases
- Cultural factors
- Gender
- Mood
- Age effects and variations over time
- Influence of drugs and hormones

Key Takeaways

Insider negligence – 27 of 75 cases

- 15 (20%) – accidental disclosure
- 10 (13%) – portable device
- 2 (3%) – physical (paper) loss

UIT-HACK – 32 of 75 cases (external actors)

- 4 (5%) – rogue USB
- 28 (37%) – rogue app/malware

Employees of the organization were responsible for 42 of the 75 cases (56%)!

Mitigation Strategies for Unintentional Insider Threats

Threat Vector		UIT-HACK	DISC	PHYS	PORT
MITIGATION / COUNTERMEASURE	Training to heighten awareness and reduce human error (BP 3, BP 18)	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)	X	X	X	X
	Email safeguards (anti-phishing, anti-malware) (BP 18)	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 7,19)		X		X
	Wireless and Bluetooth safeguards (disable, protect) (BP 13)				X
	Remote memory wipe for lost equipment (BP 13, 19)				X

Case Example 1

Able Abrams is a high ranking member of the House International Relations Committee who is a prolific user of Facebook and Twitter.

He carries his smartphone with him everywhere and always updates his constituents on his location and activities.

Rep. Abrams is visiting Misculania, a country militarily occupied by the United States.

Before and during his trip to Misculania he posts his travel plans on his Facebook page and tweets his location.

Insurgents in Misculania notice his postings and set a roadside bomb where they expect his convoy to be going.

- Is this a UIT?
- If so, what is the Threat Vector?
- What could have been done to prevent this incident?
- What can be done to detect this incident?
- What can be done to mitigate the incident?

Case Example 2

Brian Brandon works for an insurance company as a claims investigator.

He uses a flash drive to back up his case files while out on business trips.

While at the airport, Brian places his backpack down at the security screen.

One of Brian's other bags piques the TSA agent's interest, which causes Brian to focus on working with the TSA officer.

Unbeknownst to Brian, someone walks away with his backpack, including the flash drive.

His flash drive may not have been encrypted, leaving its contents available to the thief.

- Is this a UIT?
- If so, what is the Threat Vector?
- What could have been done to prevent this incident?
- What can be done to detect this incident?
- What can be done to mitigate the incident?

Case Example 3

Twenty-three employees at ACME electronics receive an e-mail.

The e-mail looks real and is sent from what looks like the HR Director's e-mail address.

The e-mail has an attachment for the new open enrollment form for health insurance and suggests that employees use this form to select health insurance options for the next year.

Twenty employees open the attachment, releasing malware into the company system.

The malware is only detected after a security company is called in to conduct a routine check of the system.

- Is this a UIT?
- If so, what is the Threat Vector?
- What could have been done to prevent this incident?
- What can be done to detect this incident?
- What can be done to mitigate the incident?

Case Example 4

Tim Taylor works for a roofing company where he does substandard work and jokes around too much.

Tim's boss, Jason, is not impressed and has confronted Tim multiple times about his lack of work quality.

In an effort to play a practical joke on Jason, Tim logs into the scheduling system, which is housed on Jason's laptop.

Tim moves several of the scheduled jobs around on the calendar.

For the next few weeks the company sends teams out to the wrong job sites, angering its customers, and losing business.

- Is this a UIT?
- If so, what is the Threat Vector?
- What could have been done to prevent this incident?
- What can be done to detect this incident?
- What can be done to mitigate the incident?

Case Example 5

Joe Jackson is an intern working for the summer with a non-profit organization focused on environmental issues.

Joe works in the Development Department where he stuffs envelopes by hand to send to donors.

In his haste to head out on a date one evening, Joe is not paying attention and working too fast.

Joe puts two letters thanking donors for their contributions in the same envelope.

The letters go out in the mail. Nothing happens.

- Is this a UIT?
- If so, what is the Threat Vector?
- What could have been done to prevent this incident?
- What can be done to detect this incident?
- What can be done to mitigate the incident?

