Insider Threats:

Actual Attacks by Current and Former Software Engineers

9 June 2011

Dawn Cappelli

Agenda

Introduction to the CERT Insider Threat Center

CERT's Insider Threat Crime Profiles

Mitigation Strategies

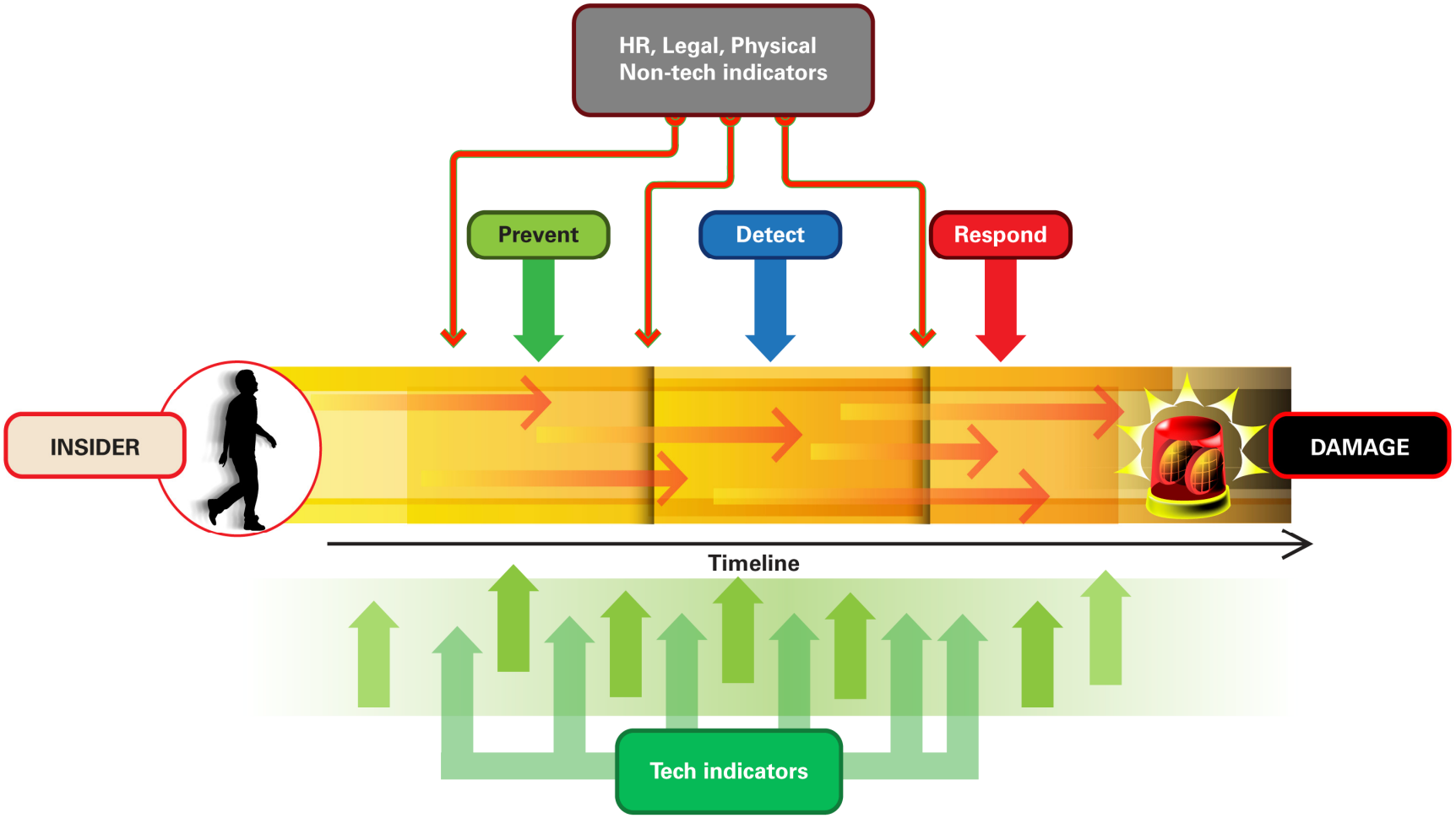
Discussion

Who is a Malicious Insider?

