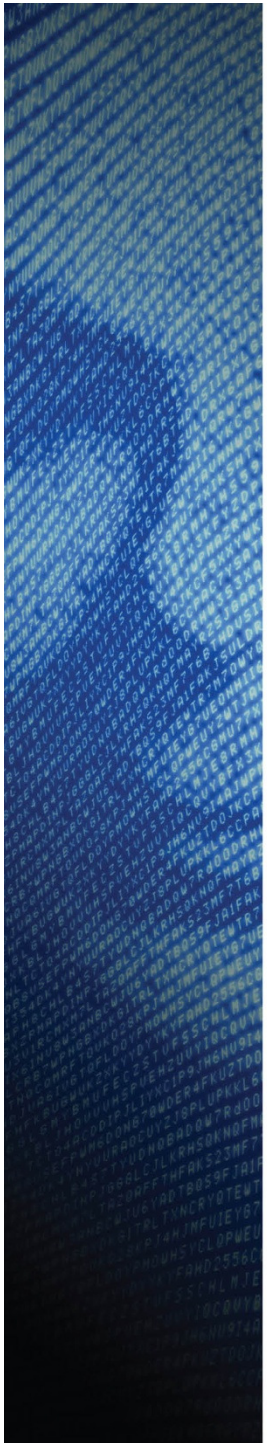


Risk Mitigation Strategies: Lessons Learned from Actual Insider Attacks

Dawn M. Cappelli
Andrew P. Moore
CERT Program – Software Engineering Institute
Carnegie Mellon University
04/09/08 | Session Code:DEF-203

Agenda

- Background
- Exploration of each type of insider crime:
  - Theft/Modification of information for financial gain
  - Theft of information for business advantage
  - IT sabotage
- Best practices
- Summary
- Discussion

TRUE STORY:

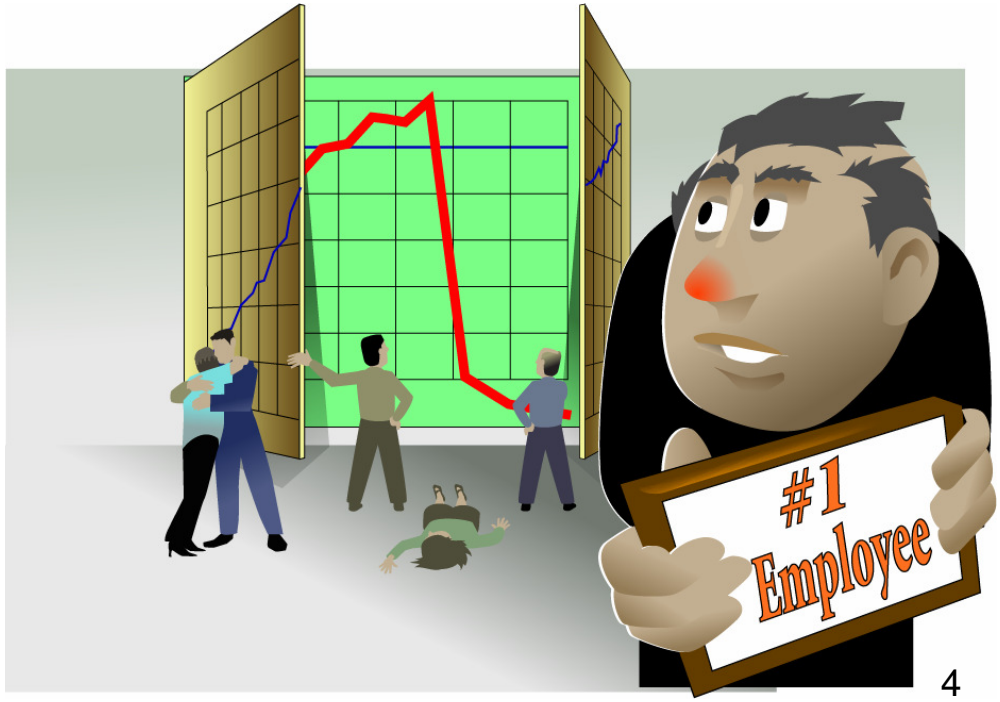
Credit union customers lose all access to their money from Friday night through Monday…

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?

