What Organizations Need to Know About Insider Cyber Crimes

Andrew P. Moore (apm@cert.org)
CERT Program
Software Engineering Institute
Carnegie Mellon University

Information Security Decisions
10:00 - 10:50 AM Thursday, 6 November 2008

Agenda

Background

Exploration of types of insider crime:

- Theft/Modification of information for financial gain
- Theft of information for business advantage
- IT sabotage

Discussion

TRUE STORY:

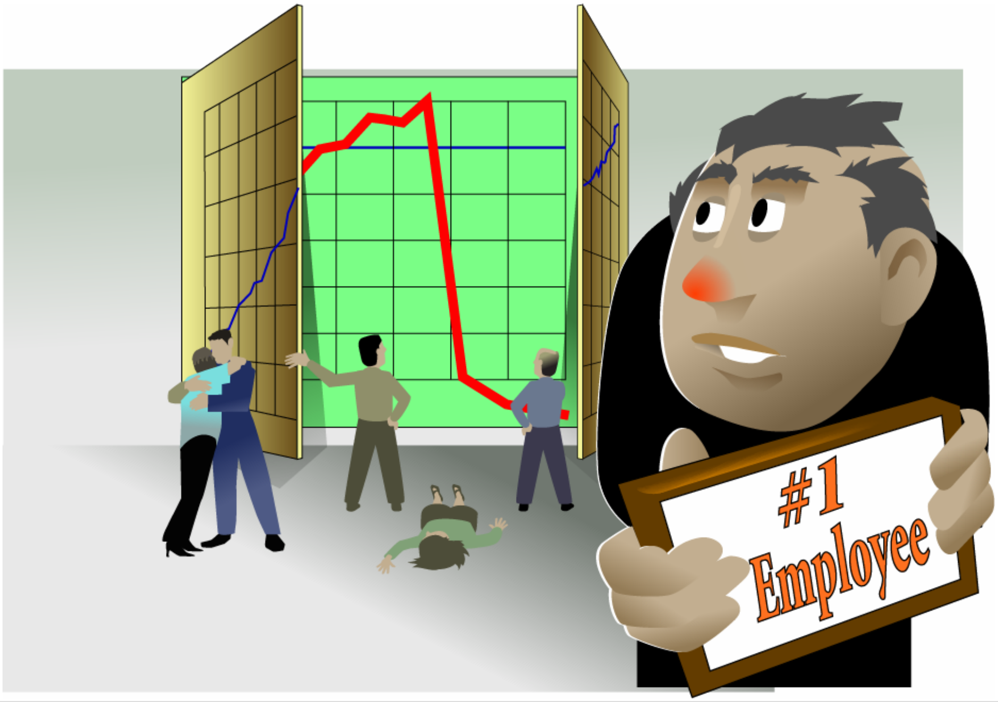
Credit union customers lose all access to their money from Friday night through Monday…

Fired system administrator sabotages systems on his way out

TRUE STORY:

Financial institution discovers $691 million in losses ...

Covered up for 5 years by trusted employee



COULD THIS HAPPEN TO YOU?

Definition of Malicious Insider

From the CERT/US Secret Service *Insider Threat Study*

Current or former employees or contractors who

- *intentionally exceeded or misused an authorized level of network, system or data access in a manner that*
- *affected the security of the organizations’ data, systems, or daily business operations.*

How bad is the insider threat?

