Understanding the Insider Threat: Lessons Learned from Actual Insider Attacks

Randy Trzeciak

14 June 2010

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

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.

Use of any trademarks in this presentation is not intended in any way to infringe on the rights of the trademark holder.

Internal use. Permission to reproduce and use this presentation in its entirety with no modifications for internal use is granted.

External use. Requests for permission to reproduce this document or prepare derivative works of this document for external and commercial use should be directed to permission@sei.cmu.edu.

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.

Agenda

Introduction

Crime Profiles

- Insider IT Sabotage
- Insider Fraud
- Insider Theft of Information

Best practices for prevention and detection

Discussion

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)

CERT Insider Threat Center—Mission

Assist organizations in identifying indications and warnings of insider threat by

- performing vulnerability assessments
- assisting in the design and implementation of policies, practices, and technical solutions

based on our ongoing research of hundreds of actual cases of insider IT sabotage, theft of intellectual property, fraud, and espionage

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.

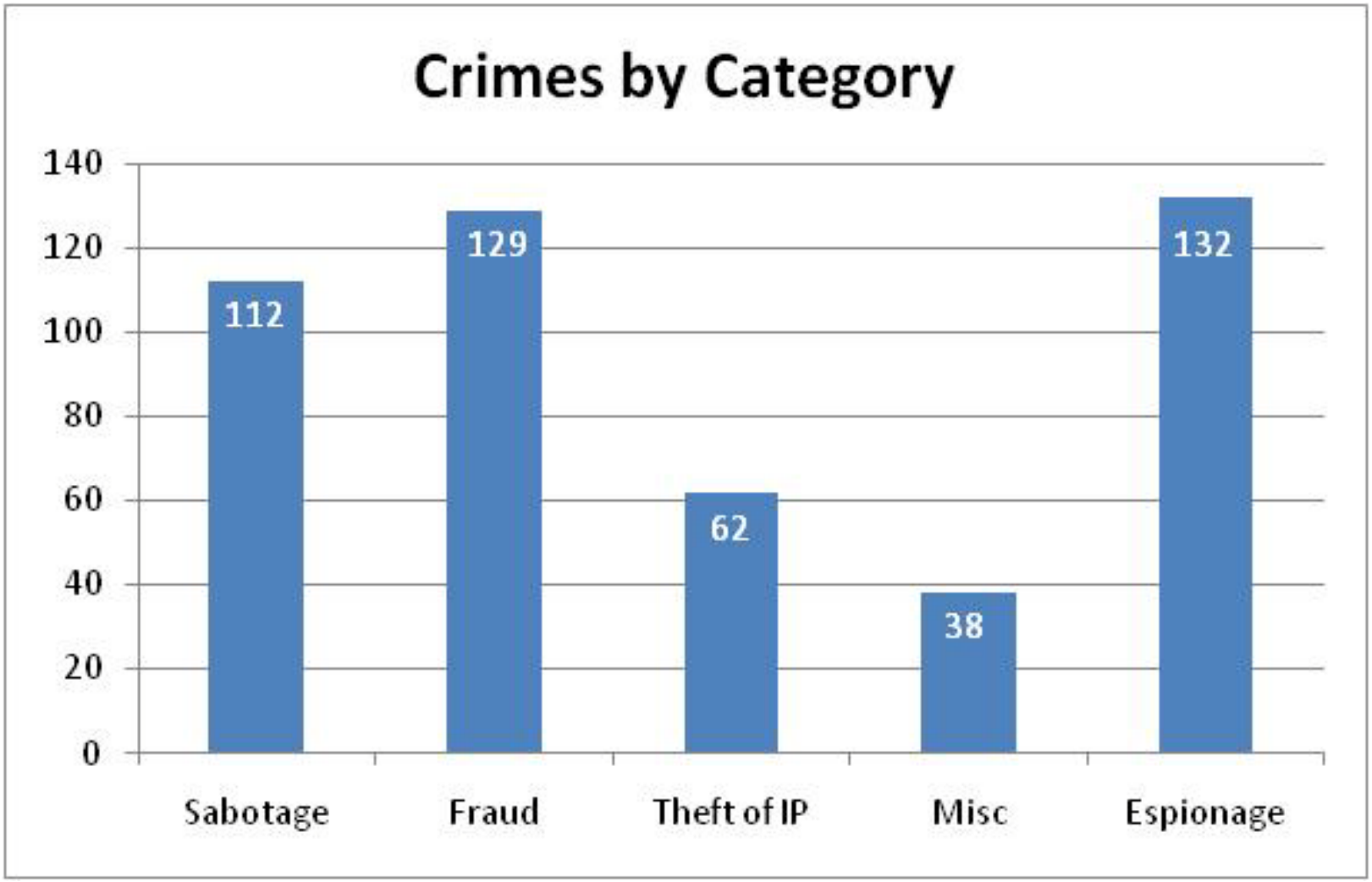
Insider theft of intellectual property (IP)

