



Solutions. Experts. Insights.

SEI TECHNOLOGIES FORUM



Software Engineering Institute

Carnegie Mellon



The Insider Threat: Lessons Learned from Actual Insider Attacks

Randall Trzeciak

Insider Threat Center at CERT

Trzeciak is currently a senior member of the technical staff at CERT. He is the technical team lead of the Insider Threat Research team; a team focusing on insider threat research; threat analysis and modeling; assessments; and training. Trzeciak has more than 20 years experience in software engineering; database design, development, and maintenance; project management; and information security.



Software Engineering Institute

Carnegie Mellon

SEI Technologies Forum

Twitter [#SEIVirtualForum](#)

© 2011 Carnegie Mellon University

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 24 OCT 2011		2. REPORT TYPE		3. DATES COVERED 00-00-2011 to 00-00-2011	
4. TITLE AND SUBTITLE The Insider Threat: Lessons Learned from Actual Insider Attacks				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Carnegie Mellon University ,Software Engineering Institute,Pittsburgh,PA,15213				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 33	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Agenda

Introduction to the CERT Insider Threat Center

CERT's Insider Threat Crime Profiles

Mitigation Strategies

Discussion



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.

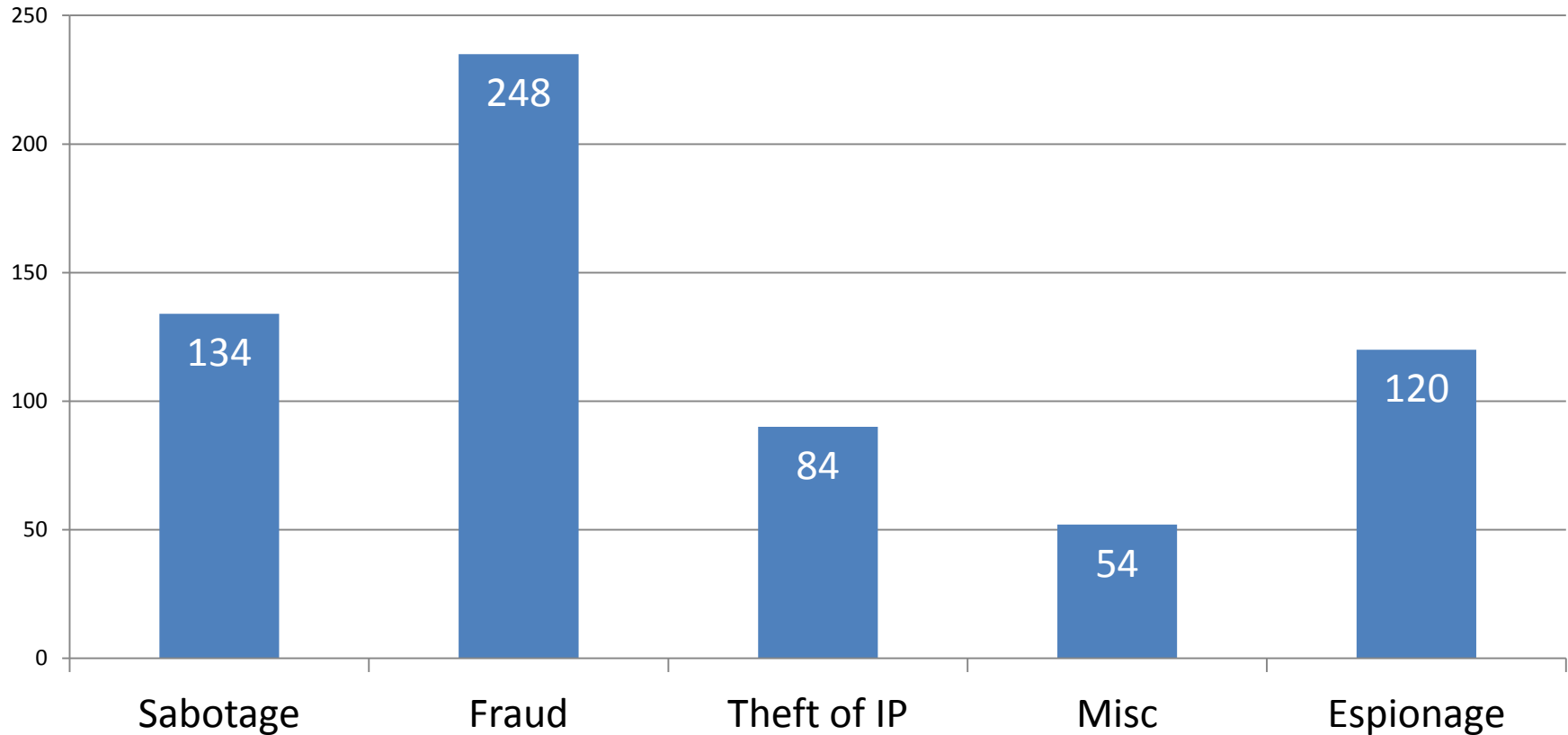
Insider fraud

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).



