



CERT Insider Threat Center

Dawn Cappelli

27 October 2009

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.

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.*



ACTUAL CASE

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.



Crimes Like These...

Are committed by [malicious insiders](#)

- Espionage (involving national security / classified information)
- Sabotage
- Fraud
- Theft of confidential information (e.g. industrial espionage)

Have unique impacts in government sector cases

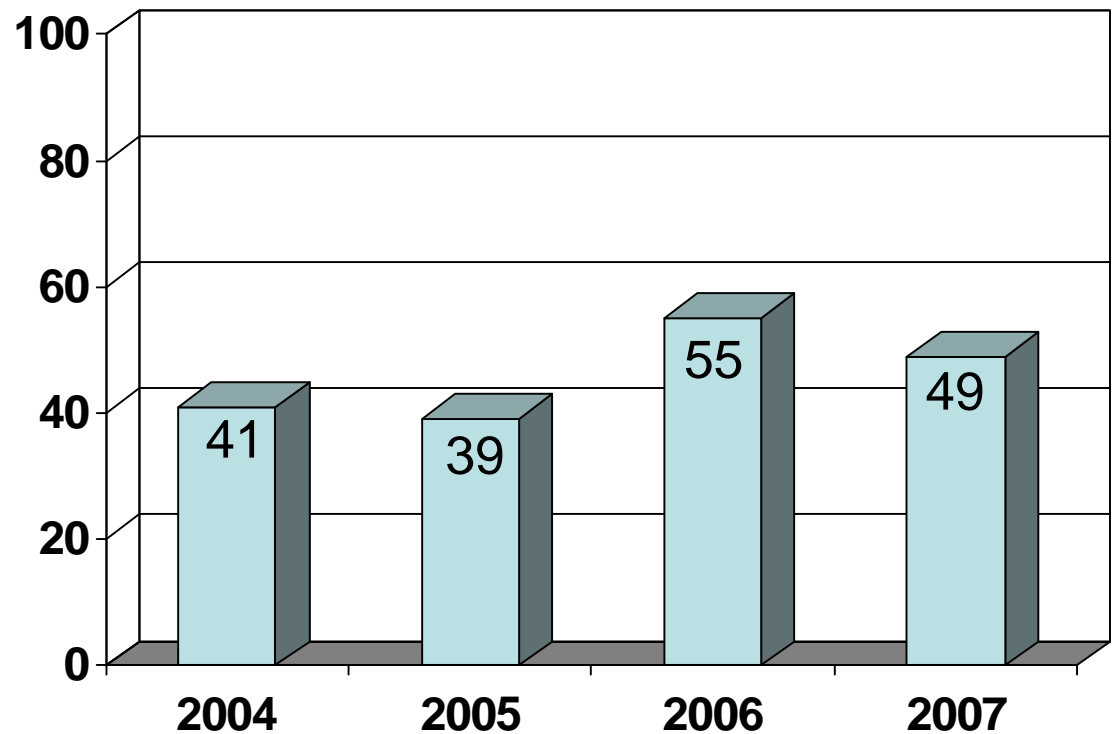
- Hundreds of illegitimate federal identity documents issued to illegal aliens
- Thousands of fraudulent state driver's licenses issued, most to illegal aliens
- Millions of dollars in credit card fraud using false identity documents

