Network Security, Incident Management, and Insider Threats in the Healthcare Industry

CERT Insider Threat Center

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Randy Trzeciak
May 11, 2011

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

Insider Threat Agenda

Introduction

How bad is the insider threat?

Exploration of each type of insider crime:

- IT sabotage
- Theft of Intellectual Property
- Fraud

Mitigation Strategies

Introduction

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)

Who is a Malicious Insider?

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.*

Types of Insider Crimes

Insider IT sabotage

An insider's use of IT to direct specific harm at an organization or an individual.

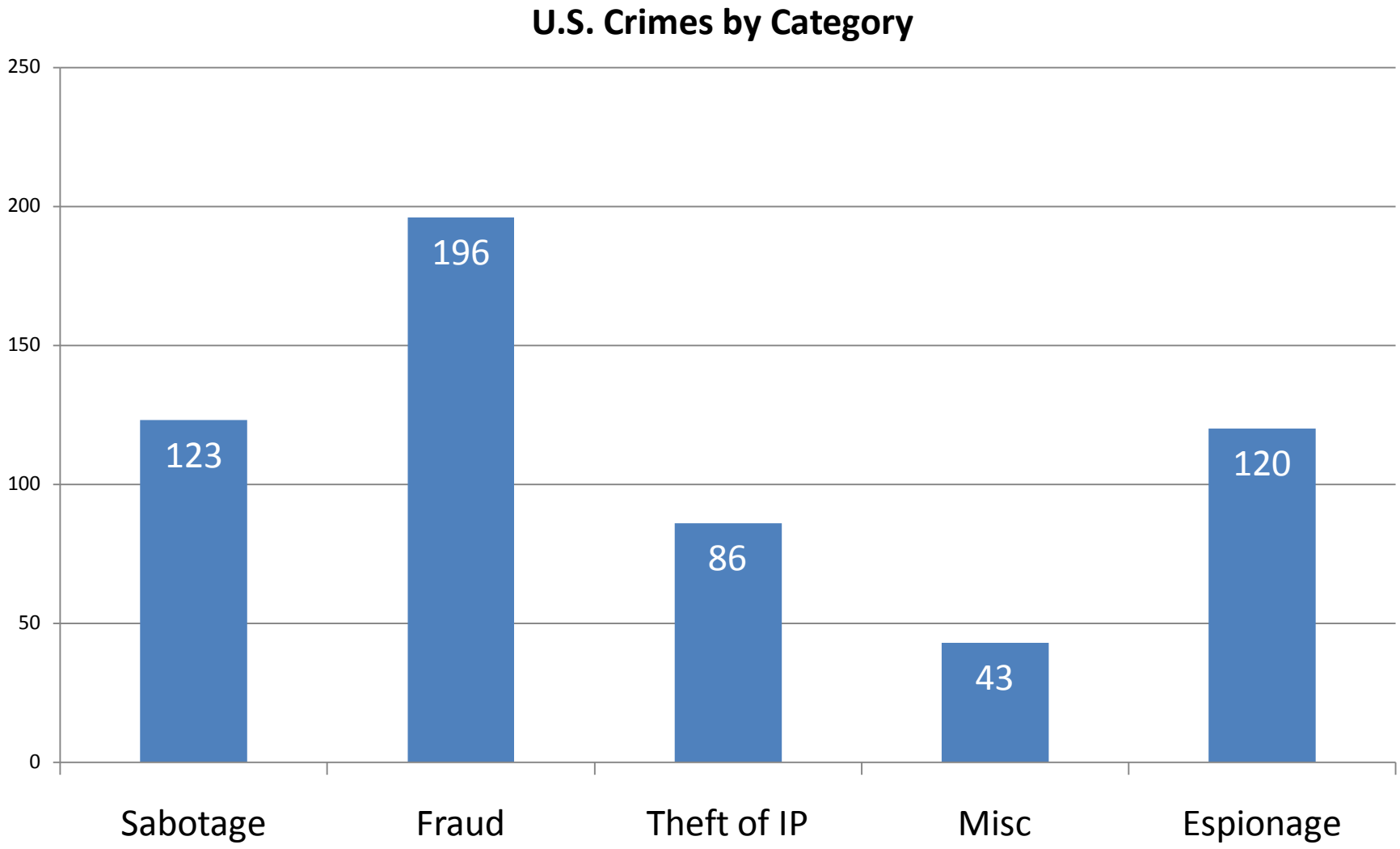
Insider theft of intellectual property (IP)

An insider's use of IT to steal intellectual property from the organization. This category includes industrial espionage involving insiders.

