Dealing with Insider Cybersecurity Threats: SEI Research and Perspectives

A Webinar co-sponsored by the Software Engineering Institute of Carnegie Mellon University and the Accredited Standards Committee X9, Financial Industry Standards

Robert Binder

Daniel Costa

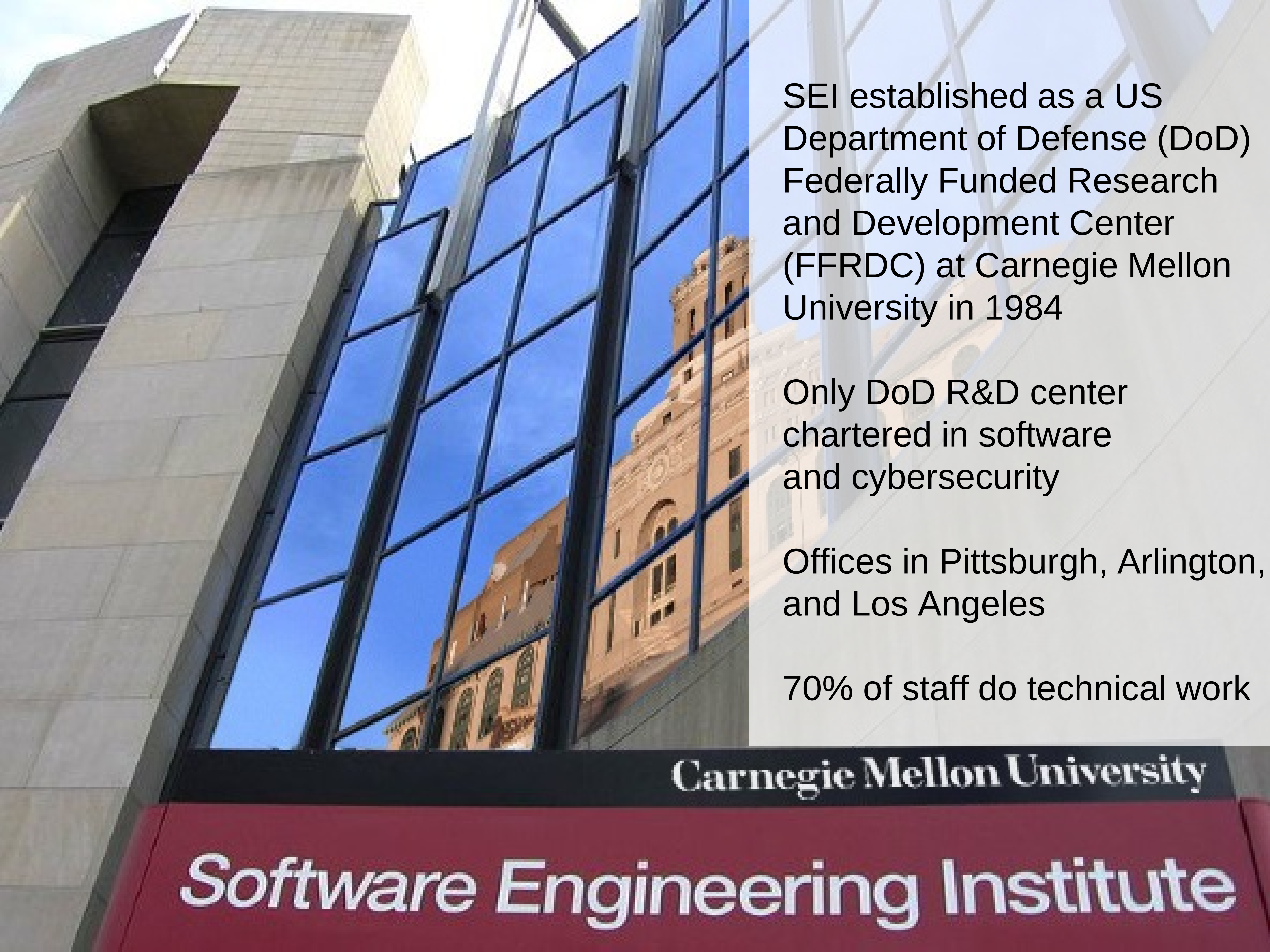
Andrew Moore

Jim Northey

Randy Trzeciak

Kurt Wallnau

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213



SEI established as a US Department of Defense (DoD) Federally Funded Research and Development Center (FFRDC) at Carnegie Mellon University in 1984

Only DoD R&D center chartered in software and cybersecurity

Offices in Pittsburgh, Arlington, and Los Angeles

70% of staff do technical work

Our Mission and Strategy

To support the Nation’s defense by advancing the science, technologies, and practices needed to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring.

We achieve our mission through

- Research
- Collaboration
- Development and Demonstration
- Transition

Focus on Assurance

Assured = Correct + Secure + Attainable

- **Correct:** the right system (validation), architected, built, and operating reliably (verification)
- **Secure:** hardened against known threats, resilient in operation to unknown threats
- **Attainable:** cost-effective (affordable), timely, and possible

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.

SEI CERT Division

The CERT Division produces, and transitions to the DoD technologies and practices that reduce the opportunity for—and limit the damage of—cyber attacks

Established in 1988 by the DoD on the heels of the Morris worm that wreaked havoc on the ARPANET

Focus areas include

- Cyber Science Foundations
- Digital Intelligence & Investigations
- Insider Threat
- Malware Analysis
- Resiliency
- Secure Coding
- Situational Awareness
- Workforce Development

Speakers

Moderators:

Bob Binder

- SEI Senior Engineer
- Co-Chair X9 D14
- Automated Testing SME

Jim Northey

- Ivititi Principal Services Consultant
- Co-Chair X9 D14
- FIX Protocol Global Technical Committee Chair

Panel:

Randy Trzeciak

- SEI Manager, Enterprise Threat and Vulnerability Management team

Daniel Costa

- SEI Insider Threat Technical Solutions Lead

Kurt Wallnau

- SEI Senior Member of the Technical Staff

Andrew Moore

- SEI Senior Member of the Technical Staff

Agenda

Randy Trzeciak

Insider Threats in the Banking & Finance Sector

Daniel Costa

Insider Anomaly Detection

Kurt Wallnau

Using Narrative Structures to Detect Insider Risks

Andrew Moore

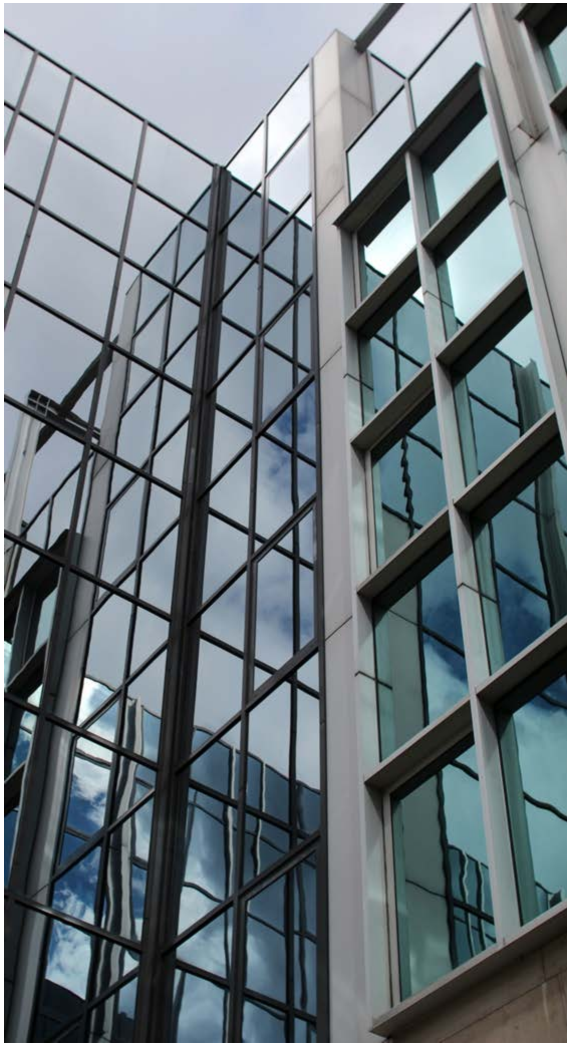
The Role of Positive Incentives in Reducing Insider Threats

