CSI 33rd Annual
COMPUTER SECURITY CONFERENCE & EXHIBITION

CERT

A Risk Mitigation Model: Lessons Learned From Actual Insider Sabotage

Software Engineering Institute | Carnegie Mellon

Dawn M. Cappelli, Andrew P. Moore, Eric D. Shaw

Attacks and Countermeasures

ATC-5&6, November 7, 2006

CSI
COMPUTER
SECURITY
INSTITUTE

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
07 NOV 2006		**00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
A Risk Mitigation Model: Lessons Learned From Actual Insider Sabotage	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 (SEI),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
CSI 33rd Annual Security Conference and Exhibition, 6-8 Nov, 2006, Orlando, FL.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**97**	

A Risk Mitigation Model: Lessons Learned From Actual Insider Sabotage

Dawn M. Cappelli

Andrew P. Moore

Eric D. Shaw

November 7, 2006

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?

Agenda

Introductions

Background

- Evolution of CERT's Insider Threat Research
- Simultaneous PERSEREC Insider Threat Research

Interactive Case Example

Key Insider IT Sabotage Observations

- Case Examples
- Statistics
- Observables

MERIT Model Overview

Best Practices

Future Work

Introductions

What is CERT?

Center of Internet security expertise

Established 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)

Background

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

Simultaneous PERSEREC Insider Threat Research

Small number of cases (10)

In-depth Personal, Organizational Psychological Perspective

Emphasis on experience of individual by those in workplace as he moves from disgruntlement to attack

Results Available (Shaw and Fischer, 2005; Shaw, 2006)

Similar Findings to CERT

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*

Insider Threat Study

Funded by US Secret Service (partially by Department of Homeland Security)

Big picture approach: examine technical & psychological aspects of the problem

Objective: Analyze actual cases to develop information for prevention & early detection

Methodology:

- Collected cases (150)
- Codebooks
- Interviews
- Reports
- Training

MERIT

Management and Education of the Risk of Insider Threat

Funded by CyLab

Develop models of insider IT sabotage

Communicate the multi-disciplinary nature of problem

- Problem and mitigation requires analysis of policies, practices, technologies over time

Develop innovative training materials

Help organizations understand how they need to work across departments to mitigate the insider sabotage risk

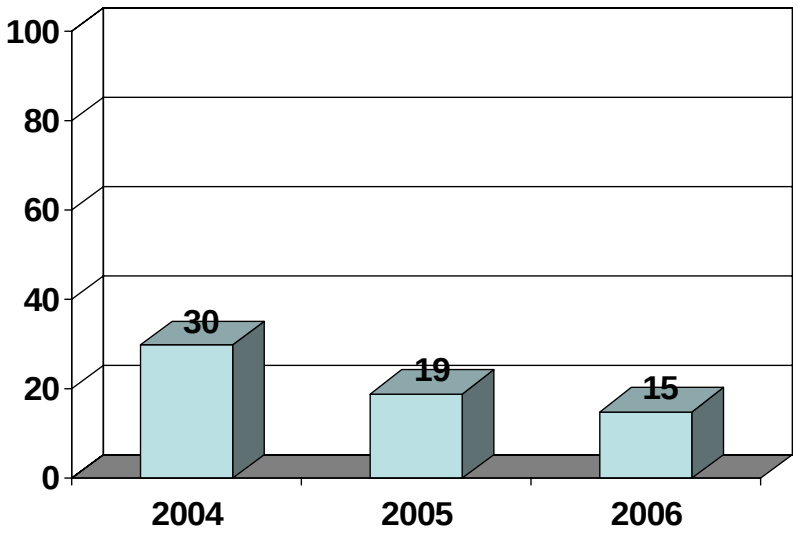
- May require mental model shift, culture change

2006 e-Crime Watch Survey

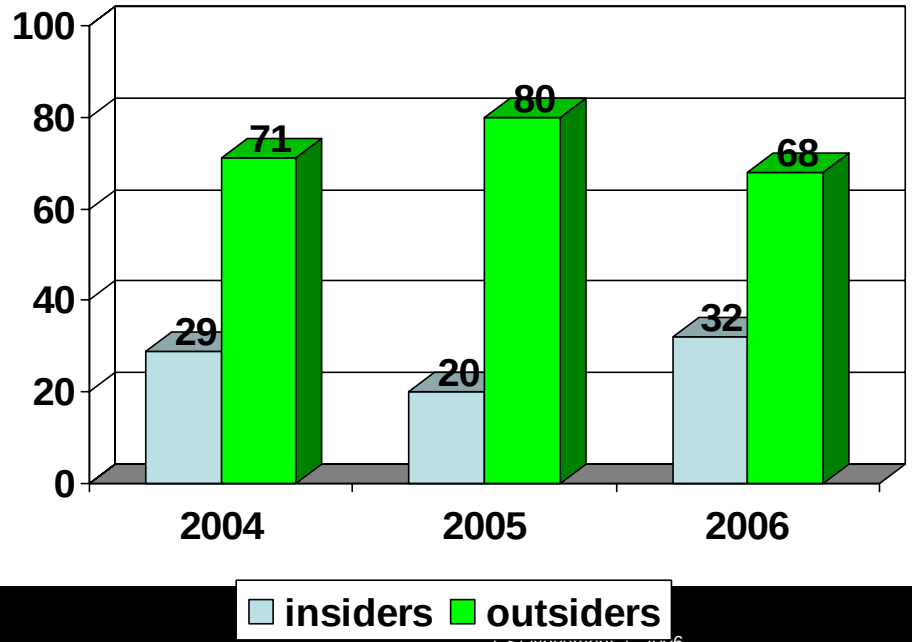
CSO Magazine, USSS & CERT

434 respondents

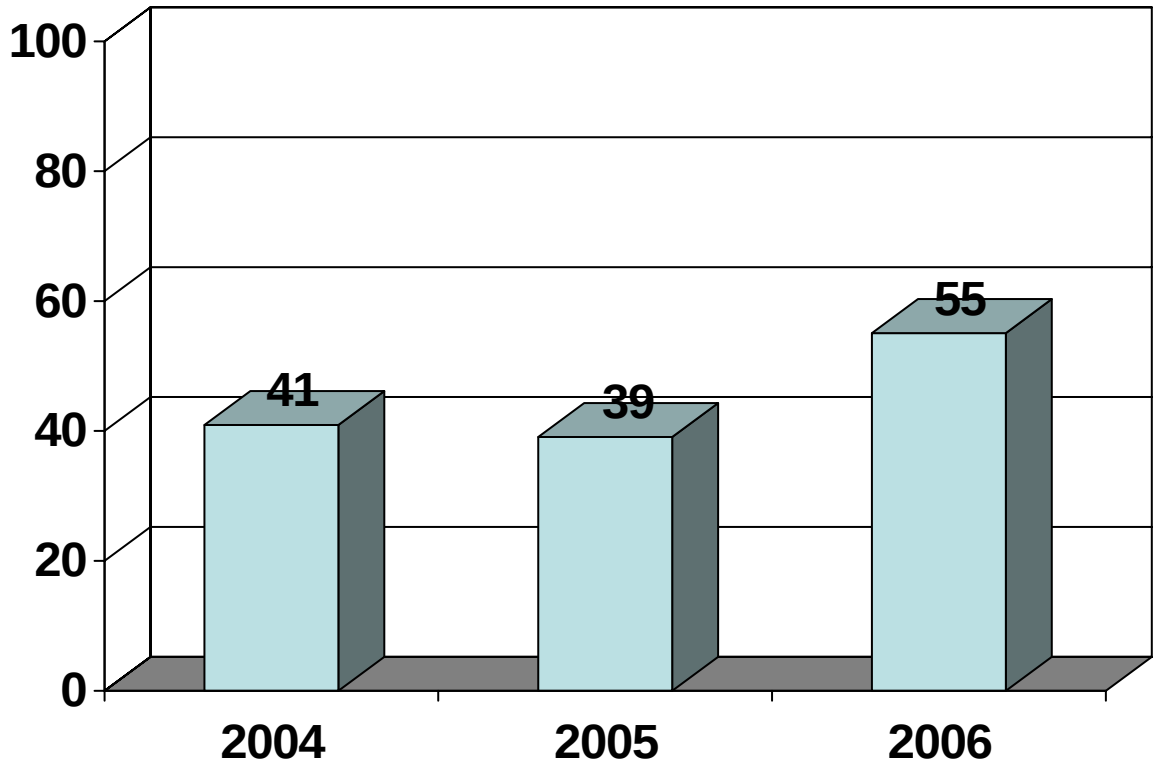
Percentage of Incidents With no Source Identified



