

Combat IT Sabotage: Technical Solutions From The CERT Insider Threat Lab

Dawn Cappelli

Joji Montelibano

Software Engineering Institute -
CERT Insider Threat Center

Session ID: HT2-108

Session Classification: Intermediate



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 FEB 2011		2. REPORT TYPE		3. DATES COVERED 00-00-2011 to 00-00-2011	
4. TITLE AND SUBTITLE Combat IT Sabotage: Technical Solutions From The CERT Insider Threat Lab				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 RSA Conference 2011, held in San Francisco, CA from February 14-18, 2011.					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT Same as Report (SAR)	18. NUMBER OF PAGES 28	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Notices

© 2007-2011 Carnegie Mellon University

These slides are available to RSA Conference delegates only. Except for the U.S. government purposes described below, the 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).



Demonstration: Malicious Modification of Source Code



Agenda

Background

Crime Profile: Insider IT Sabotage

Countermeasures: Insider IT Sabotage

Wrap-Up / Discussion

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.*



CERT Insider Threat Center

- A decade of experience in the insider threat area
- Sponsors / partners include:
 - US Secret Service
 - Department of Homeland Security
 - Carnegie Mellon CyLab
 - DoD Personnel Security Research Center
 - DoD and Counterintelligence
 - Office of the National Counterintelligence Executive
 - Air Force Research Laboratory
 - Defense Industrial Base members
 - Other federal agencies

Mission of the CERT Insider Threat Center

Improve the preparedness level of the community to prevent, detect, and respond to insider crimes

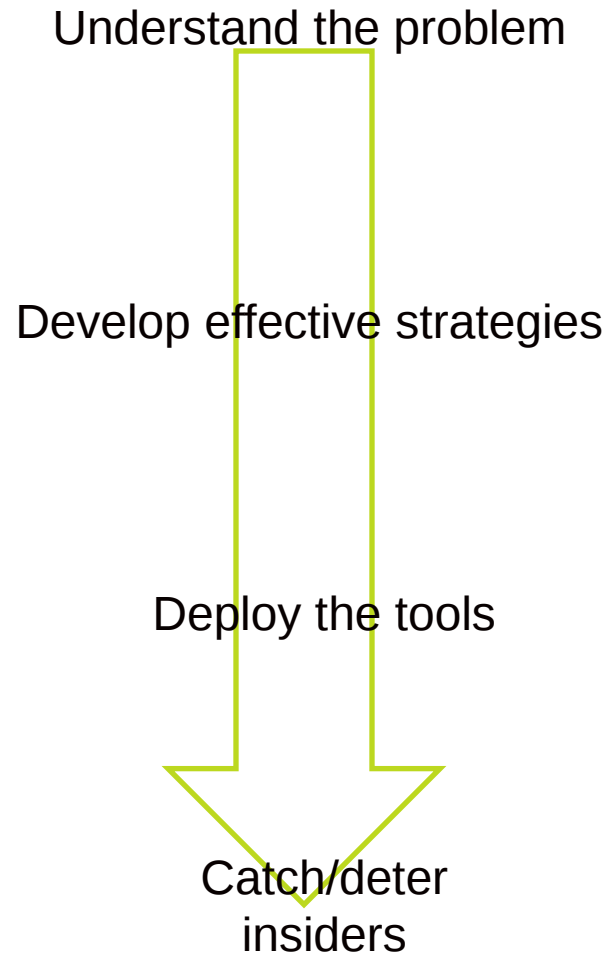
Desired impact:

- Organizations will have
 - A more accurate understanding of the lifecycle of insider threats
 - Improved defenses against the types of compromises seen in actual cases
 - Reduction in the number and impact of insider incidents
- National security should improve as a result