Q&A

Insider Threats in the Banking & Finance Sector

Randy Trzeciak

The CERT Insider Threat Center

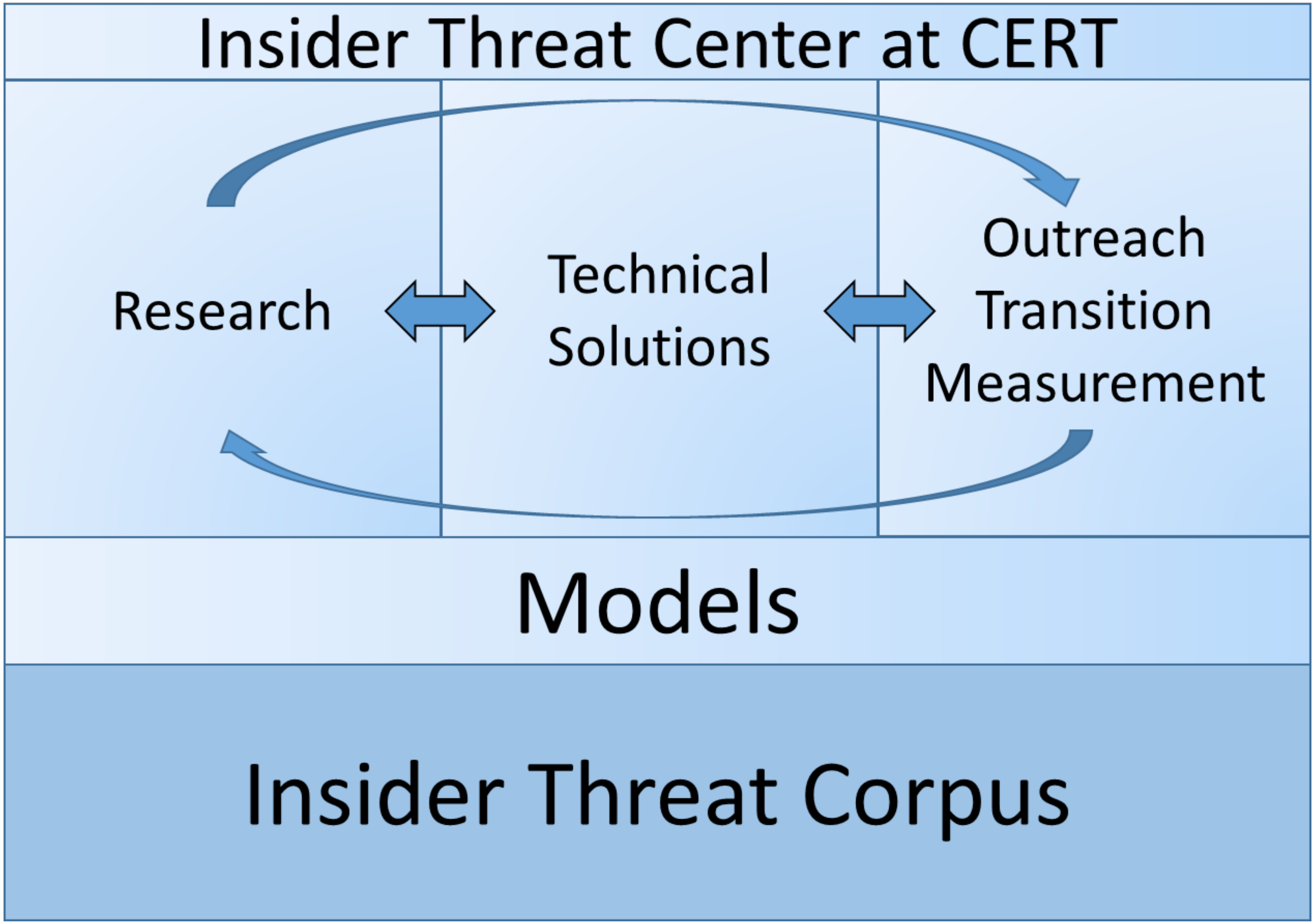


Center of insider threat expertise since 2001

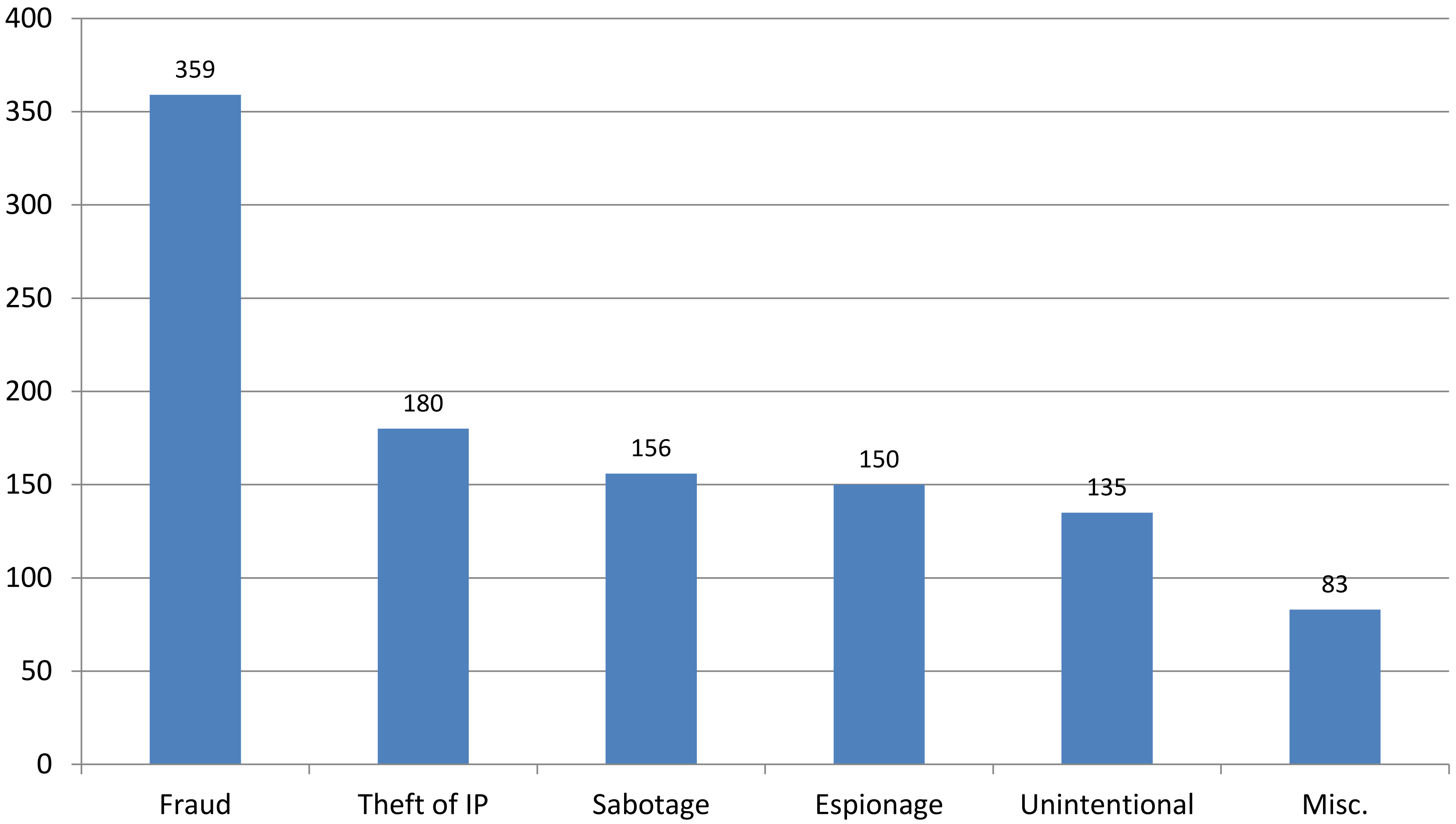
Mission: enable effective insider threat mitigation, incident management practices, and develop capabilities for deterring, detecting, and responding to evolving cyber threats

Action and Value: conduct research, modeling, analysis, and outreach to develop & transition socio-technical solutions to combat insider threats