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)

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.*

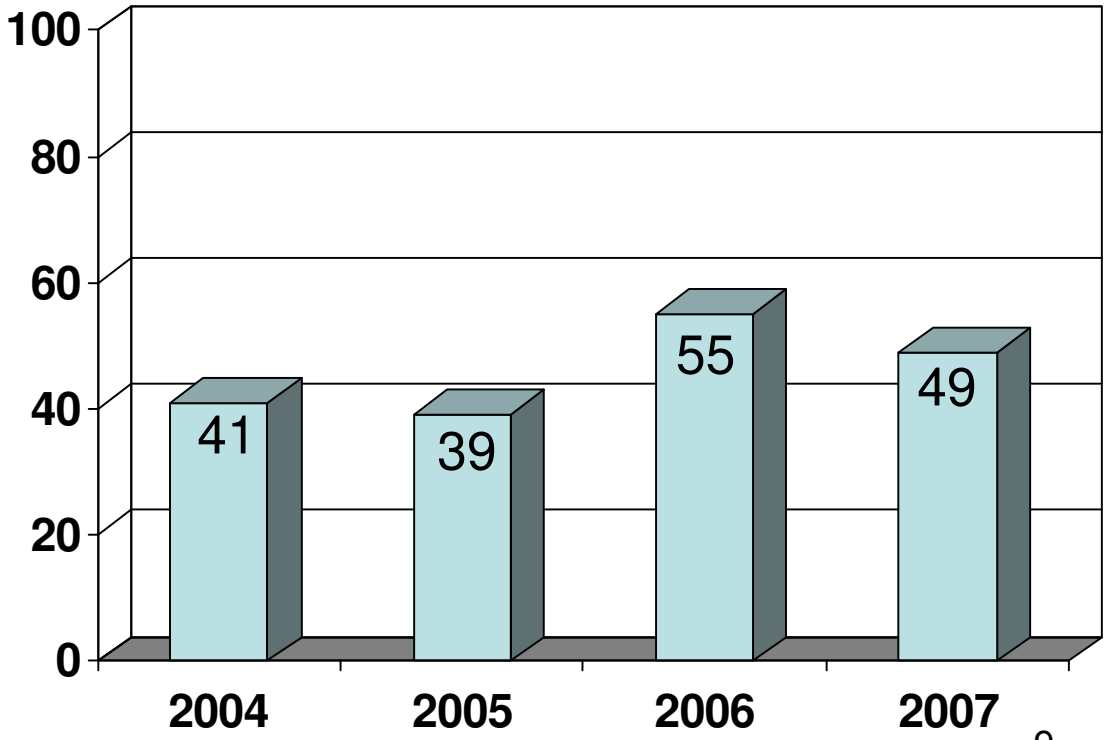
Carnegie Mellon
Software Engineering Institute

How bad is the insider threat?

2007 e-Crime Watch Survey

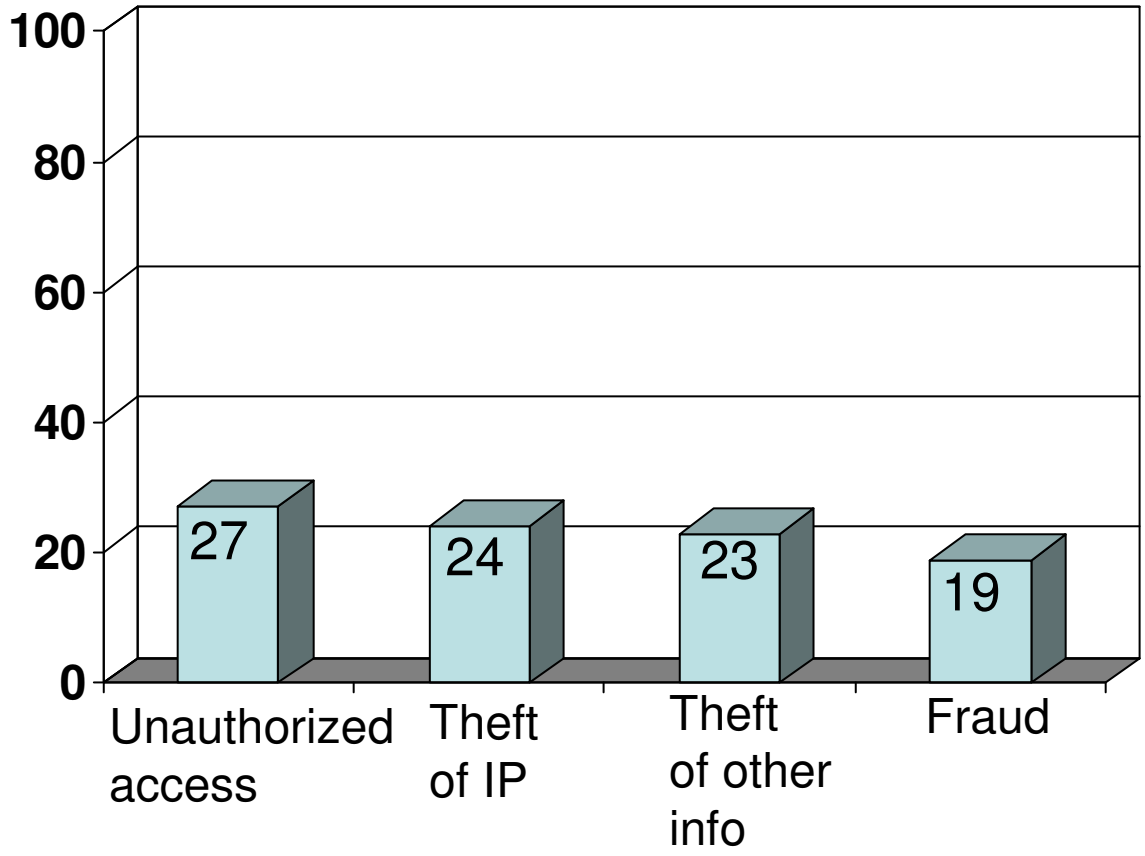
- CSO Magazine, USSS, Microsoft & CERT
- 671 respondents