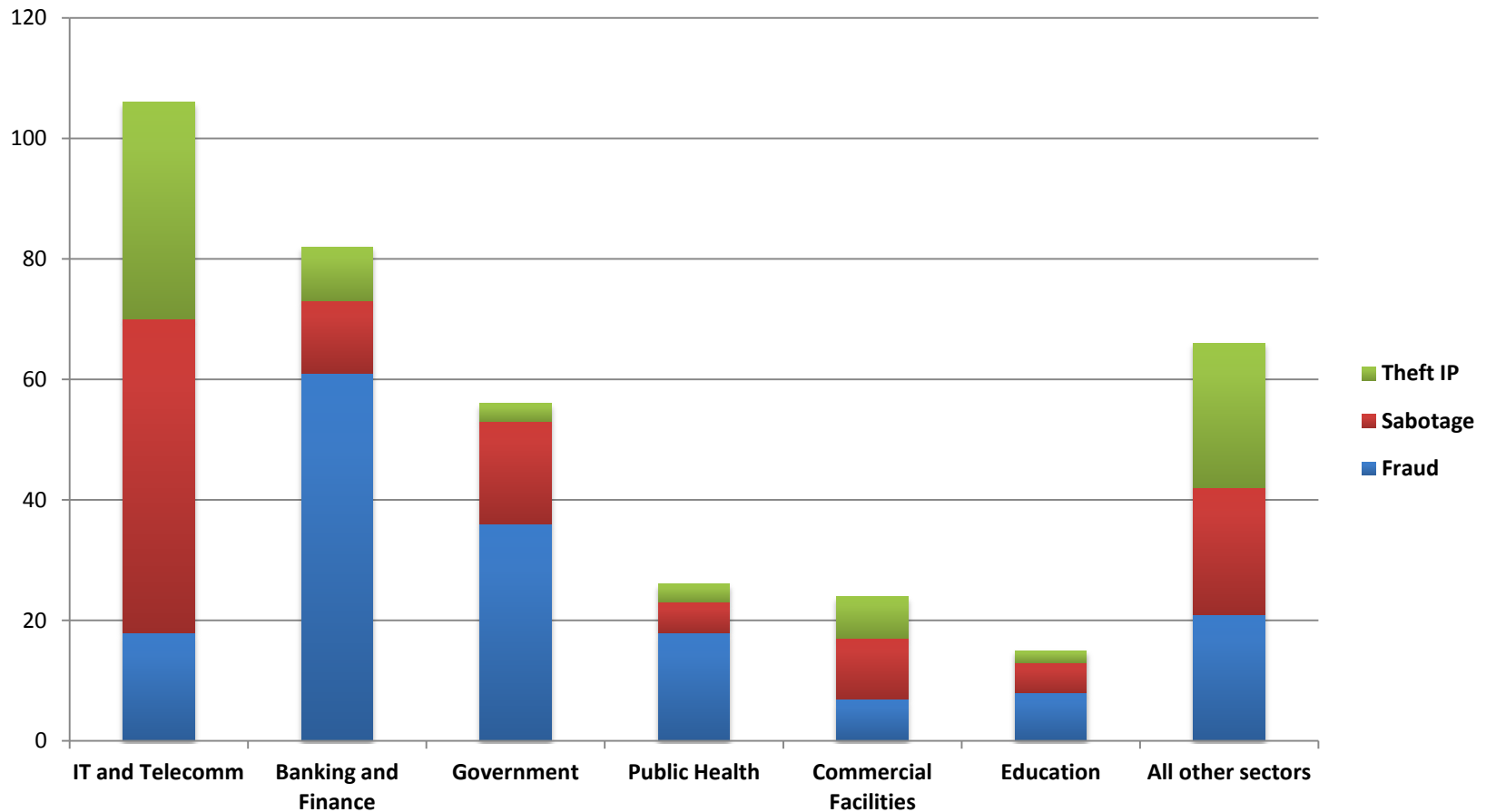
CERT's Insider Threat Case Database