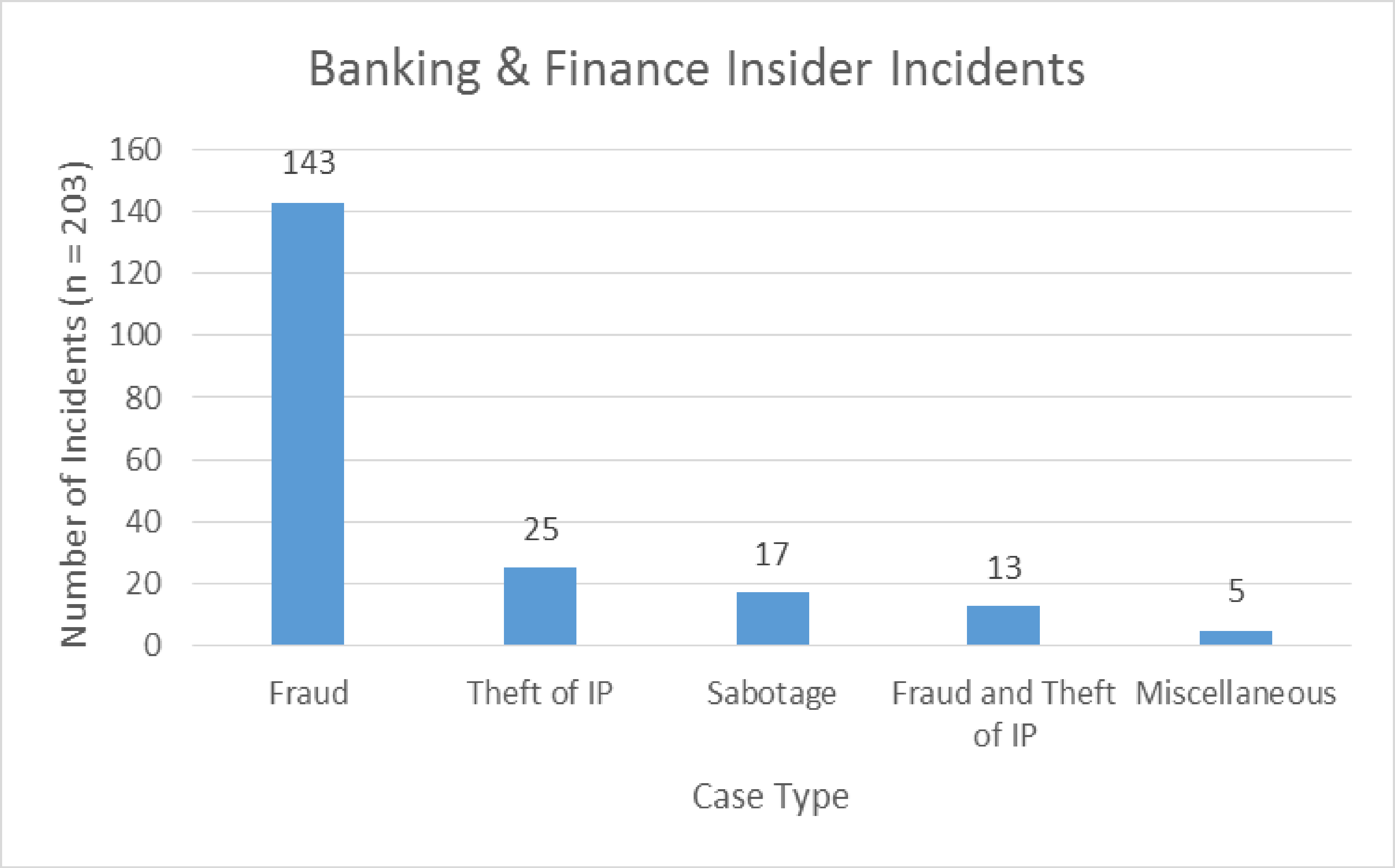
CERT's Unique Approach to the Problem



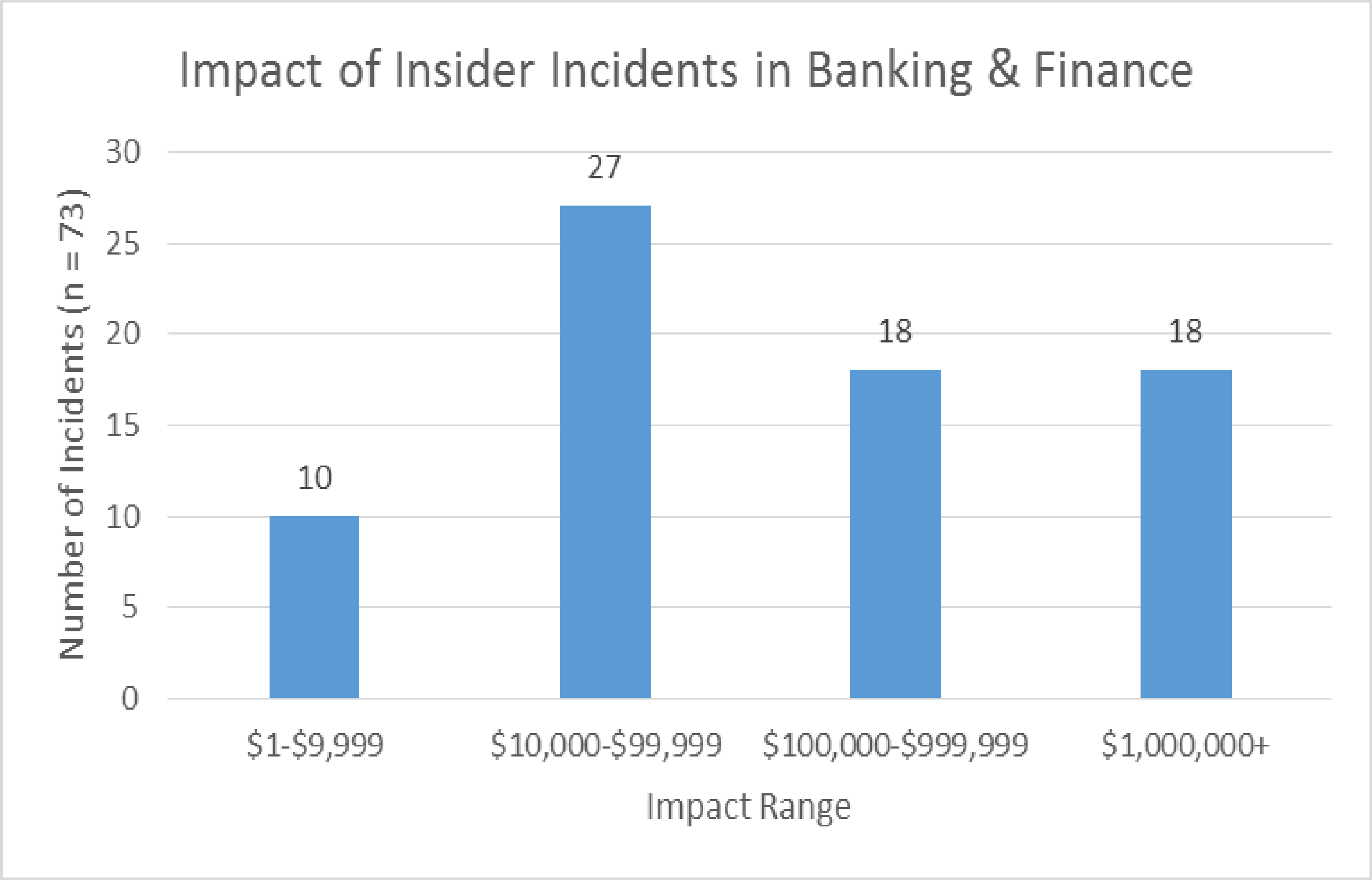
CERT’s Insider Incident Corpus



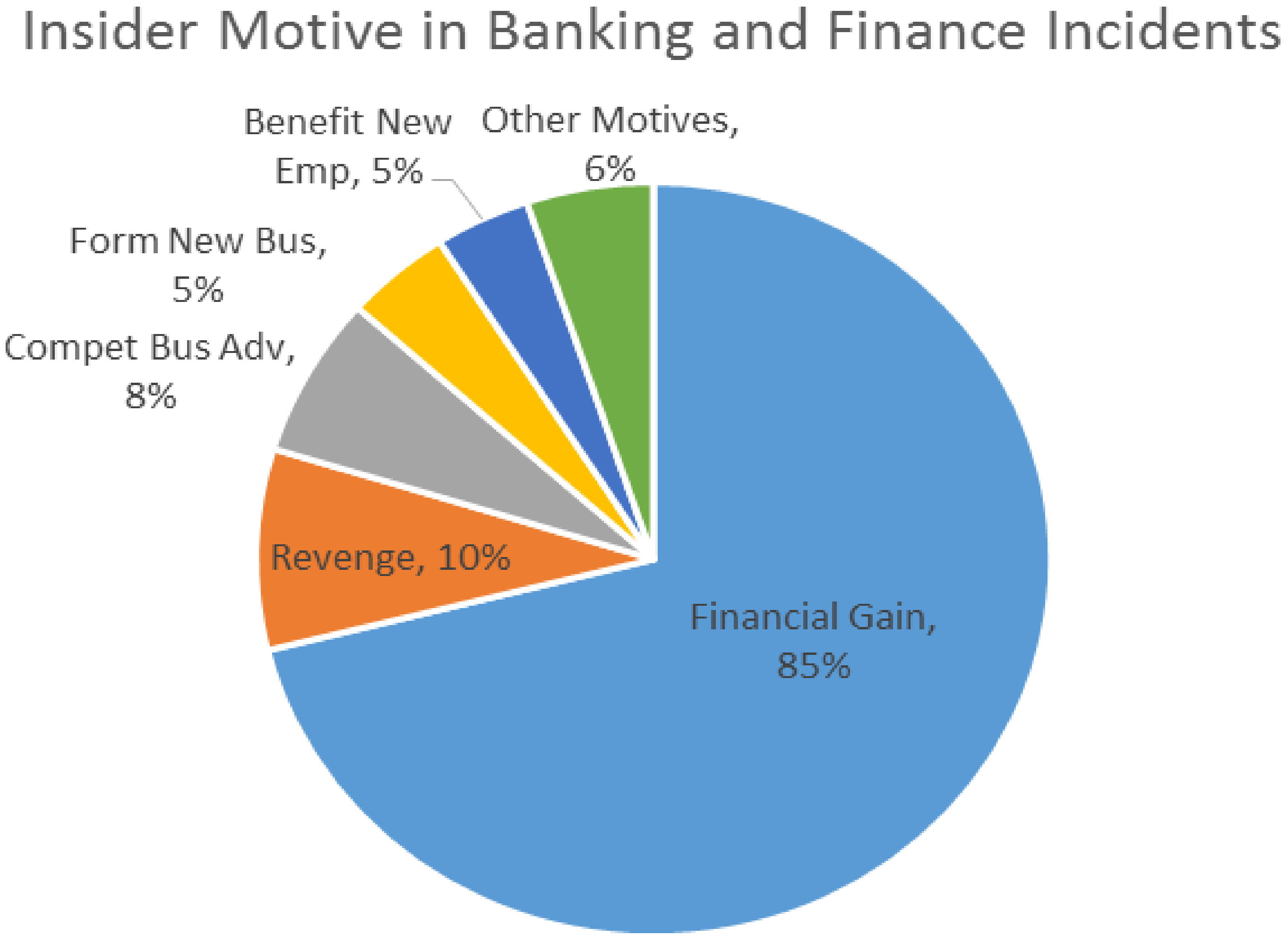
CERT’s Insider Incidents in B&F Sector



Financial Impact



Motivations



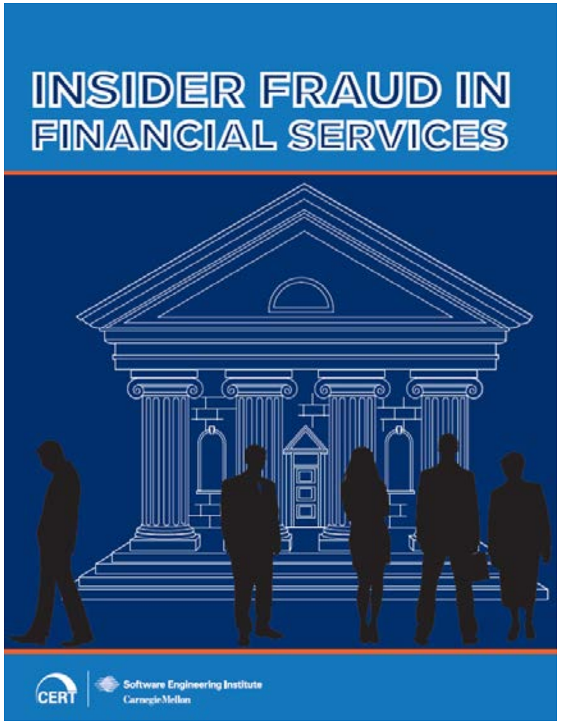
Insider Fraud Study

Funded by U.S. Department of Homeland Security (DHS) Science and Technology Directorate (S&T)

Conducted by the CERT Insider Threat Center in collaboration with the U.S. Secret Service (USSS)

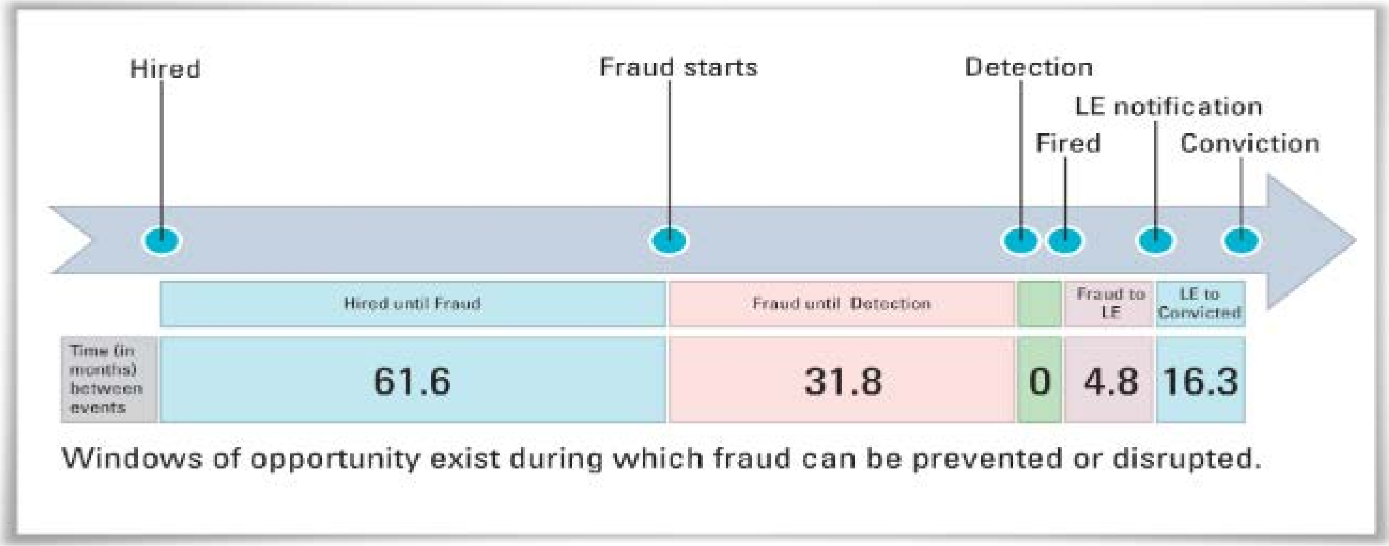
Full report: “Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector” (http://www.sei.cmu.edu/library/abstracts/reports/12sr004.cfm)