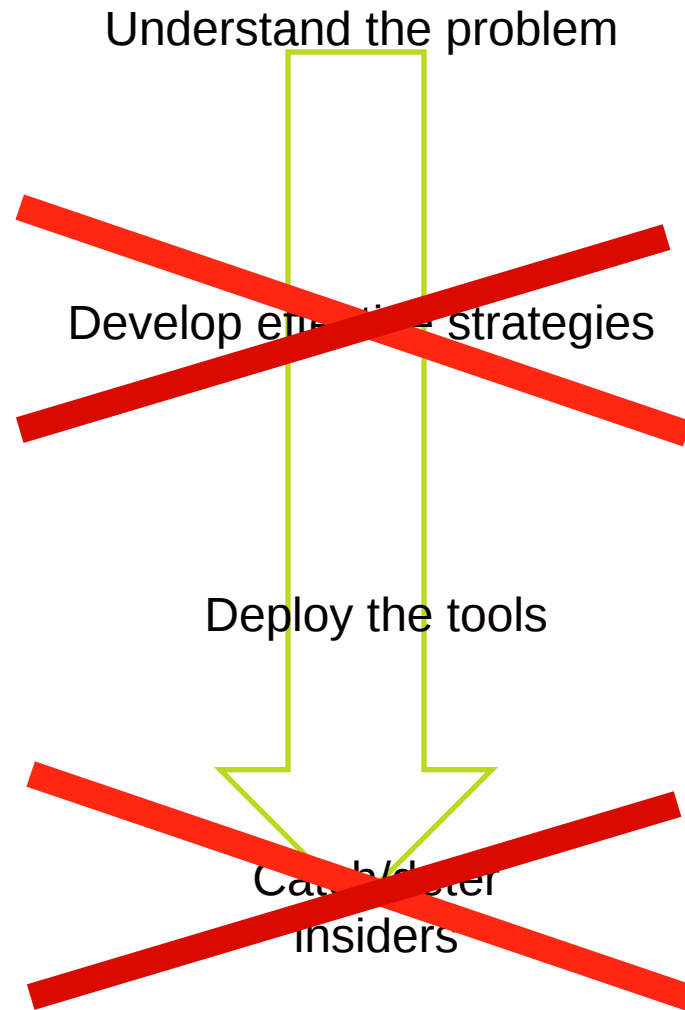
CERT Insider Threat Center Goals

- Identify policies, procedures, and technologies that can mitigate the risk of insider threat
- Develop and validate new and existing insider threat controls (including improved automated sensors)
- Transition controls and influence standards