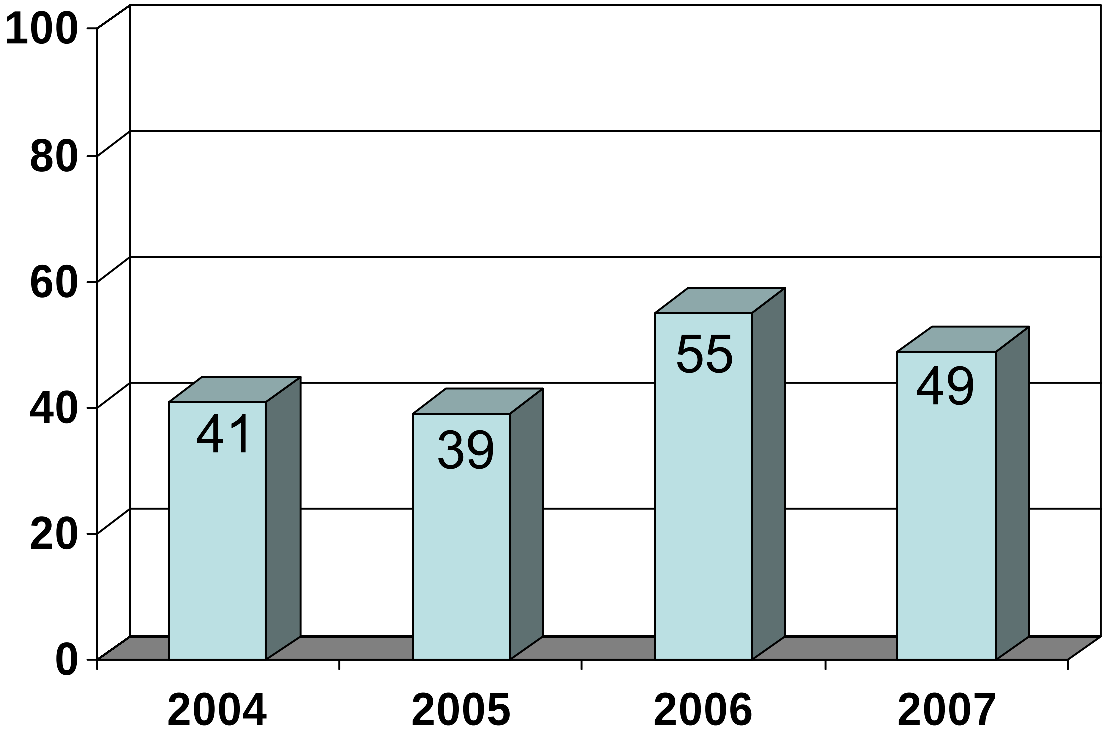
2007 e-Crime Watch Survey

CSO Magazine, USSS,

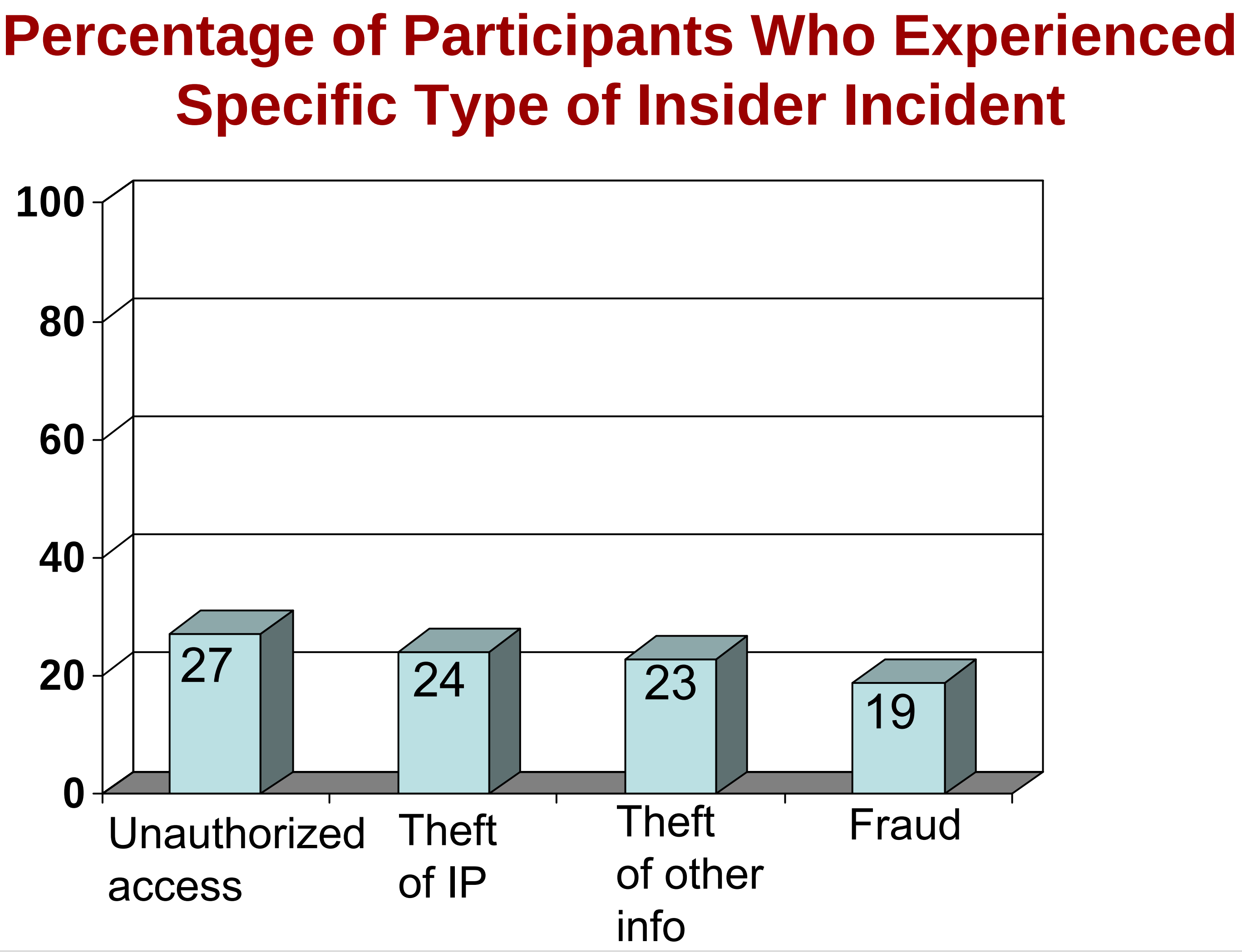
Microsoft & CERT

671 respondents

Percentage of Participants Who Experienced an Insider Incident



Most Common Insider Incidents



Source of CERT's Insider Threat Case Data

CERT/U.S. Secret Service *Insider Threat Study*

- 150 actual insider threat cases
- 1996-2002

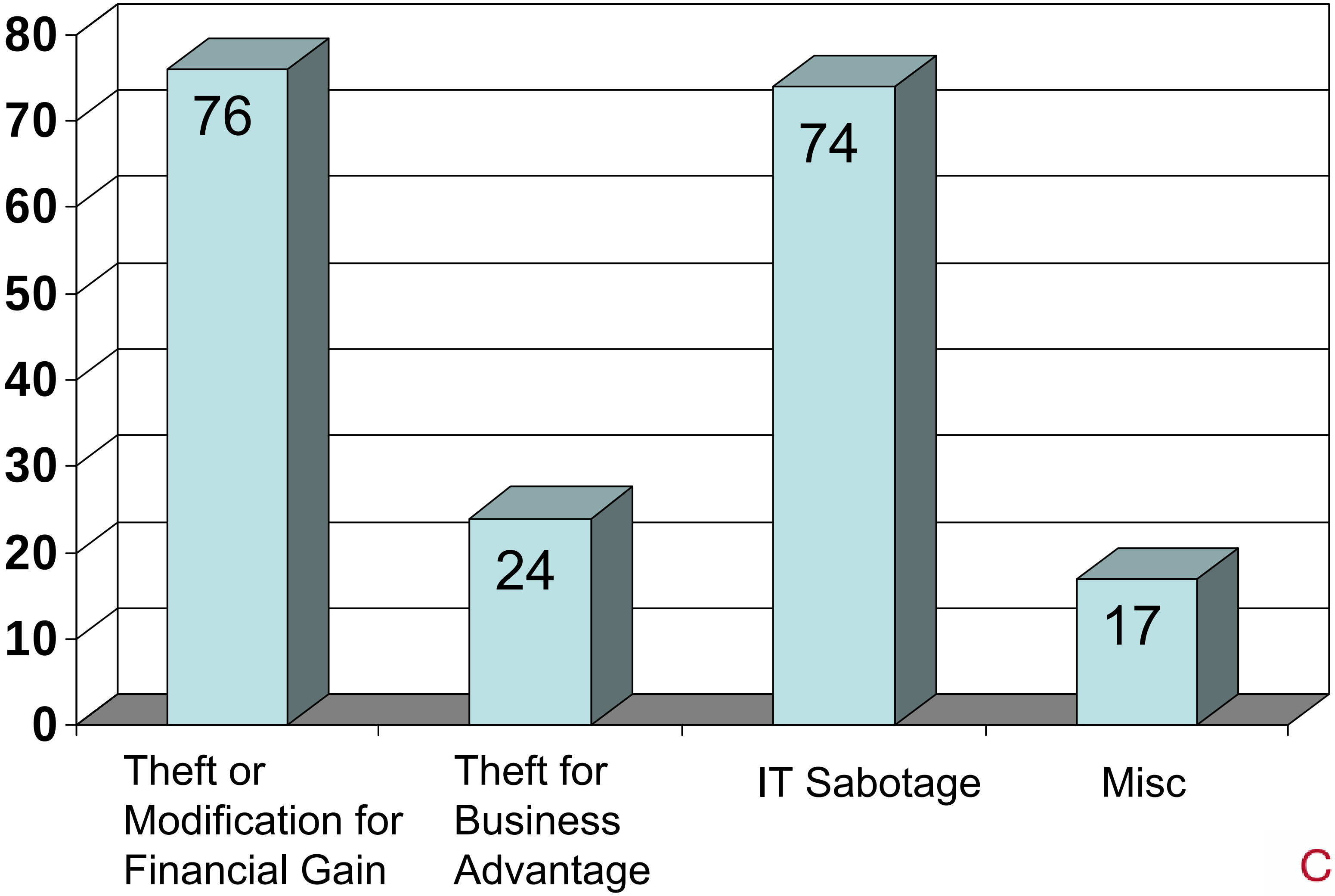
Carnegie Mellon CyLab *MERIT** Project