Booklet: “Insider Fraud in Financial Services” (http://www.sei.cmu.edu/library/abstracts/brochures/12sr004-brochure.cfm)


INSIDER FRAUD IN FINANCIAL SERVICES
CERT
Software Engineering Institute
Carnegie Mellon

Low and Slow

Criminals who executed a "low and slow" approach accomplished more damage and escaped detection for longer.



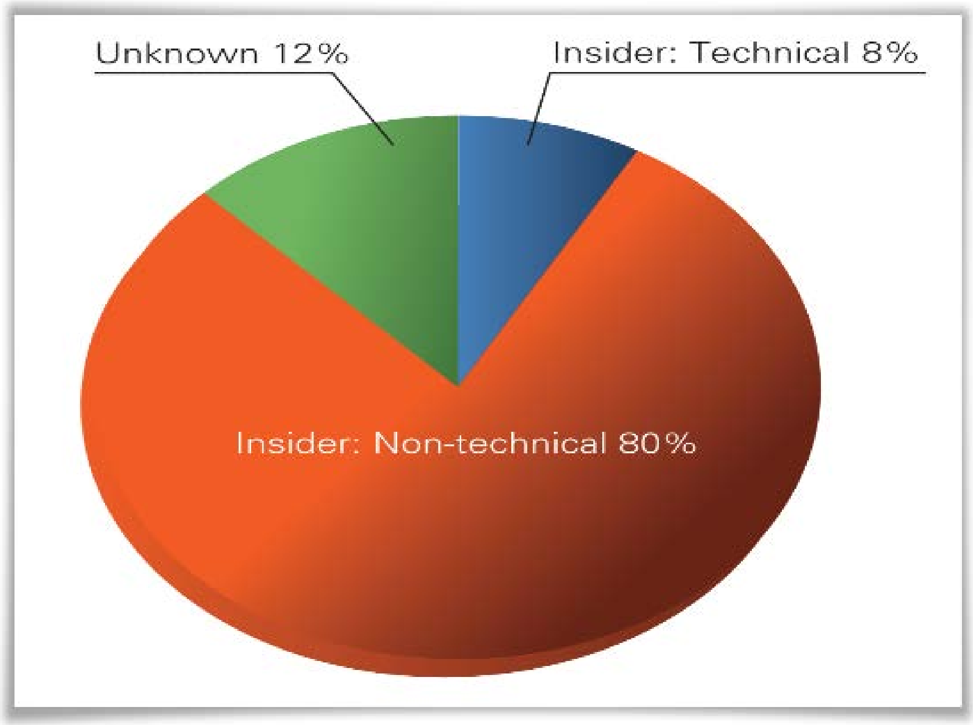
	Hired until Fraud	Fraud until Detection		Fraud to LE	LE to Convicted
Time (in months) between events	61.6	31.8	0	4.8	16.3

Windows of opportunity exist during which fraud can be prevented or disrupted.