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

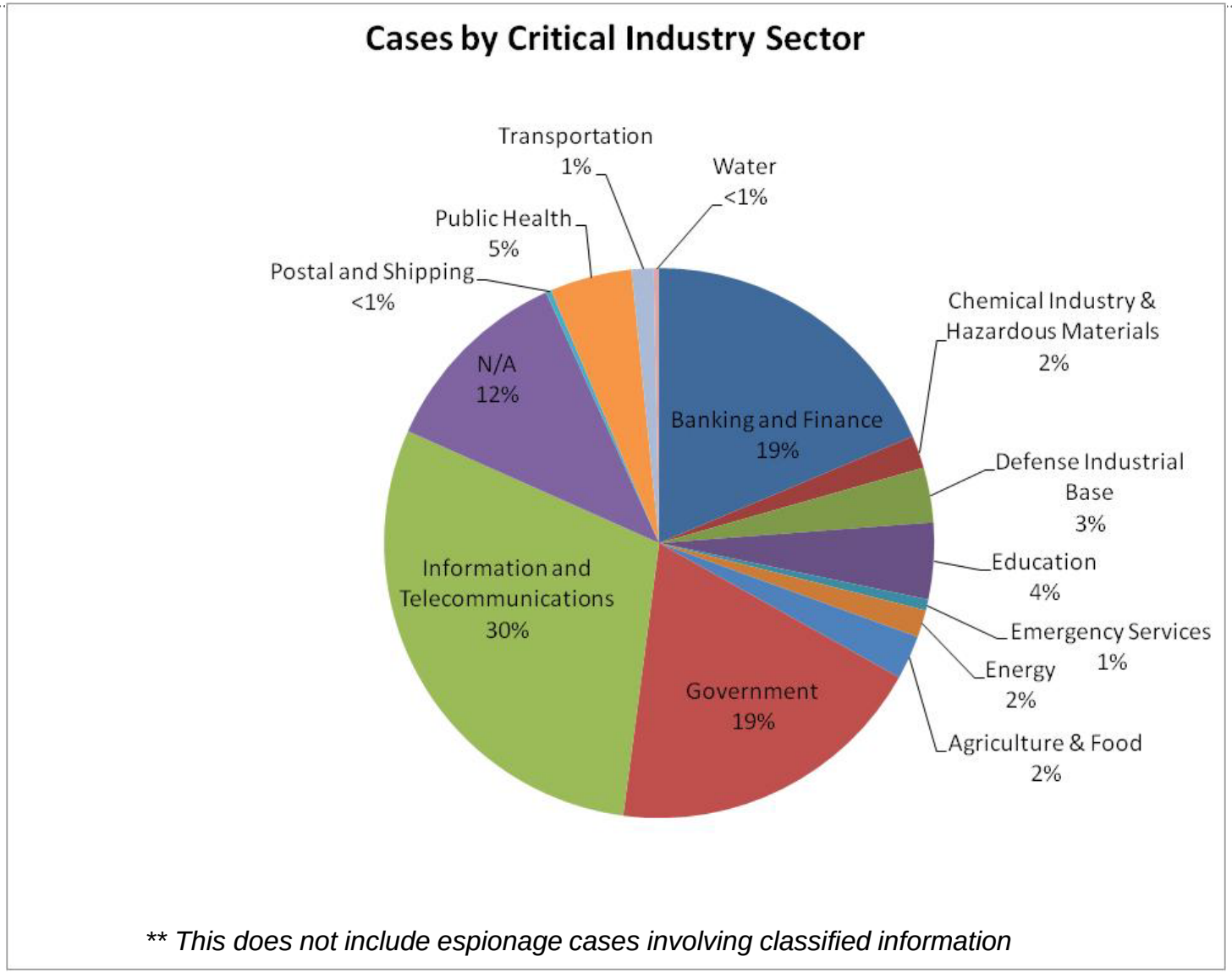
Insider fraud

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).