Percentage of Participants Who Experienced an Insider Incident



Most Common Insider Incidents

Percentage of Participants Who Experienced Specific Type of Insider Incident



Source of CERT's Insider Threat Case Data

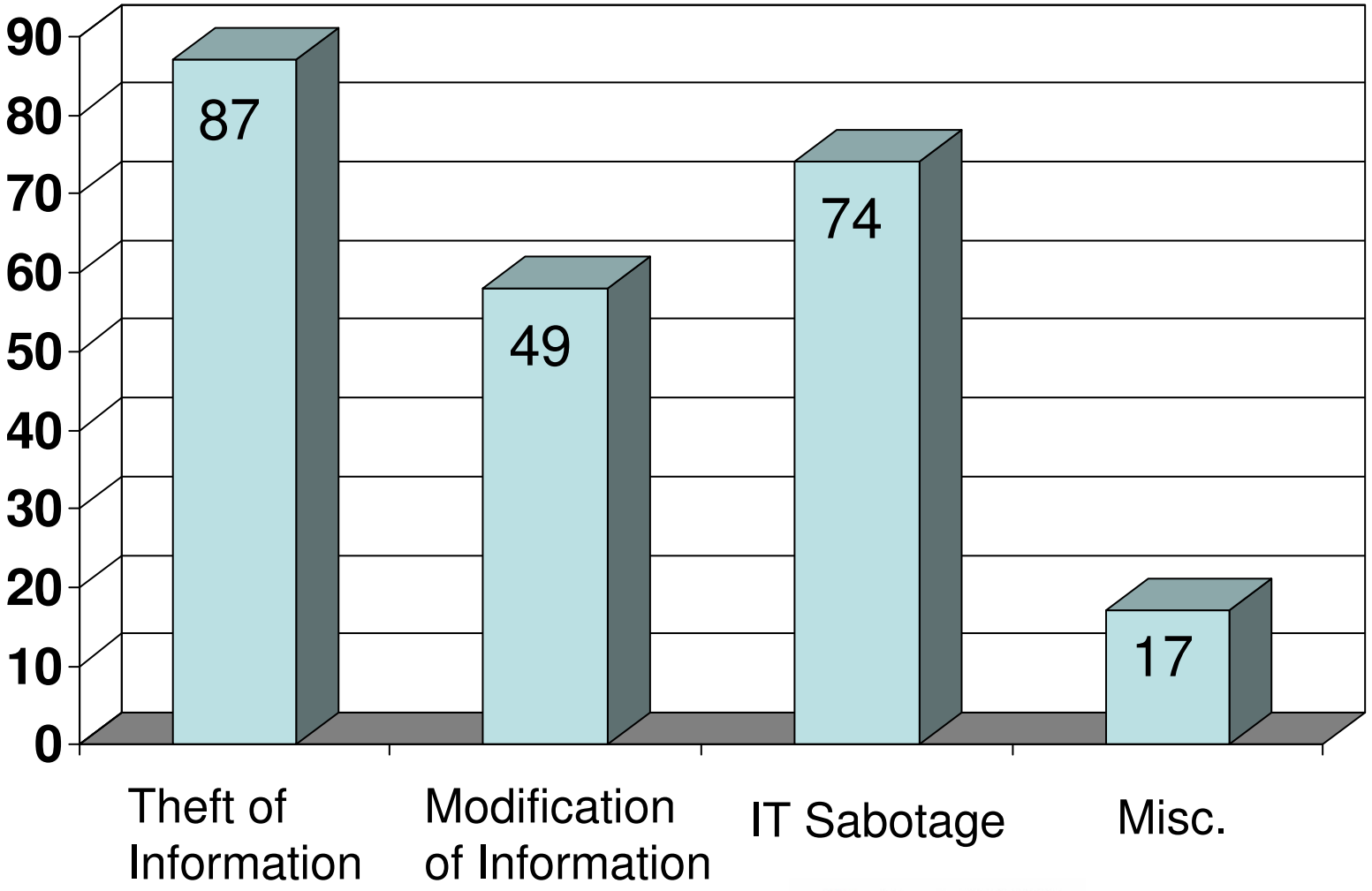
- CERT/U.S. Secret Service *Insider Threat Study*
  - 150 actual insider threat cases
  - 1996-2002
- Carnegie Mellon CyLab *MERIT** Project
  - Approximately 100 insider threat cases
  - Cases not included in the CERT/US Secret Service study
  - Cases through 2007
- Case data includes both technical and behavioral information