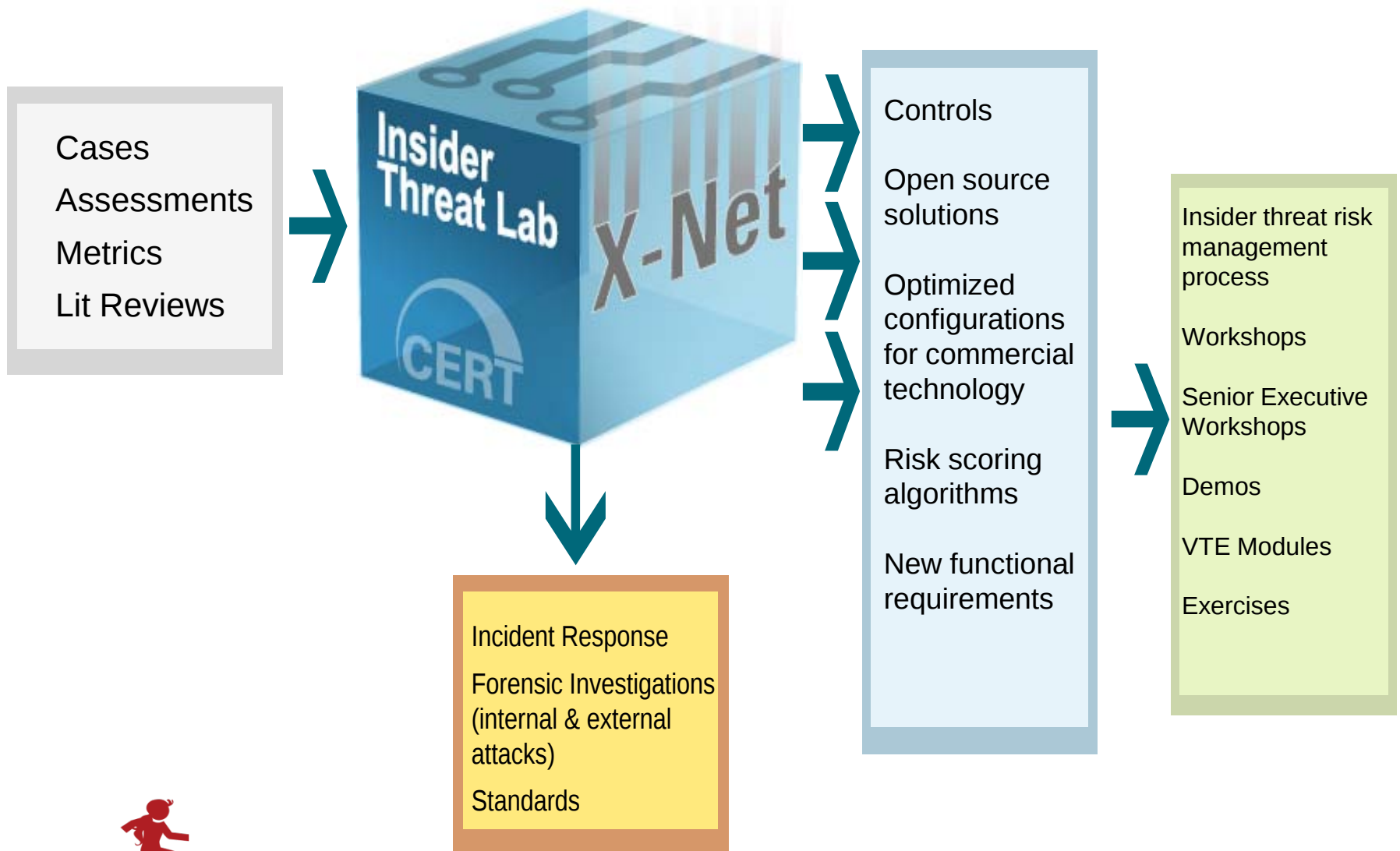
Desired State



Current State

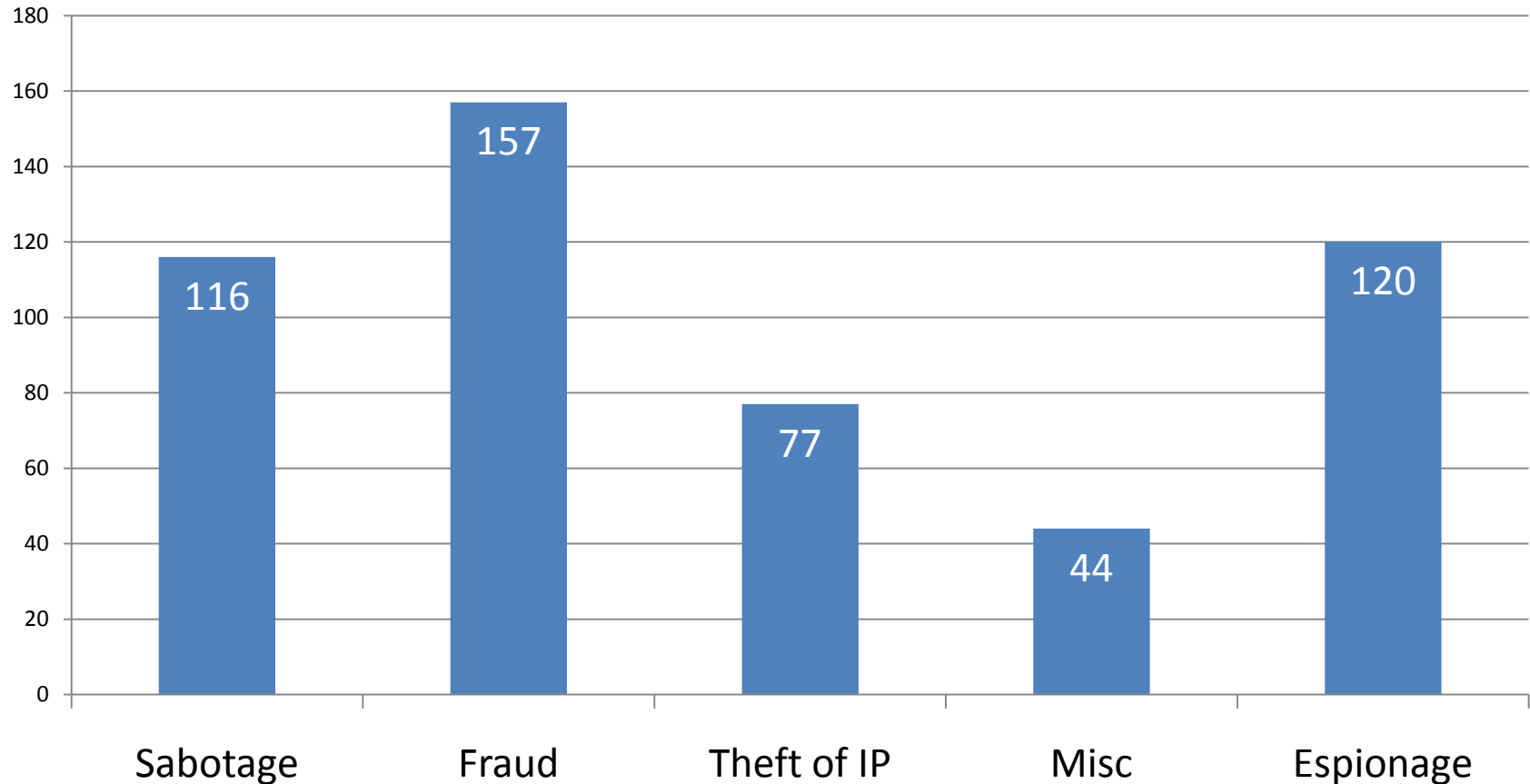


Current Body of Work



CERT's Insider Threat Case Database

U.S. Crimes by Category



This Presentation

- Starts with a quick overview of CERT's crime profile for insider IT sabotage
- Follows with demonstrations based on actual case examples to present potential countermeasures
- Then you can compare your defensive strategies to our controls, and determine whether your existing controls are sufficient to prevent and detect insider attacks such as those shown in the case studies.