Current or former employee, contractor, or other business partner who

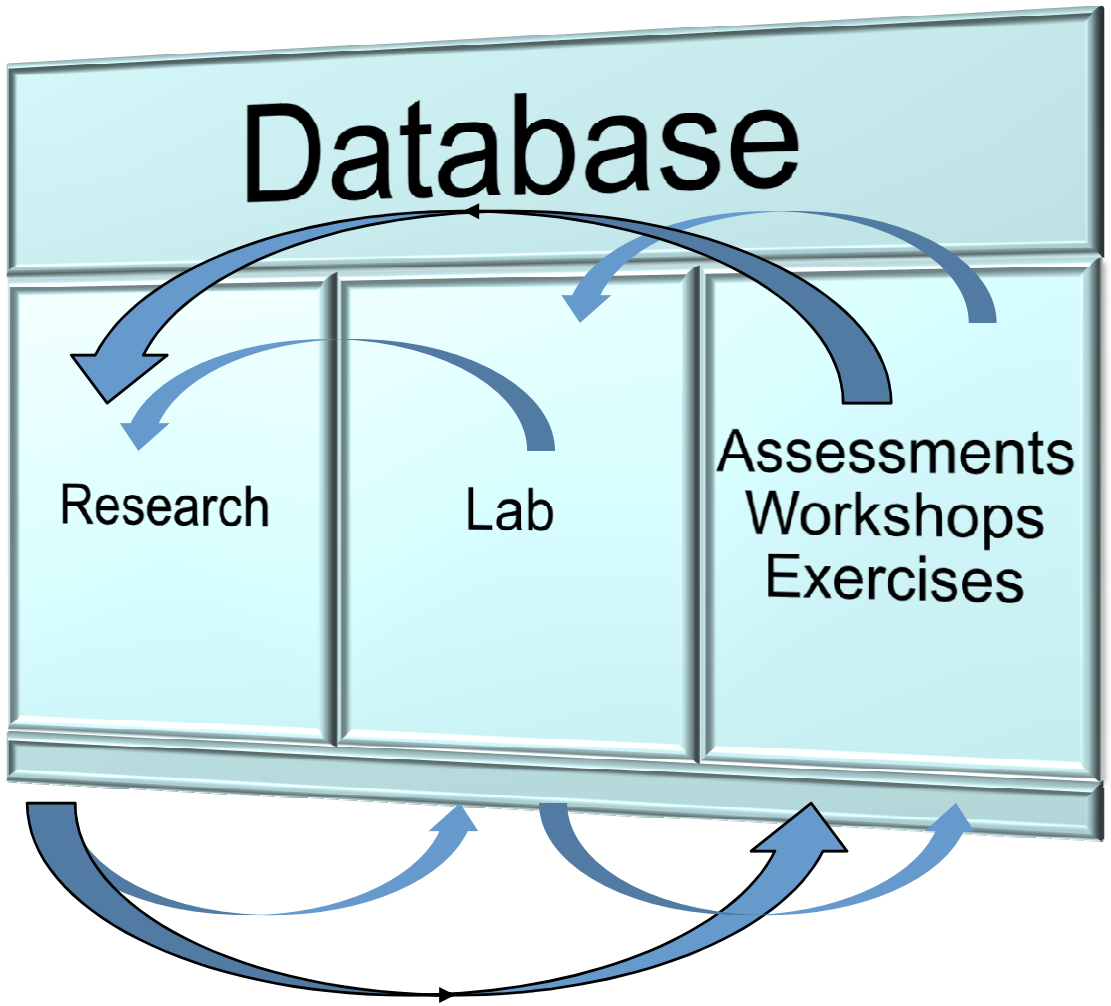
- *has or had authorized access to an organization's network, system or data and*
- *intentionally exceeded or misused that access in a manner that*
- *negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.*