U.S. Crimes by Category

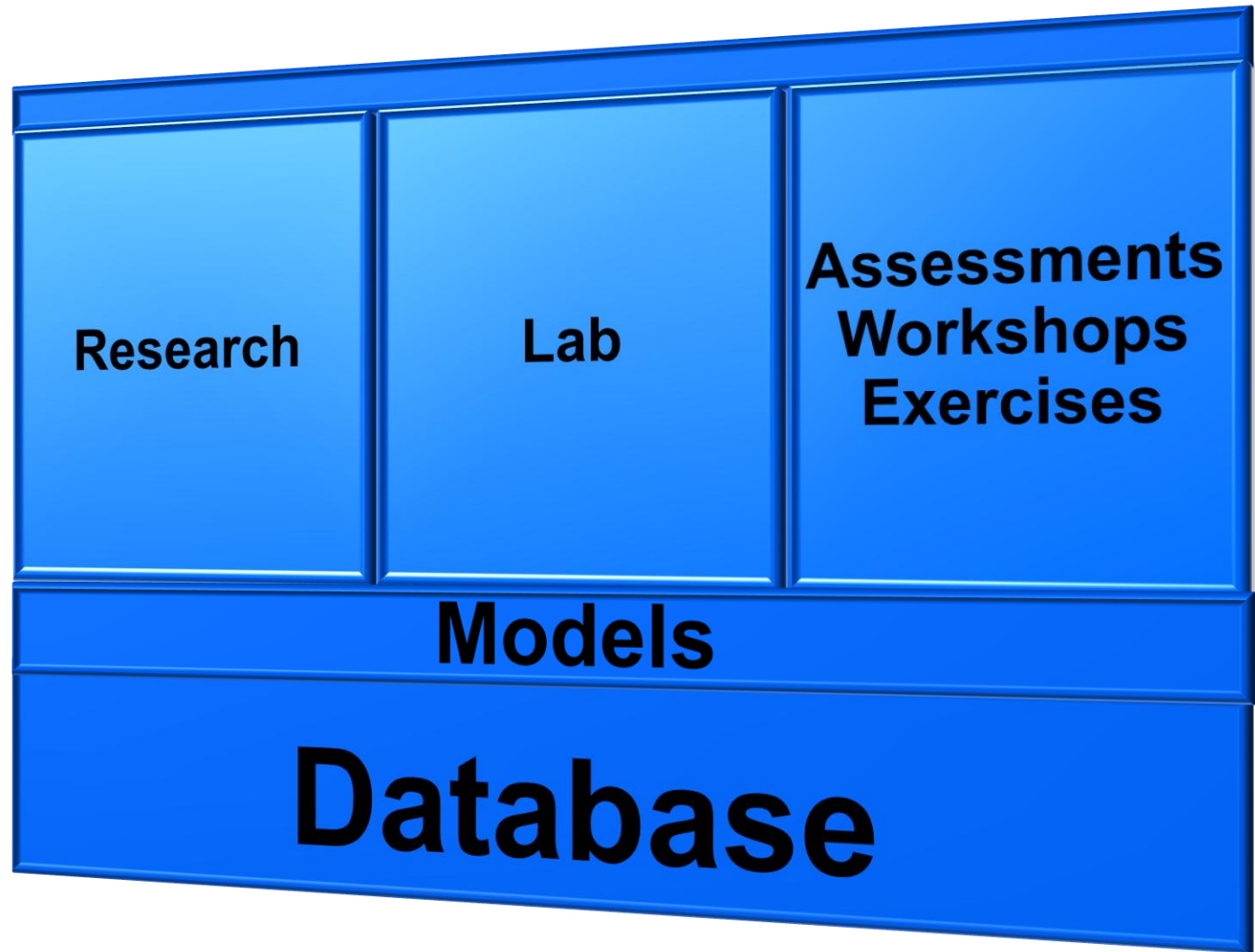


Critical Infrastructure Sectors