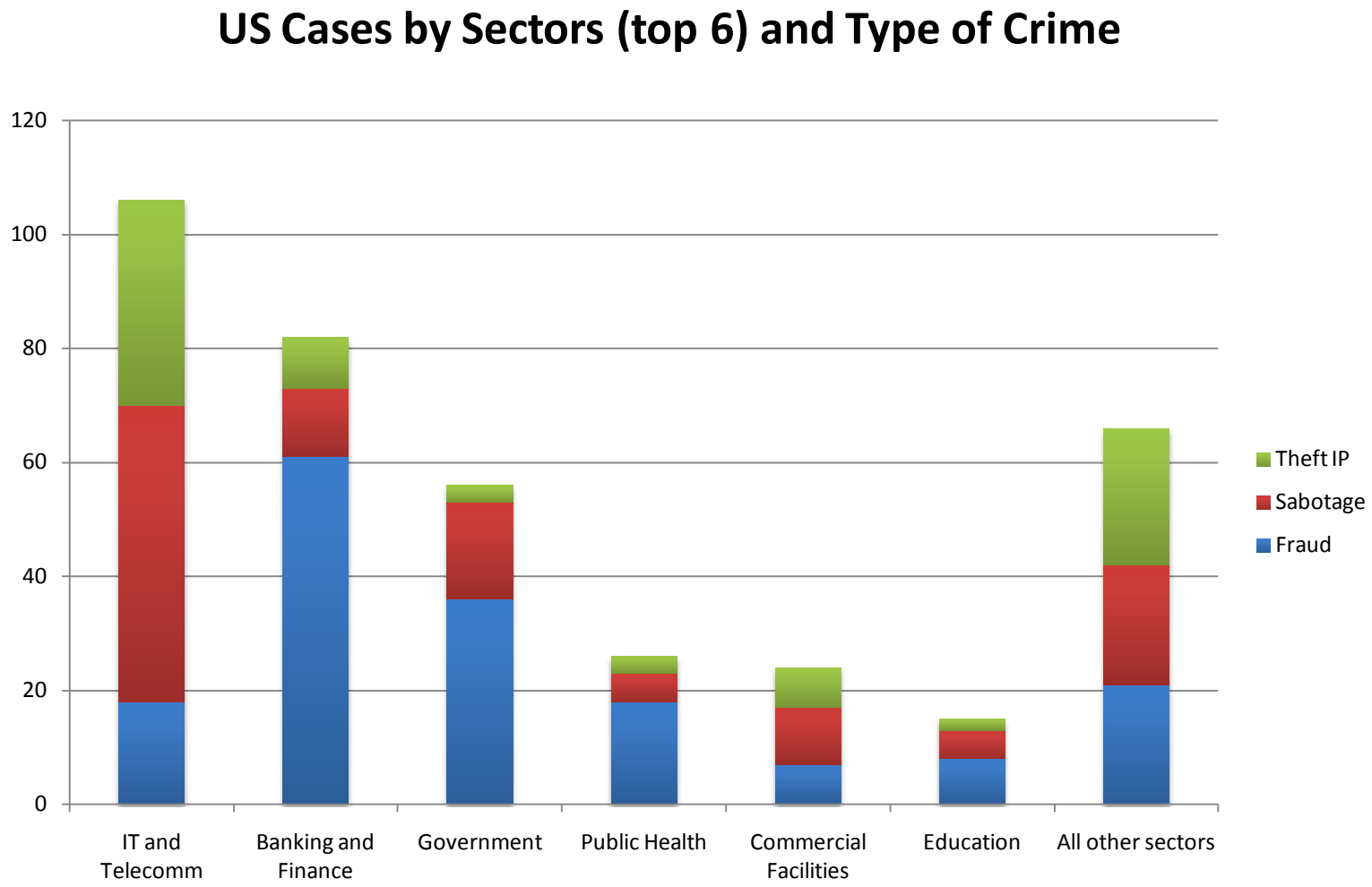
Insider fraud

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).