There are, on average, over 5 years between a subject's hiring and the start of the fraud. There are 32 months between the beginning of the fraud and its detection.

Low-Tech

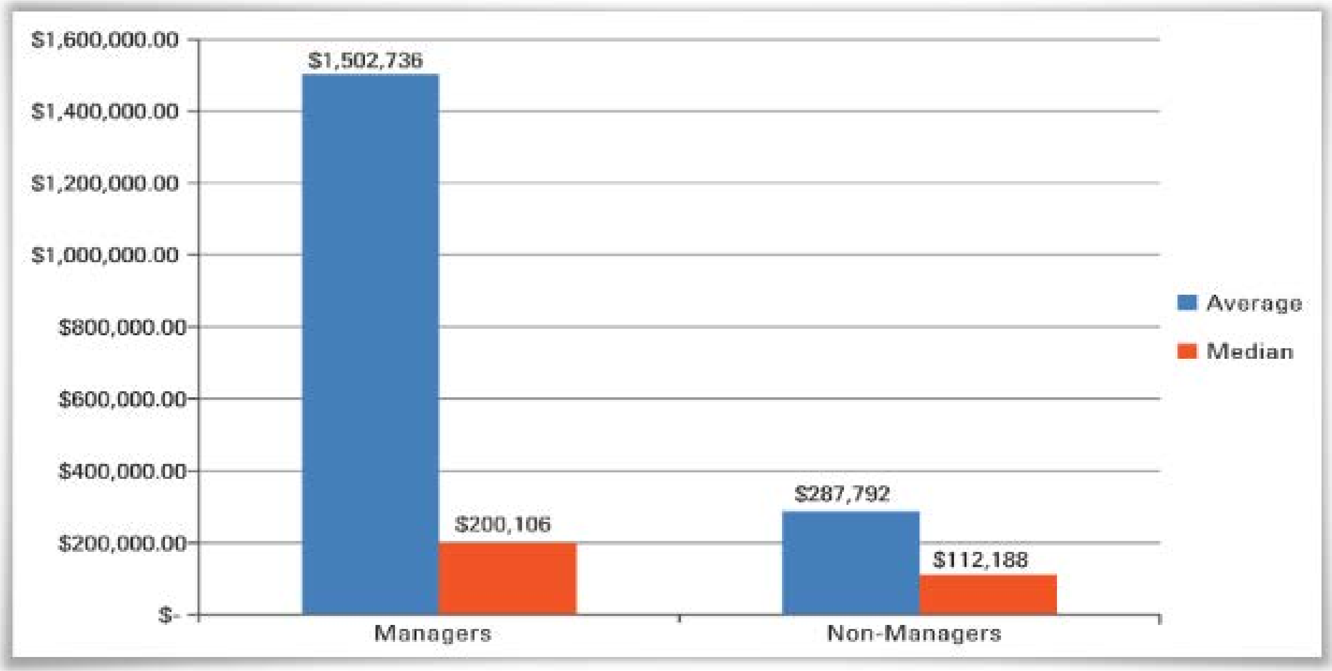
Insiders' means were not very technically sophisticated.



Non-technical subjects were responsible for 65 (81 percent) incidents. Seven were external attackers, but their methods were also non-technical.

Managers vs. Non-Managers

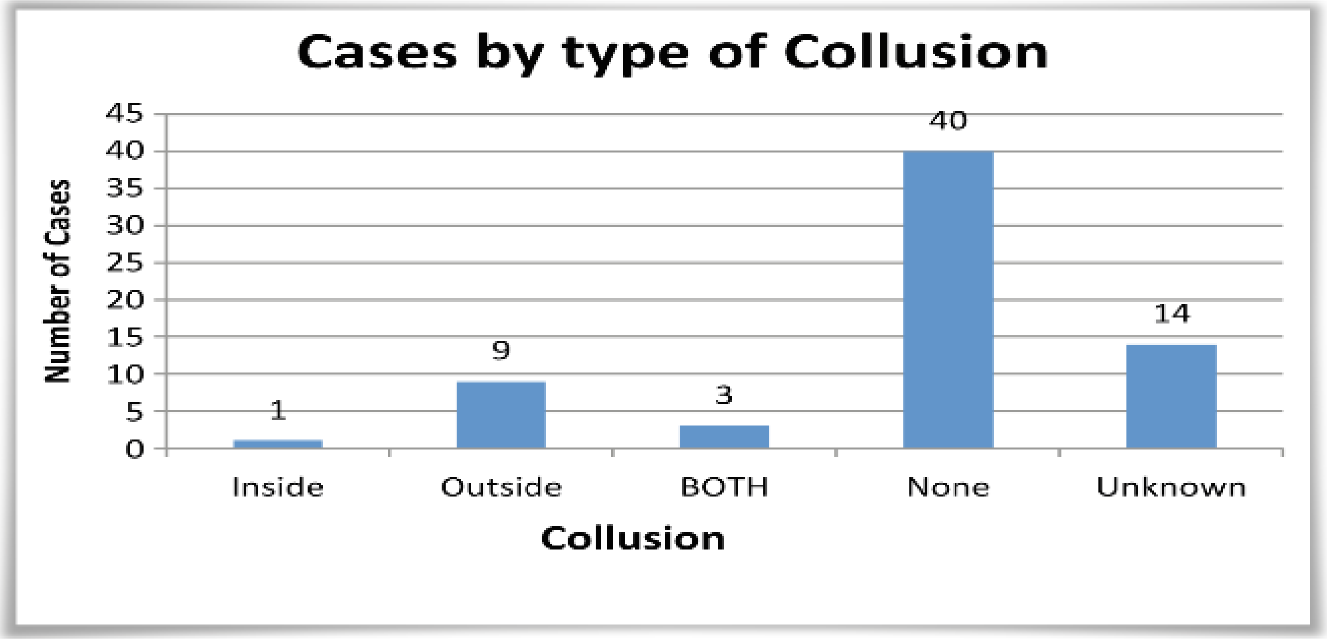
Fraud by managers differs substantially from fraud by non-managers by damage and duration.



Of 61 subjects, 31 (51 percent) were managers, VPs, bank officers, or supervisors. The median results show that managers consistently caused more actual damage ($200,106) than non-managers ($112,188).

Collusion

Most cases do not involve collusion.



There was not a significant number of cases involving collusion, but those that did occur generally involved external collusion (i.e., a bank insider colluding with an external party to facilitate the crime).

Audits, Complaints, and Suspicions

Most incidents were detected through an audit, customer complaints, or co-worker suspicions.

The most common way attacks were detected was through routine or impromptu audits.

Over half of the insiders were detected by other victim organization employees, though none of the employees were members of the IT staff.

As expected, most initial responders to the incidents were managers or internal investigators (75 percent).

Recommended Best Practices for Insider Threat Mitigation

1 - Know and protect your critical assets.	11 - Institute stringent access controls and monitoring policies on privileged users.
2 - Develop a formalized insider threat program.	12 - Deploy solutions for monitoring employee actions and correlating information from multiple data sources.
3 - Clearly document and consistently enforce policies and controls.	13 - Monitor and control remote access from all endpoints, including mobile devices.
4 - Beginning with the hiring process, monitor and respond to suspicious or disruptive behavior.	14 - Establish a baseline of normal behavior for both networks and employees
5 - Anticipate and manage negative issues in the work environment.	15 - Enforce separation of duties and least privilege.
6 - Consider threats from insiders and business partners in enterprise-wide risk assessments.	16 - Define explicit security agreements for any cloud services, especially access restrictions and monitoring capabilities.
7 - Be especially vigilant regarding social media.	17 - Institutionalize system change controls.
8 - Structure management and tasks to minimize unintentional insider stress and mistakes.	18 - Implement secure backup and recovery processes.
9 - Incorporate malicious and unintentional insider threat awareness into periodic security training for all employees.	19 - Close the doors to unauthorized data exfiltration.
10 - Implement strict password and account management policies and practices.	20 - Develop a comprehensive employee termination procedure.

