



***Pay Attention!  
What are Your Employees  
Doing?***

**Dawn M. Cappelli**

**[http://www.cert.org/insider\\_threat/](http://www.cert.org/insider_threat/)**



# Financial Institution Discovers \$691 Million in Losses...

*Covered up for 5 Years by Trusted  
Employee*

# Manufacturer Loses \$10 Million- Lays Off 80 Employees...

*Sabotage by Employee of Eleven Years  
Nearly Puts Company Out of Business*



COULD THIS HAPPEN TO  
YOU?



# Introduction

# What is CERT?

---



Center of Internet security expertise

Established in 1988 by the US Department of Defense in 1988 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)

# Overview of Talk

---

## Background

- Introduction
- Evolution of CERT's insider threat research

## Insider IT Sabotage – Key Observations

- Case examples
- Statistics

## *MERIT* Models of Insider IT Sabotage

## Common Sense Guide – Best Practices

## Future Work



---

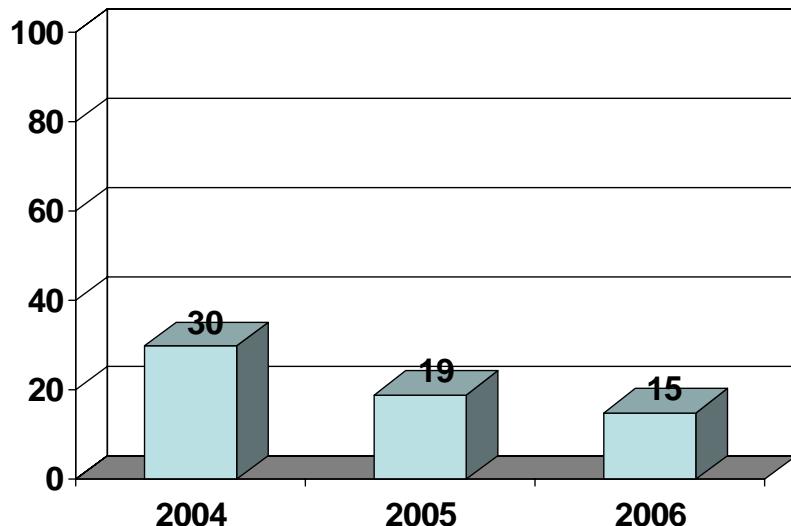
# *Background*

# 2006 e-Crime Watch Survey

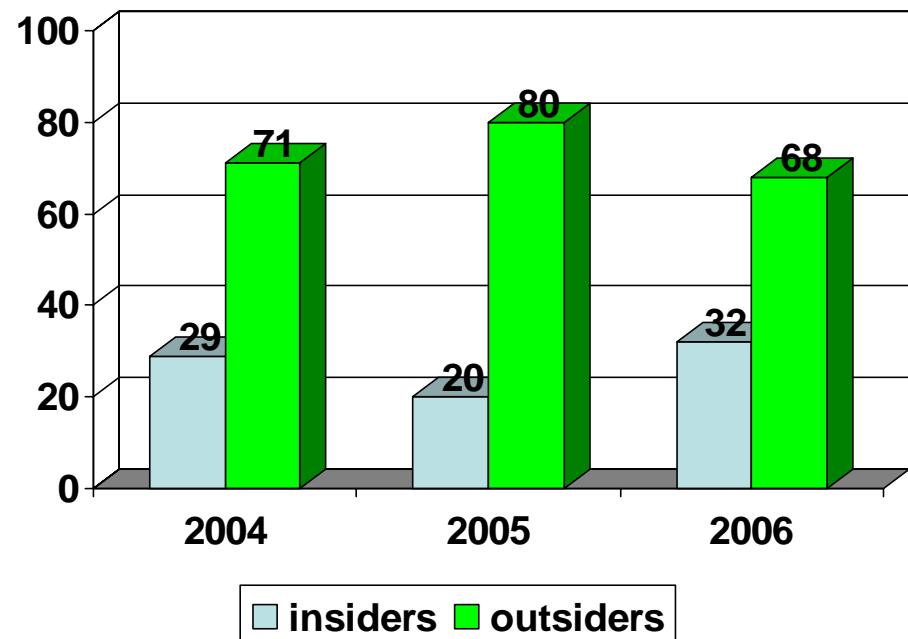
CSO Magazine, USSS & CERT

434 respondents

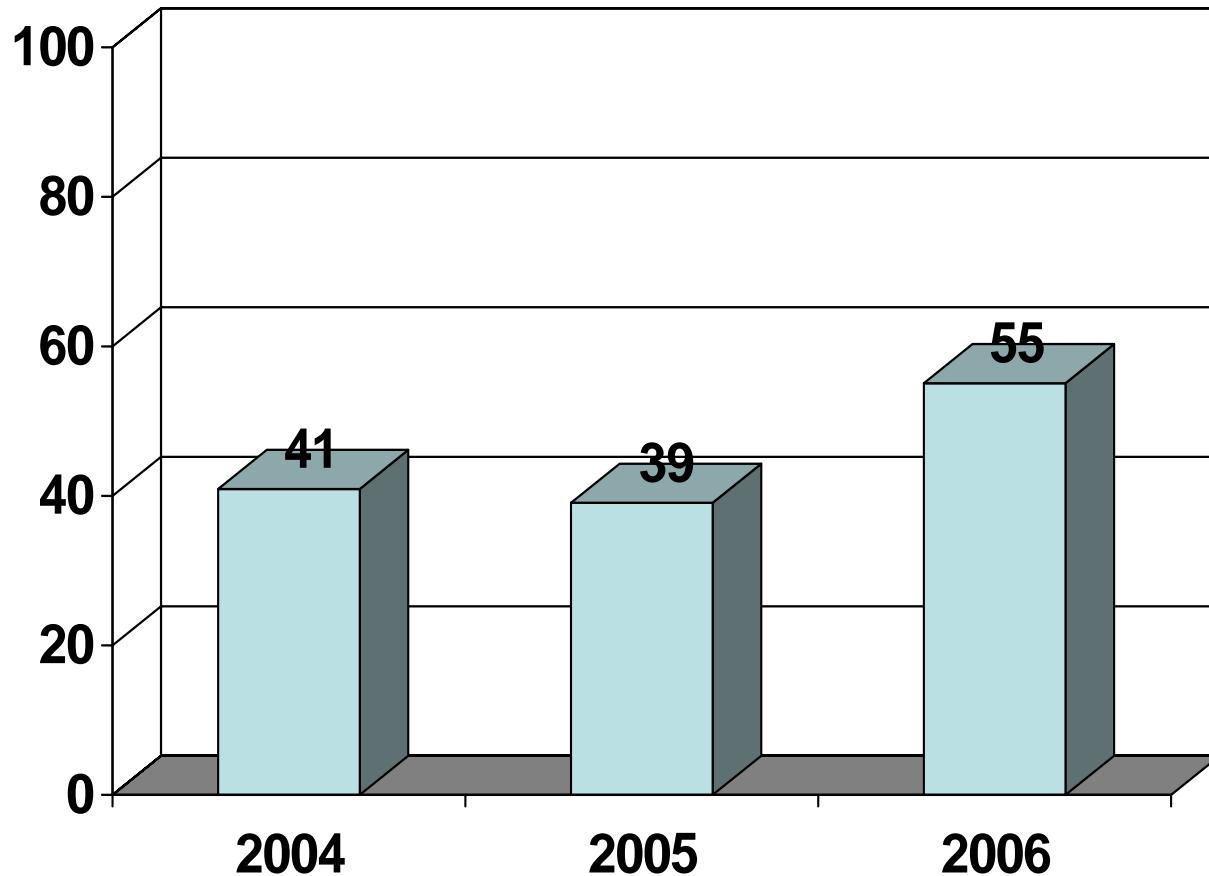
**Percentage of  
Incidents With no  
Source Identified**



**Percentage of insiders  
versus outsiders**



# Percentage of Participants Who Experienced an Insider Incident (2004-2006)



# Types of Insider Crimes

---

**Fraud:** obtaining property or services from the organization unjustly through deception or trickery.

**Theft of Information:** stealing confidential or proprietary information from the organization.

**IT Sabotage:** acting with intention to harm a specific individual, the organization, or the organization's data, systems, and/or daily business operations.

# Examples of Insider Crimes

---