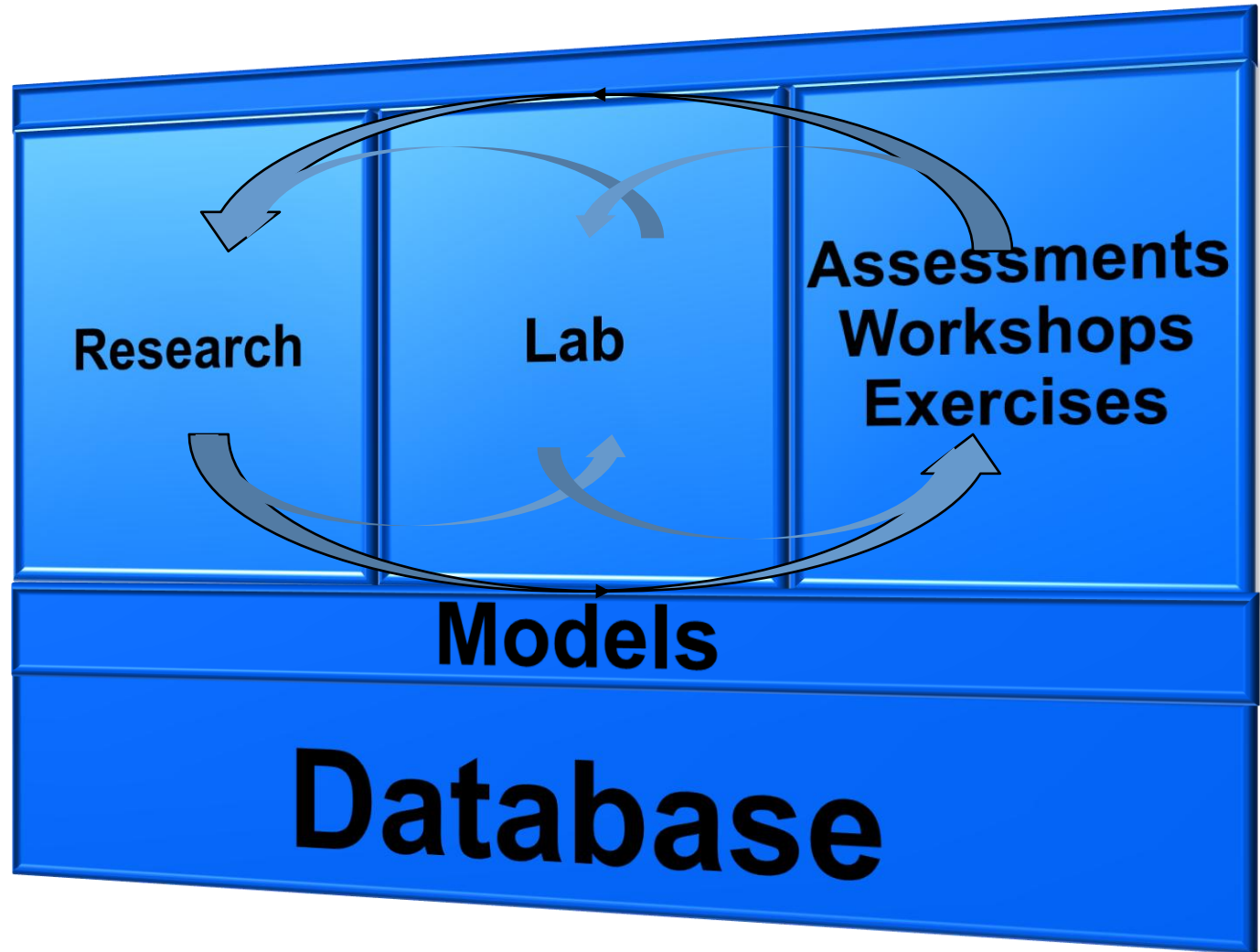
US Cases by Sectors (top 6) and Type of Crime