Contact Information

Randy Trzeciak

Director, CERT Insider Threat Center

Telephone: +1 412.268.7040

Email: rft@sei.cmu.edu

Insider Anomaly Detection

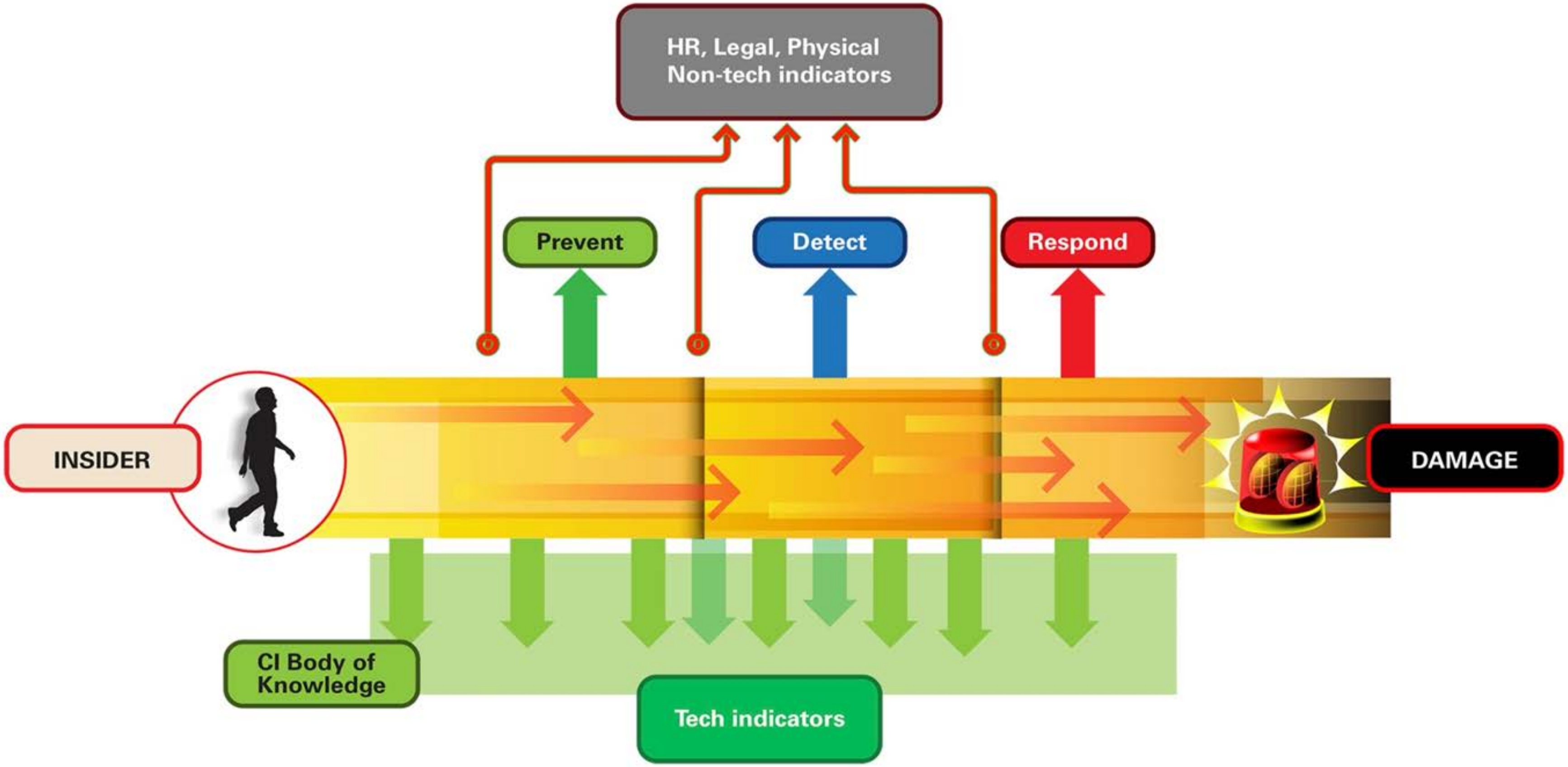
Daniel Costa

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

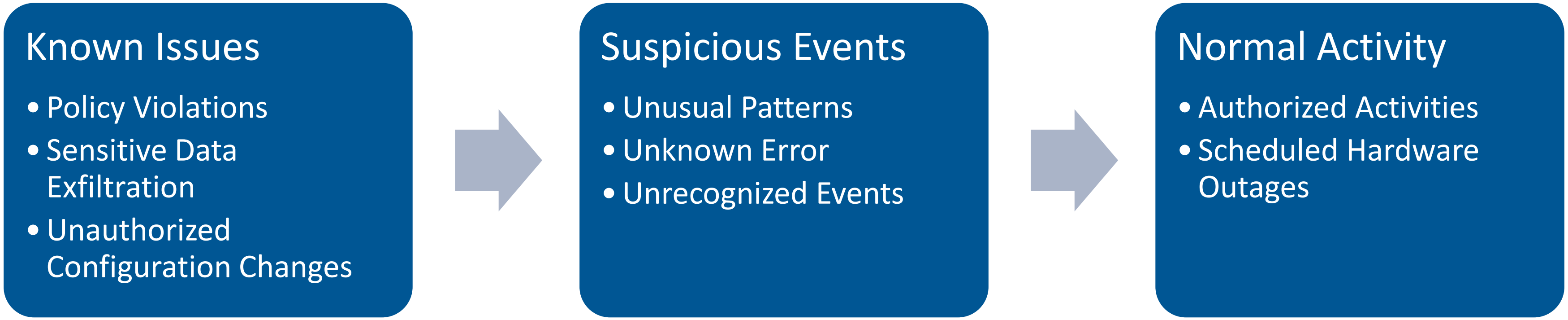
Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

DM-0004462

Goal for an Insider Threat Program



A Phased Approach to Insider Threat Anomaly Detection



Known Issues

- Policy Violations
- Sensitive Data Exfiltration
- Unauthorized Configuration Changes

Suspicious Events

- Unusual Patterns
- Unknown Error
- Unrecognized Events

Normal Activity

- Authorized Activities
- Scheduled Hardware Outages

Vectors for Insider Anomaly Detection

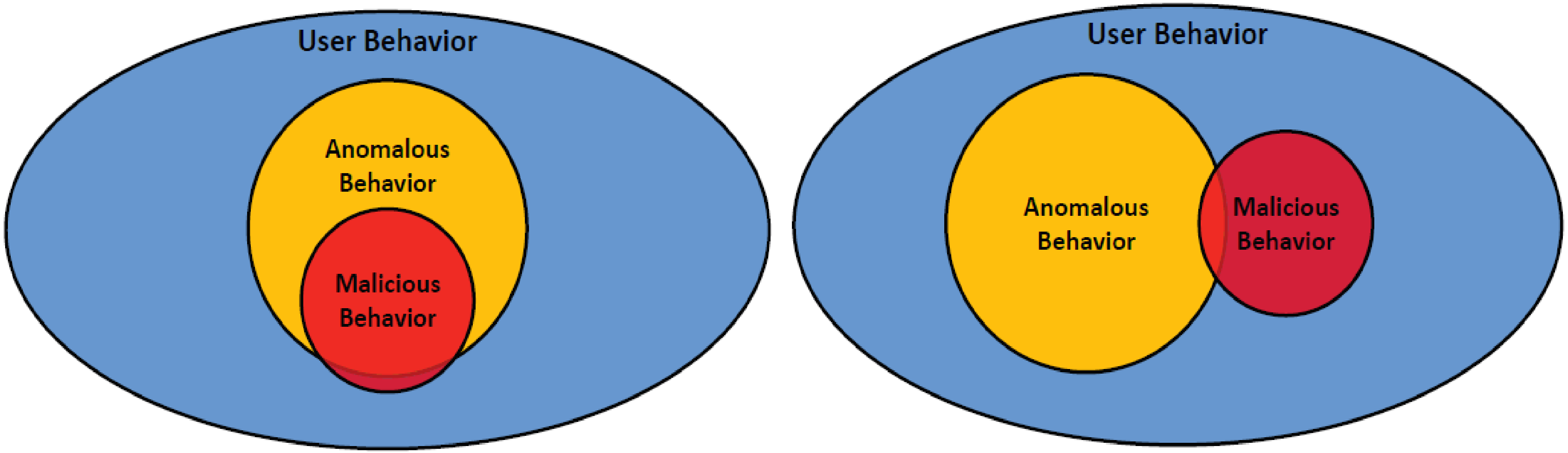
Vector	Examples
Time of Activity	After-hours logins, print jobs, or facility access
Volume of Activity	Large data uploads, file deletions, or print jobs
Account Activity	Service / machine accounts logging in interactively, browsing the web, or
File Access	Authorized access, but no need-to-know for a particular critical asset
Application Use	Administrative assistant executing PowerShell commands, excessive clearing of host-based security logs, excessive use of regedit.exe

Context is Key

… Anomalous relative to what?