## Fraud examples:

- Sale of confidential information (SSN, credit card numbers, etc...)
- Modification of critical data for pay (driver's license records, criminal records, welfare status, etc...)
- Stealing of money (financial institutions, government organizations, etc...)

## Theft of Information examples:

- Theft of customer information
- Theft of source code
- Theft of organization's data

## Sabotage examples:

- Deletion of information
- Bringing down systems
- Web site defacement to embarrass organization

# Evolution of CERT Insider Threat Research

---

## Insider threat case studies

- U.S. Department Of Defense Personnel Security Research Center (PERSEREC)
- CERT/U.S. Secret Service *Insider Threat Study*

## Best practices

- Carnegie Mellon CyLab *Common Sense Guide to Prevention and Detection of Insider Threats*

## System dynamics modeling

- Carnegie Mellon CyLab – *Management and Education on the Risk of Insider Threat (MERIT)*
- PERSEREC

# CERT/USSS *Insider Threat Study*

Definition of insider:

***Current or former employees or contractors who***

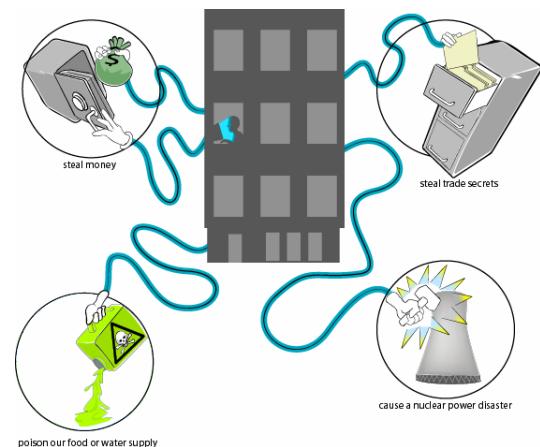
- *intentionally exceeded or misused an authorized level of access to networks, systems or data in a manner that*
- *targeted a specific individual or affected the security of the organization's data, systems and/or daily business operations*