CERT Insider Threat Center Objective

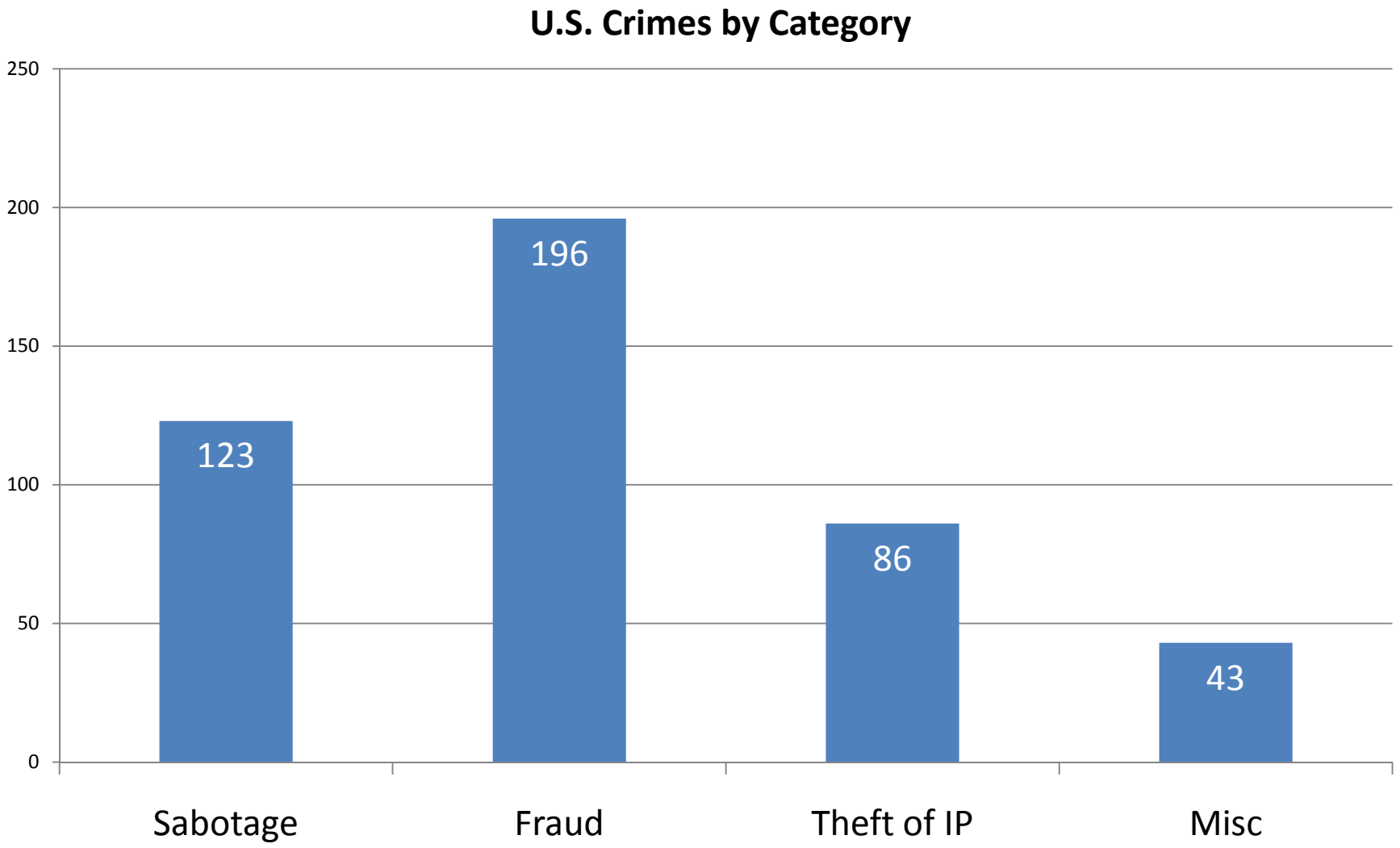


Opportunities for prevention, detection, and response for an insider attack

CERT's Unique Approach to the Problem



CERT's Insider Threat Case Database



IT Sabotage

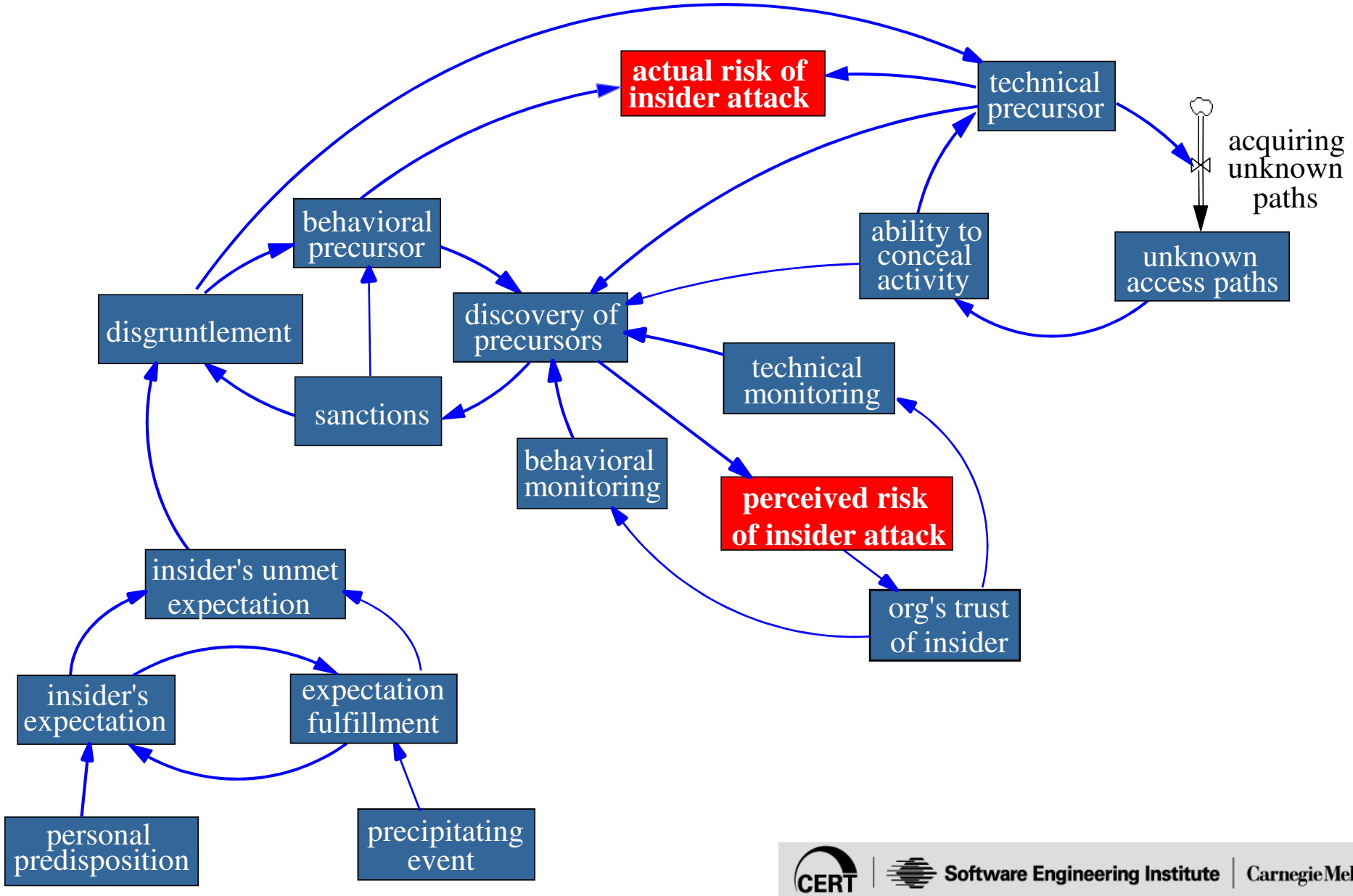

DAN
DAN
SLAM!
Attach File(s)
Do you want
to attach DAN_BACKDOOR.EXE?
YES
No

TRUE STORY:

A company's mobile devices were suddenly disabled for almost 1000 employees, grinding sales and delivery operations to a halt for several days …

Logic bomb went off three months to the day after a demoted system architect's retaliatory resignation.