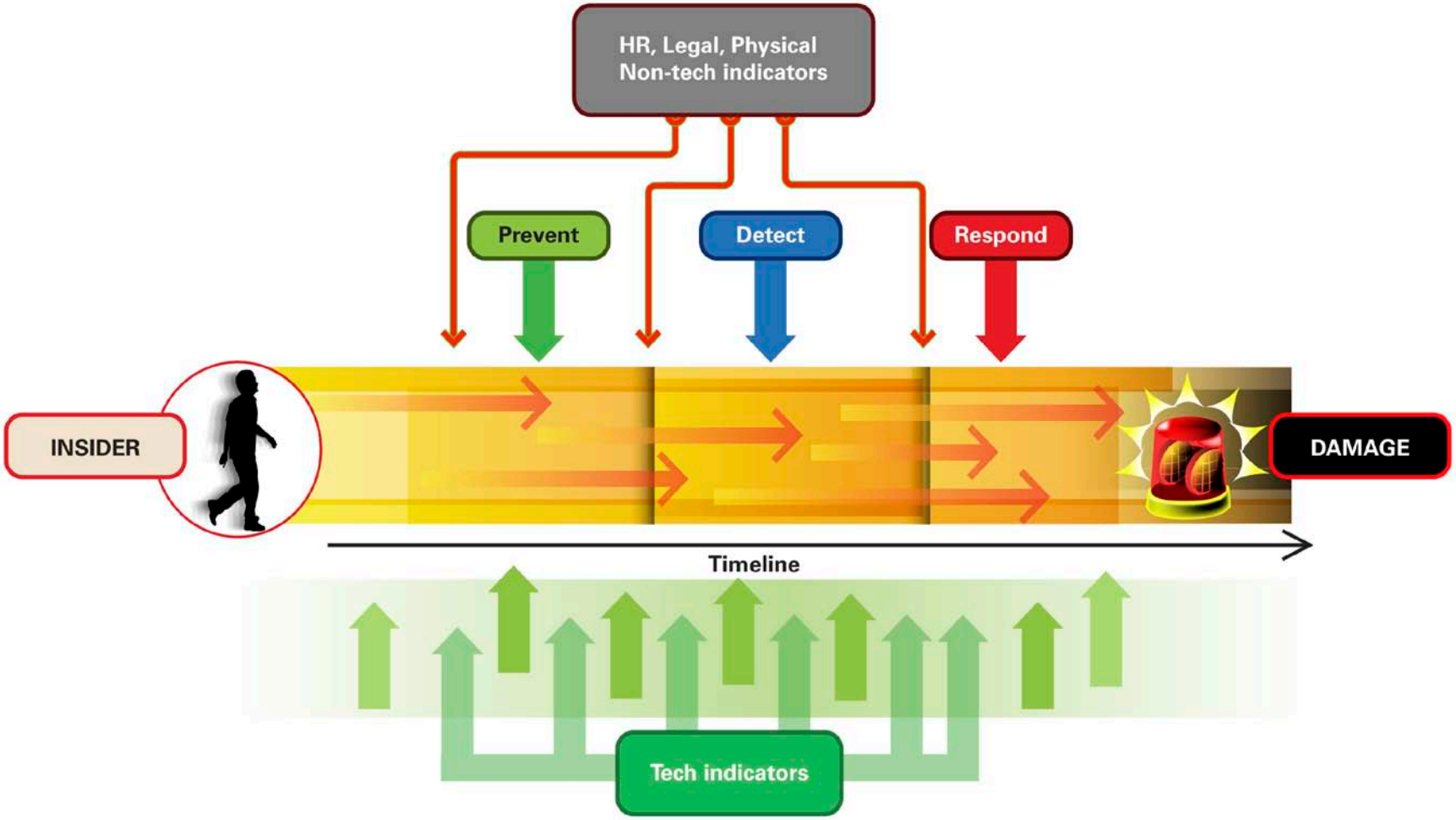
CERT's Insider Threat Case Database



Critical Infrastructure Sectors



CERT Insider Threat Center Objective



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

How bad is the insider threat?

Insider Threat Issue

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.