Percentage of insiders versus outsiders



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



Overview of Insider Crimes

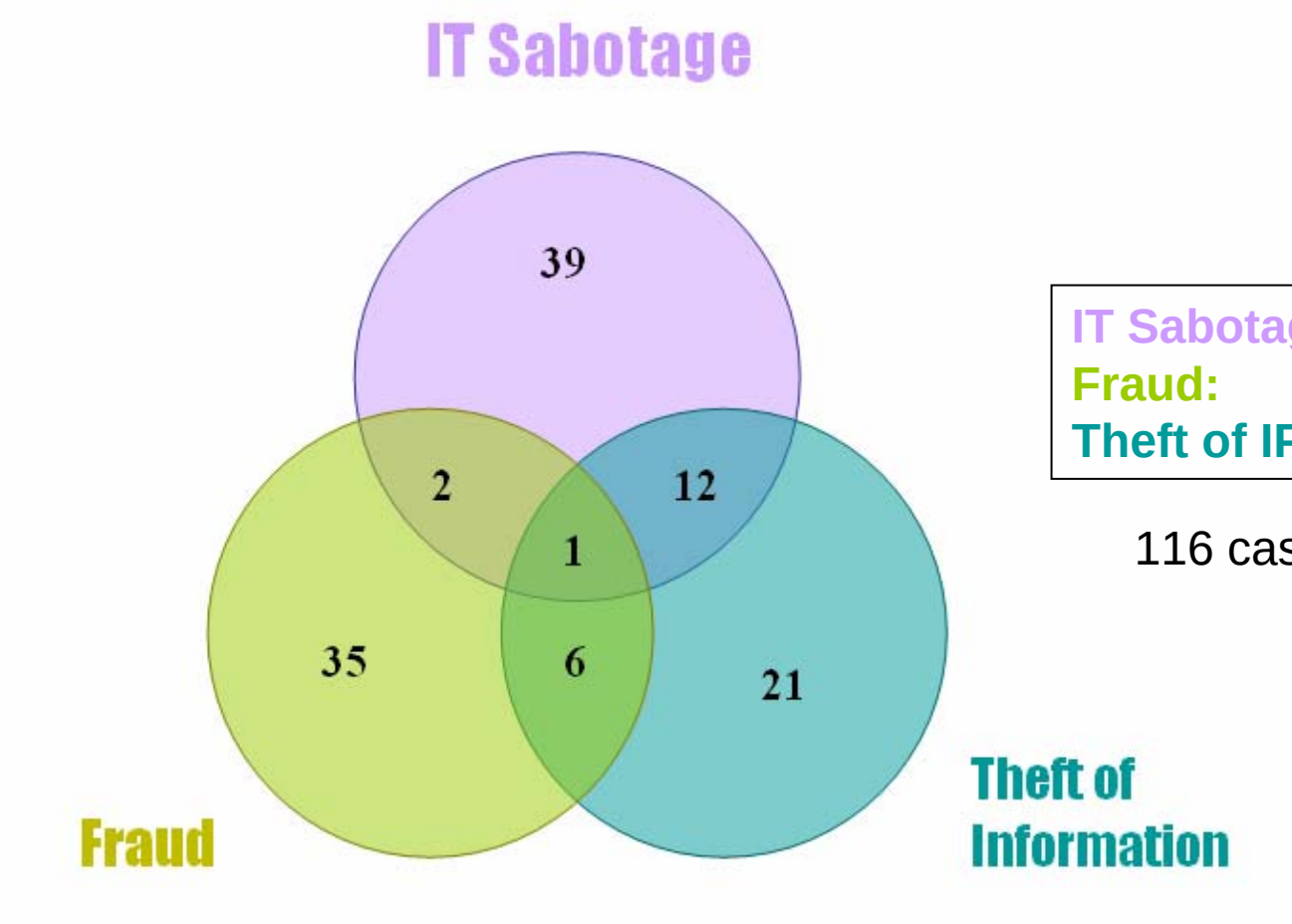
Types of Insider Crimes

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.

Insider Threat Study Case Breakdown



IT Sabotage:	54
Fraud:	44
Theft of IP:	40

116 cases total

Typical Fraud Incidents

Who were they?

- Current employees
- Half male; half female
- Non-technical; non-management positions

Why did they do it?

- Greed

How did they attack?

- Many had privileged access
- Only legitimate user commands
- Used their own username & password
- Acted during working hours from within the workplace

Typical Fraud Incidents - 2

How was it detected?

- System irregularity
- Non-technical means

How was the insider identified?

- System logs

What were the impacts?

- Financial impacts to employer
- Impacts to innocent victims

Typical Theft of Confidential Information Incidents

Who were they?

- Current employees (but almost half of them had already accepted another position)
- Male
- Over half held technical positions

Why did they do it?

- Financial
- Entitlement (some didn't realize it was wrong)
- Disgruntled

How did they attack?

- Used their own username & password, but half also compromised an account
- Acted during working hours from within the workplace

Typical Theft of Confidential Information Incidents - 2

How was it detected?

- Non-technical means
- Half by system irregularity

How was the insider identified?

- System logs

What were the impacts?

- Financial impacts to employer
- Organization & customer confidential information revealed
- Trade secrets stolen
- Innocent victim murdered
- Insider committed suicide

Typical IT Sabotage Attack

Who were they?

- Former employees
- Male
- Highly technical positions

Why did they do it?

- Disgruntled
- Revenge for negative work-related event

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

Typical IT Sabotage Attack - 2

How was it detected?

- Manually by non-security personnel
- System failure or irregularity

How was the insider identified?

- System logs
- Most took steps to conceal identity and/or actions

What were the impacts?

- Inability to conduct business, loss of customer records, inability to produce products
- Negative media attention
- Private information forwarded to customers, competitors, or employees
- Exposure of personal or confidential information
- Web site defacements
- Many individuals harmed

Insider Case Exercise

Ian Archer's Attack of iAssemble, Inc.

We will hand out a description of a fictional but representative case.

Please take a few minutes to review the case description.

We will be leading an interactive discussion of this case.

iAssemble Case Timeline

1997

iAssemble established – Eagles and Thompson partners, and Archer employed

Archer builds network and computing support for critical iAssemble processes

Fall 2000

Archer's father diagnosed with lung cancer

Archer looses driver's license for DUI

Winter 2000-2001

Adams hired as lead administrator

Archer moves all programs off of local workstations and onto central server

Allen hired as junior administrator to work with Archer

Archer tests malicious program four times at work on test server

iAssemble Case Timeline (cont.)

Spring 2001

Allen shares password with Archer

Formal complaint filed by coworker against Archer for harassment

Archer reprimanded

Summer 2001

Archer begins interviewing for other jobs

Archer creates backdoor; intimidates coworker out of backup tapes

Archer fired; remote access via Allen's account; logic bomb planted via backdoor

Law enforcement brought in; forensics examination started

Aftermath

Archer indicted in Fall 2001; convicted Spring 2002. Company never recovered.

Questions & Discussion

Questions about Case

Why did Archer attack iAssemble?

Why was Archer able to harm iAssemble's systems after firing?