MERIT: Management and Education of the Risk of Insider Threat

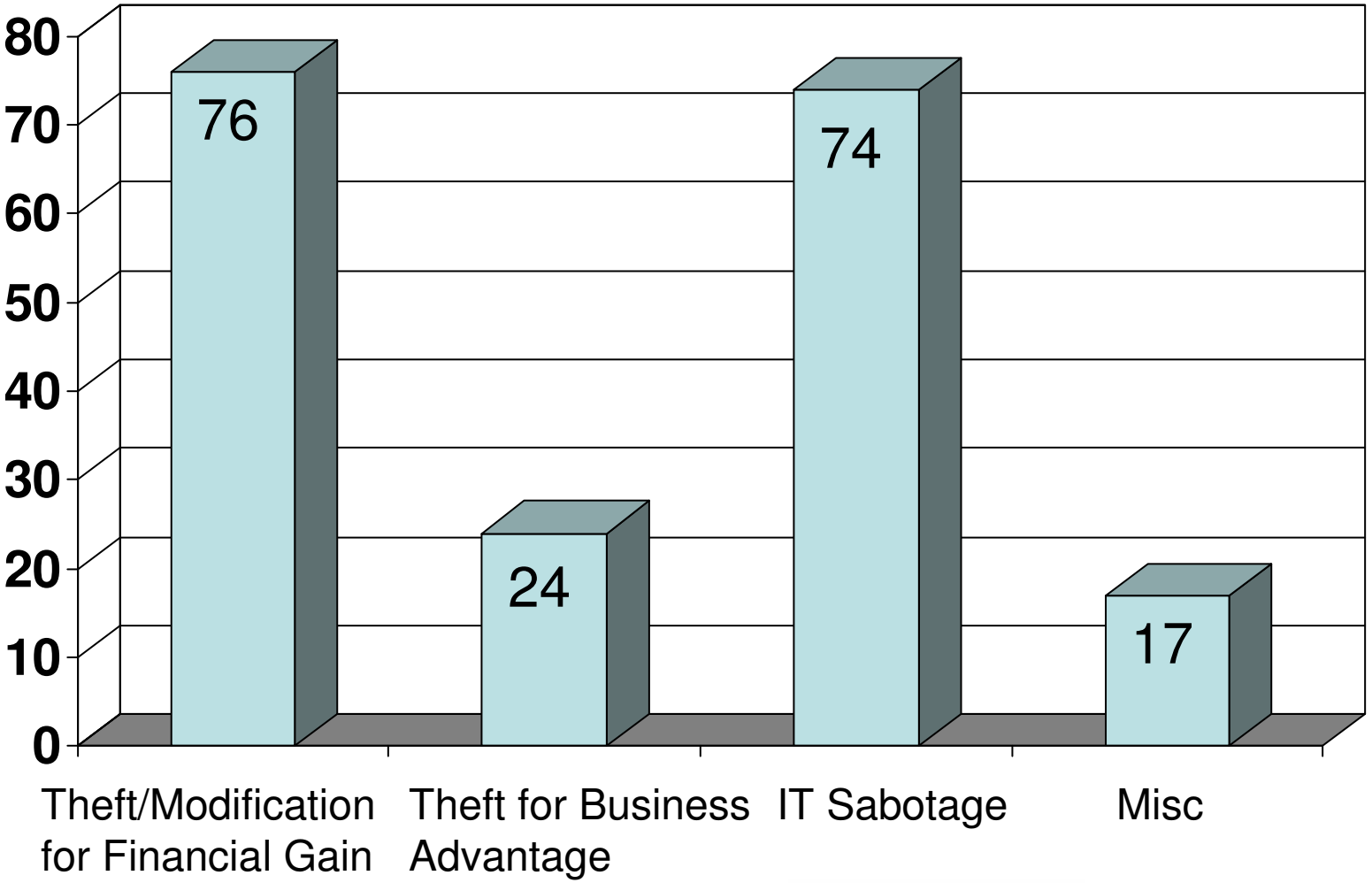
CyLab Common Sense Guide Best Practices

- Institute periodic enterprise-wide risk assessments.
- Institute periodic security awareness training for all employees.
- Enforce separation of duties and least privilege.
- Implement strict password and account management policies and practices.
- Log, monitor, and audit employee online actions.
- Use extra caution with system administrators and privileged users.
- Actively defend against malicious code.
- Use layered defense against remote attacks.
- Monitor and respond to suspicious or disruptive behavior.
- Deactivate computer access following termination.
- Collect and save data for use in investigations.
- Implement secure backup and recovery processes.
- Clearly document insider threat controls.