2011 CyberSecurity Watch Survey -1

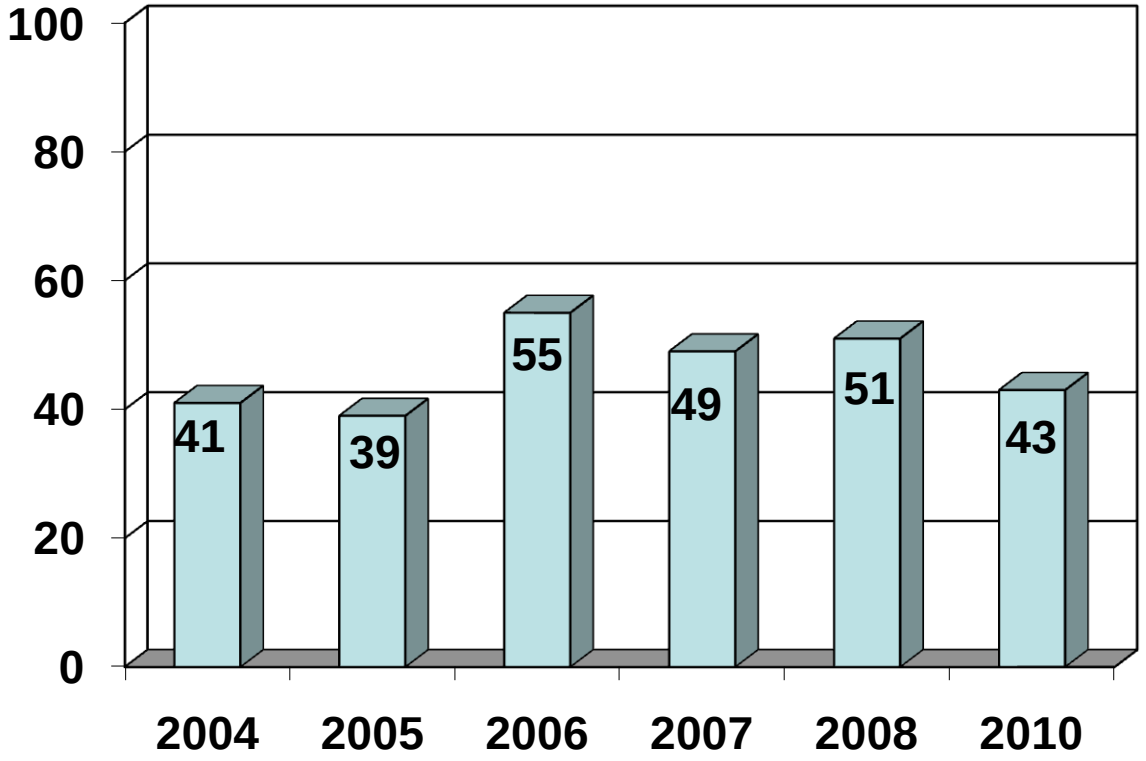
CSO Magazine, USSS, CERT & Deloitte

607 respondents

38% of organizations have more than 5000 employees

37% of organizations have less than 500 employees

Percentage of Participants Who Experienced an Insider Incident



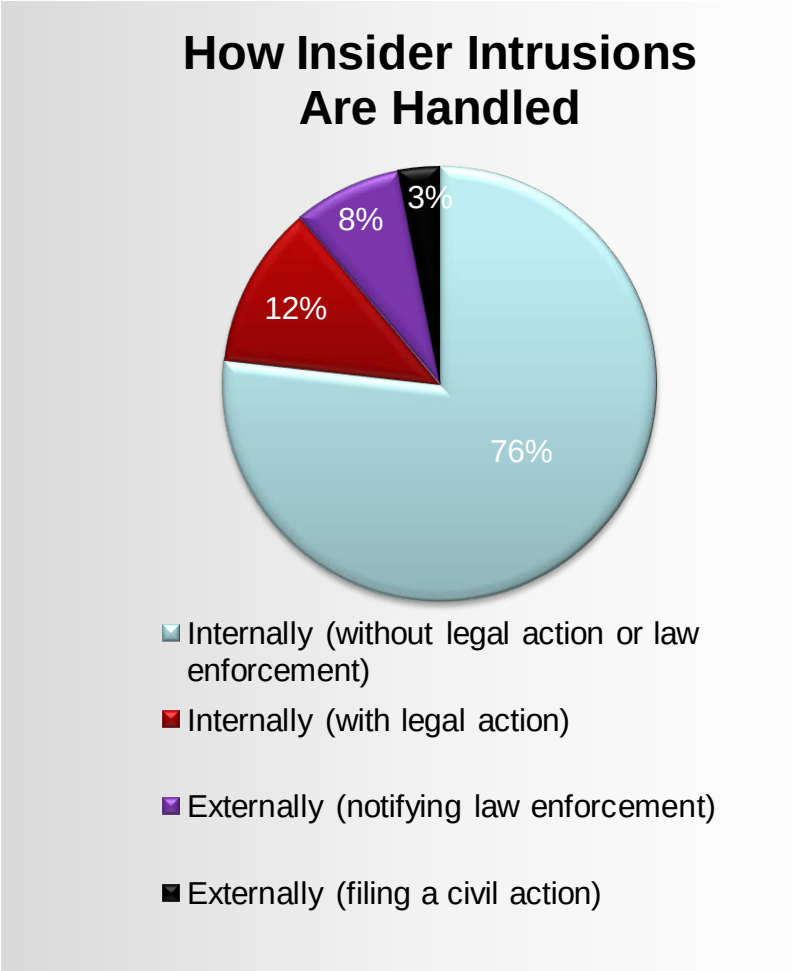
Source: 2011 CyberSecuirty Watch Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, January 2011.