What could iAssemble have done to prevent the attack?

What should iAssemble do in the future?

Why did Archer attack iAssemble?

Key Concepts

Unmet expectation as origin of disgruntlement

- What can cause expectation to grow?
- What other types of unmet expectation might lead to disgruntlement?

Predisposition to attack

- What personal risk factors might have indicated that Archer was predisposed to attack?

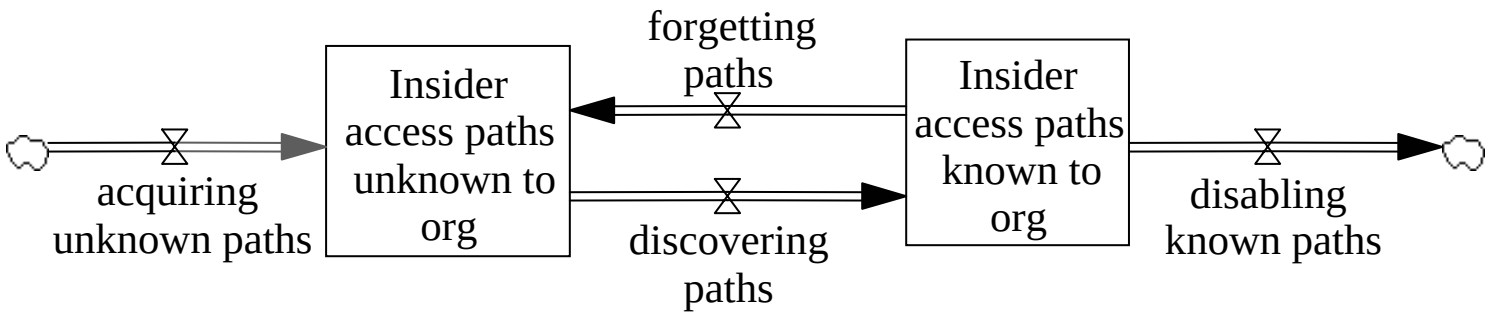
Why was Archer able to harm iAssemble after firing?

Key Concepts

Access path

- A sequence of one or more access points that lead to a critical system

An organization may not know about all of the access paths to its critical systems.



What could iAssemble have done to prevent the attack?

Key Concepts

Behavioral precursors

- Actions (offline) by the insider that might indicate an increased risk of cyber attack

Technical precursors

- Online actions by the insider that might involve setting up the attack

What should iAssemble do in the future?

iAssemble Case Summary

Questions about Case

Why did Archer attack iAssemble?

Why was Archer able to harm iAssemble's systems after firing?

What could iAssemble have done to prevent the attack?

What should iAssemble do in the future?

iAssemble Case Lessons (Behavioral)

Management should recognize potential impact of negative work-related events, e.g.

- New supervisor
- Layoffs
- Start or end of new project
- Change in salary/bonus structure

Management must be alert for behavioral precursors

Management should increase auditing and monitoring for technical preparatory actions

Bottom line: Management must understand and pay attention to the conditions that increase risk of insider threat.

iAssemble Case Lessons (Technical)

Management must recognize technical precursors

Ability to disable access must be on-demand and absolute (particularly for system administrators & privileged users)

- Negative events like demotion and firing are critical points

But this is often easier said than done

- Disabling access requires management to understand access paths available to insider
  - Management's understanding depends on rigorous access management practices
    - Practices tend to degrade over time without regular reinforcement
      - It takes time to recover from poor access management practices

Bottom line: Proactive, ongoing access management needed

MERIT

Management and Education of the Risk of Insider Threat

Funded by CyLab

Develop models of insider IT sabotage

Communicate the multi-disciplinary nature of problem

- Problem and mitigation requires analysis of policies, practices, technologies over time

Develop innovative training materials

Help organizations understand how they need to work across departments to mitigate the insider sabotage risk

- May require mental model shift, culture change

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).

Summary of Sabotage Crimes

- Constructed or downloaded, tested, planted logic bomb
- Deleted files, databases, or programs
- Destroyed backups
- Revealed derogatory, confidential, or pornographic information to customers, employees, or public
- Modified system or data to present pornography or embarrassing info
- Denial of Service by modifying authentication info, deleting data, or crashing systems
- Modified system logs to frame supervisor or innocent person & conceal identity
- Downloaded customer credit card data & posted to website
- Cut cables
- Sabotaged own project
- Physically stole computers and/or backups
- Planted virus on customers' computers
- Extortion for deleted data & backups
- Defaced organization's website
- Listed person as deceased in federal government database

Key Insider IT Sabotage Observations

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).

Agenda

Introductions

Background

- Evolution of CERT's Insider Threat Research
- Simultaneous PERSEREC Insider Threat Research

Interactive Case Example

Key Insider IT Sabotage Observations

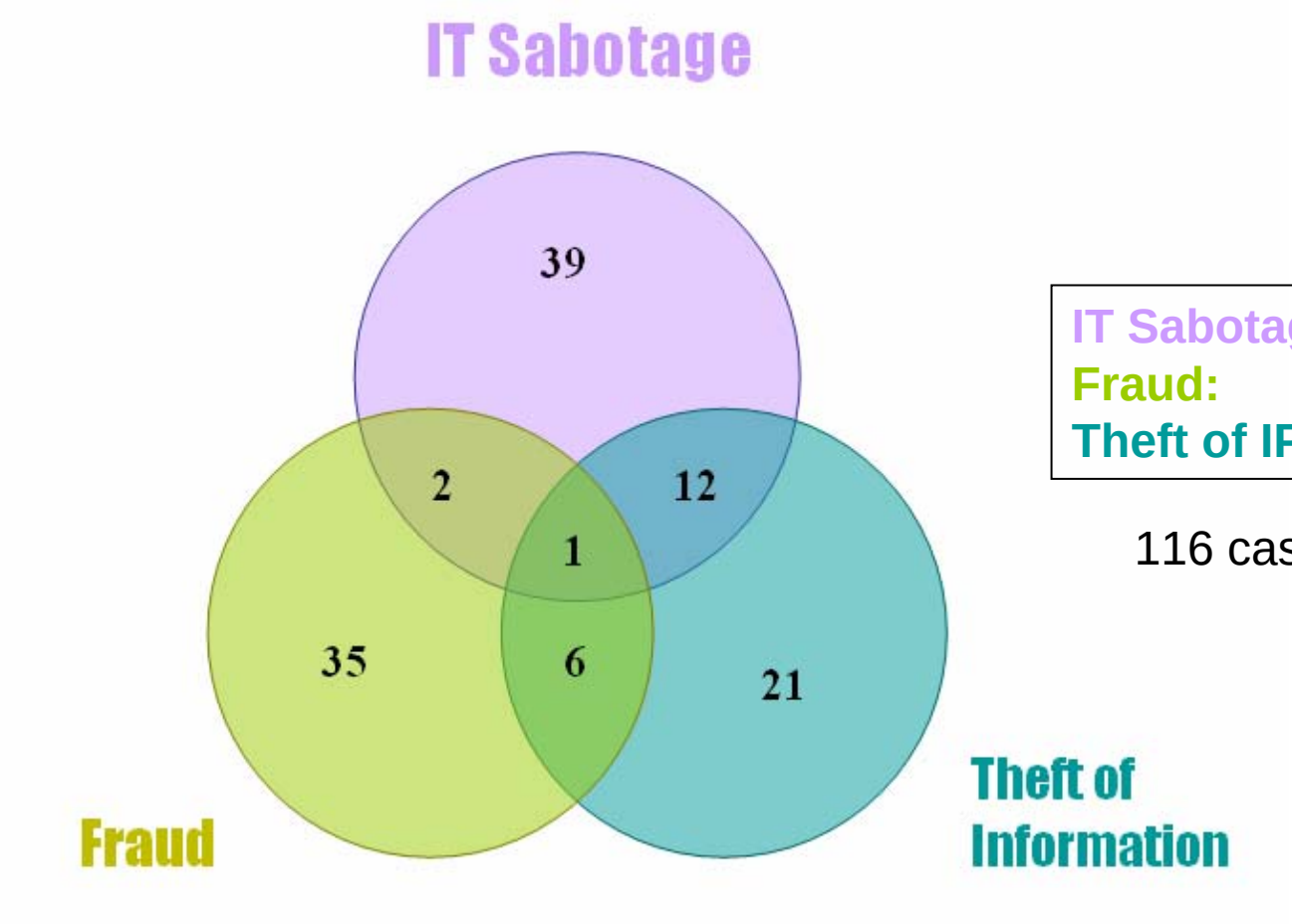
- Case Examples
- Statistics
- Observables

MERIT Model Overview

Best Practices

Future Work

Insider Threat Study Case Breakdown



IT Sabotage:	54
Fraud:	44
Theft of IP:	40

116 cases total

Who Were the Saboteurs?