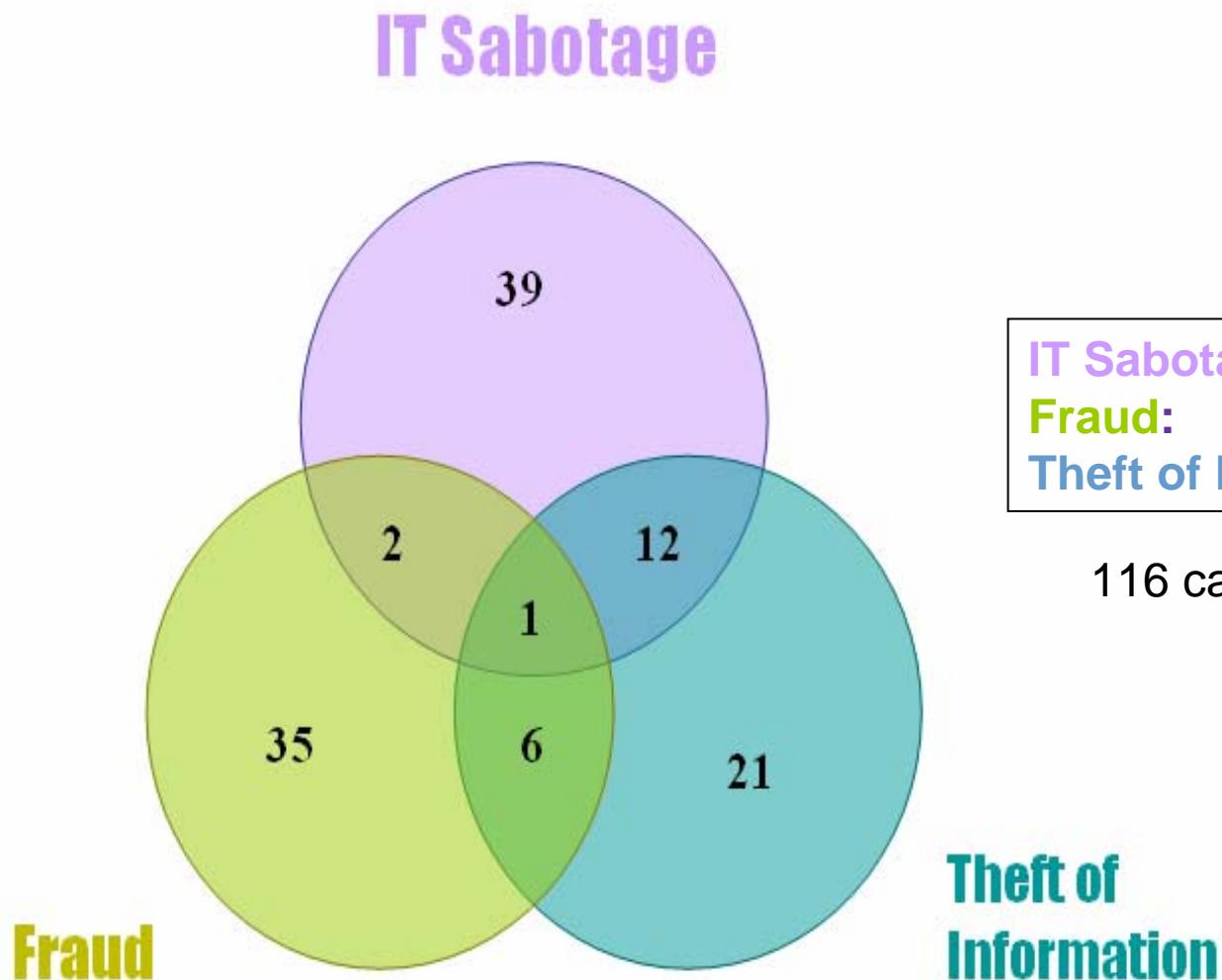
Carnegie Mellon  
Software Engineering Institute

# *Insider Threat Study*

- Funded by US Secret Service (partially by Department of Homeland Security)
- Examined technical & psychological aspects
- Analyzed actual cases to develop information for prevention & early detection
- Methodology:
  - Collected cases (150)
  - Codebooks
  - Interviews
  - Reports
  - Training



# Insider Threat Study Case Breakdown



# Next: The Big Picture

---

Important aspects of the insider threat problem:

- Interaction of policies, practices, and technology over time
- Interaction between psychological & technical aspects of the problem

Need for innovative training materials

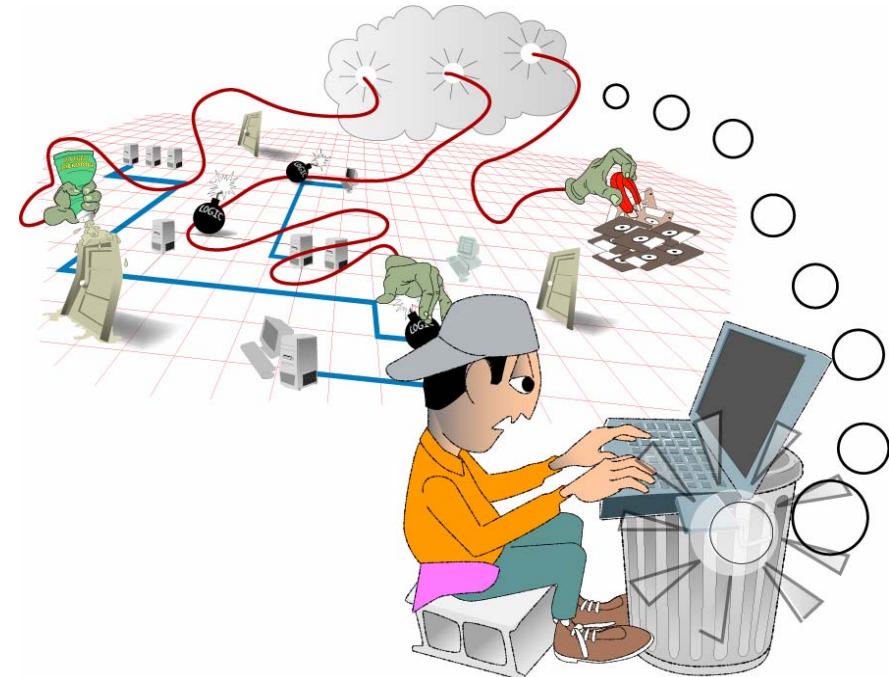
CyLab funding:

- *MERIT: Management and Education of the Risk of Insider Threat*
- Initial Proof of Concept: insider IT sabotage

# Definition of Insider IT Sabotage

## Cases

- across critical infrastructure sectors
- in which the insider's primary goal was to
  - sabotage some aspect of an organization or
  - direct specific harm toward an individual(s).