- A fixed threshold
  - More than five ‘Access Denied’ errors generated in an hour
- An individual’s established patterns
  - Abnormally high level of cloud-based data uploads, based on a 30-day rolling average
  - Sudden increase in the use of language associated with negative emotions
- A peer group’s established patterns
  - Abnormally low number of help desk trouble ticket resolutions compared to all system administrators

Current Research Challenges in Insider Threat Mitigation



Source: Claycomb, William R., Philip A. Legg, and Dieter Gollmann. "Guest Editorial: Emerging Trends in Research for Insider Threat Detection." JoWUA 5.2 (2014): 1-6.

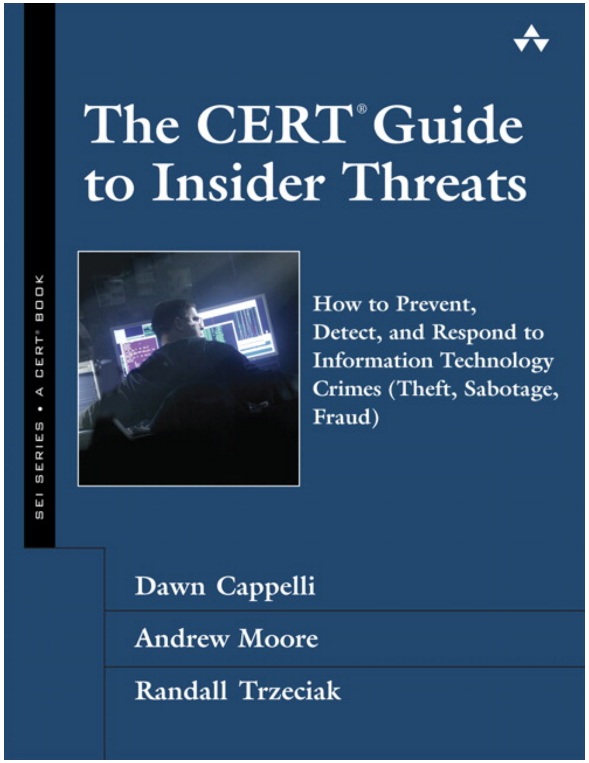
Measuring the effectiveness of indicators

- Across different contexts

Rates of occurrence for probabilistic models

- Access to incident data
- Access to 'baseline' data

CERT Insider Threat Resources and Services


The CERT® Guide to Insider Threats
How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)
SEI SERIES • A CERT® BOOK
Dawn Cappelli
Andrew Moore
Randall Trzeciak

www.cert.org/insider-threat

- Insider Threat Awareness Training
- Insider Threat Certificate Programs
- Insider Threat Vulnerability Assessments
- Insider Threat Program Evaluations
- Technical Reports
  - CERT Common Sense Guide to Mitigating Insider Threats, 5th Edition
  - Analytic Approaches to Detect Insider Threats
- Technical Controls
  - Using Plagiarism Detection Algorithms to Prevent Data Exfiltration in Near Real Time
  - Using a SIEM signature to detect potential precursors to IT Sabotage
- Insider Threat Blog
- Insider Threat Analytics Development and Tool Testing
- Customized Insider Threat Research

Contact Information

Presenter / Point of Contact

Dan Costa, CISSP

Technical Solutions Team Lead,
CERT Insider Threat Center

Telephone: +1 412.268.8006

Email: dlcosta@sei.cmu.edu

Using Narrative Structures to Detect Insider Risks

Kurt Wallnau

This material is based upon work supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

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.

ADAMS Red Team Task and Protocol (High Level)

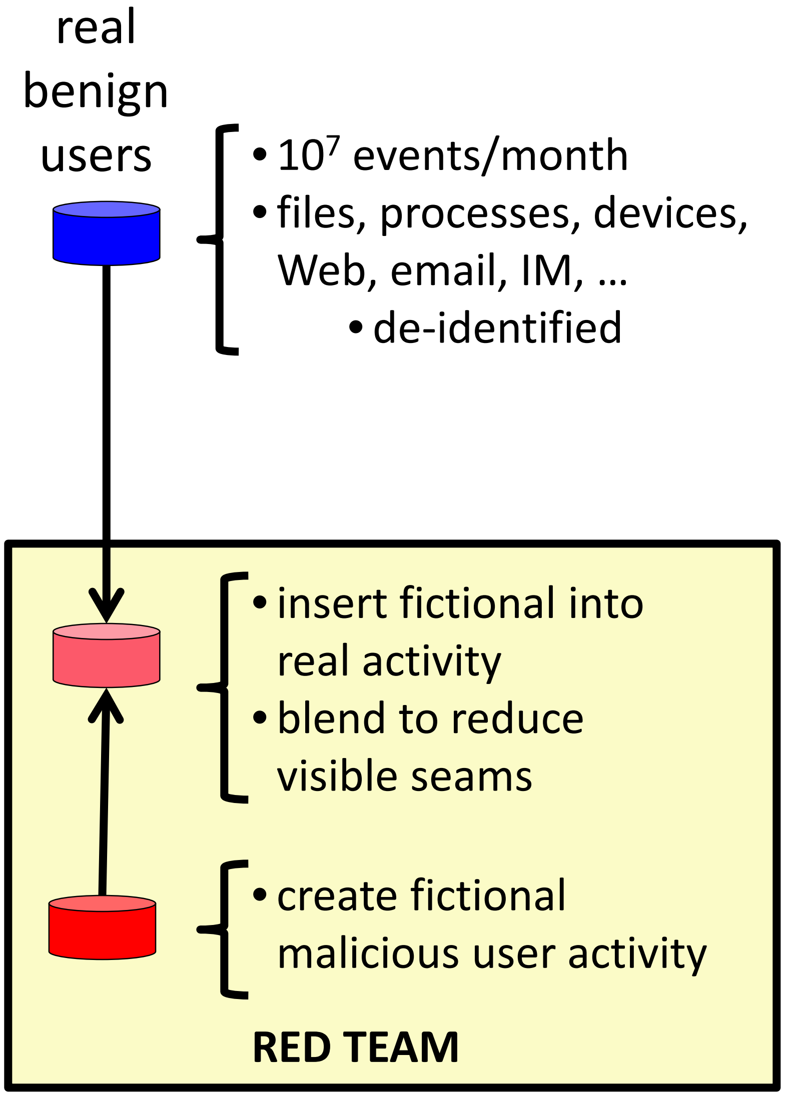
DARPA/ADAMS: Anomaly Detection at Multiple Scales (Rand Waltzman, PM)

Provide test data to support research:

- Inject “simulated” threat activity into “real” but benign background data
- Realistic social complexity of threats
  - unfold over days, weeks, months, …
  - precursor and violation behavior
  - single/multiple actors
- Valid and representative test sample with low risk of distracting data artifacts

Anomaly vs. Violation

- Q: How to specify test data that does not degenerate to a “violation”?
- A: Abstraction to dramatic narratives and dramatic performance!



real benign users

- 10^7 events/month
- files, processes, devices, Web, email, IM, …
  - de-identified