CERT's Insider Threat Case Breakdown



Slightly Different Breakdown



Insider Scenarios

Scenario 1: Insider uses IT to steal or modify information for financial gain

Scenario 2: Insider uses IT to steal information for business advantage

Scenario 3: Insider uses IT in a way that is intended to cause harm to the organization or an individual

Misc: Cases that do not fall in to the above categories

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	almost 1/3	2/3	1/2	> 1/3
Modification	almost 1/2	1/2	almost 1/3	1/3

Known Issues

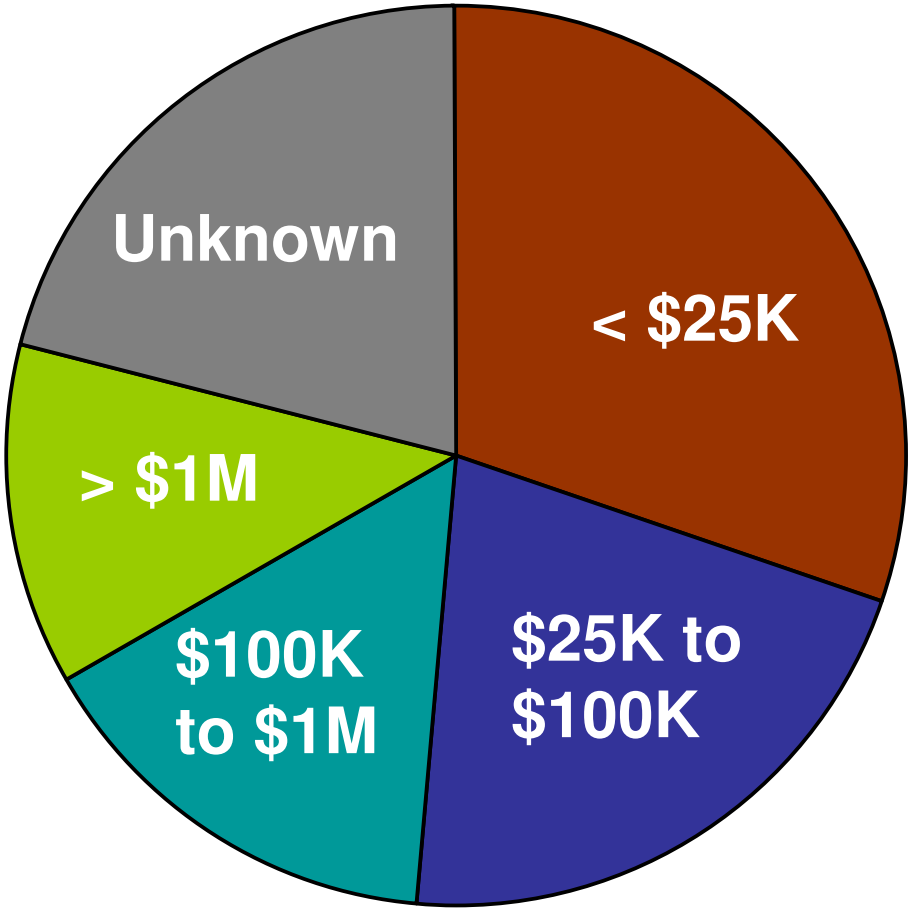
- Family medical problems
- Substance abuse
- Physical threat of outsiders
- Financial difficulties
- Financial compensation issues
- Hostile work environment
- Problems with supervisor
- Layoffs