---

# *Insider IT Sabotage Key Observations*

# Who Were the Saboteurs?

---

Age: 17 – 60

Gender: mostly males

Variety of racial & ethnic backgrounds

Marital status: fairly evenly split married versus single

Almost 1/3 had previous arrests

---

## ***Observation #1:***

***Most insiders had personal predispositions that contributed to their risk of committing malicious acts.***

# Case Example – Observation #1

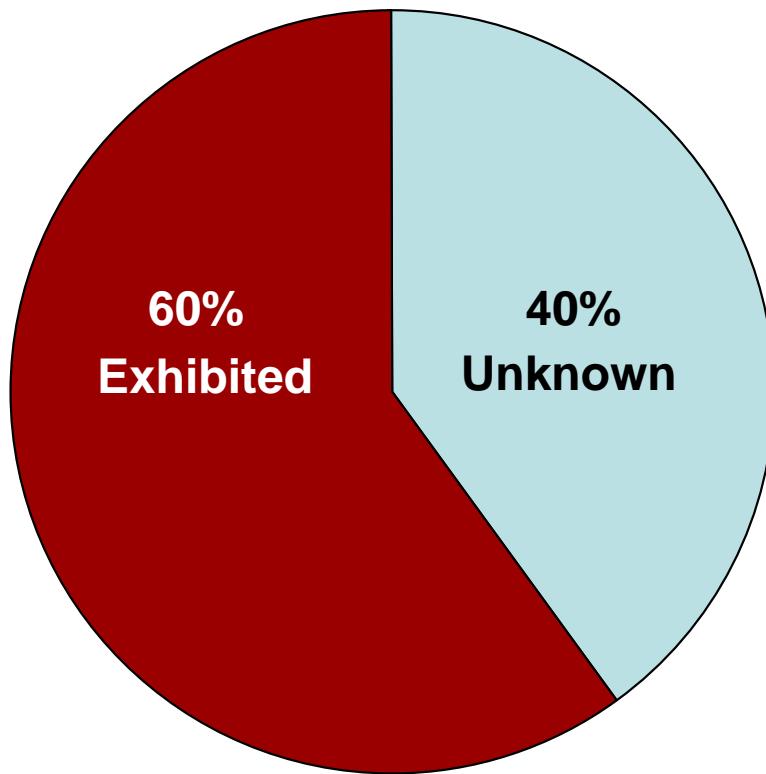
---

A database administrator wipes out critical data after her supervisor and coworkers undermine her authority.



# Personal Predispositions

---



---

## ***Observation #2:***

***Most insiders' disgruntlement is due to unmet expectations.***

# Case Example – Observation #2

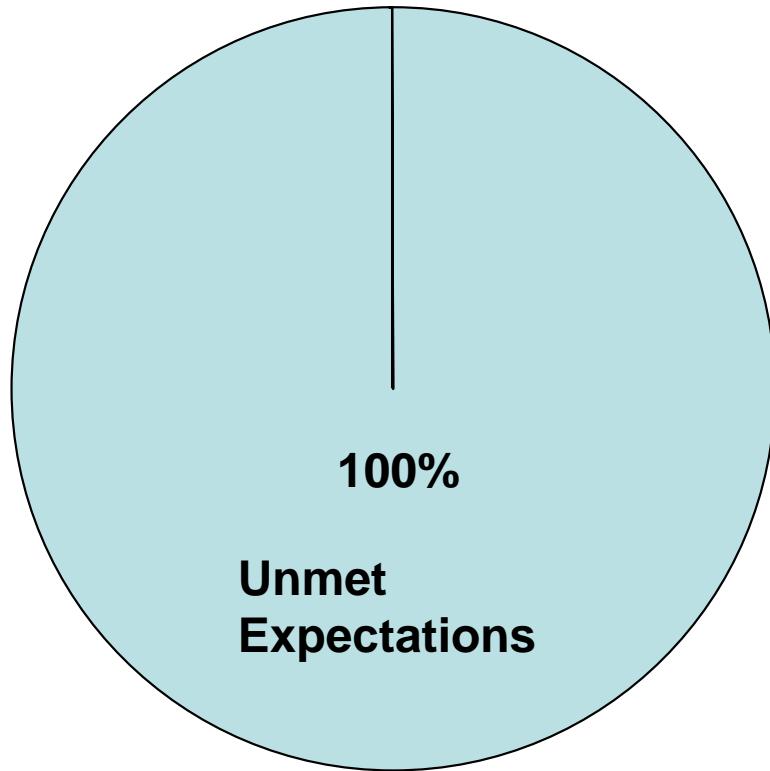
---

A network engineer retaliates after his hope of recognition and technical control are dashed.