Crime Profile: Insider IT Sabotage

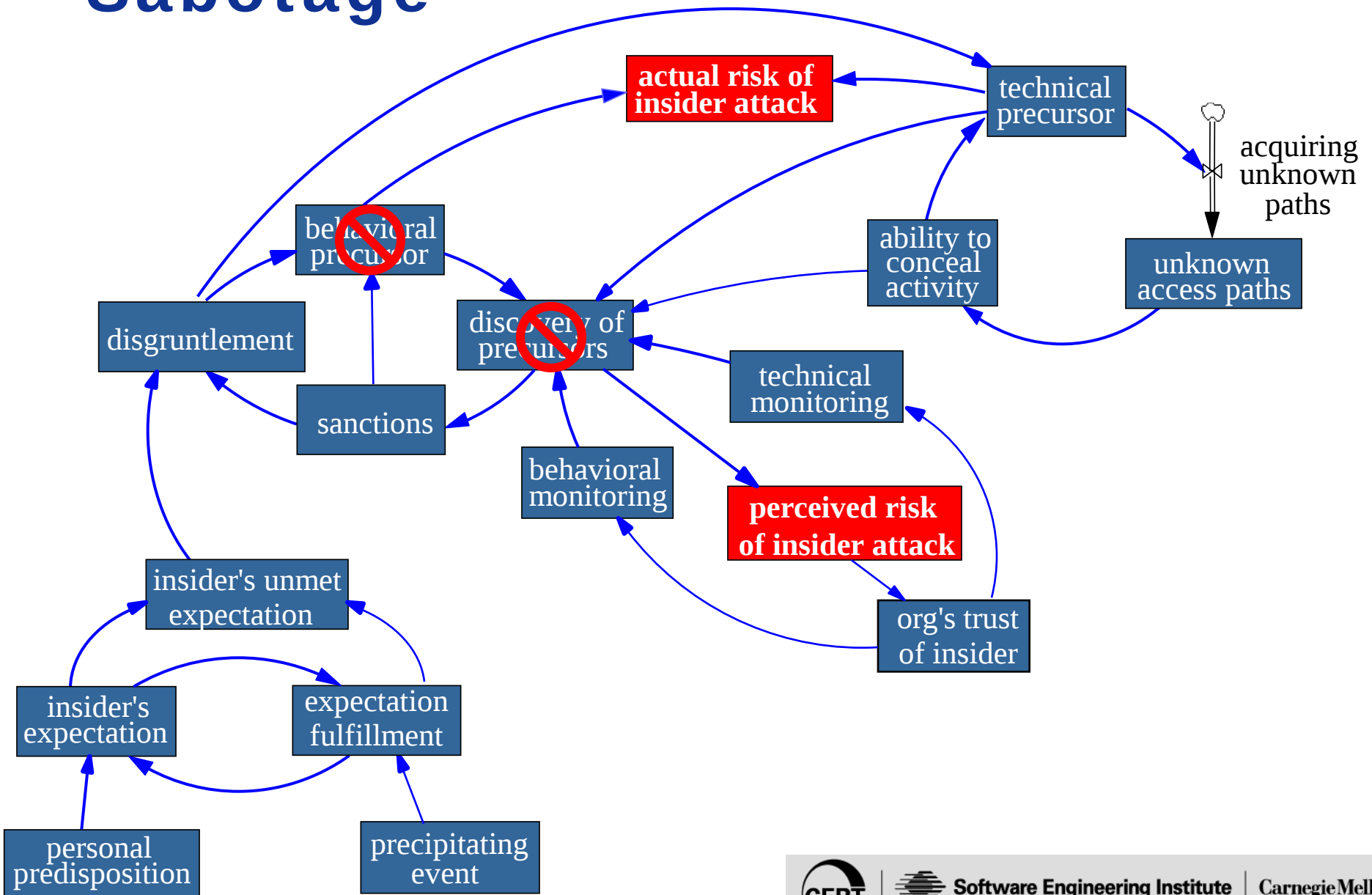


Summary of Findings – IT Sabotage

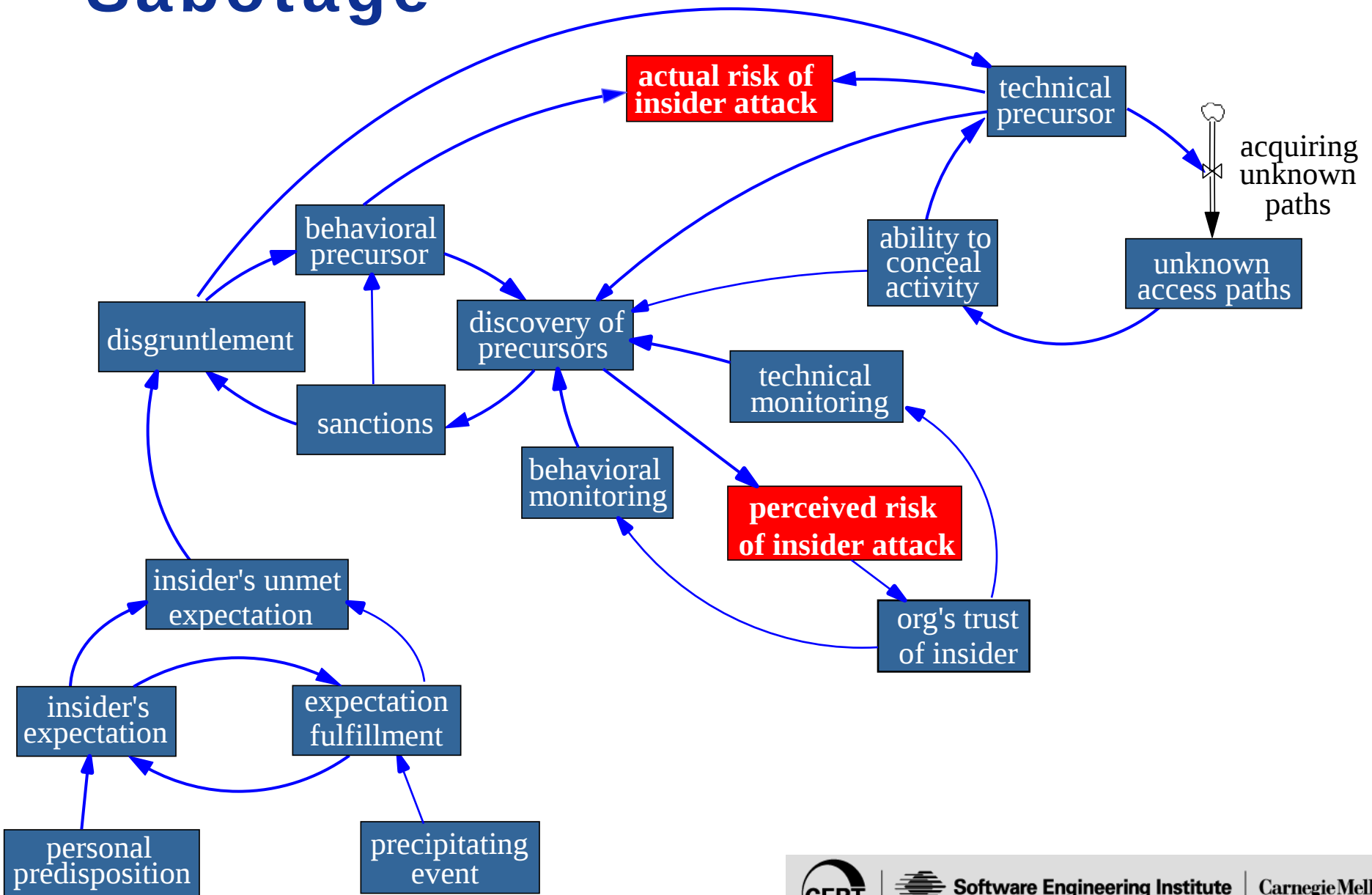
Current or former employee?	<i>Former</i>
Type of position	<i>Technical (e.g., system or database admins)</i>
Gender	<i>Primarily male</i>
Target	<i>Network, systems, or data</i>
Access used	<i>Unauthorized</i>
When	<i>Outside normal working hours</i>
Where	<i>Remote access</i>
Recruited by outsiders	<i>None</i>
Collusion	<i>None</i>