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

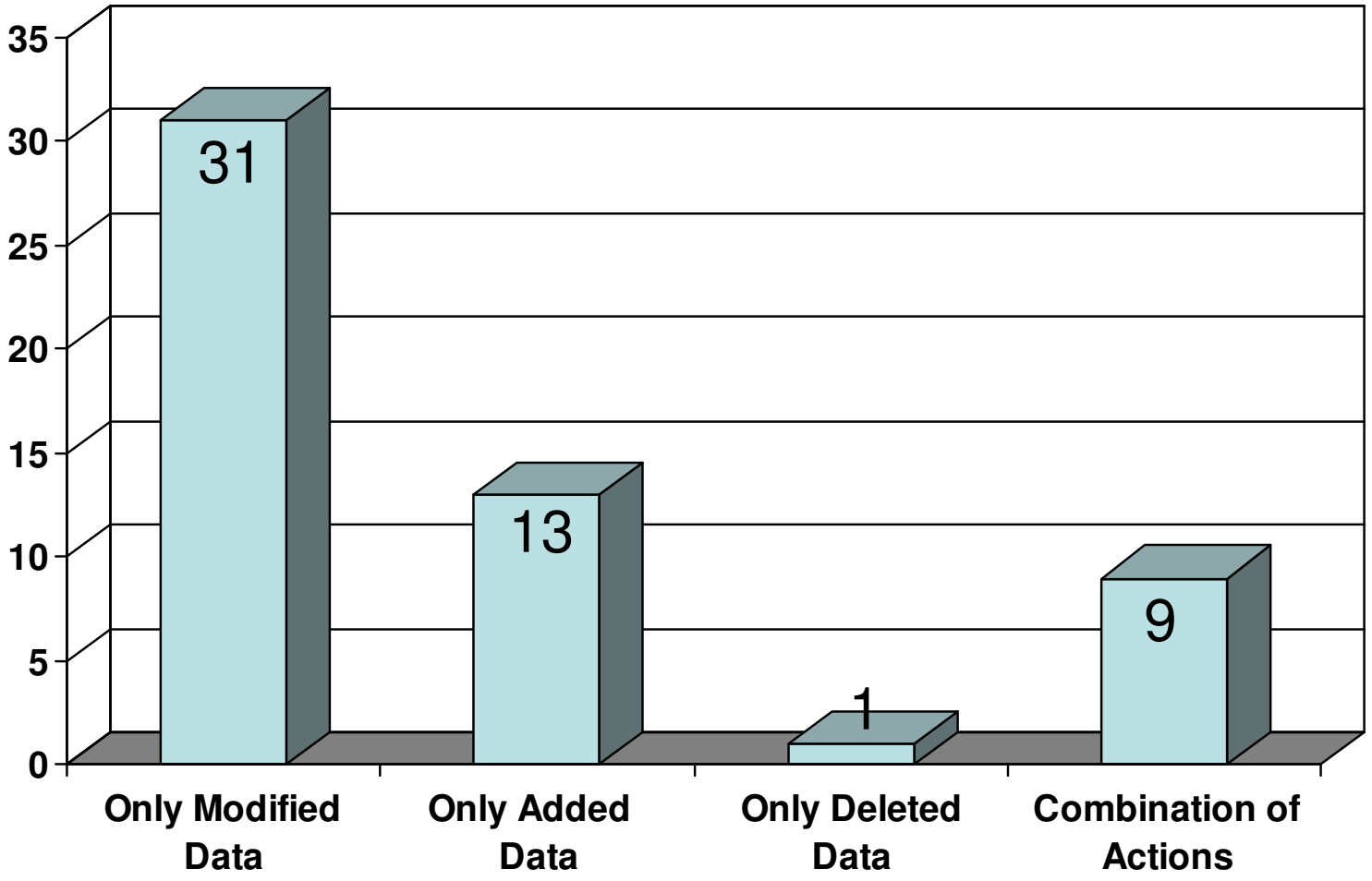


Additional Countermeasures - Theft for Financial Gain

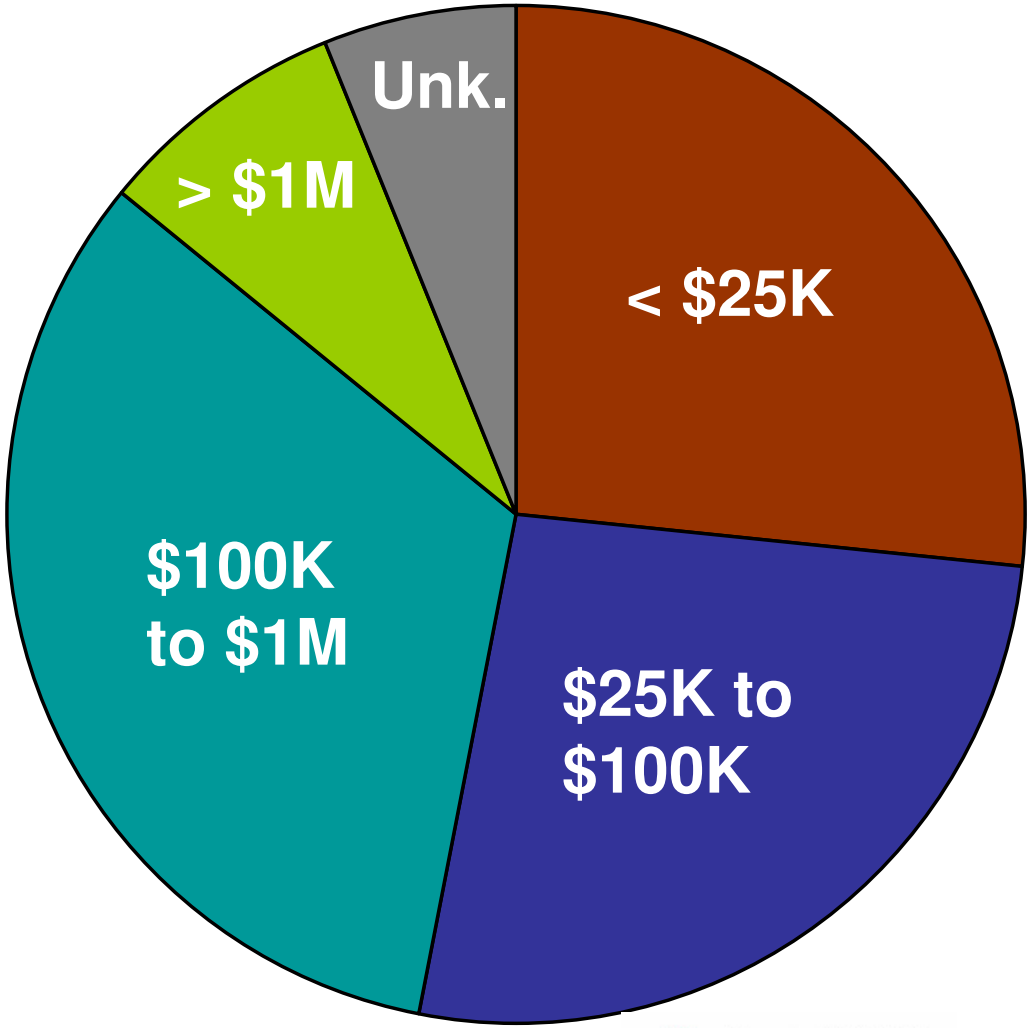
- Train managers on social networking issues
- Provide Employee Assistance Program or other recourse for employees experiencing personal problems
- Log, monitor, and audit for unusually large queries, downloads, print jobs, emails
- Do not overlook physical access controls
- Change passwords for all accounts upon termination, including EXTERNAL accounts!