- Approximately 100 insider threat cases
- Cases not included in CERT/US Secret Service study
- Cases through 2007

Case data includes both technical and behavioral information

MERIT: Management and Education of the Risk of Insider Threat

CERT’s Insider Threat Case Breakdown



CyLab
www.cylab.cmu.edu

Scenario 1:

Theft or Modification of Information for Financial Gain

Theft or Modification for Financial Gain

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

Dynamics of the Crime

Most attacks were *long, ongoing* schemes *

	At least 1 Insider Colluder	*At least 1 Outsider Colluder*	*Outsider Induced*	*Acted Alone*
Theft	⅓	⅔	½	⅓
Modification	½	½	⅓	⅓

* Approximations used for simplicity of presentation

A Closer Look at THEFT for Financial Gain

Technical Aspects - Theft for Financial Gain

Electronically

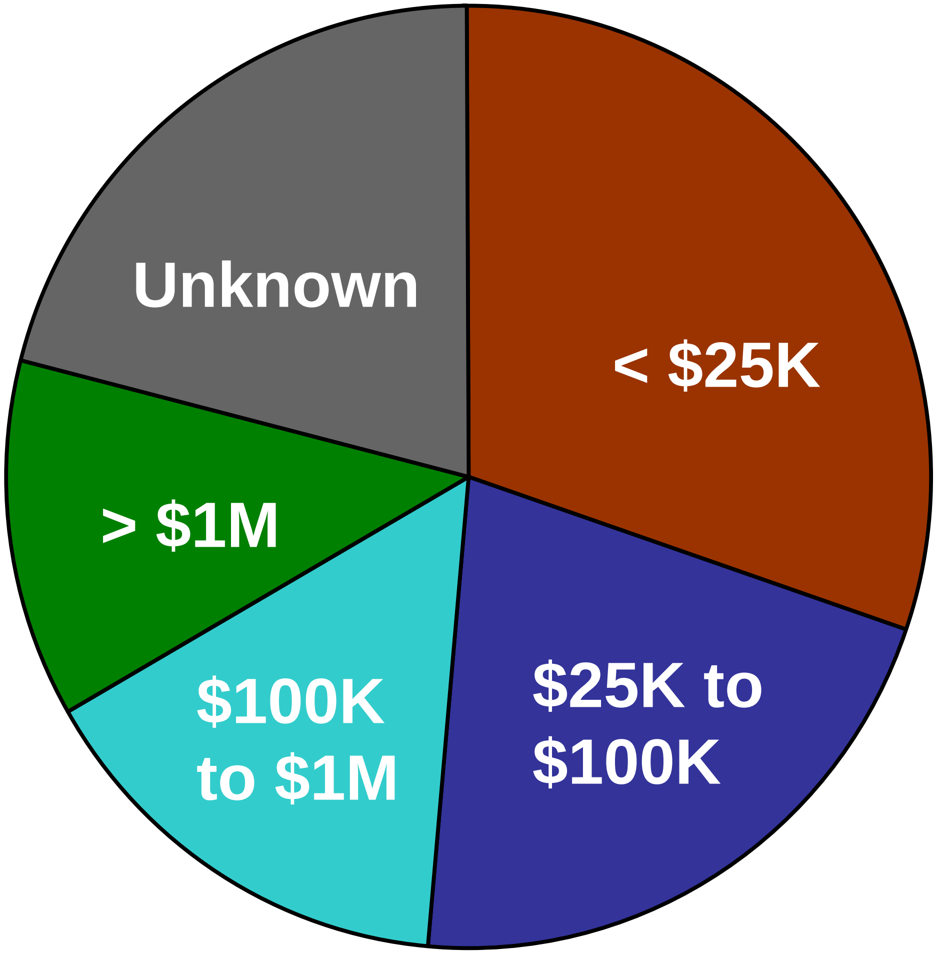
- Downloaded to home
- Looked up and used immediately
- Copied
- Phone/fax
- Email
- Malicious code