2007 e-Crime Watch Survey

CSO Magazine, USSS,
Microsoft, & CERT

671 respondents

Percentage of Participants Who Experienced an Insider Incident



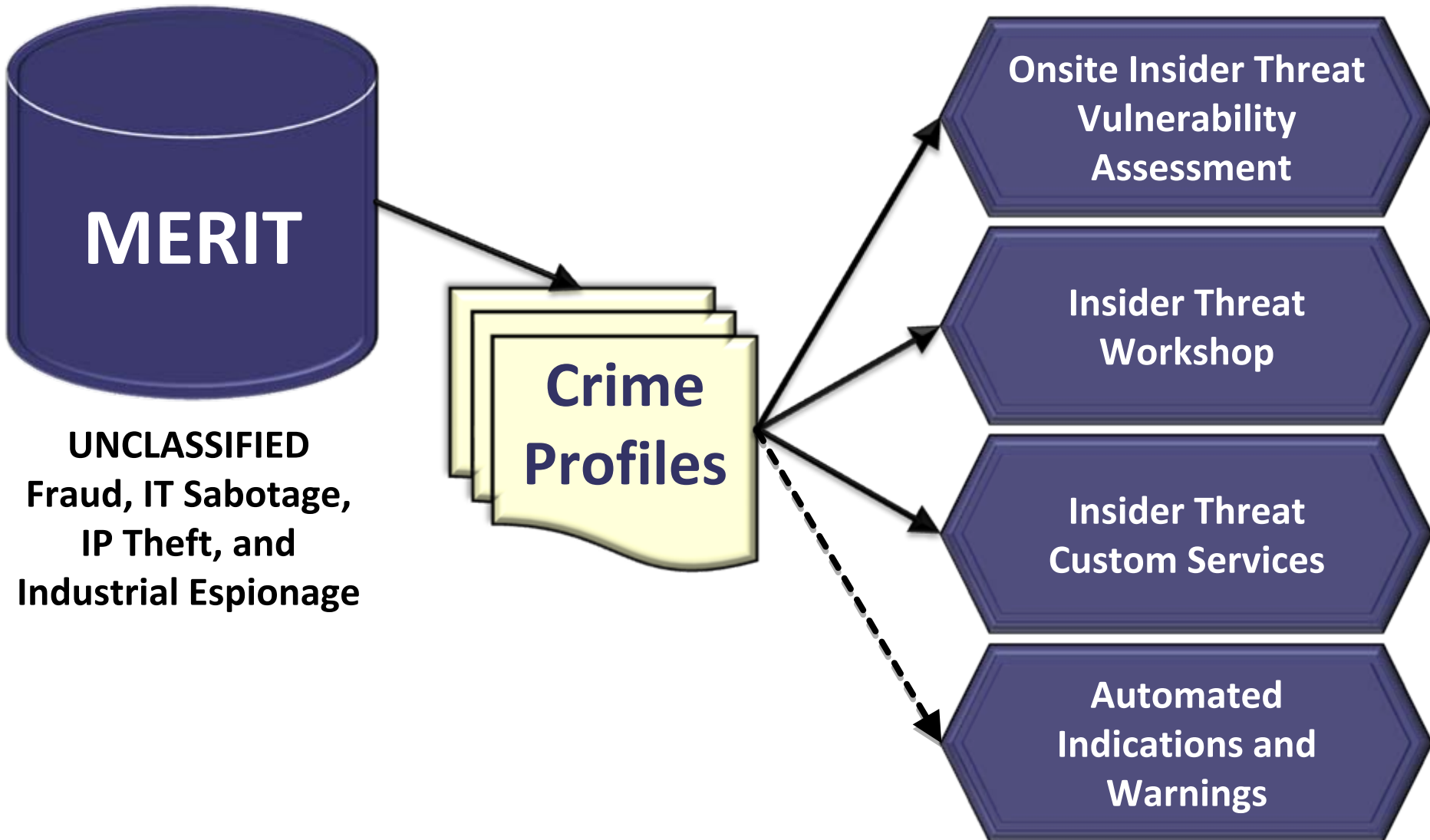
CERT Insider Threat Center—Mission

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

Insider Threat Portfolio



UNCLASSIFIED
Fraud, IT Sabotage,
IP Theft, and
Industrial Espionage

**Crime
Profiles**

**Onsite Insider Threat
Vulnerability
Assessment**

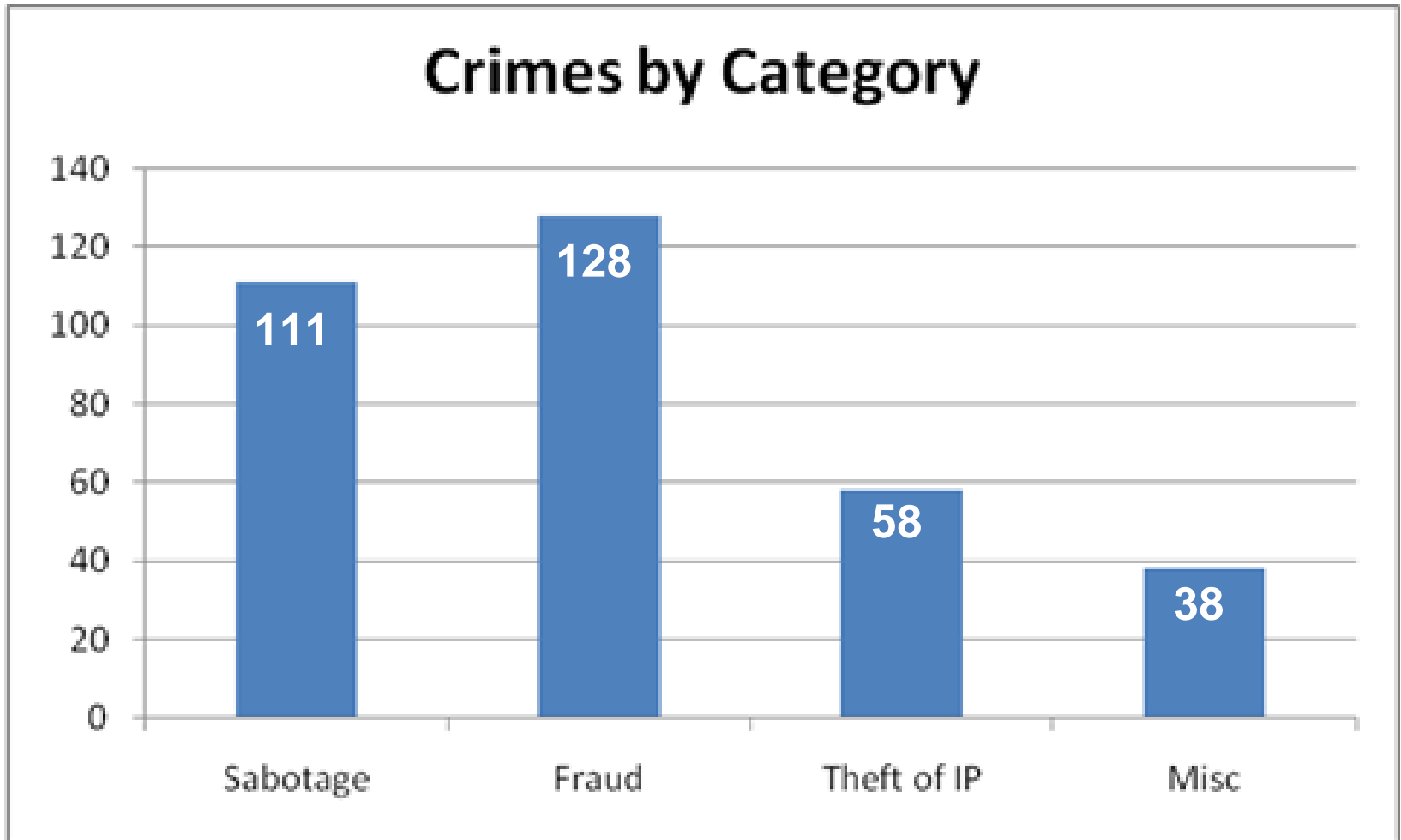
**Insider Threat
Workshop**

**Insider Threat
Custom Services**

**Automated
Indications and
Warnings**