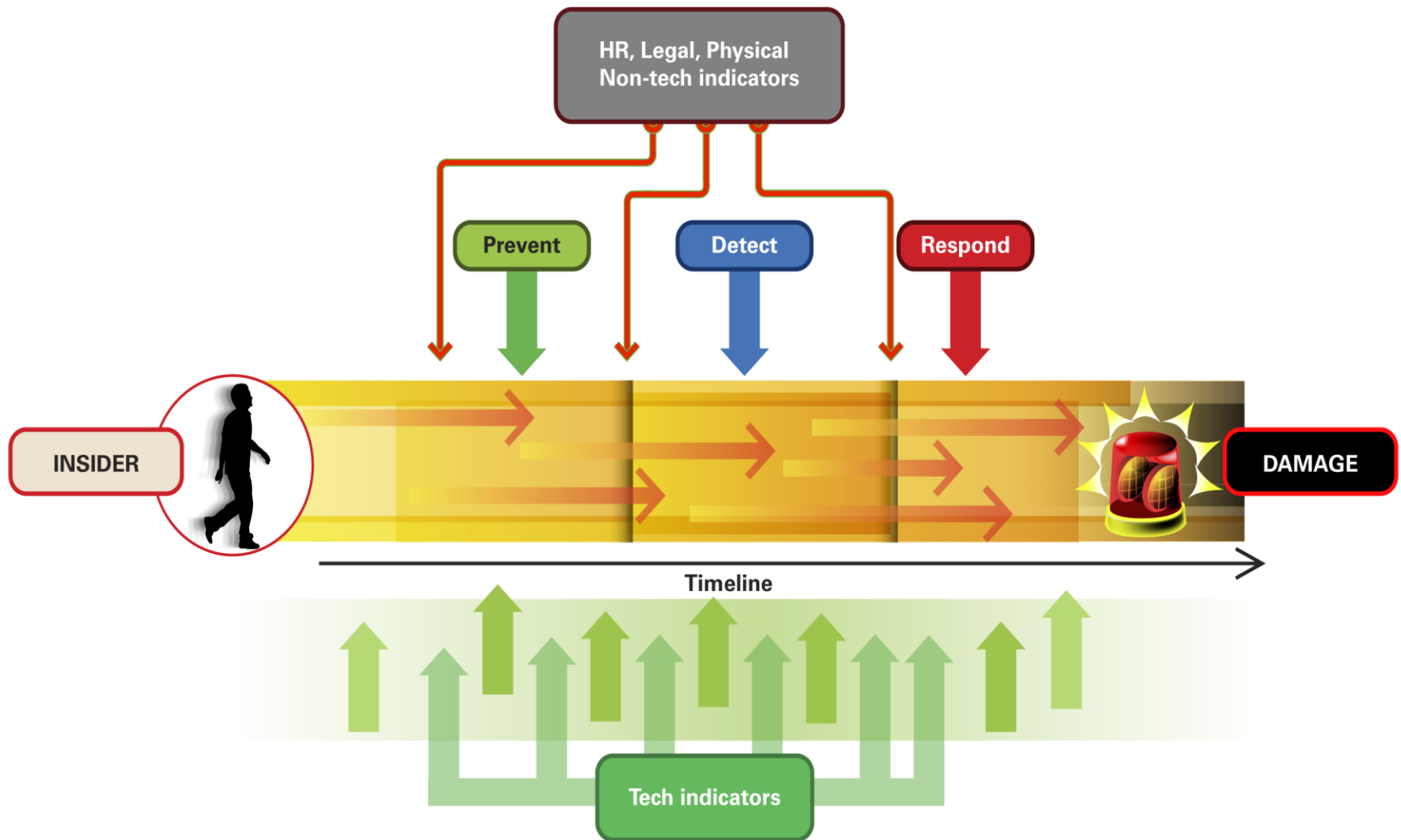
CERT's Unique Approach to the Problem



CERT's Unique Approach to the Problem



CERT Insider Threat Center Objective



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





Insider Crime Profiles



IT Sabotage



Software Engineering Institute

Carnegie Mellon

SEI Technologies Forum

Twitter #SEIVirtualForum

© 2011 Carnegie Mellon University

TRUE STORY:

SCADA systems for an oil-exploration company is temporarily disabled...

A contractor, who's request for permanent employment was rejected, planted malicious code following termination



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



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 7 person identity theft ring consisted of 7 employees who sold more than 200 fake licenses for more than \$1 Million.