# Unmet Expectations

---



**\*\* Data was only available for 25 cases**

---

## ***Observation #3:***

***In most cases, stressors, including sanctions and precipitating events, contributed to the likelihood of insider IT sabotage.***

# Case Example – Observation #3

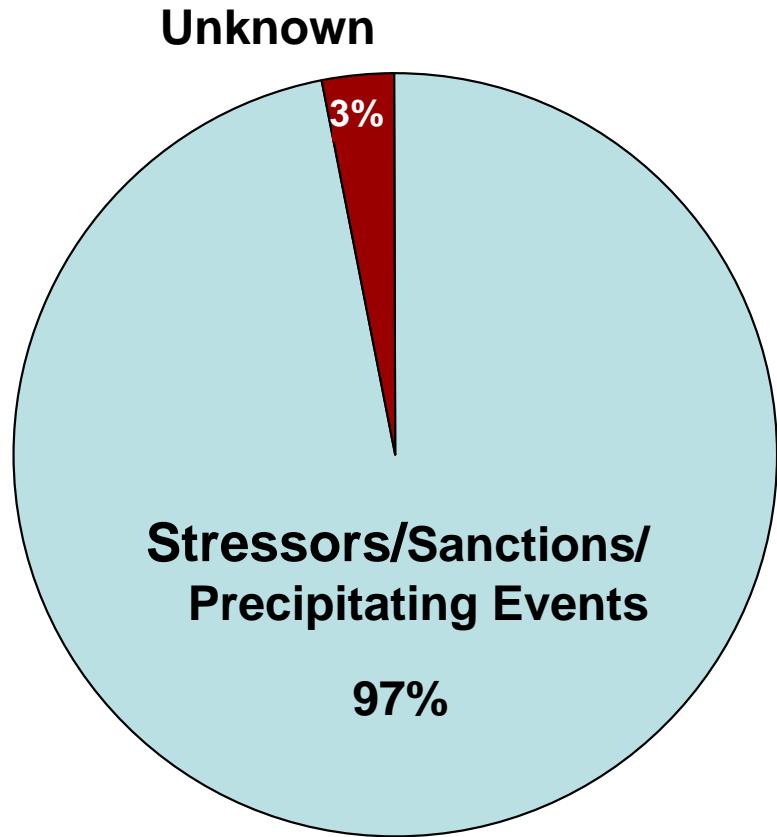
---

A disgruntled system administrator strikes back after his life begins to fall apart personally and professionally.



# Stressors /Sanctions/Precipitating Events

---



---

## ***Observation #4:***

***Behavioral precursors were often observable in insider IT sabotage cases but ignored by the organization.***

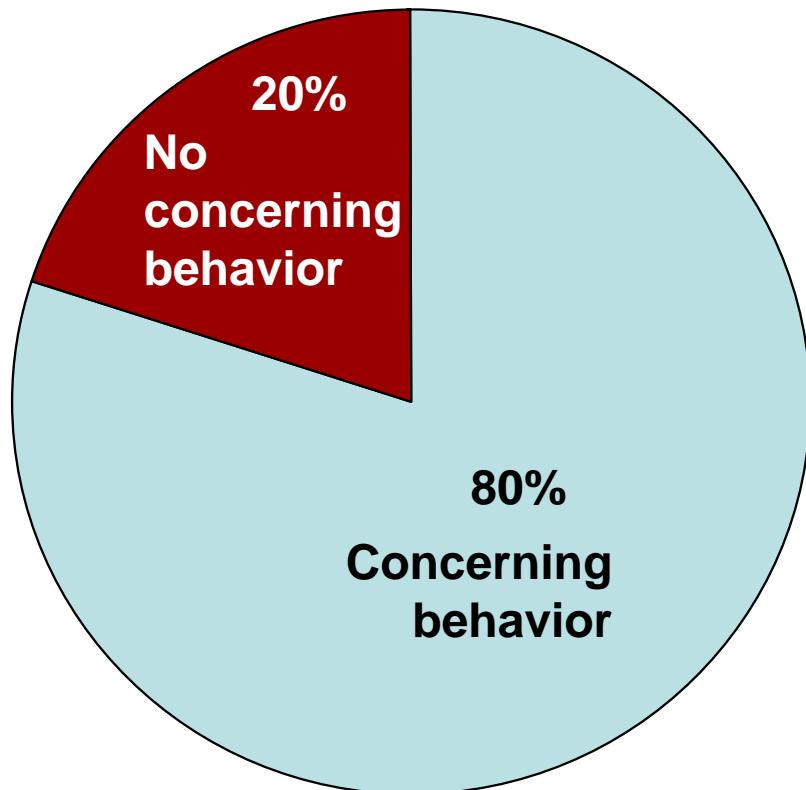
# Case Example – Observation #4

A “weird tech guy” is able to attack following termination because no one recognizes the danger signs.



# Behavioral Precursors

---



---

## ***Observation #5:***

***Insiders created or used access paths unknown to management to set up their attack and conceal their identity or actions.***

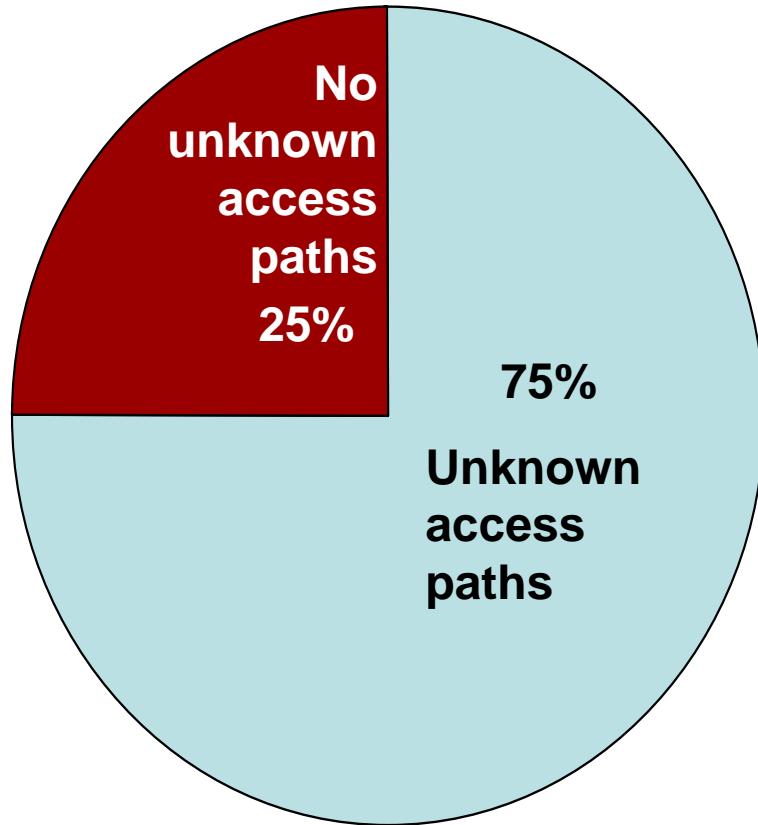
***The majority attacked after termination.***