2011 CyberSecurity Watch Survey -2

46 % of respondents	Damage caused by insider attacks more damaging than outsider attacks
Most common insider e-crime	
Unauthorized access to / use of corporate information	(63%)
Unintentional exposure of private or sensitive data	(57%)
Virus, worms, or other malicious code	(37%)
Theft of intellectual property	(32%)

Source: 2011 CyberSecuirty Watch Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, January 2011.

2011 CyberSecurity Watch Survey - 3



Reason(s) CyberCrimes were not referred for legal action

	2011	2010
Damage level insufficient to warrant prosecution	42%	37%
Could not identify the individual/ individuals responsible for committing the eCrime	40%	29%
Lack of evidence/not enough information to prosecute	39%	35%
Concerns about negative publicity	12%	15%
Concerns about liability	8%	7%
Concerns that competitors would use incident to their advantage	6%	5%
Prior negative response from law enforcement	5%	7%
Unaware that we could report these crimes	4%	5%
Other	11%	5%
Don't know	20%	14%
Not applicable	N/A	24%

Source: 2011 CyberSecuirty Watch Survey, CSO Magazine, U.S. Secret Service, Software Engineering Institute CERT Program at Carnegie Mellon University and Deloitte, January 2011.

Insider Crime Profiles

IT Sabotage


DAN
SLAM!
DAN
Attach File(s)
Do you want
to attach DAN_BACKDOOR.EXE?
YES
NO

IT Sabotage Incidents

An IT consultant for a hospital medical supply facility seeks revenge when he loses control of his company

…System administrator sabotages systems on his way out

A security guard at a U.S. hospital, after submitting resignation notice, obtained physical access to computer rooms

…Installed malicious code on hospital computers, accessed patient medical records

Insider IT Sabotage

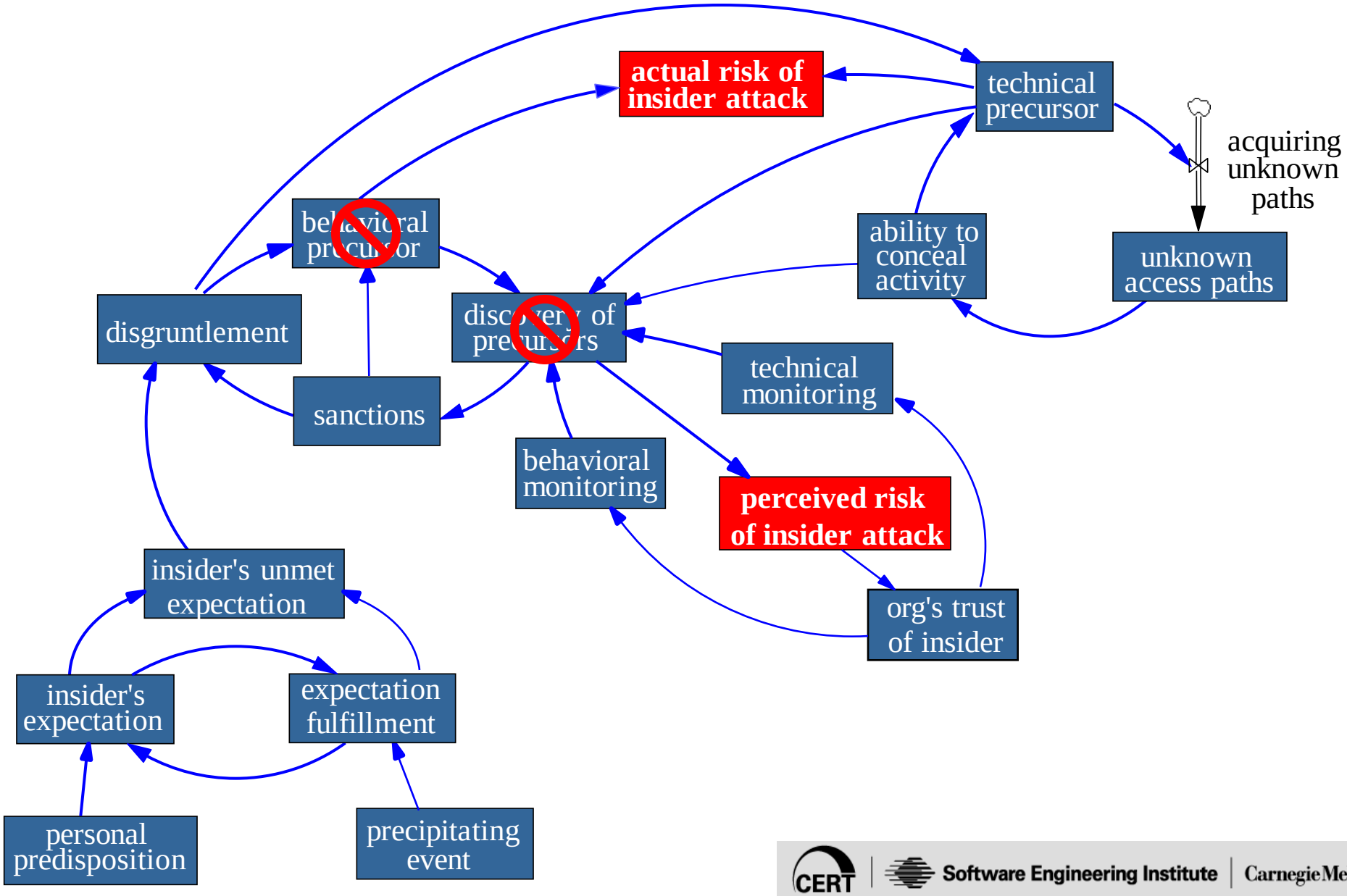
Who did it?