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



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



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



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

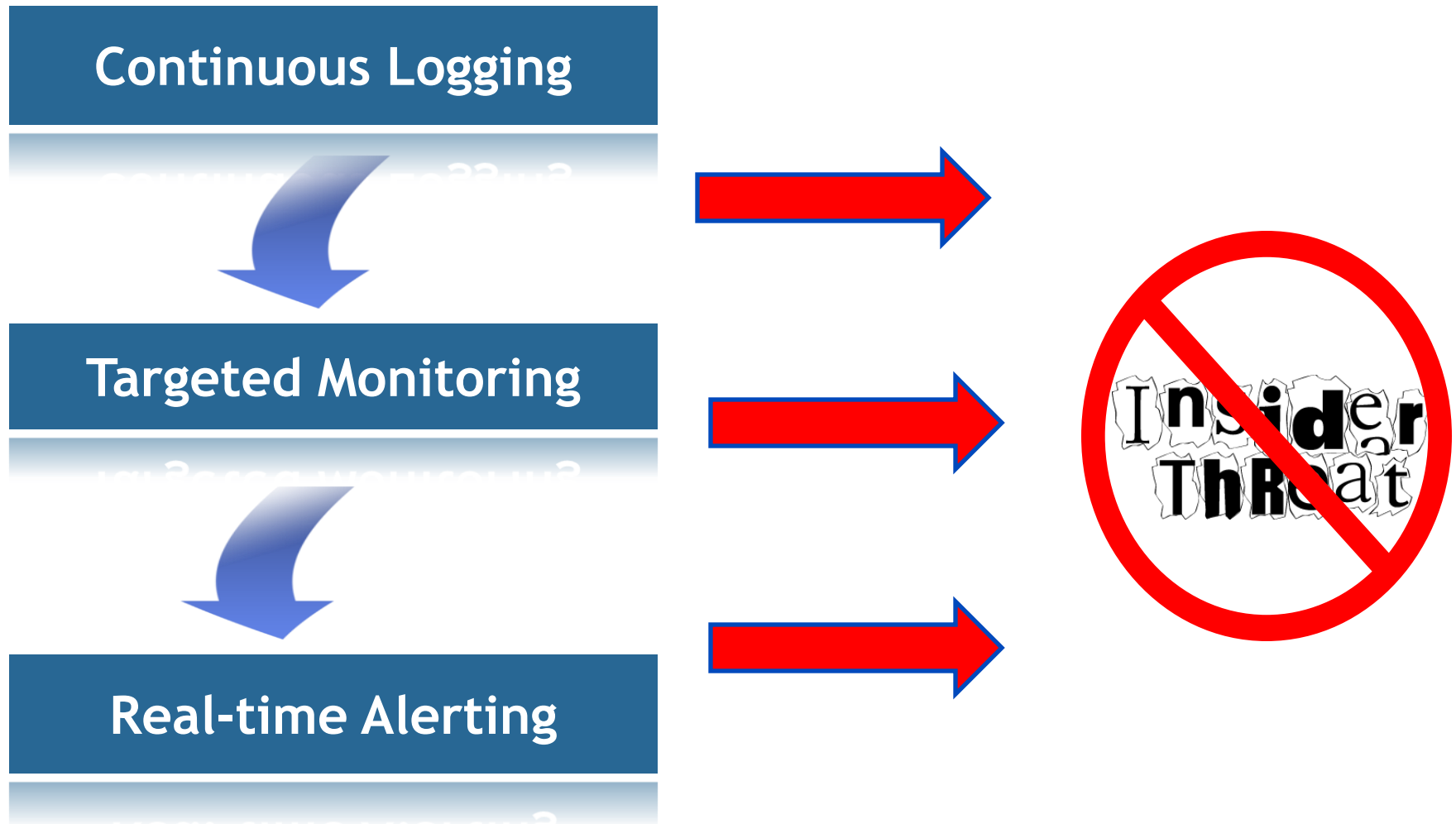




Mitigation Strategies



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.

Clearly document and consistently enforce policies and controls.

Institute periodic security awareness training for all employees.

Monitor and respond to suspicious or disruptive behavior, beginning with the hiring process.

Anticipate and manage negative workplace issues.

Track and secure the physical environment.

Implement strict password and account management policies and practices.

Enforce separation of duties and least privilege.

Consider insider threats in the software development life cycle.

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

Implement system change controls.

Log, monitor, and audit employee online actions.

Use layered defense against remote attacks.

Deactivate computer access following termination.

Implement secure backup and recovery processes.

Develop an insider incident response plan.



Point of Contact

Insider Threat Technical Team Lead

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/



Software Engineering Institute

Carnegie Mellon

SEI Technologies Forum

Twitter [#SEIVirtualForum](https://twitter.com/SEIVirtualForum)

© 2011 Carnegie Mellon University

Notices

© 2011 Carnegie Mellon University

Except for the U.S. government purposes described below, 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.

This material 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 U.S. government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.

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.

THE MATERIAL IS PROVIDED ON AN “AS IS” BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).

CERT ® is a registered mark owned by Carnegie Mellon University.





SEI Training

Merging software engineering research and real-world problems.

We offer a diverse range of learning products—including classroom training, eLearning, certification, and more—to serve the needs of customers and partners worldwide.