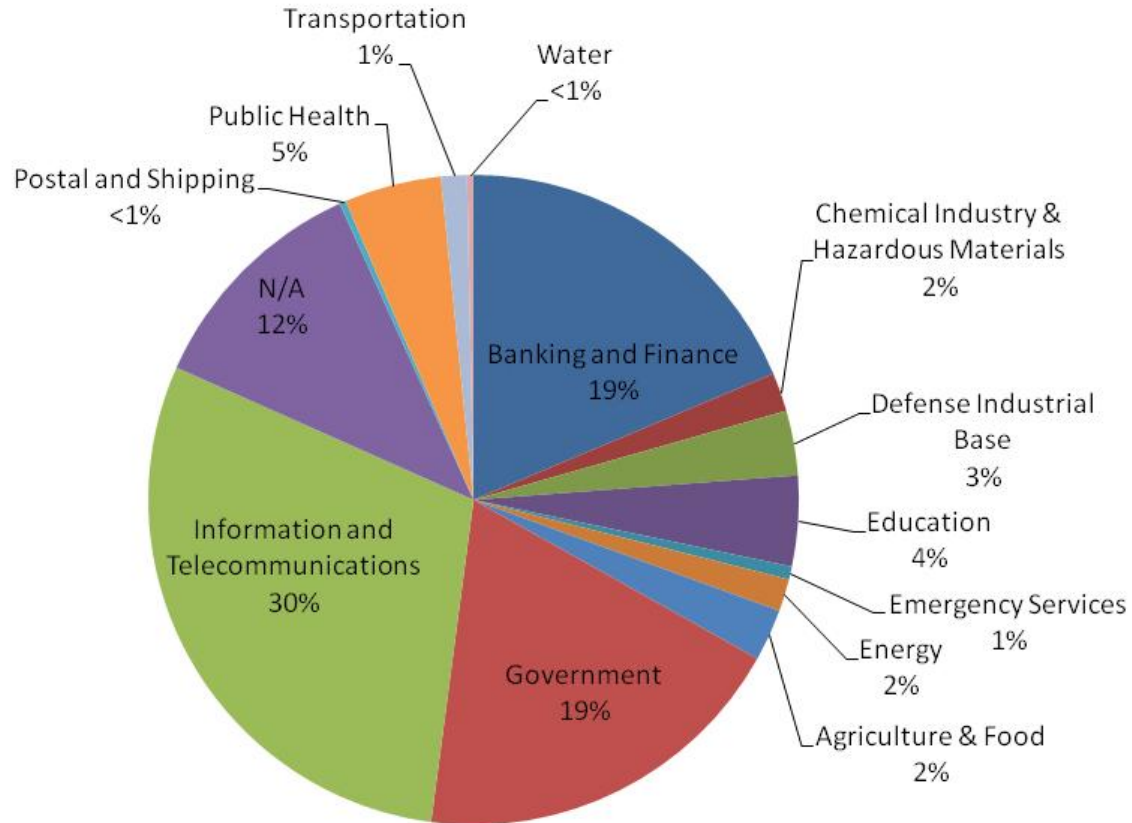
MERIT – Management and Education of the Risk of Insider Threat

MERIT Insider Threat Case Breakdown



Critical Infrastructure Sectors

Cases by Critical Industry Sector



** This does not include espionage cases involving classified information

[Back](#)

Points of Contact

Technical Manager, Threat and Incident Management

Dawn M. Cappelli

CERT Program

Software Engineering Institute

Carnegie Mellon University

4500 Fifth Avenue

Pittsburgh, PA 15213-3890

+1 412 268-9136 – Phone

dmc@cert.org – Email

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