Physically

- Printouts
- Handwritten

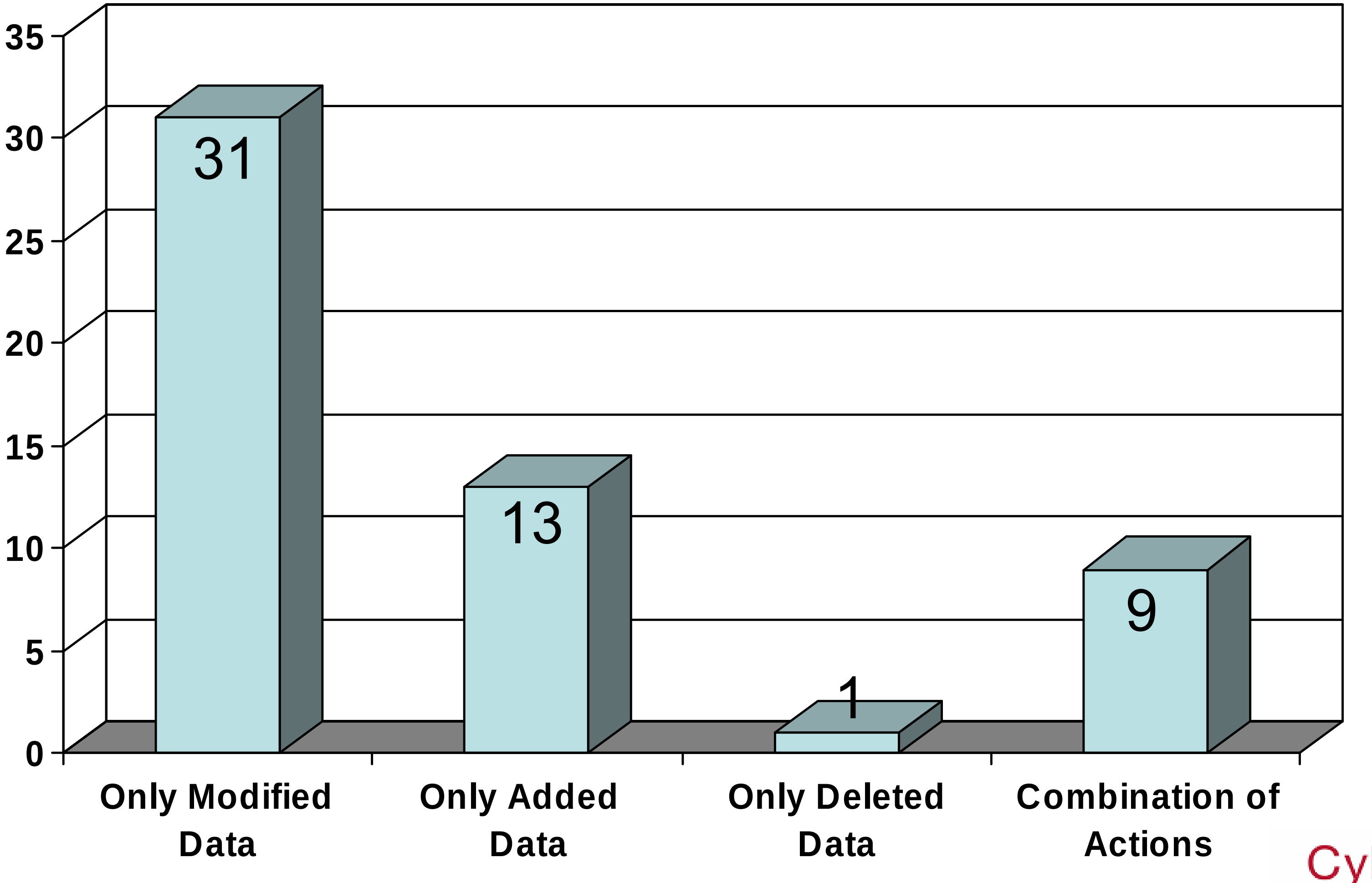
Remaining unknown

Organizational Impacts - Theft for Financial Gain

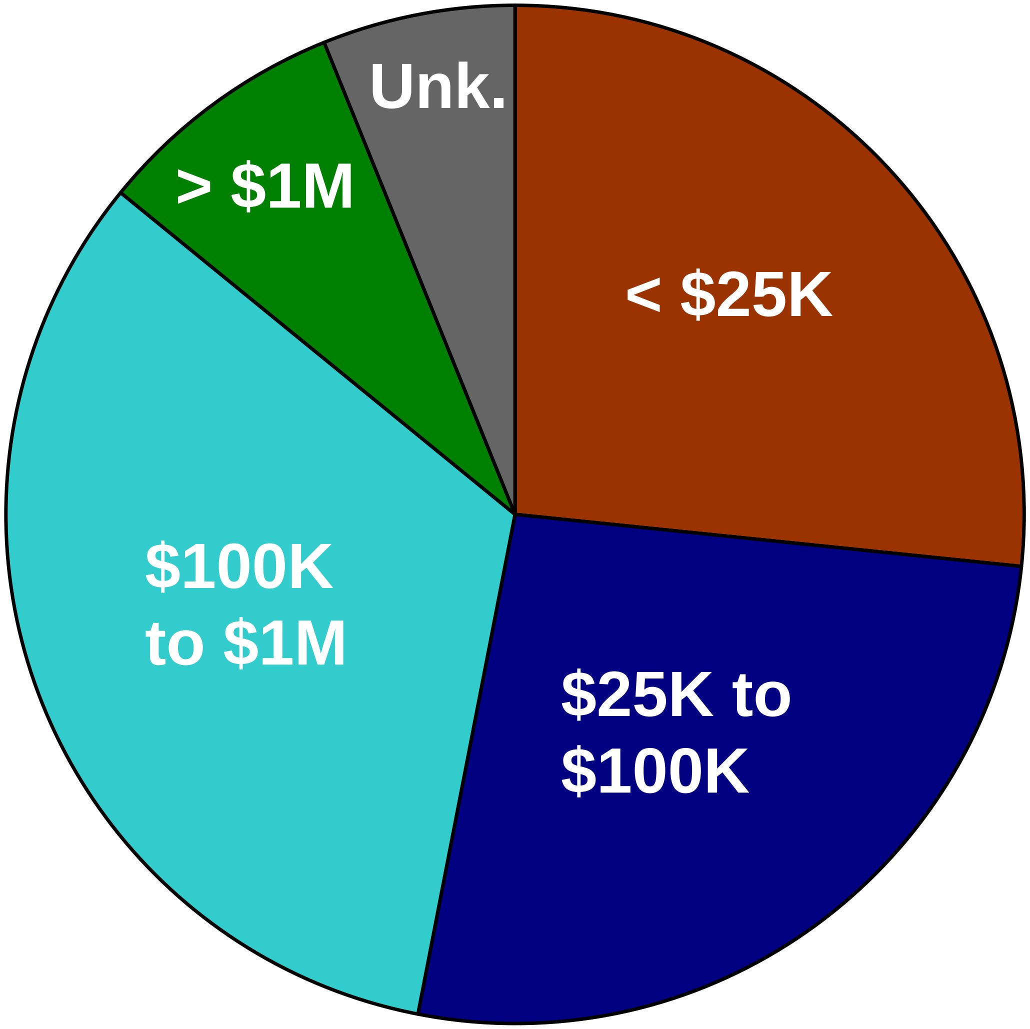


A Closer Look at MODIFICATION for Financial Gain