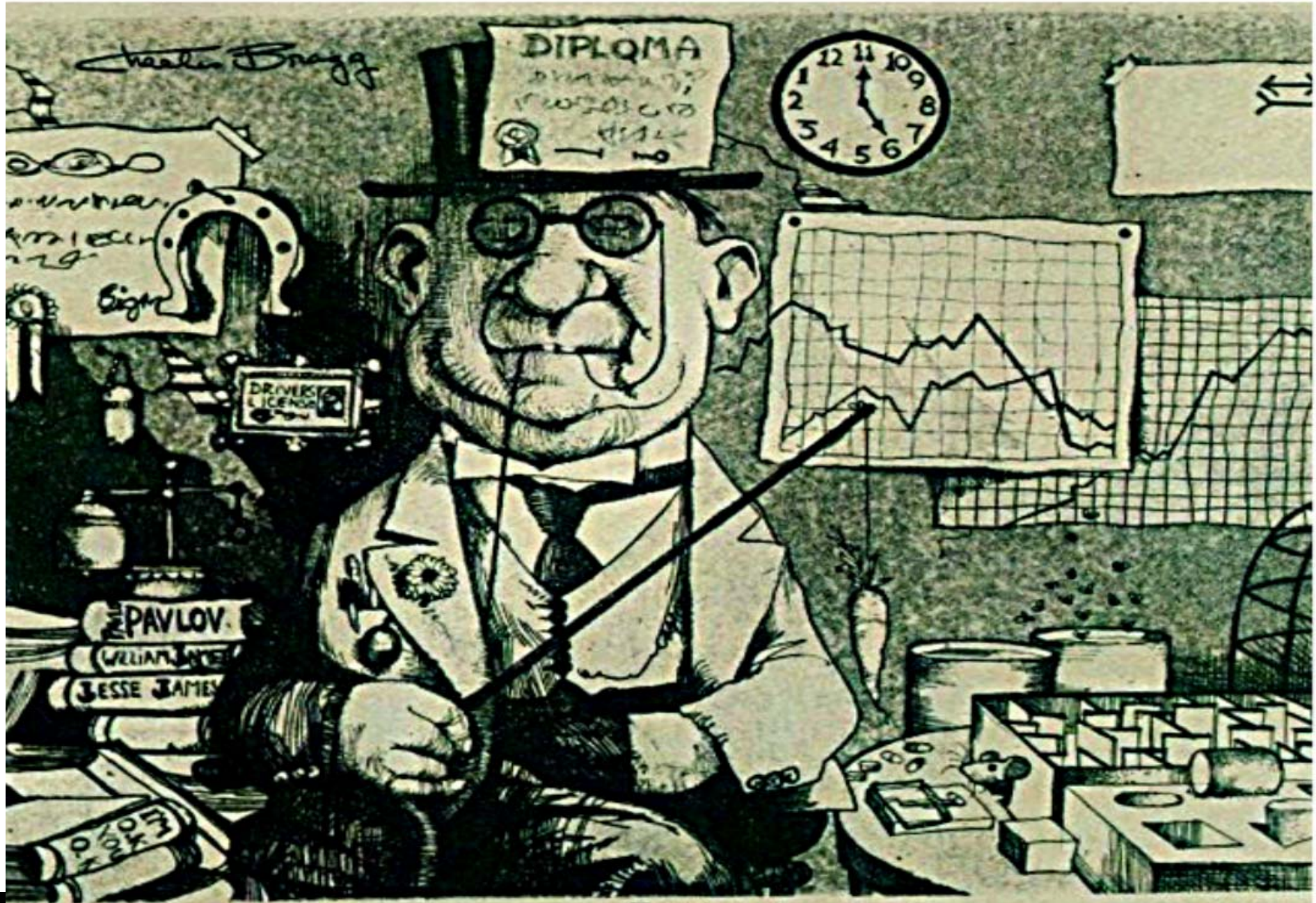
Age: 17 – 60

Gender: mostly males

Variety of racial & ethnic backgrounds

Marital status: fairly evenly split married versus single

Almost 1/3 had previous arrests



Psychologist

Observation #1:

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

Personal Predispositions

Serious mental health disorders

Personality problems

Social skills and decision-making biases

History of rule conflicts

Serious Mental Health Disorders

A diagnosed mental health problem for which treatment was recommended or sought.

Examples:

- Treated with anti-anxiety and anti-depressant medications
- Alcohol and drug addiction
- Panic attacks
- Mental health treatment for stress
- Physical spouse abuse
- Seizure disorder
- Examples: “Bill” and “Archer”

Personality Problems

Biased views of self and others that cause maladaptive relations.

Examples:

- Sensitivity to criticism & needs for attention
- Chronic frustration & feeling unappreciated
- Difficulties controlling anger with bursts of inappropriate temper
- Chronic sense of victimization or mistreatment
- Chronic grudges against others
- Grandiose/above the rules
- Subject is avoided by others or they “walk on eggshells” around him or her
- Bragging, bullying, spending on fantasy-related items
- Compartmentalizes
- Lack of conscience, impulse control, empathy for others, social impact
- Example: CTO

Social skills and Decision-Making Biases

Chronic withdrawal or conflicts with fellow workers, supervisors and security personnel.

Examples:

- Bullying and intimidation of fellow workers
- Refusal to confront supervisors with legitimate work-related complaints due to shyness while complaining to competitors
- Serious personality conflicts
- Unprofessional behavior
- Personal hygiene problems
- Inability to conform to rules
- Example: Silent hacker

History of Rule Violations

Past legal, security, or procedural violations.

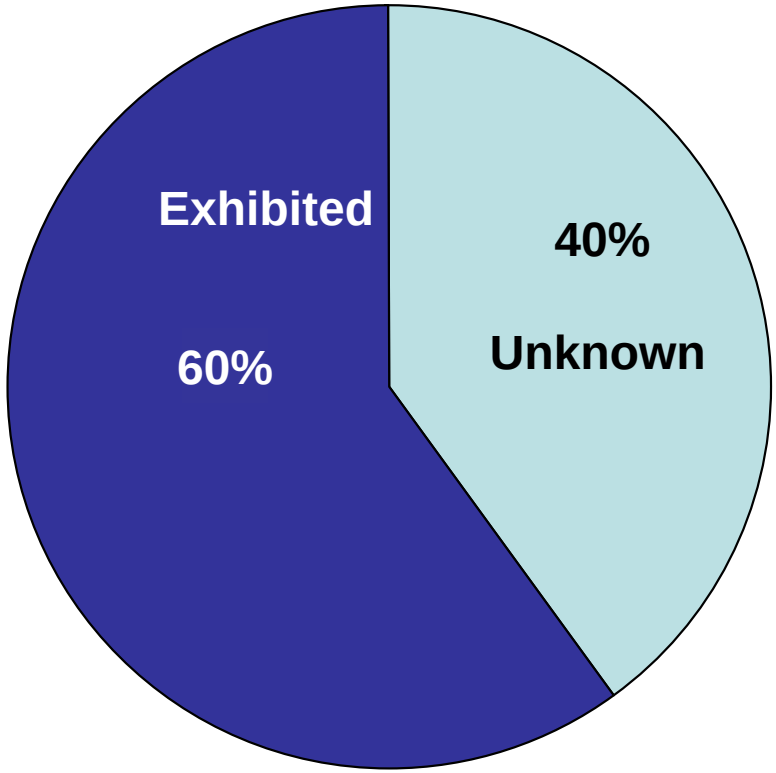
Examples:

- Arrests
- Hacking
- Security violations
- Harassment or conflicts resulting in official sanctions or complaints
- Misuse of travel, time, expenses
- Example: Heavy metal

Case Example – Observation #1

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

Personal Predispositions



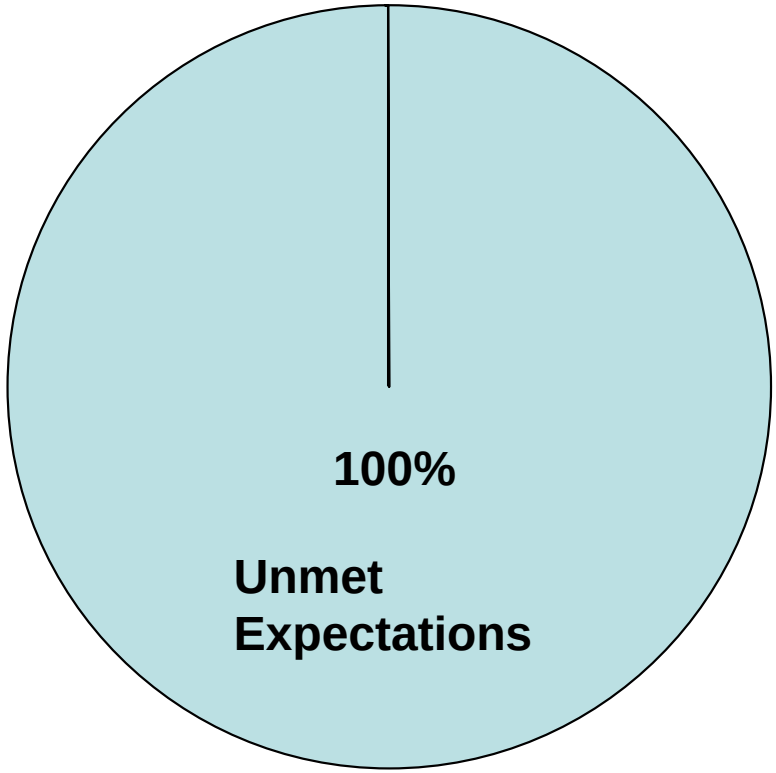
Observation #2:

Most insiders' disgruntlement is due to unmet expectations.

Case Example – Observation #2

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

Unmet Expectations



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

Unmet Expectations Observed in Cases

Salary/bonus

Promotion

Freedom of on line actions

Use of company resources

Privacy

Work ethic

Authority/ Responsibilities

Project requirements - deadlines, milestones

Job dissatisfaction

Supervisor demands

Coworker relations

Overestimated abilities

Access to information following termination

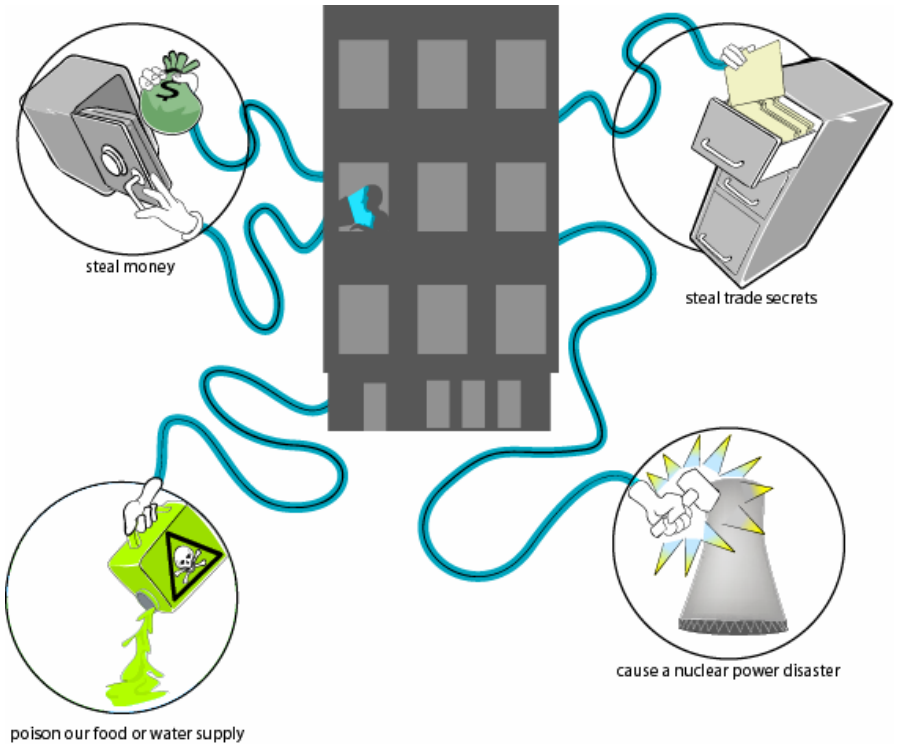
Unmet Expectations Generated by Personal Predispositions

Observation #3:

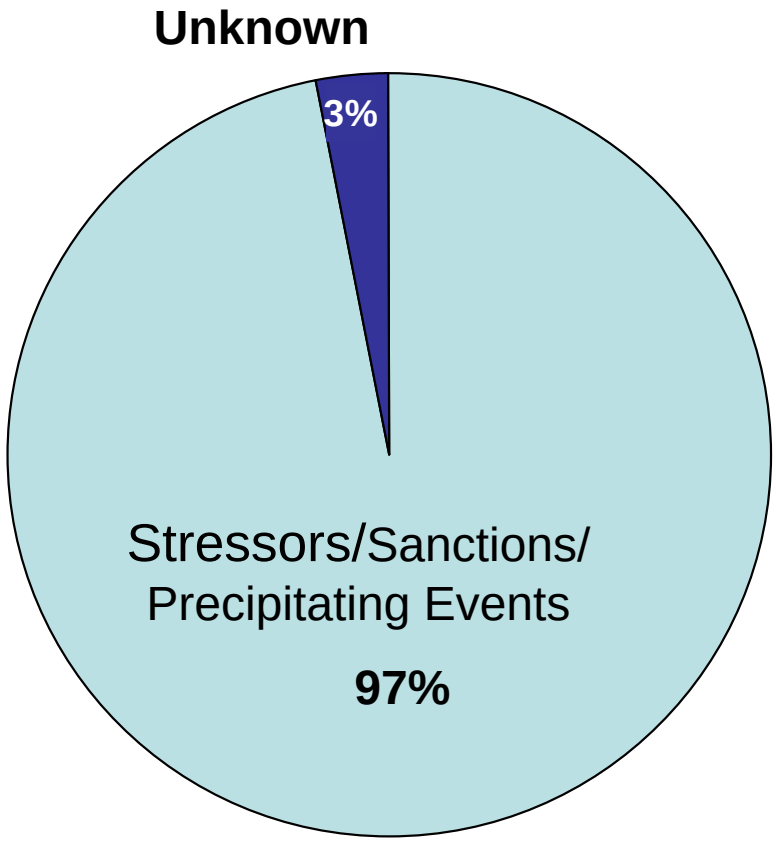
In most cases, stressors, including sanctions and precipitating events, contributed to the likelihood of insider IT sabotage.