A Closer Look at MODIFICATION for Financial Gain

Technical Aspects - Modification for Financial Gain



Organizational Impacts - Modification for Financial Gain



Additional Countermeasures - Modification for Financial Gain

- Audit/monitor for suspicious transactions
- Train managers on social networking issues
- Provide Employee Assistance Program or other recourse for employees experiencing personal problems

Scenario 2

Theft of Information for Business Advantage

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

Known Issues

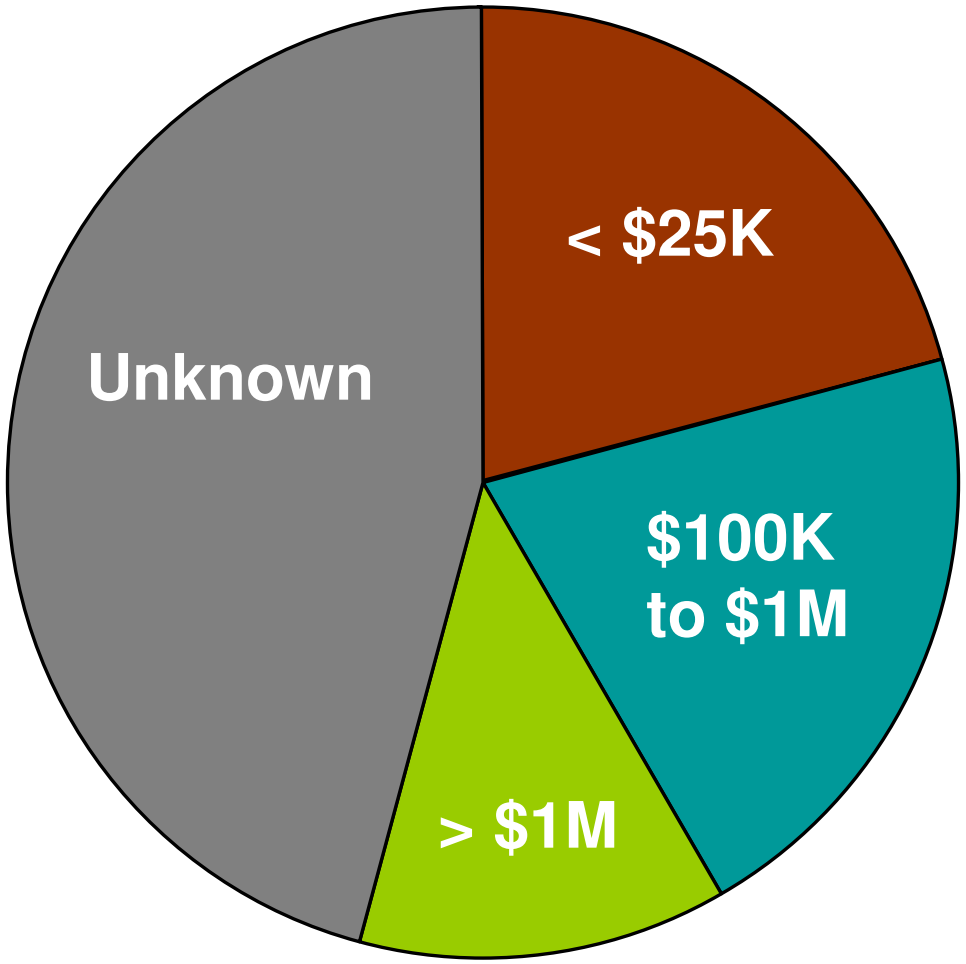
- Disagreement over ownership of intellectual property
- Financial compensation issues
- Relocation issues
- Hostile work environment
- Mergers & acquisitions
- Company attempting to obtain venture capital
- Problems with supervisor
- Passed over for promotion
- Layoffs