MERIT Model of Insider IT Sabotage



MERIT Model of Insider IT Sabotage



Countermeasures: Insider IT Sabotage



Strategy for Prevention of Insider IT Sabotage

- Need to prevent creation of unknown access paths
- Sample unknown access paths in the cases:
 - Planted logic bombs
 - Created backdoor accounts
 - Downloaded and installed malicious code or “hacker tools” such as rootkits, password sniffers, password crackers , viruses, ...
 - Installed remote administration tool
 - Modified logs to conceal malicious activity
 - Disabled anti-virus and planted virus
- Why is prevention so difficult?
 - Privileged users have the ability to override system controls without detection
 - Information overload: can't realistically monitor everything everyone does online

Solution Strategies

- Implement continuous logging and centralized, secure log server.
- Detect and investigate changes that should occur infrequently, such as:
 - Changes to operating system files, scripts, and executables
 - Changes to stable production systems
 - Services killed on host
- Audit individual actions in logs for privileged accounts.
 - Especially for insiders who are “on the HR radar”

➡ Targeted Monitoring

Audit access to backup information and the results of backup and recovery tests carefully. **This is your last line of defense!**

Demos



Demo #2: Logic Bomb



Demo #3: Keylogger



Application to Your Organization

- In the first three months following this presentation you should:
 - Create policies and processes for proactive monitoring of employees with privileged access who are “on the HR radar”
 - Create an incident handling plan for detection and response to services killed on hosts, suspicious changes to operating system files, and modifications to stable production systems
- Within six months you should:
 - Implement and consistently enforce employee monitoring processes defined above
 - Implement incident handling plan for detection and response to services killed on hosts, suspicious changes to operating system files, and modifications to stable production systems
- ***This is a good place to start - stay tuned for what to do next!***

Caveats

- We only have data on criminals
 - Our findings/recommendations could result in a high false-positive rate.
 - We would like to work with organizations that are willing to be pilot sites. Please contact us.
- Monitoring techniques are not a guarantee.
 - In the event of a missed insider attack, these methods will be tremendously beneficial for incident response and forensic analysis teams.
- Consider legal, privacy, and policy issues before implementing any employee-monitoring program.

Food for Thought

- Which of the monitoring techniques we present today might also be effective in detecting external intruders if they manage to gain access?
- Could controls be effective against both insiders and outsiders?

Points of Contact

Technical Manager

CERT Insider Threat Center

Dawn M. Cappelli

Software Engineering Institute

Carnegie Mellon University

4500 Fifth Avenue

Pittsburgh, PA 15213-3890

+1 412 268-9136 – Phone

dmc@cert.org – Email

Team Lead, Insider Threat Technical Solutions & Standards

Joji Montelibano

CERT Insider Threat Center

Software Engineering Institute

Carnegie Mellon University

4500 Fifth Avenue

Pittsburgh, PA 15213-3890

+1 412 268-6946 – Phone

jmm137@cert.org – Email

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