# Case Example – Observation #5

The “weird tech guy” realizes the end is near so he sneakily sets up his attack.



# Created or used unknown access paths



---

## *Observation #6:*

*In many cases, organizations failed to detect technical precursors.*

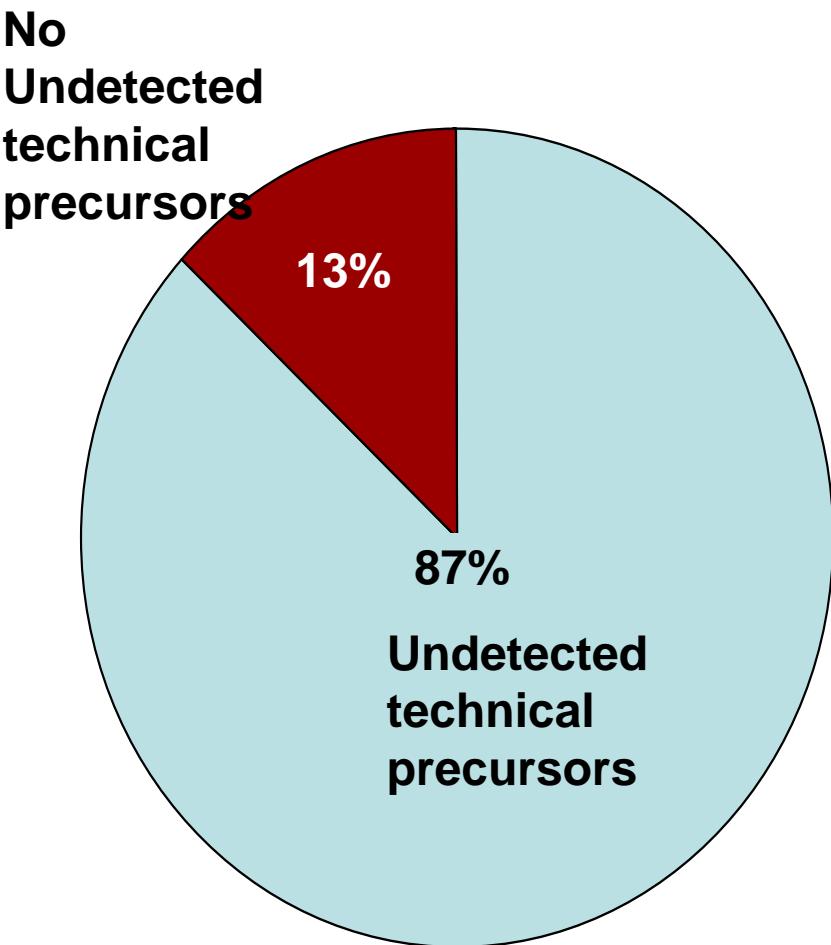
# Case Example – Observation #6

A logic bomb sits undetected for 6 months before finally wreaking havoc on a telecommunications firm.



# Technical precursors undetected

---



---

## *Observation #7:*

***Lack of physical and electronic access controls facilitated IT sabotage.***

# Case Example – Observation #7

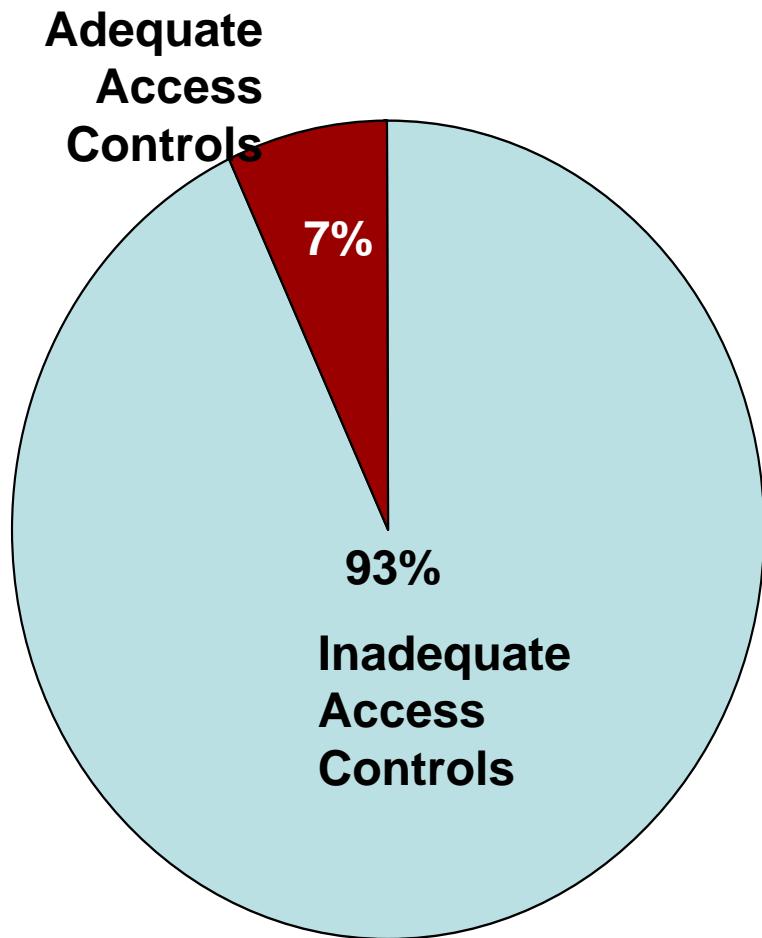
---

Emergency services are forced to rely on manual address lookups for 911 calls when an insider sabotages the system.