Technical Aspects – Modification for Financial Gain



Organizational Impacts - Modification for Financial Gain



Scenario 2

Theft of Information for Business Advantage

CyLab
www.cylab.cmu.edu

Theft For Business Advantage

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

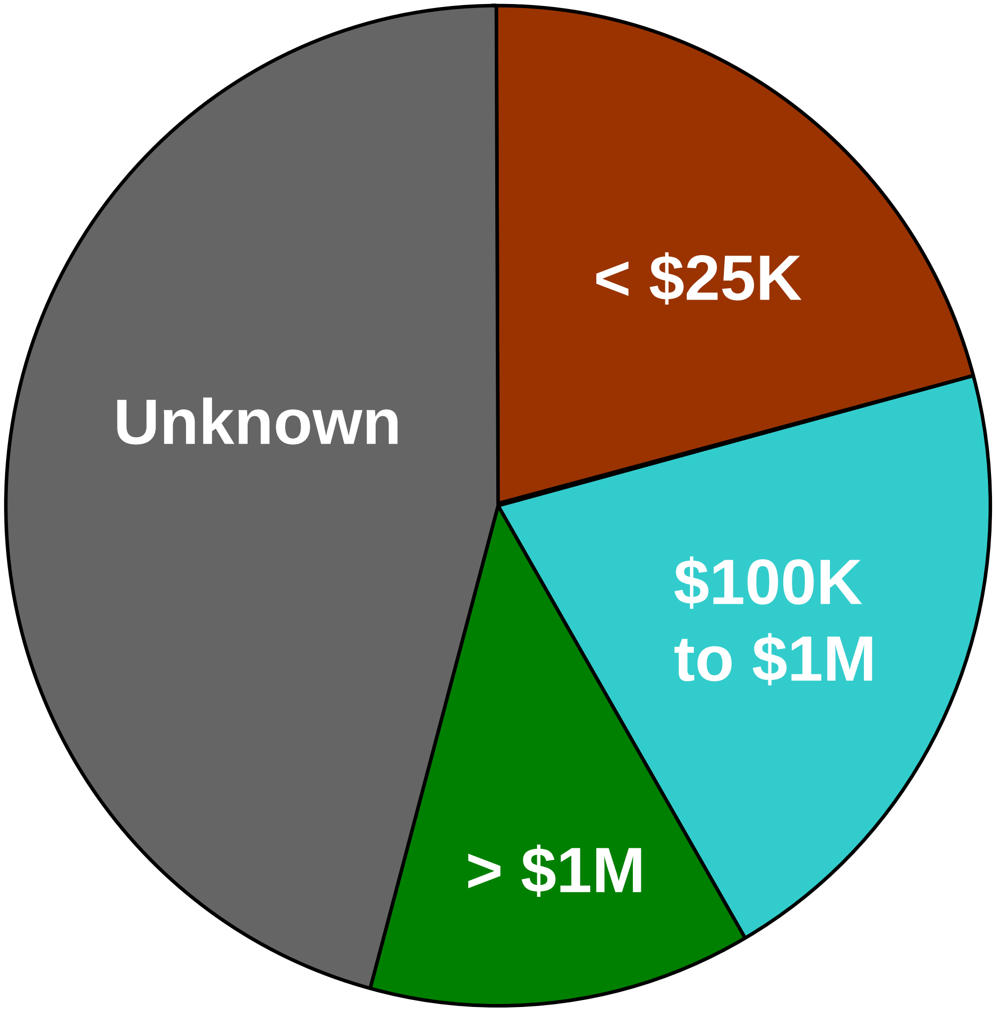
Technical Aspects – Theft for Business Advantage

In order of prevalence:

- Copied/downloaded information
- Emailed information
- Accessed former employer’s system
- Compromised account