Case Example – Observation #3

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



Stressors /Sanctions/Precipitating Events



Stressors/Sanctions/Precipitating Events Observed in Cases

Termination
- gross insubordination
- violation of company rules
- poor performance
- not being a team player
- false information on background check
- discussion about termination of employment

Sanctions
- Reprimands
  - work related issues
  - aggressive and malicious behavior
- Suspension for excessive absenteeism
- Demotion due to poor performance
- Responsibilities removed from projects
- Suspension of Internet access

Death in family ; Divorce

Financial
- Disagreement re: salary/compensation
- Bonuses lower than expected or removed
- Failure to offer severance package

Passed over for promotion

Disagreements
- with supervisor
- with colleagues

Transfer between departments

New supervisor hired

Access changed

Termination of subcontractor contract

Termination of partnership

Termination of other employees

Outsourcing of project

Demotion due to project completion

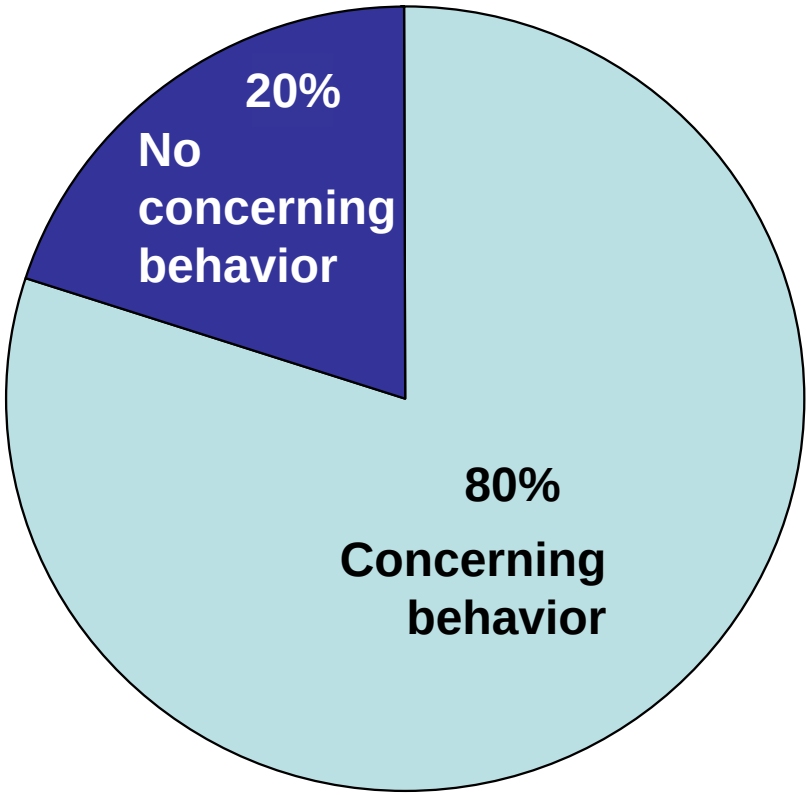
Observation #4:

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



Behavioral Precursors Observed in Cases

Drug use

Conflicts (coworkers, supervisor)

Aggressive or violent behavior

Web surfing, chat rooms at work

Mood swings

Bizarre behavior

Used organization's computers for personal business

Poor performance

EEO complaint

Absence/tardiness

Sexual harassment

Poor hygiene

Behavioral Rule Violations Ignored in Cases

- Inappropriate purchases on company accounts
- Lack of background / reference / employment references
- Lied about professional certifications
- Poor work habits
- Irregular hours
- Drinking / smoking on the job
- Sexist comments to co-workers
- Excessive unproductive time
- Worked from home against company policy
- Propositioned co-workers with numerous computer ventures - using organization resources
- Violated dress code

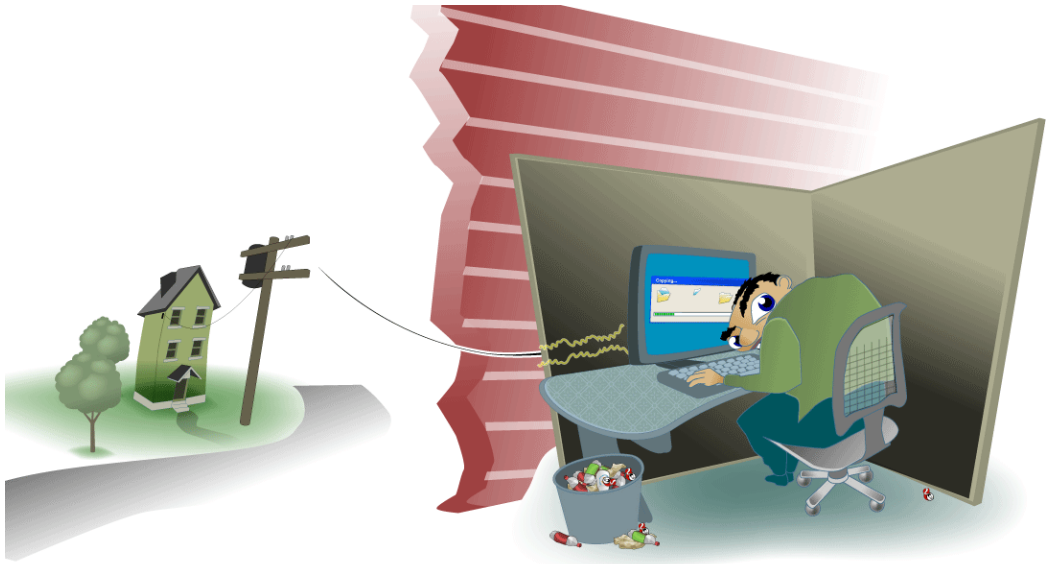
Observation #5:

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

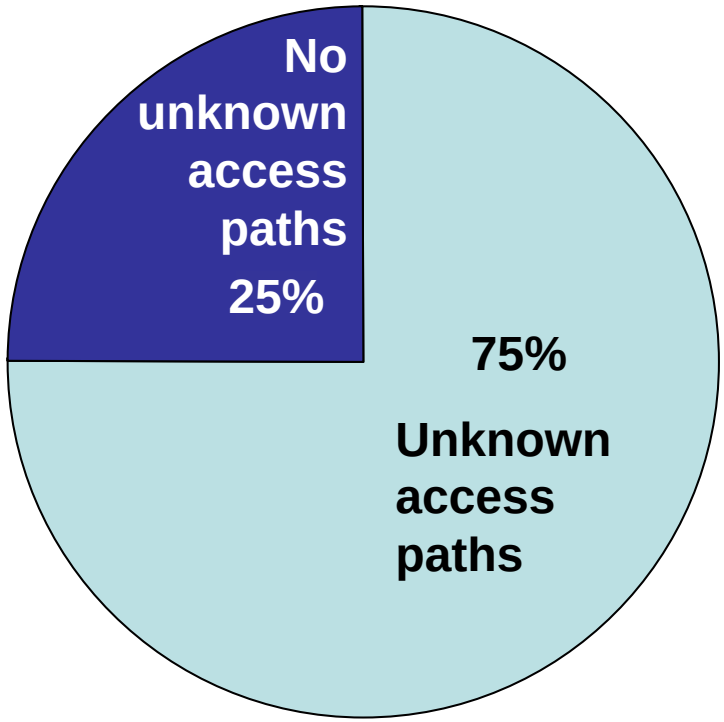
The majority attacked after termination.