Insider Threat Case Breakdown

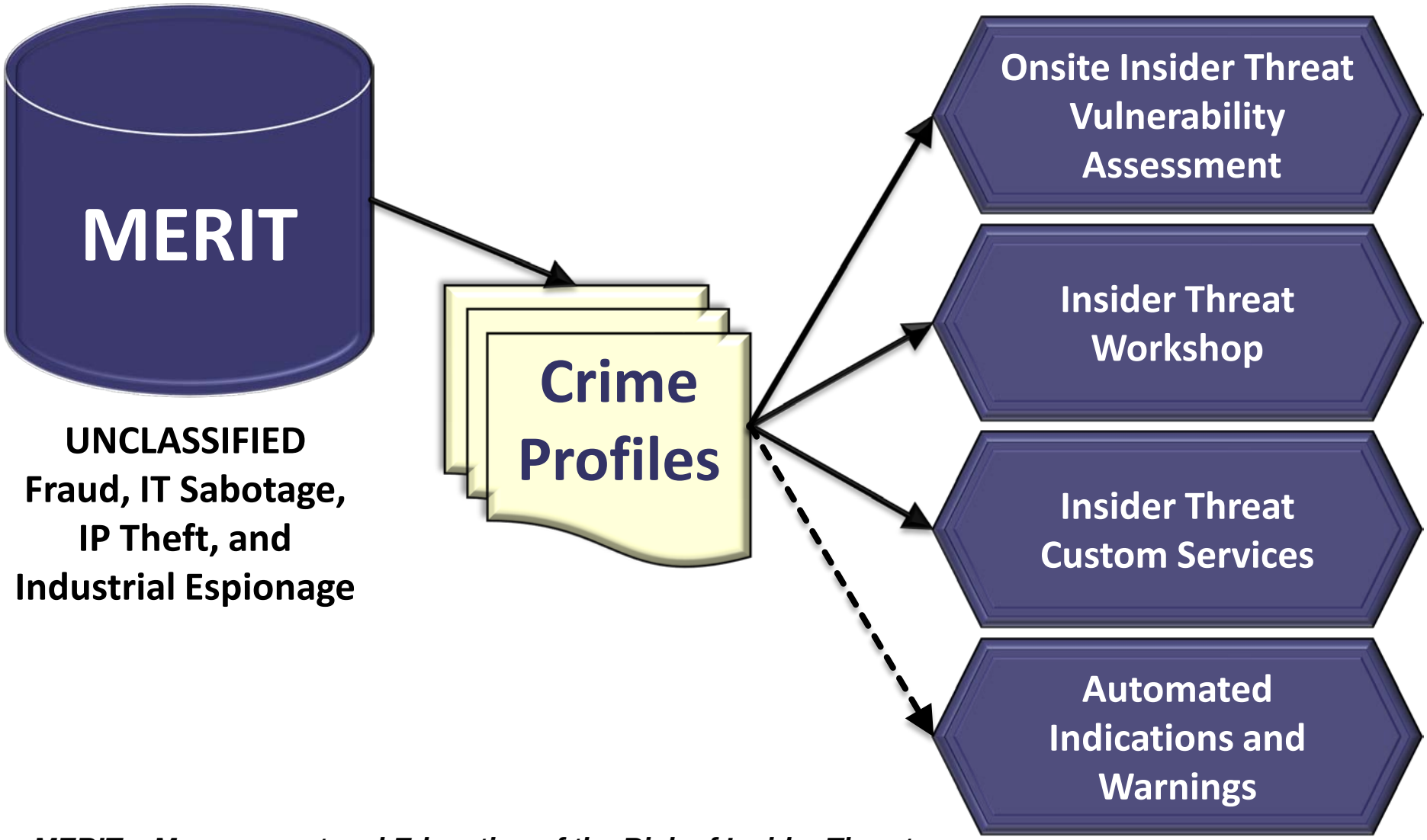


Critical Infrastructure Sectors



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

CERT's Insider Threat Portfolio



MERIT – Management and Education of the Risk of Insider Threat

How bad is the insider threat?