- Former employees
- Male
- Highly technical positions
- Age: 17 – 60

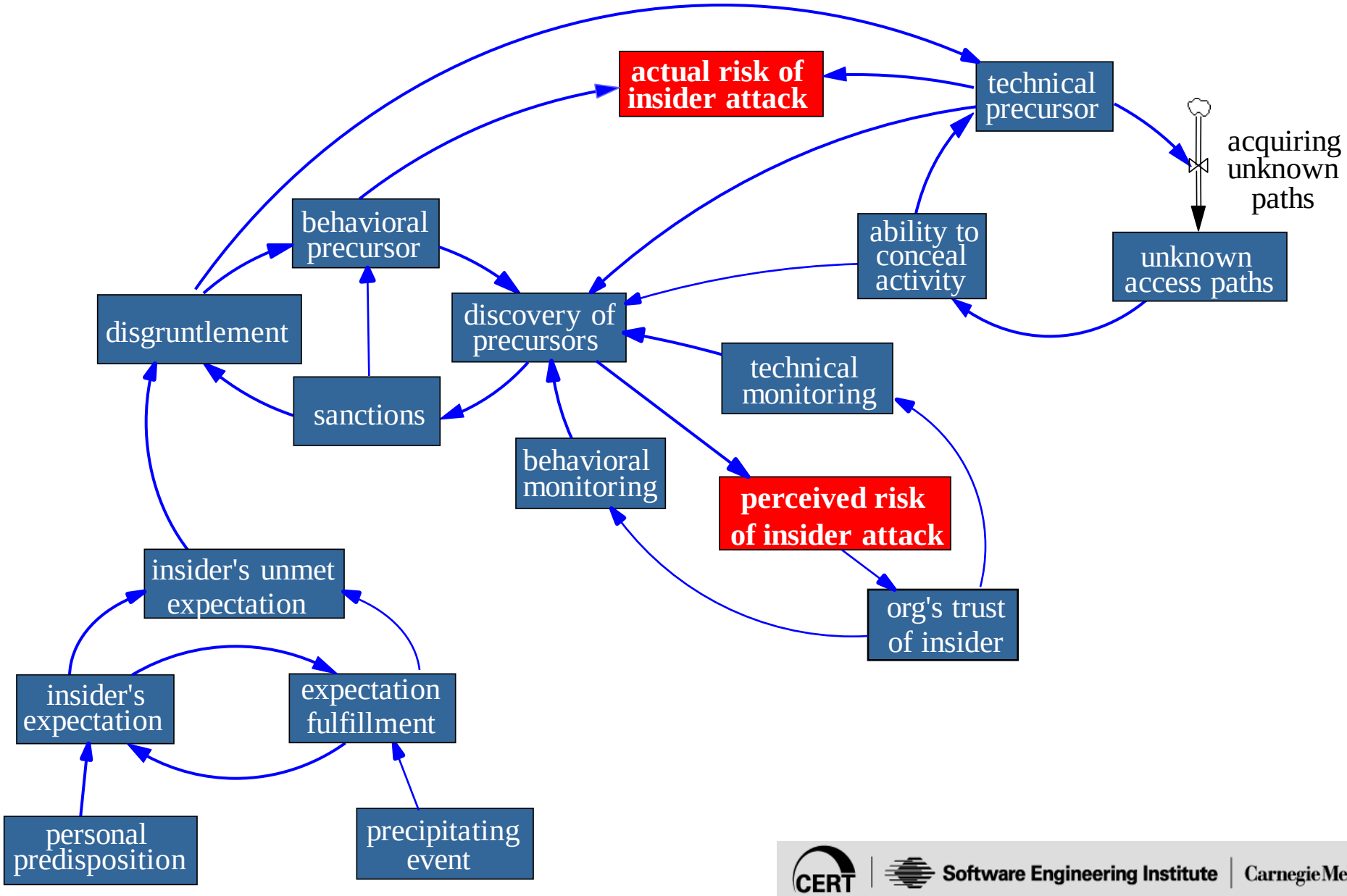
How did they attack?