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



Unknown Access Paths Observed in Cases

- Planted logic bomb while still employed
- Created backdoors before termination or after being notified of termination
- Installed modem for access following termination
- Changed all passwords right before resignation
- Disabled anti-virus on desktop & tested virus
- Network probing
- Installed remote network administration tool
- Download and installation of malicious code and tools (e.g., password cracker or virus)
- Disabling of system logs & removal of history files

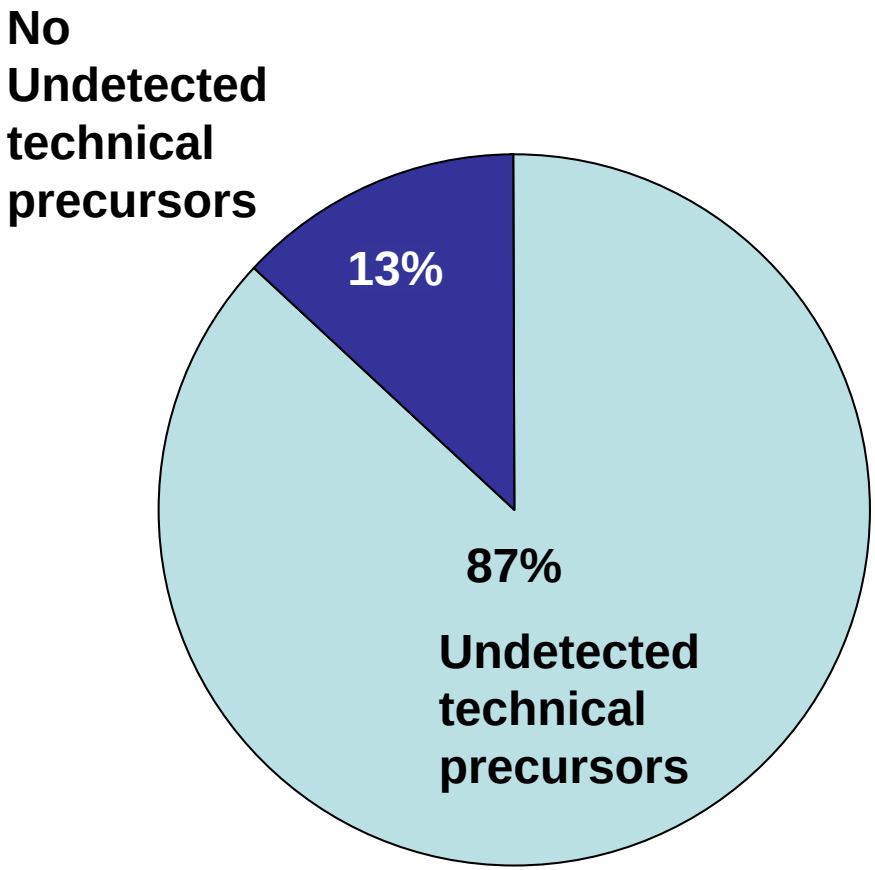
Observation #6:

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



Undetected Technical Precursors Observed in Cases

- Downloading and use of “hacker tools” such as rootkits, password sniffers, or password crackers
- Failure to create backups as required
- Failure to document systems or software as required
- Unauthorized access of customers’ systems
- Unauthorized use of coworkers machines left logged in
- Sharing passwords with others & demanded passwords from subordinates
- System access following termination
- Refusal to swipe badge to record physical access
- Access of web sites prohibited by acceptable use policy
- Refusal to return laptop upon termination
- Use of backdoor accounts
- Use of organization’s system for game playing, violating acceptable use policy
- Set up every new computer so he could access it remotely

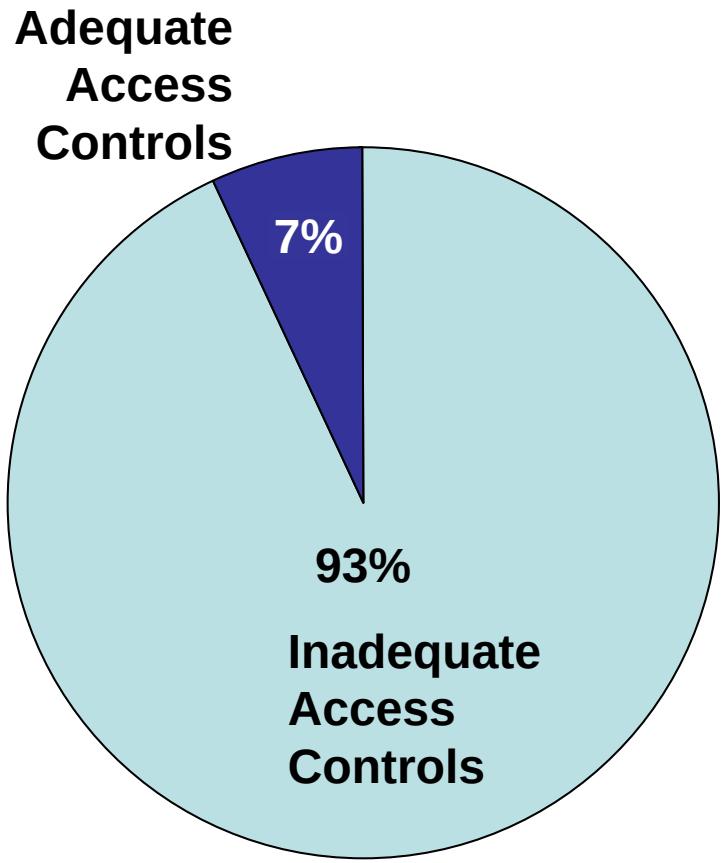
Observation #7:

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



Access Control Vulnerabilities Observed in Cases

- Access following termination
- Did not remove system administrator privileges
- Only physical access controls – no electronic
- Insider permitted to have sole copy of source code
- Physical & electronic access permitted the rest of the day after termination
- Ability to release changes to customer systems with no two man rule
- Insider permitted to retain computer account following termination (with reduced privileges)
- Insider able to release logic bomb to production system – no 2 man rule
- Use of coworker's computer left logged in unattended
- Insider never swiped badge
- Insiders created backdoor accounts that were not detected

MERIT Model Overview

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

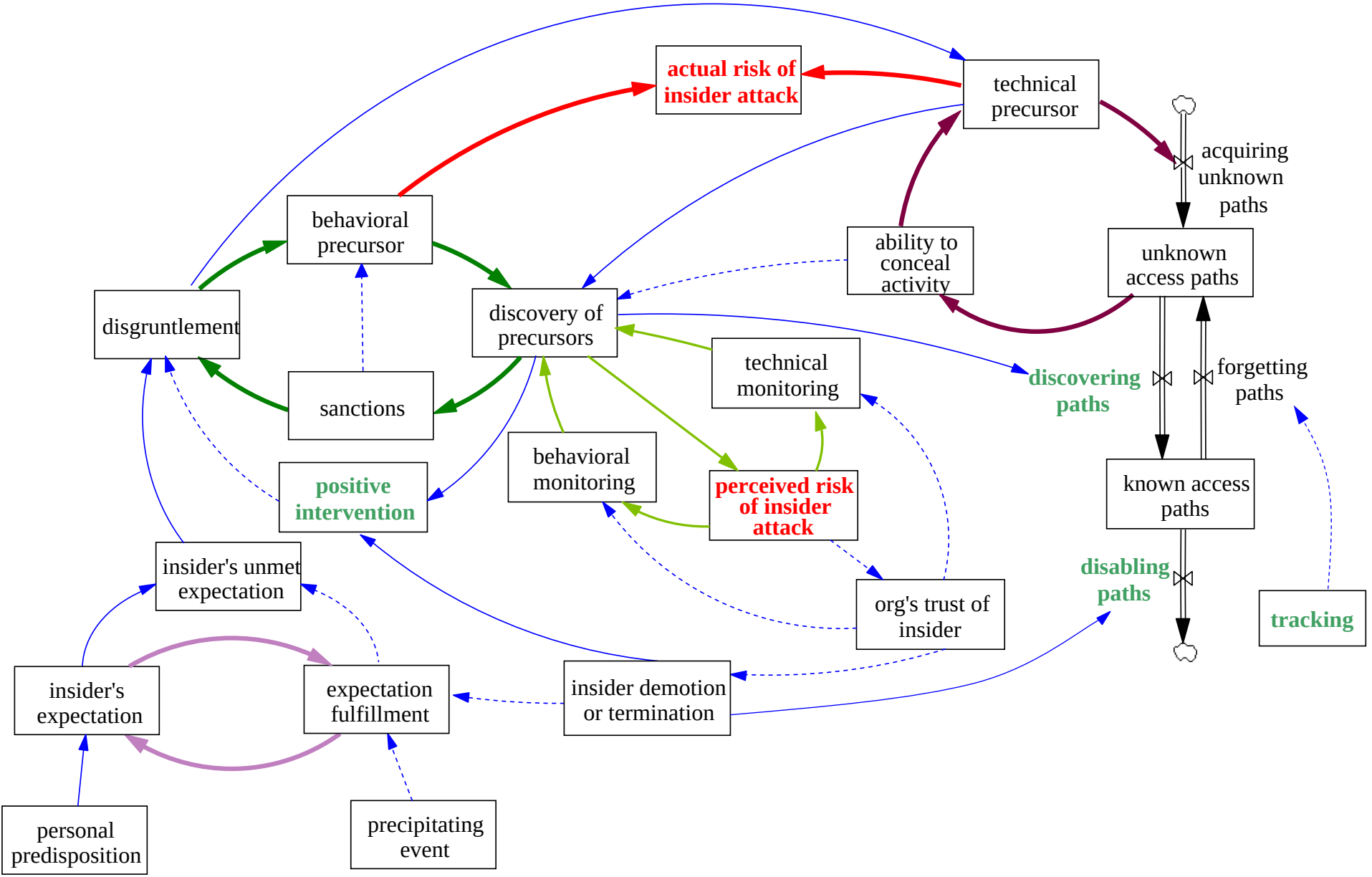
- Validate characterization of problem
- Test out alternate mitigation strategies