Technical Aspects - Theft for Business Advantage

- In order of prevalence:
  - Copied/downloaded information at work
  - Emailed information from work
  - Accessed former employer's system
  - Compromised account

- Many other methods

Organizational Impacts - Theft for Business Advantage



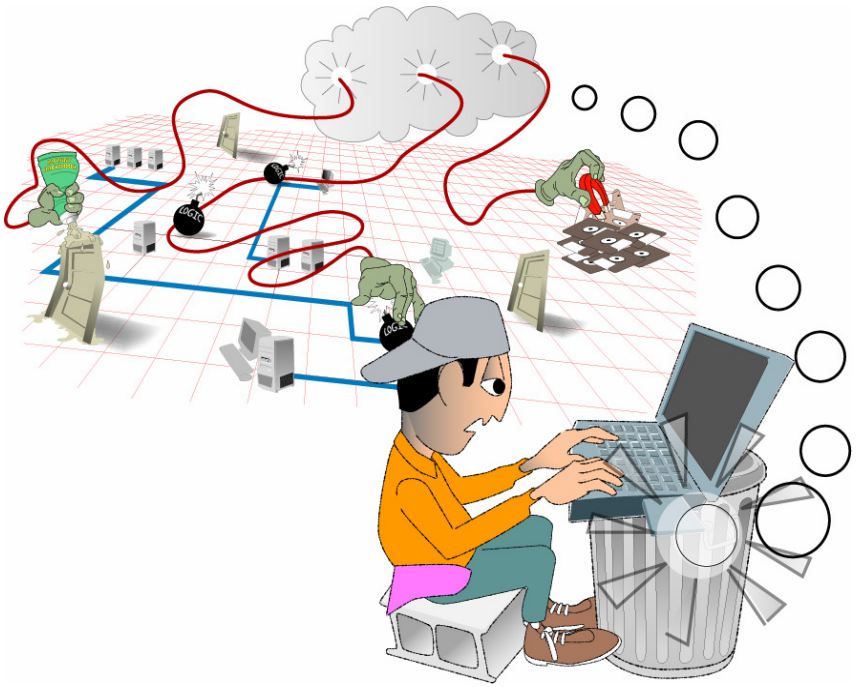
*** Note: None in range $25K to $100K.**

Additional Countermeasures - Theft for Business Advantage

- Log, monitor, and audit access to critical information
- Enforce “need to know” access controls, including encryption
- Protect software in development
- Prohibit use of personal computers for any work-related activity

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

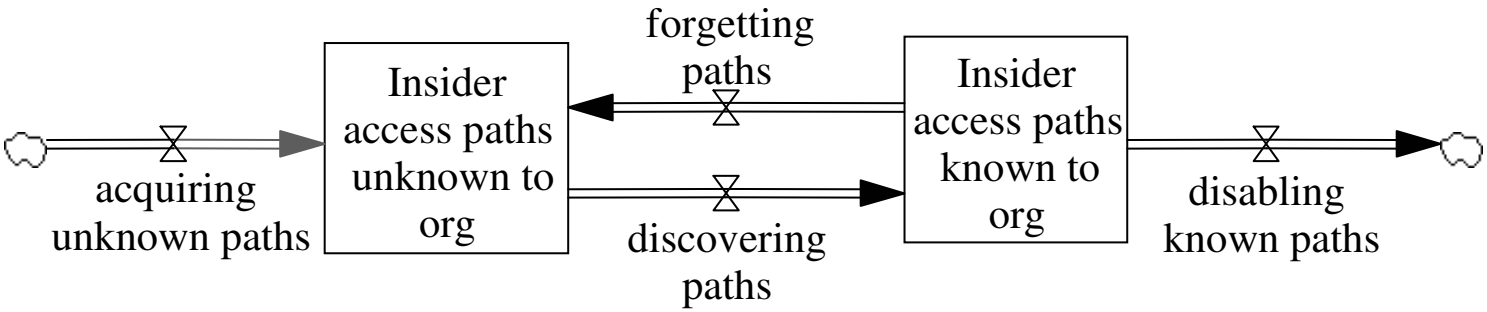
Technical Aspects of Insider IT Sabotage

- 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

More About Access Paths

- Access path
  - A sequence of one or more access points that lead to a critical system

An organization may not know about all of the access paths to its critical systems.



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

Additional Countermeasures - IT Sabotage

- Train management on the patterns of behavior that could indicate an IT sabotage attack

Miscellaneous:

Cases not in the above scenarios

Examples of Miscellaneous Cases

- Reading executive emails for entertainment
- Providing organizational information to lawyers in lawsuit against organization (ideological)
- Transmitting organization's IP to hacker groups
- Unauthorized access to information to locate a person as accessory to murder

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

Discussion

Points of Contact

Insider Threat Team Lead:
Dawn M. Cappelli
Senior Member of the Technical Staff
CERT Programs
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/