2009 e-Crime Watch Survey

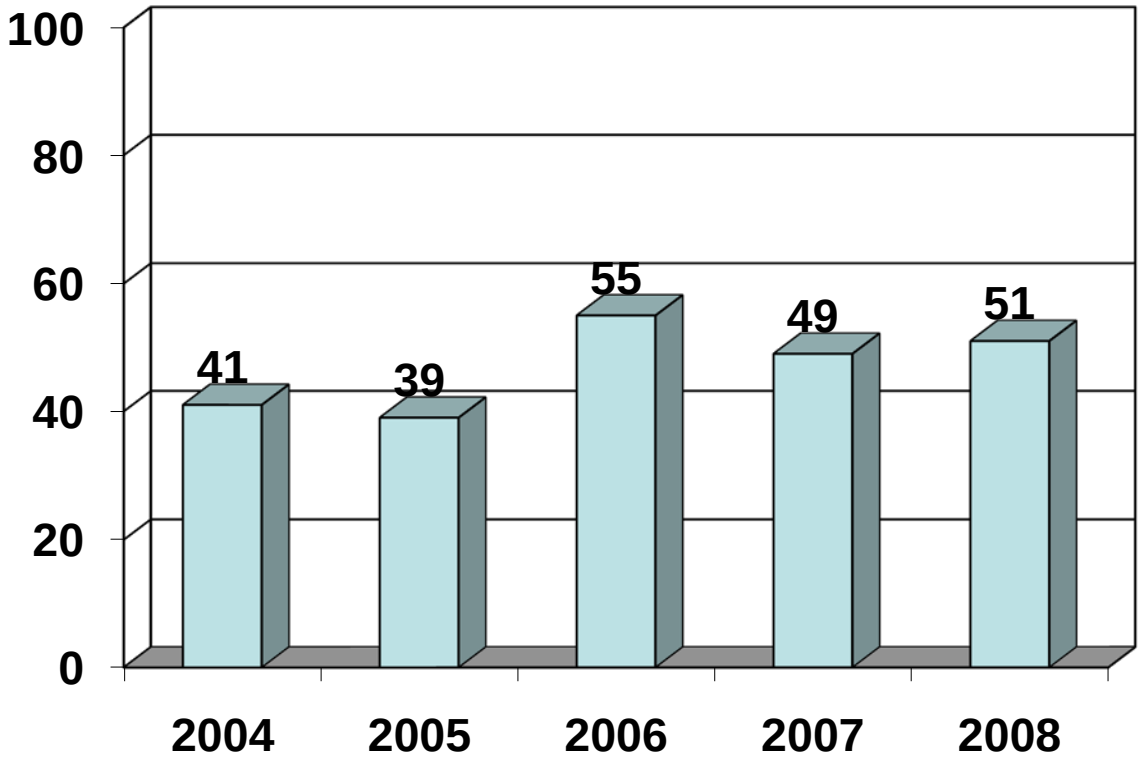
CSO Magazine, USSS, CERT & Deloitte

523 respondents

39% of organizations have less than 500 employees

23% of organizations have less than 100 employees

Percentage of Participants Who Experienced an Insider Incident



2009 e-Crime Watch Survey -2

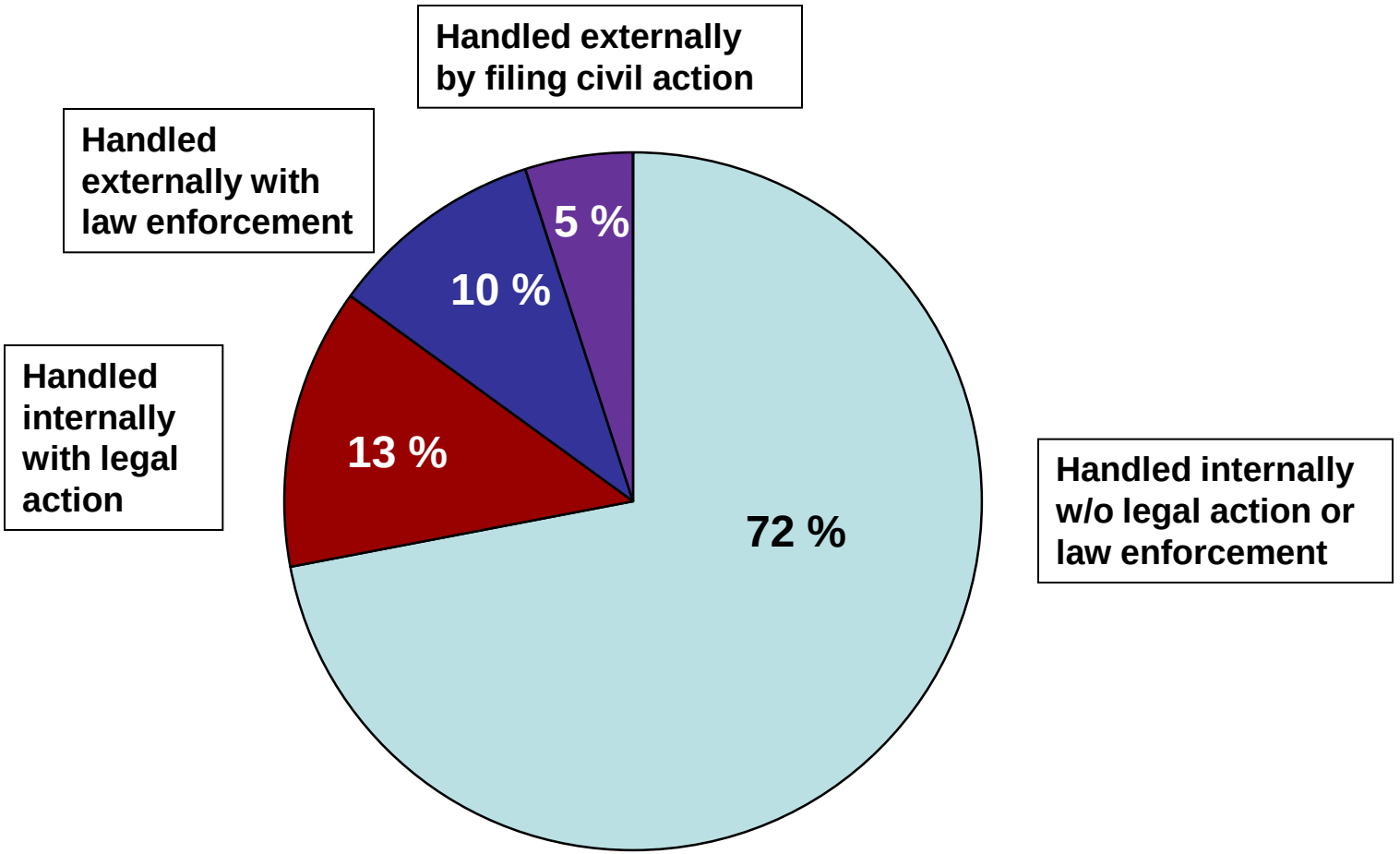
43 % of respondents	Insiders posed the greatest cyber security threat to their organization during the past 12 months
67 % of respondents	Damage caused by insider attacks more damaging than outsider attacks

Most common insider e-crime

Unauthorized access to / use of corporate information	(23%)
Theft of intellectual property	(16%)
Theft of other information (financial & customer data)	(15%)
Fraud	(11%)
Intentional exposure of private or sensitive data	(11%)

2009 E-Crime Survey Results - 3

Which percentage of Electronic Crimes committed by insiders were:



Insider Crime Profiles

Scenario 1:

IT Sabotage

TRUE STORY

A government agency's former database administrator wipes out all critical data in their mission critical database…

The agency's systems are down for 3 days while 115 employees spend 1800 hours to recover & re-enter the data.