Model Exposition

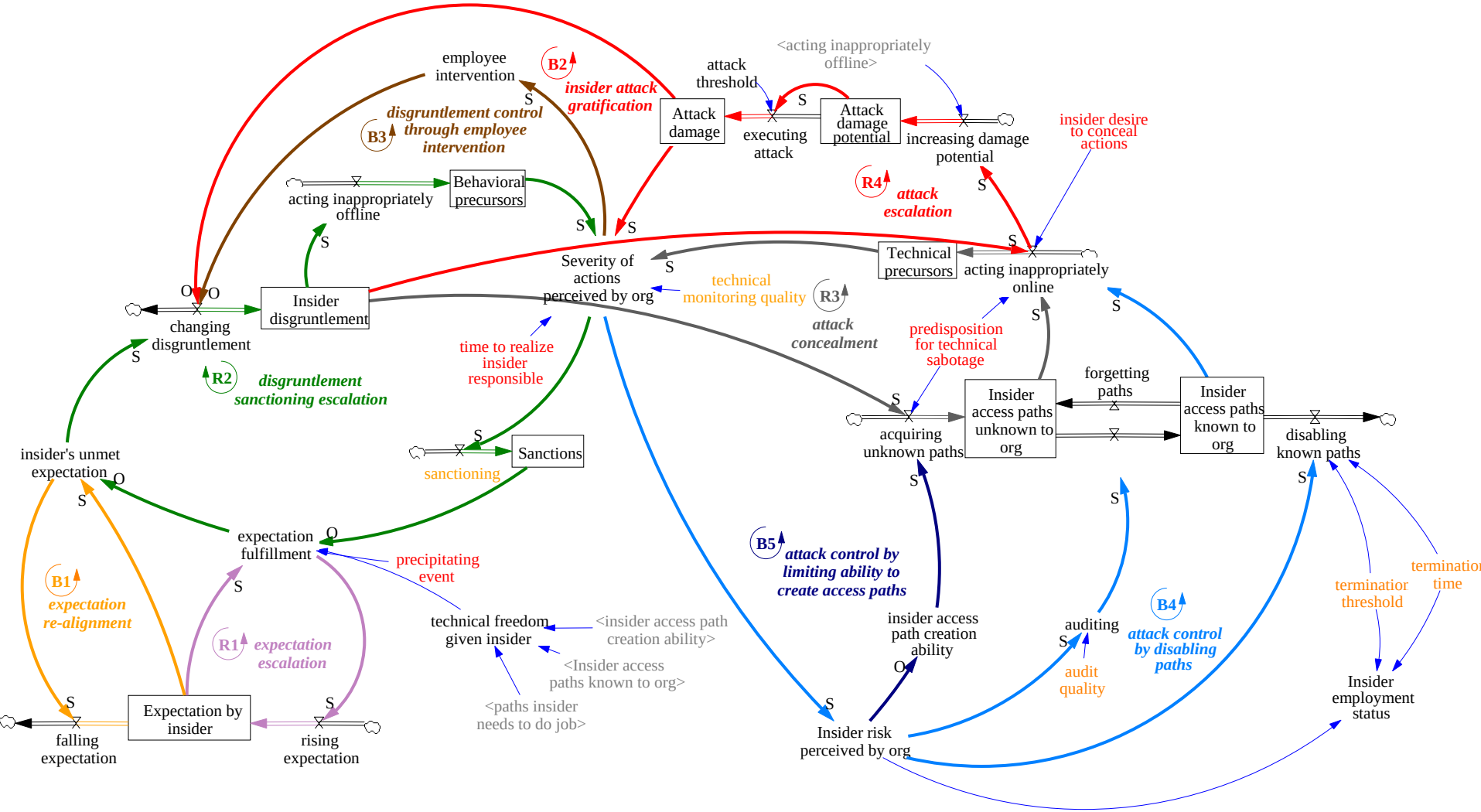
Our system dynamics model is described as a sequence of feedback loops that tells how the problem (i.e., insider sabotage) unfolds

- Each feedback loop describes a single aspect of the problem
- Multiple feedback loops interact to describe the complex nature of the problem

MERIT Model – Extreme Overview



MERIT Simulation Model



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.

Future Work

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

CERT Insider Threat Reports

CERT Insider Threat Website: http://www.cert.org/insider_threat/

Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors: http://www.cert.org/archive/pdf/insidercross051105.pdf

Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector: http://www.cert.org/archive/pdf/bankfin040820.pdf

Management and Education of the Risk of Insider Threat (MERIT): Mitigating the Risk of Sabotage to Employers' Information, Systems, or Networks: http://www.cert.org/archive/pdf/merit.pdf

*Common Sense Guide to Prevention and Detection of Insider Threats:*http://www.us-cert.gov/reading_room/prevent_detect_insiderthreat0504.pdf

2006 eCrime Survey: http://www.cert.org/archive/pdf/ecrimesurvey06.pdf

Other related Insider reports

Shaw, E.D. (2006) “The Role of Behavioral Research and Profiling in Malicious Cyber Insider Investigations,” Digital Investigation, The International Journal of Digital Forensics and Incident Response, Vol. 3, Elsevier Publications, Exeter, UK

Shaw, E.D. and Fischer, L. (2005) Ten Tales of Betrayal: An Analysis of Attacks on Corporate Infrastructure by Information Technology Insiders, ” Monterrey, CA.: Defense Personnel Security Research and Education Center.

Shaw, E.D. (2004). “The insider threat: Can it be managed?” In Parker, T. (Ed.), *Cyber Adversary Characterization: Auditing the Hacker Mind,* June. Syngress Publications,Rockland, Mass.

Shaw, E.D., & Stroz, E. (2004). WarmTouch software: Assessing Friend, Foe and Relationship.” In Parker, T. (Ed.), *Cyber Adversary Characterization: Auditing the Hacker Mind.* June. Syngress Publications, Rockland, Mass.

Points of Contact

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 – Email

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 – Email

Eric D. Shaw, Ph.D.
Consulting & Clinical Psychology, Ltd.
5225 Connecticut Ave. NW
Washington, DC 20015
202-686-9150
eshaw@msn.com

CERT Insider Threat Web Site:

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