# Lack of Access Controls

---



---

# *MERIT Model(s) Insider IT Sabotage*

# System Dynamics Approach

---

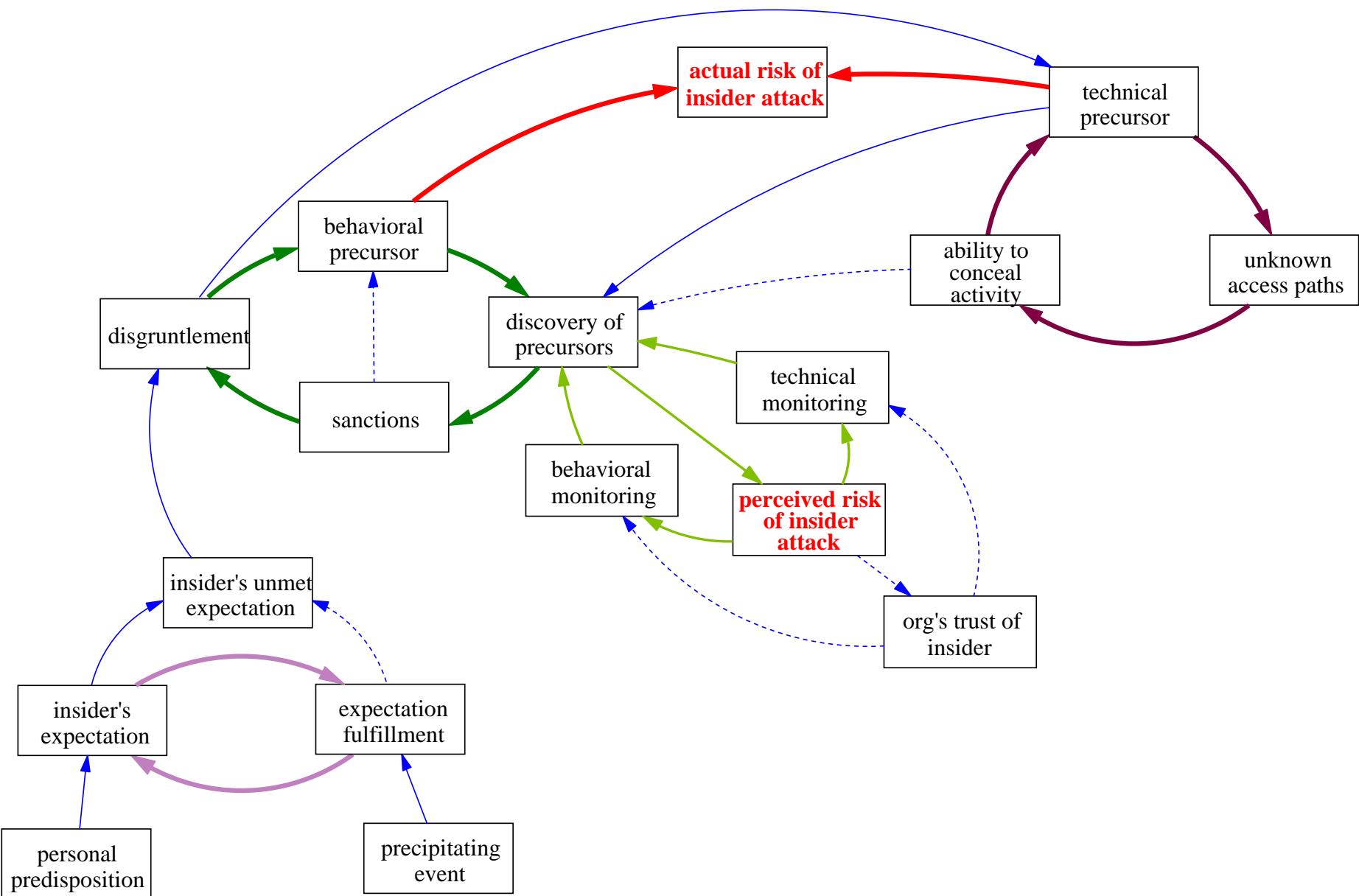
A method and supporting toolset

- To holistically model, document, and analyze
- Complex problems as they evolve over time
- And develop effective mitigation strategies
- That balance competing concerns