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

Notices

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

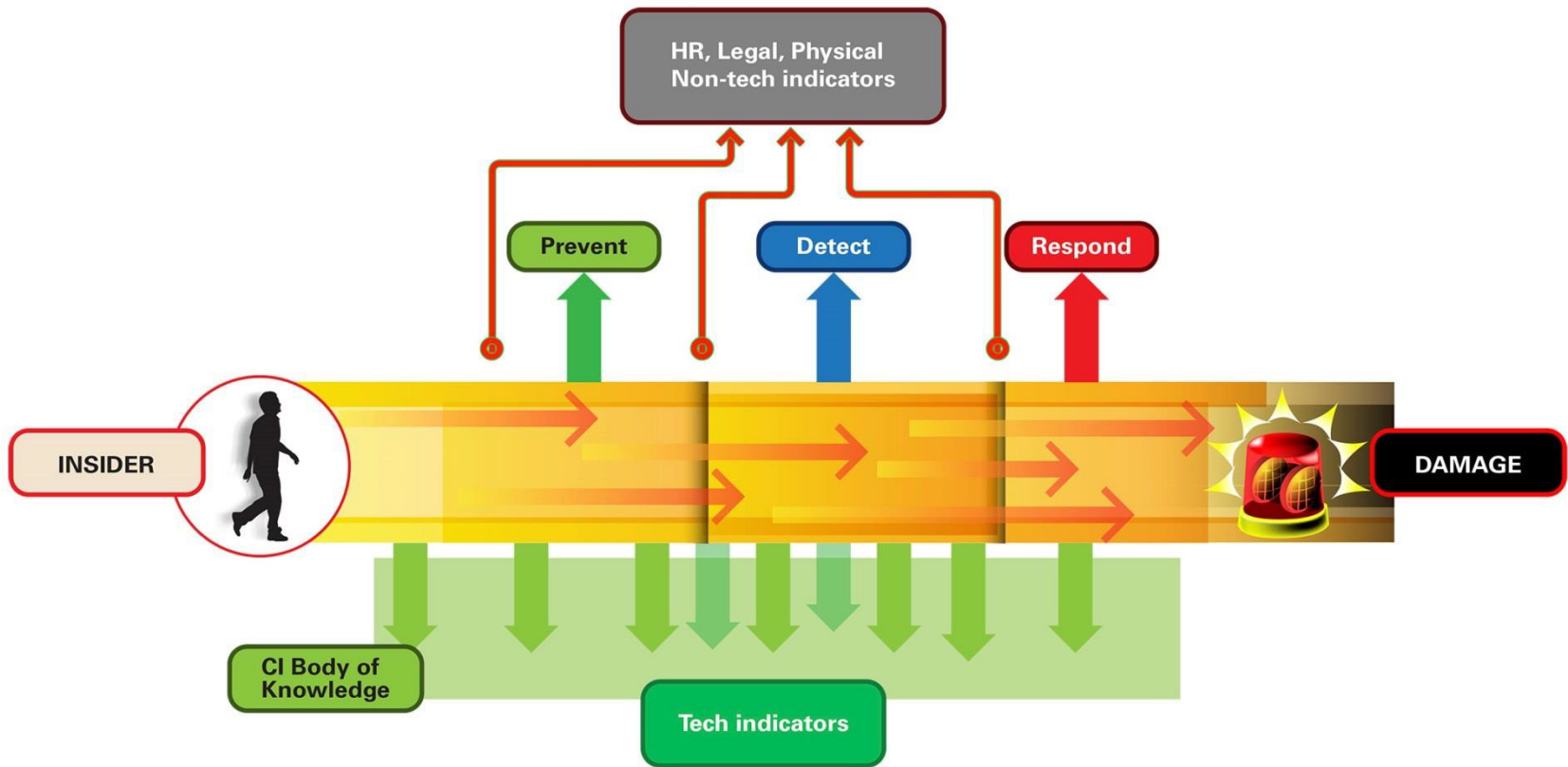
Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

CERT® and CERT Coordination Center® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-0486

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



Stages of Insider Threat Mitigation



Common Sense Guide to Mitigating Insider Threats

<http://www.sei.cmu.edu/library/abstracts/reports/12tr012.cfm>

Best Practices for Insider Threat Mitigation -1

Consider threats from insiders and business partners in enterprise-wide risk assessments.

Clearly document and consistently enforce policies and controls.