- No authorized access
- Backdoor accounts, shared accounts, other employees' accounts, insider's own account
- Many technically sophisticated
- Remote access outside normal working hours

MERIT Model of Insider IT Sabotage



MERIT Model of Insider IT Sabotage



Summary of Findings

	IT Sabotage
% of crimes in case database	35%
Current or former employee?	Former
Type of position	Technical (e.g. sys admins or DBAs)
Gender	Male

Summary of Findings

	IT Sabotage
Target	Network, systems, or data
Access used	Unauthorized
When	Outside normal working hours
Where	Remote access
Recruited by outsiders	None
Collusion	None

Theft of Intellectual Property

Theft of Information Incidents

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
- Technical or sales positions
- All male
- Average age: 37

What was stolen?

- Intellectual Property (IP)
- Customer Information (CI)

How did they steal it?

- During normal working hours
- Using authorized access

Dynamics of the Crime

Most were *quick* theft upon resignation

Stole information to

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

Collusion

- Collusion with at least one *insider* in almost 1/2 of cases
- Outsider *recruited* insider in less than 1/4 of cases
- Acted *alone* in 1/2 of cases

Summary of Findings

	IT Sabotage	Theft of Intellectual Property
% of crimes in case database	35%	18%
Current or former employee?	Former	Current
Type of position	Technical (e.g. sys admins or DBAs)	Technical (71%) - scientists, programmers, engineers Sales (29%)
Gender	Male	Male

Summary of Findings

	IT Sabotage	Theft of Intellectual Property
Target	Network, systems, or data	IP (trade secrets) – 71% Customer Info – 33%
Access used	Unauthorized	Authorized
When	Outside normal working hours	During normal working hours
Where	Remote access	At work
Recruited by outsiders	None	Less than 1/4
Collusion	None	Almost ½ colluded with at least one insider; ½ acted alone

Fraud

Fraud Incidents

An accounts payable clerk, over a period of 3 years, issues 127 unauthorized checks to herself an 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

Fraud: Theft or Modification

Most attacks were long, ongoing schemes

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)
- Very few cases involved trade secrets

How did they steal/modify it?

- During normal working hours
- Using authorized access

Summary of Findings

	IT Sabotage	Theft of Intellectual Property	Fraud
% of crimes in case database**	35%	18%	40%
Current or former employee?	Former	Current	Current
Type of position	Technical (e.g. sys admins or DBAs)	Technical (71%) - scientists, programmers, engineers Sales (29%)	Non-technical, low-level positions with access to confidential or sensitive information (e.g. data entry, customer service)
Gender	Male	Male	Fairly equally split between male and female