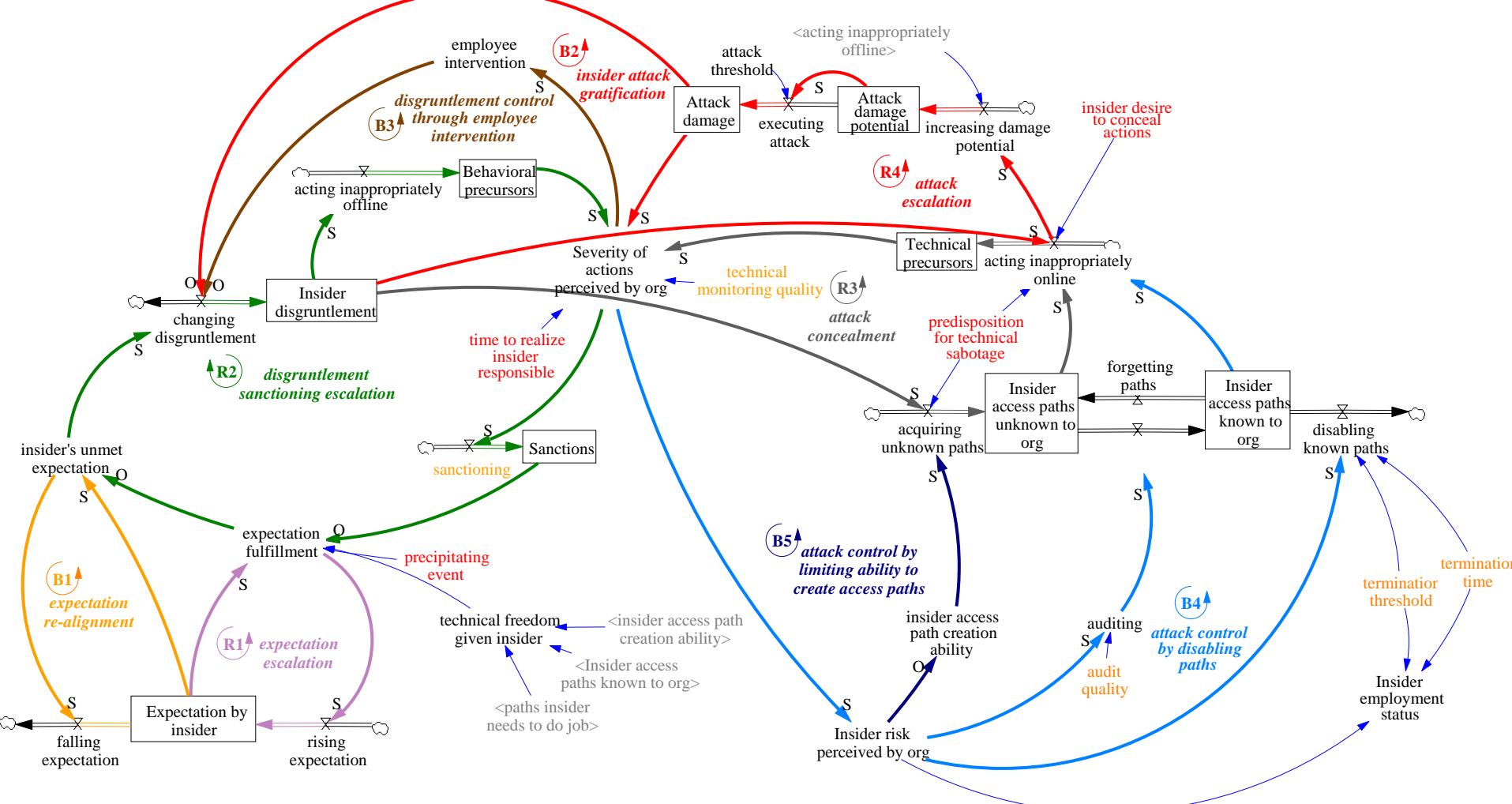
System Dynamics supports simulation to

- Validate characterization of problem
- Test out alternate mitigation strategies

# MERIT Model – Extreme Overview



# MERIT Model Details



---

# *Best Practices*

# CyLab Common Sense Guide - Best Practices

---

Institute periodic enterprise-wide risk assessments.

Institute periodic security awareness training for all employees.

Enforce separation of duties and least privilege.

Implement strict password and account management policies and practices.

Log, monitor, and audit employee online actions.

Use extra caution with system administrators and privileged users.

Actively defend against malicious code.

Use layered defense against remote attacks.

Monitor and respond to suspicious or disruptive behavior.

Deactivate computer access following termination.

Collect and save data for use in investigations.

Implement secure backup and recovery processes.

Clearly document insider threat controls.

# New Starts & Future Work

---

## New Starts

- Requirements for insider threat detection tools
- CyLab *MERIT-IA (MERIT InterActive)*
  - Analysis of current cases

## Future Work

- Self-directed risk assessment
- Best practice collaboration
- Investigative guidelines
- Extension/analysis of MERIT model
- Insider threat workshops

---

# *Questions / Comments*

# Points of Contact

---

## Insider Threat Team Lead:

Dawn M. Cappelli  
Senior Member of the Technical Staff  
CERT Programs  
Software Engineering Institute  
Carnegie Mellon University  
4500 Fifth Avenue  
Pittsburgh, PA 15213-3890  
+1 412 268-9136 – Phone  
[dmc@cert.org](mailto:dmc@cert.org) – Email

## Business Development:

Joseph McLeod  
Business Manager  
Software Engineering Institute  
Carnegie Mellon University  
4500 Fifth Avenue  
Pittsburgh, PA 15213-3890  
+1 412 268-6674 – Phone  
+1 412-291-3054 – FAX  
+1 412-478-3075 – Mobile  
[jmcleod@sei.cmu.edu](mailto:jmcleod@sei.cmu.edu) – Email

## System Dynamics Modeling Lead:

Andrew P. Moore  
Senior Member of the Technical Staff  
CERT Programs  
Software Engineering Institute  
Carnegie Mellon University  
4500 Fifth Avenue  
Pittsburgh, PA 15213-3890  
+1 412 268-5465 – Phone  
[apm@cert.org](mailto:apm@cert.org) – Email

[http://www.cert.org/insider\\_threat/](http://www.cert.org/insider_threat/)