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

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

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

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

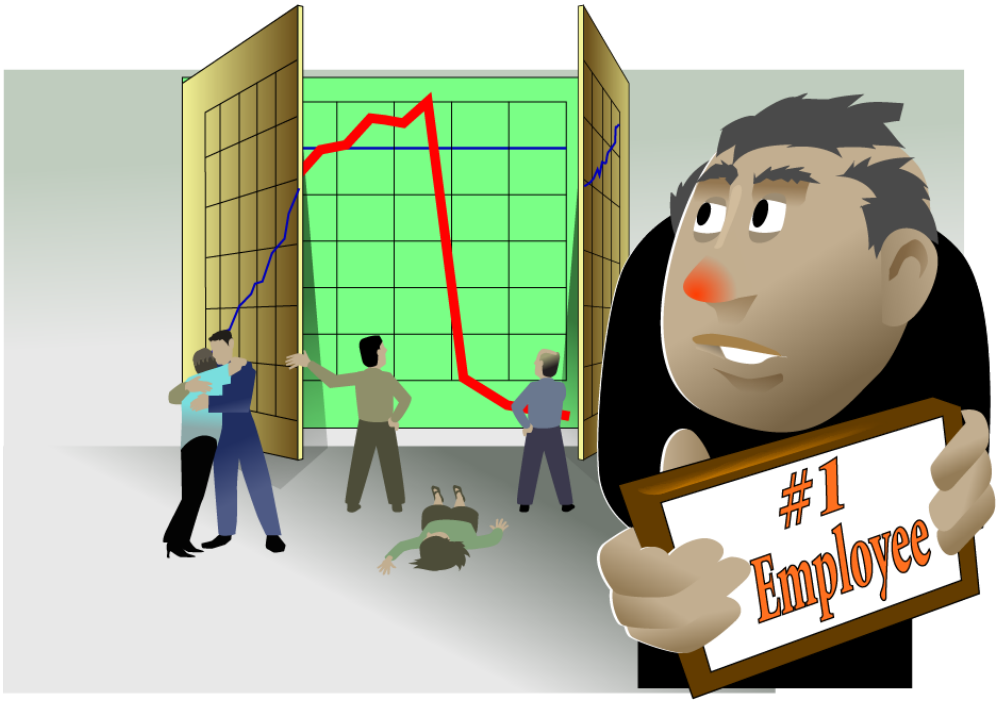
Scenario 2:

Fraud

TRUE STORY:

Financial institution discovers close to $700 million in losses ...

Covered up for 5 years by trusted employee



Fraud: Theft or Modification

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

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

Summary of Findings

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

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

Summary of Findings

	IT Sabotage	Fraud
Target	Network, systems, or data	PII or Customer Information
Access used	Unauthorized	Authorized
When	Outside normal working hours	During normal working hours
Where	Remote access	At work
Recruited by outsiders	None	½ recruited for theft; less than 1/3 recruited for mod
Collusion	None	Mod: almost ½ colluded with another insider Theft: 2/3 colluded with outsiders

Scenario 3:

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

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

Technical Aspects – Theft of Intellectual Property

In order of prevalence:

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

Many other methods

Summary of Findings

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

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

Summary of Findings

	IT Sabotage	Fraud	Theft of Intellectual Property
Target	Network, systems, or data	PII or Customer Information	IP (trade secrets) – 71% Customer Info – 33%
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	½ recruited for theft; less than 1/3 recruited for mod	Less than 1/4
Collusion	None	Mod: almost ½ colluded with another insider Theft: 2/3 colluded with outsiders	Almost ½ colluded with at least one insider; ½ acted alone

Best practices for insider threat risk mitigation

Best Practice #1

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

Phone companies, credit card companies and banks contract with an organization that hires another organization whose system administrator steals personal information for millions of their customers.

Organizations need to develop a risk-based security strategy to protect its critical assets from external threats, insiders, and trusted business partners.

Best Practice #2

Clearly document and consistently enforce policies and controls.

A former contractor remotely connects to the organization's servers, copies business plans and software, then sends email to the organization instructing them to stop using the software because he owns it.

A consistent, clear message on organizational policies and controls will help reduce the chance that employees will inadvertently commit a crime or lash out at the organization for a perceived injustice.

Best Practice #3 :

Institute periodic security awareness training.

A contract programmer enters the organization the night before his last day on the job, enters a co-worker's office, and steals critical source code…to take to his new job with a competitor.