MERIT Model of Insider IT Sabotage



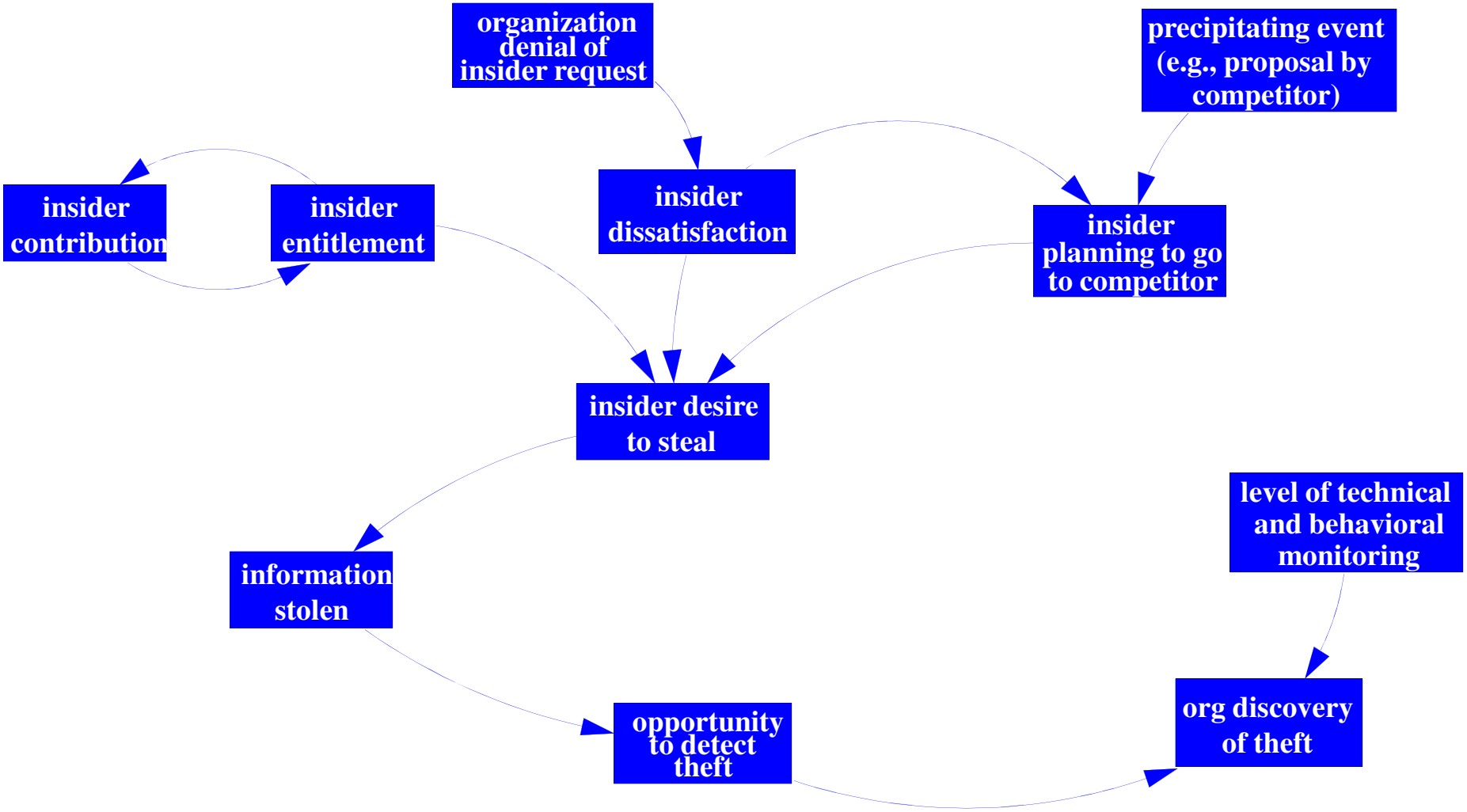
Theft of Intellectual Property

TRUE STORY:

A company sues a former programmer found selling a competing product at a tradeshow….

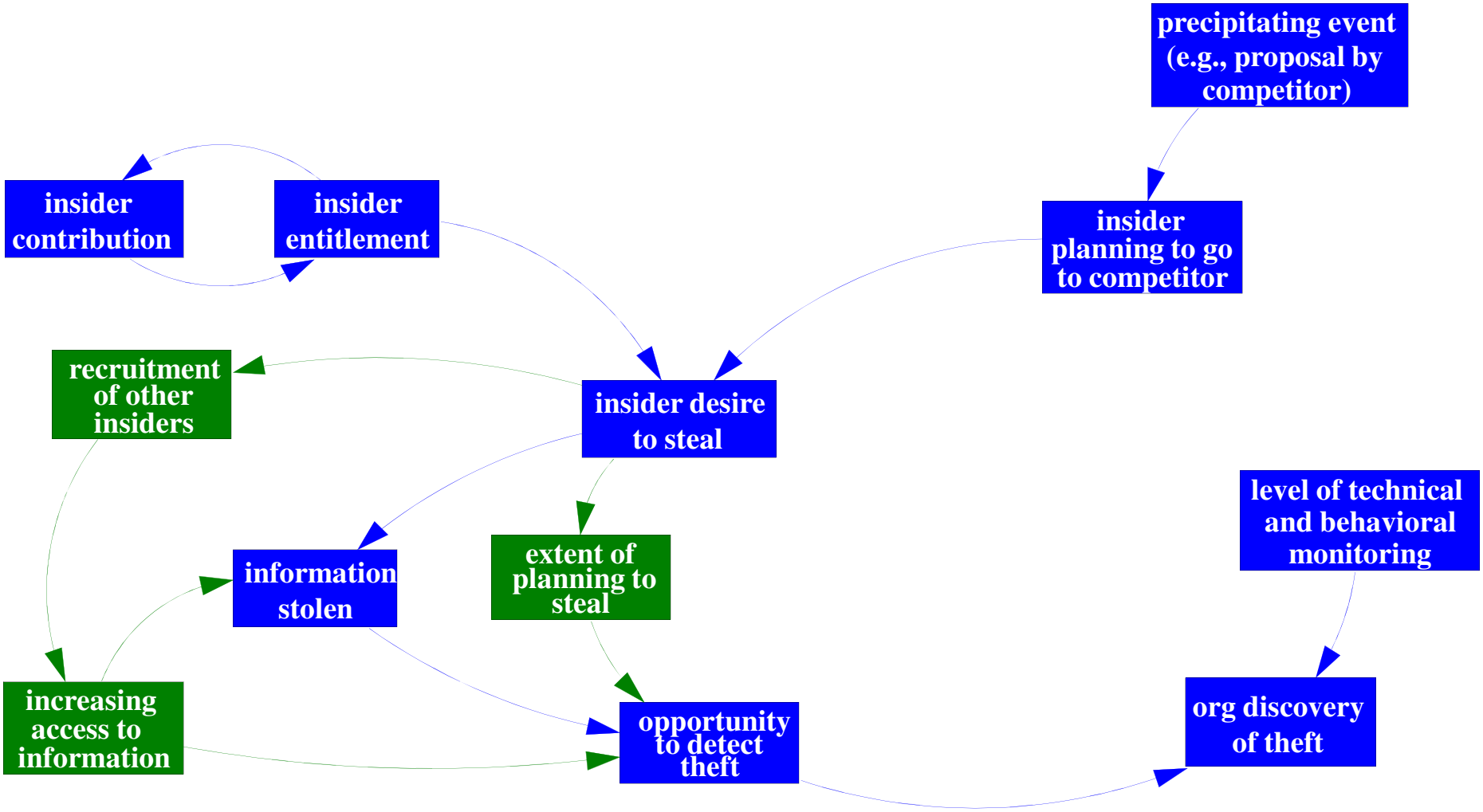
Investigators found copies of the company's source code on his home computer that was stolen on his last day of work at the company.