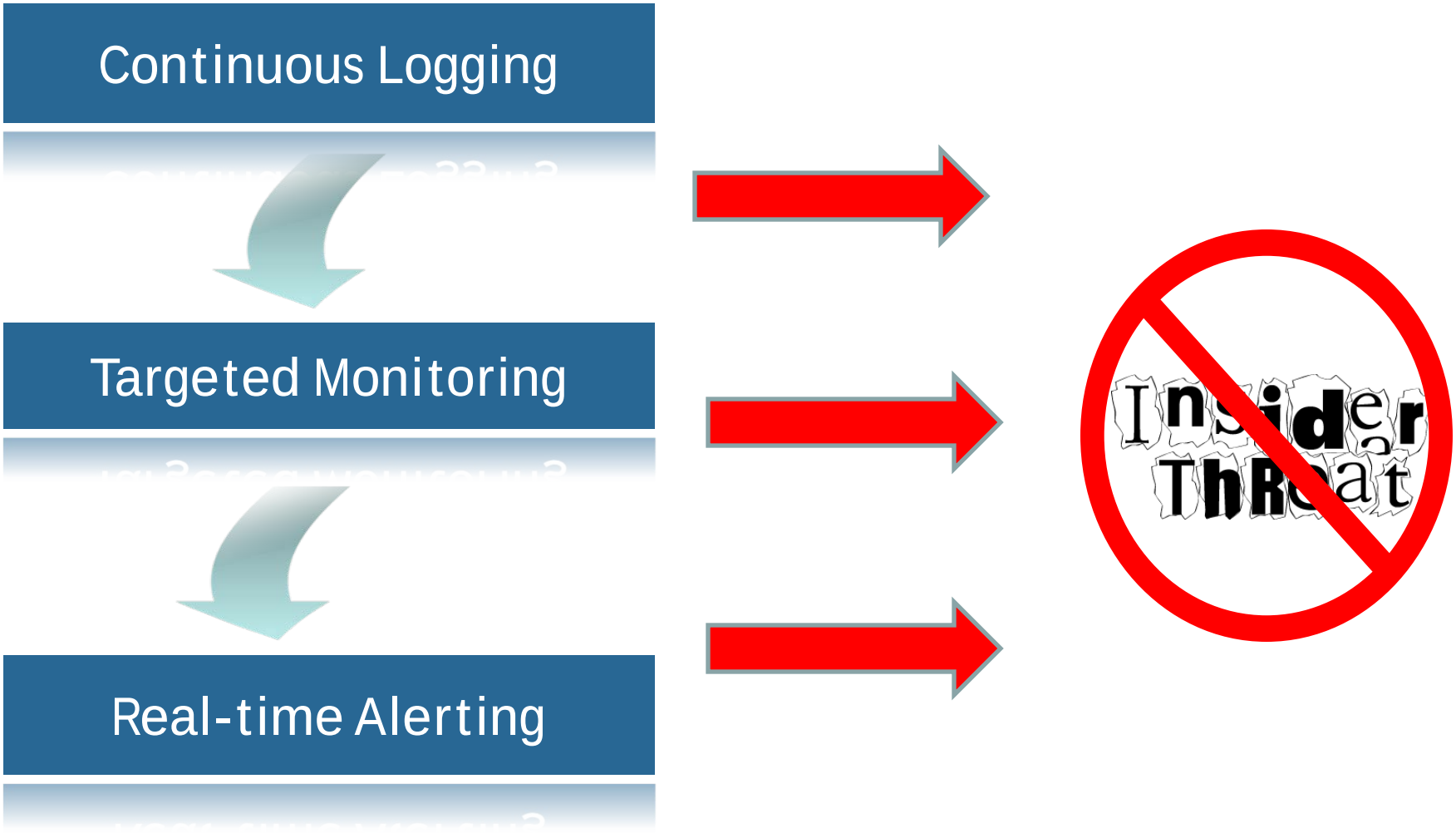
***** Does not include national security espionage***

Summary of Findings

	IT Sabotage	Theft of Intellectual Property	Fraud
Target	Network, systems, or data	IP (trade secrets) – 71% Customer Info – 33%	PII or Customer Information
Access used	Unauthorized	Authorized	Authorized
When	Outside normal working hours	During normal working hours	During normal working hours
Where	Remote access	At work	At work
Recruited by outsiders	None	Less than 1/4	½ recruited for theft; less than 1/3 recruited for mod
Collusion	None	Almost ½ colluded with at least one insider; ½ acted alone	Mod: almost ½ colluded with another insider Theft: 2/3 colluded with outsiders

Mitigation Strategies

Our Suggestion



Common Sense Guide to Prevention and Detection of Insider Threats

http://www.cert.org/archive/pdf/CSG-V3.pdf

Summary of Best Practices in CSG

Consider threats from insiders and business partners in enterprise-wide risk assessments.	Consider insider threats in the software development life cycle.
Clearly document and consistently enforce policies and controls.	Use extra caution with system administrators and technical or privileged users.
Institute periodic security awareness training for all employees.	Implement system change controls.
Monitor and respond to suspicious or disruptive behavior, beginning with the hiring process.	Log, monitor, and audit employee online actions.
Anticipate and manage negative workplace issues.	Use layered defense against remote attacks.
Track and secure the physical environment.	Deactivate computer access following termination.
Implement strict password and account management policies and practices.	Implement secure backup and recovery processes.
Enforce separation of duties and least privilege.	Develop an insider incident response plan.

Publicly Available Information

Reports

Podcasts

Insider Threat Study

System Dynamics

Cyber Crime Survey

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

Point of Contact

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

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