Many other methods

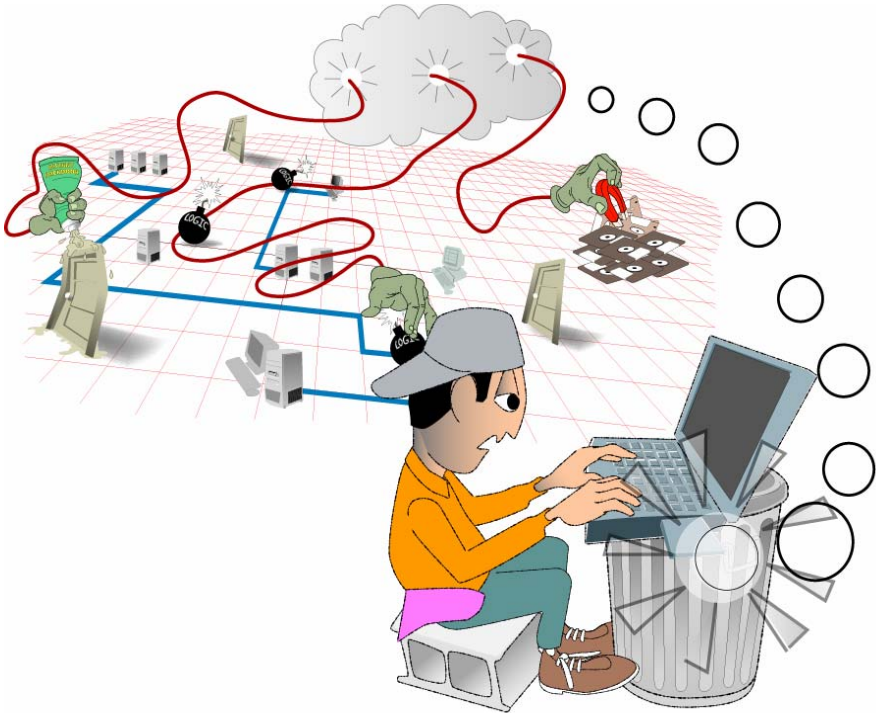
Organizational Impacts - Theft for Business Advantage



* Note: None in range $25K to $100K.

Scenario 3:

IT Sabotage with the Intent to Harm Organization or Individual



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

Dynamics of Insider IT Sabotage

Most insiders were disgruntled due to unmet expectations

- Period of heightened expectations, followed by a precipitating event triggering precursors

Behavioral precursors were often observed but ignored by the organization

- Significant behavioral precursors often came before technical precursors

Technical precursors were observable, but not detected by the organization

Known Issues

Unmet Expectations

- Insufficient compensation
- Lack of career advancement
- Inflexible system policies
- Coworker relations; supervisor demands

Behavioral precursors

- Drug use; absence/tardiness
- Aggressive or violent behavior; mood swings
- Used organization's computers for personal business
- Sexual harassment
- Poor hygiene

Technical Aspects of Insider IT Sabotage

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

The majority attacked after termination.

Organizations failed to detect technical precursors

Lack of physical or electronic access controls facilitated the attack

Organizational Impacts of IT Sabotage

Inability to conduct business, loss of customer records

Inability to produce products

Negative media attention

Private information forwarded to customers, competitors, or employees

Exposure of personal or confidential information

Web site defacements

Many individuals harmed

CyLab
www.cylab.cmu.edu

Summary

Insider threat is a problem that impacts and requires understanding by everyone

- Information Technology
- Information Security
- Human Resources
- Management
- Physical Security
- Legal

Use enterprise risk management for protection of critical assets from ALL threats, including insiders

Incident response plans should include insider incidents

Create a culture of security – all employees have responsibility for protection of organization’s information

Points of Contact

Insider Threat Team Lead:
Dawn M. Cappelli
Senior Member of the Technical Staff
CERT Program
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-3890
+1 412 268-9136 – Phone
dmc@cert.org – Email

Business Development:
Joseph McLeod
Business Manager
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-3890
+1 412 268-6674 – Phone
+1 412-291-3054 – FAX
+1 412-478-3075 – Mobile
jmcleod@sei.cmu.edu – Email

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

NO WARRANTY

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The Government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.