Without broad understanding and buy-in from the organization, technical or managerial controls may be ineffective.

Best Practice #4:

Monitor and respond to suspicious or disruptive behavior.

A disgruntled system administrator amplifies the impact of a logic bomb by centralizing critical programs and intimidating a coworker out of backup tapes.

One method of reducing the threat of malicious insiders is to deal proactively with suspicious or disruptive employees.

Best Practice #5:

Anticipate and manage negative workplace issues.

A database administrator retaliates after a long period of serious conflict with her supervisor and coworkers by wiping out critical data, requiring 115 employees to spend 1800 hours to recover and re-enter the lost data.

Clearly defined and communicated organizational policies for dealing with employee issues will help ensure consistent enforcement and reduce risk when negative workplace issues arise.

Best Practice #6:

Track and secure the physical environment.

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.

Although organizations are becoming more reliant on electronic communication and online transactions to do business, it is still essential that they track and secure the physical environment against internal and external threats.

Best Practice #7:

Implement strict password & account management practices.

A system administrator is terminated for poor job performance, then spends weeks afterward setting up his attack remotely using accounts he created before he left.

If an organization's computer accounts can be compromised, insiders can circumvent manual and automated control mechanisms.

Best Practice #8:

Enforce separation of duties and least privilege.

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.

Separation of duties and least privilege must be implemented in business processes and for technical modifications to critical systems or information to limit the damage that malicious insiders can inflict.

Best Practice #9:

Consider insider threats in the software development life cycle.

A telecommunications company's services to its customers are suddenly disrupted; the investigation shows that a disgruntled programmer inserted malicious code into their inter-network communication protocol one year earlier, six months before leaving the company to take a new job.

Technical employees have taken advantage of defects introduced in the software development life cycle to deliberately perform malicious technical actions; likewise non-technical employees have recognized vulnerabilities and used them to carry out their fraudulent activities.

Best Practice #10:

Use extra caution with system administrators and technical or privileged users.

An organization refuses to pay a system administrator for his last two days of work when he suddenly quits without advanced notice; he then changes all administrator passwords and demands payment in exchange for the passwords.

System administrators and technical or privileged users have the technical ability, access, and oversight responsibility to commit and conceal malicious activity.

Best Practice #11:

Implement system change controls.

A programmer comments out a single line of code that notifies security whenever a seldom used screen is used to modify critical data, then uses that screen to commit criminal activity without detection for over a year and a half.

Changes to systems and applications must be controlled to prevent insertion of backdoors, keystroke loggers, logic bombs, and other malicious code or programs.

Best Practice #12:

Log, monitor, and audit employee online actions.

A research chemist takes a new job with a competitor but prior to leaving downloads over 38,000 files containing organization trade secrets.

Logging, monitoring, and auditing can lead to early discovery and investigation of suspicious insider actions.

Best Practice #13:

Use layered defense against remote attacks.

After resigning following a salary dispute, a CTO remotely accesses his former employer's systems and re-routes voice mail to a pornographic telephone service, floods email servers with thousands of messages with pornographic images, and sends threatening email to the CEO.

Remote access provides a tempting opportunity for insiders to attack with less risk.

Best Practice #14:

Deactivate computer access following termination.

A system administrator, fired for poor performance, uses a remote connection he had open at the time of termination to shut down and disable the company's manufacturing process on the night of his termination.

It is important that organizations follow rigorous termination procedures that disable all access paths into the organization's networks and systems for terminated employees.

Best Practice #15:

Implement secure backup and recovery processes.

Emergency services are forced to rely on manual address lookups for 911 calls when an insider sabotages the system and steals backup media from an off-site location.

It is important that organizations enhance organizational resiliency by implementing secure backup and recovery processes that are tested periodically, since despite all of the precautions, it is still possible that an insider will successfully attack.

Best Practice #16:

Develop an insider incident response plan.

A manager, suspended because he is suspected of fraudulent activity, uses social engineering to manipulate his employees to unwittingly destroy evidence of his crime.

Procedures for investigating and dealing with malicious insiders present unique challenges; response must be planned, clearly documented, and agreed to by organization managers and attorneys.

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.

Discussion

Point of Contact

Insider Threat Technical Manager
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/