Incorporate insider threat awareness into periodic security training for all employees.

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

Anticipate and manage negative issues in the work environment.

Know your assets.

Implement strict password and account management policies and practices.

Enforce separation of duties and least privilege.

Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.

Institute stringent access controls and monitoring policies on privileged users.

Best Practices for Insider Threat Mitigation -2

Institutionalize system change controls.

Use a log correlation engine or security information and event management (SIEM) system to log, monitor, and audit employee actions.

Monitor and control remote access from all end points, including mobile devices.

Develop a comprehensive employee termination procedure.

Implement secure backup and recovery processes.

Develop a formalized insider threat program.

Establish a baseline of normal network device behavior.

Be especially vigilant regarding social media.

Close the doors to unauthorized data exfiltration.



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.

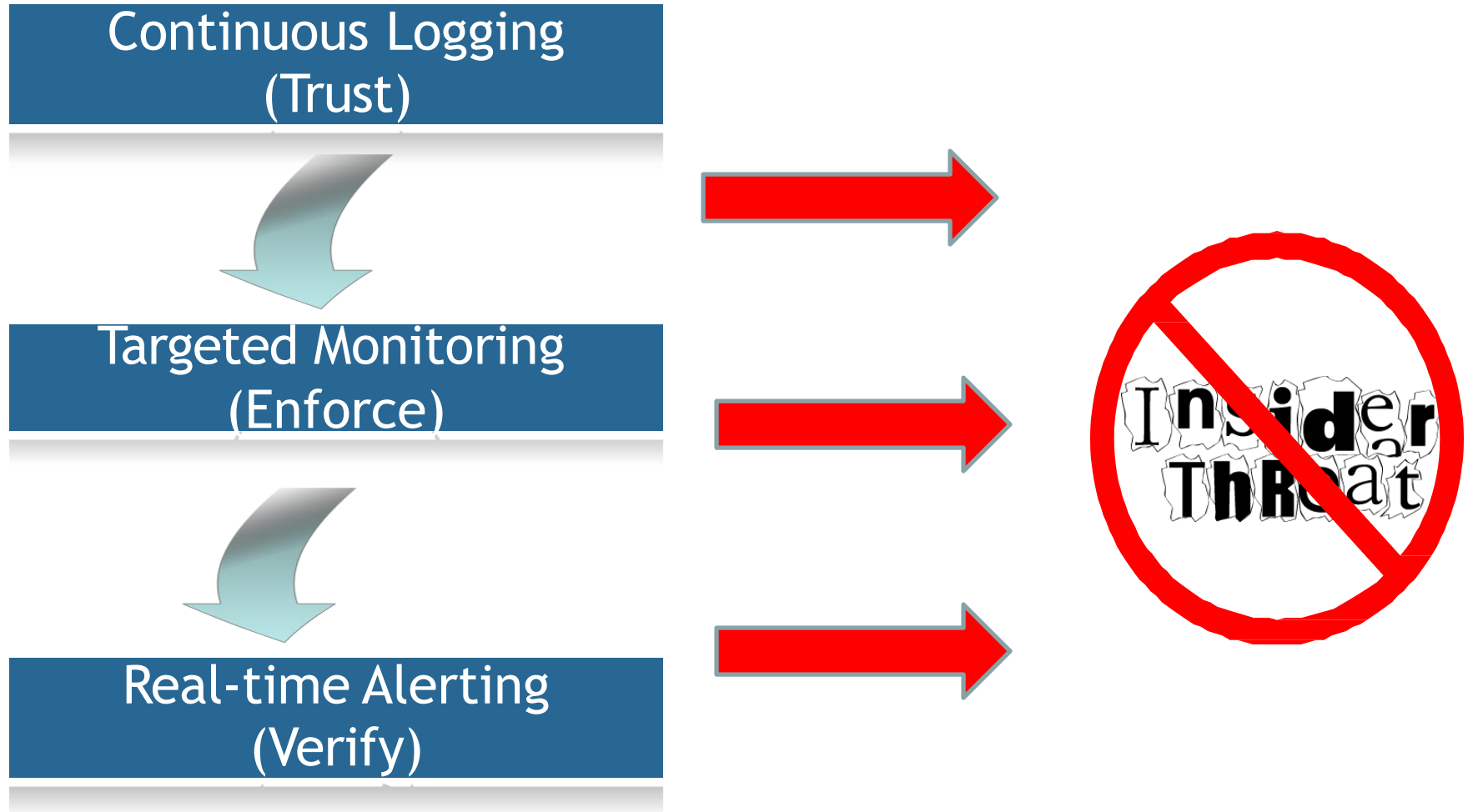
- Identify critical proprietary information / files.
- Consider digital rights management.
- Consider encryption.
- Log access to critical proprietary information / files.
- Consider host-based monitoring, including laptops.
- Consider data leakage protection tools for detection of exfiltration of critical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