MERIT Model of Insider Theft of IP – Entitled Independent



CERT | Software Engineering Institute | Carnegie Mellon

MERIT Model of Insider Theft of IP – Ambitious Leader



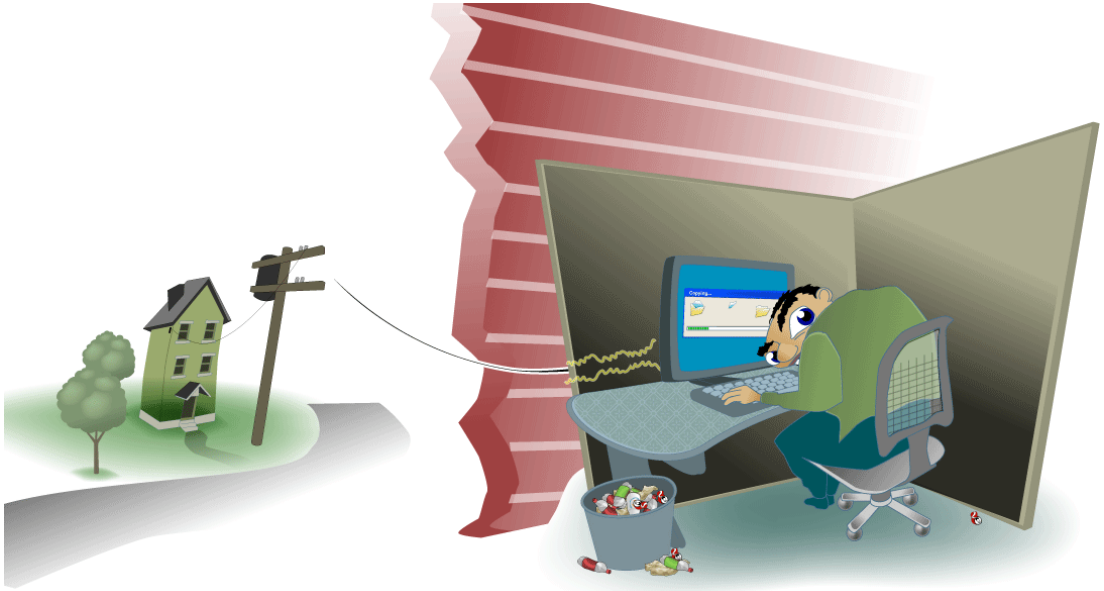
CERT | Software Engineering Institute | Carnegie Mellon

Fraud

TRUE STORY:

A financial organization's routine audit discovers a $90,000 discrepancy in one of their software engineer's personal loan accounts…

The employee modified critical source code to siphon off money to cover fraudulent personal loans he had created.



[1

Summary of Findings - Fraud

Current or former employee?	Current
Type of position	Non-technical, low-level positions with access to confidential or sensitive information (e.g. data entry, customer service)
Gender	Fairly equally split between male and female
Target	PII or Customer Information
Access used	Authorized
When	During normal working hours
Where	At work
Recruited by outsiders	½ recruited for theft; less than 1/3 recruited for mod
Collusion	Mod: almost ½ colluded with another insider Theft: 2/3 colluded with outsiders

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.	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

Points of Contact

Insider Threat Center
CERT Program
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-3890

Dawn Cappelli
Technical Manager
+1 412 268-9136
dmc@cert.org

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