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:

- We only have data on criminals
 - Our findings / recommendations could result in a high false positive rate
 - We would like to work with organizations that are willing to be pilot sites – please contact us!!
- 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 successfully 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.

Course Conclusion

Notices

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

CERT® and CERT Coordination Center® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-0486

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

1. Form an insider threat team that includes HR, Legal, IT, Information Security, Data Owners, Management, Security
2. Create policies that cross organizational boundaries – work with legal counsel
3. Consistently enforce the policies
4. Develop processes and implement controls that enforce communication across departments

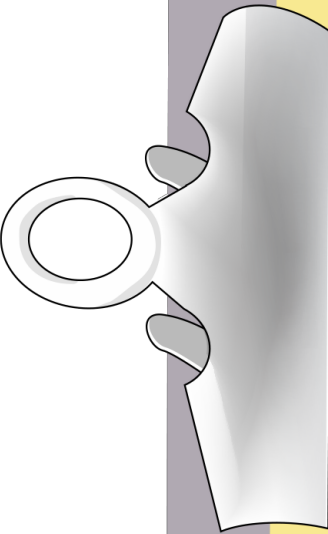
Long Term

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

TOP
TEN

- 
10. Learn from past incidents
 9. Focus on protecting the "crown jewels"
 8. Use your current technologies differently
 7. Mitigate threats from trusted business partners
 6. Recognize concerning behaviors as a potential indicator
 5. Educate employees regarding potential recruitment
 4. Pay close attention at resignation/termination
 3. Address employee privacy issues with General Counsel
 2. Work together across the organization
 1. Create an Insider threat program NOW!

Resources

Notices

Copyright 2019 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

CERT® and CERT Coordination Center® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM19-0486

CERT Resources

Insider Threat Center website (http://www.cert.org/insider_threat/)

Common Sense Guide to Mitigating Insider Threats, 4th Ed.
(<http://www.sei.cmu.edu/library/abstracts/reports/12tr012.cfm>)

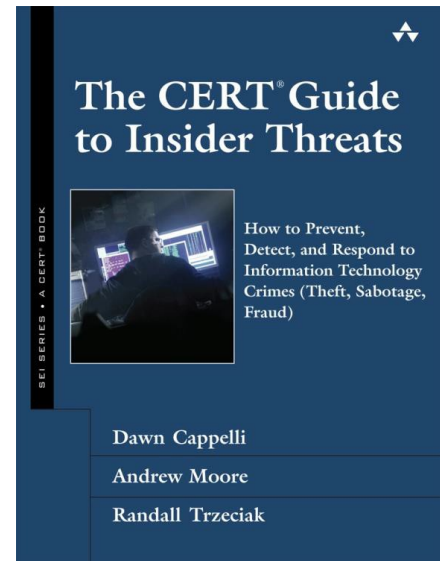
The Insider Threat and Employee Privacy: An Overview of Recent Case Law, Computer Law and Security Review, Volume 29, Issue 4, August 2013 by Carly L. Huth

Insider threat workshops

Insider threat assessments

New controls from CERT Insider Threat Lab

Insider threat exercises



[The CERT® Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes \(Theft, Sabotage, Fraud\) \(SEI Series in Software Engineering\)](#) by Dawn M. Cappelli, Andrew P. Moore and Randall F. Trzeciak

For More Information

Insider Threat Center website
(http://www.cert.org/insider_threat/)

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

Insider Threat Blog (http://www.cert.org/blogs/insider_threat/)