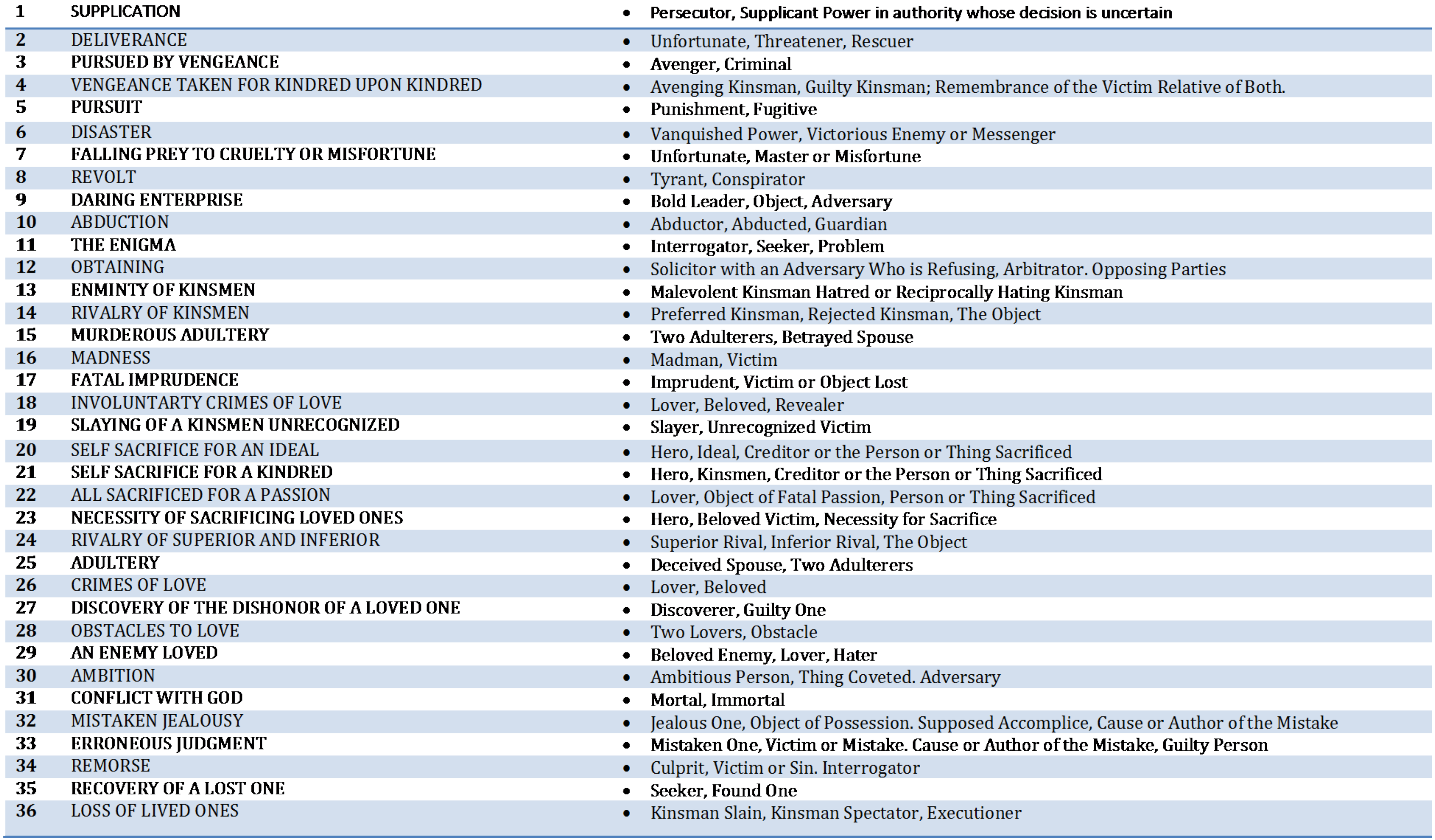
- insert fictional into real activity
- blend to reduce visible seams

- create fictional malicious user activity

RED TEAM

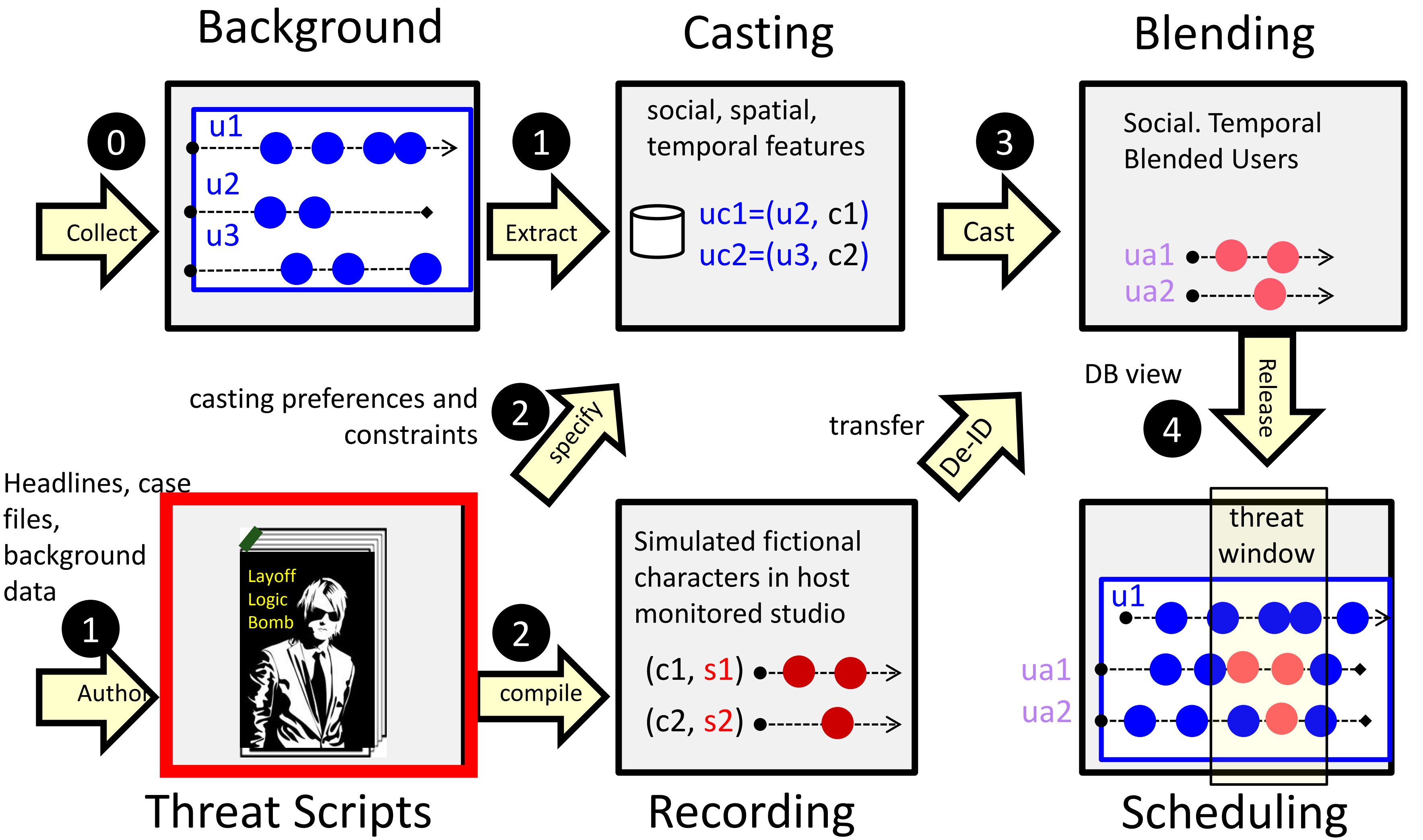
Drama is a foundational source of socio-conflict patterns

To illustrate, this summarizes the top-level structure of Polti’s “Thirty-Six Dramatic Situations” (1921):



1	**SUPPLICATION**	• **Persecutor, Supplicant Power in authority whose decision is uncertain**
2	DELIVERANCE	• Unfortunate, Threatener, Rescuer
3	**PURSUED BY VENGEANCE**	• **Avenger, Criminal**
4	VENGEANCE TAKEN FOR KINDRED UPON KINDRED	• Avenging Kinsman, Guilty Kinsman; Remembrance of the Victim Relative of Both.
5	**PURSUIT**	• **Punishment, Fugitive**
6	DISASTER	• Vanquished Power, Victorious Enemy or Messenger
7	**FALLING PREY TO CRUELTY OR MISFORTUNE**	• **Unfortunate, Master or Misfortune**
8	REVOLT	• Tyrant, Conspirator
9	**DARING ENTERPRISE**	• **Bold Leader, Object, Adversary**
10	ABDUCTION	• Abductor, Abducted, Guardian
11	**THE ENIGMA**	• **Interrogator, Seeker, Problem**
12	OBTAINING	• Solicitor with an Adversary Who is Refusing, Arbitrator. Opposing Parties
13	**ENMINTY OF KINSMEN**	• **Malevolent Kinsman Hatred or Reciprocally Hating Kinsman**
14	RIVALRY OF KINSMEN	• Preferred Kinsman, Rejected Kinsman, The Object
15	**MURDEROUS ADULTERY**	• **Two Adulterers, Betrayed Spouse**
16	MADNESS	• Madman, Victim
17	**FATAL IMPRUDENCE**	• **Imprudent, Victim or Object Lost**
18	INVOLUNTARTY CRIMES OF LOVE	• Lover, Beloved, Revealer
19	**SLAYING OF A KINSMEN UNRECOGNIZED**	• **Slayer, Unrecognized Victim**
20	SELF SACRIFICE FOR AN IDEAL	• Hero, Ideal, Creditor or the Person or Thing Sacrificed
21	**SELF SACRIFICE FOR A KINDRED**	• **Hero, Kinsmen, Creditor or the Person or Thing Sacrificed**
22	ALL SACRIFICED FOR A PASSION	• Lover, Object of Fatal Passion, Person or Thing Sacrificed
23	**NECESSITY OF SACRIFICING LOVED ONES**	• **Hero, Beloved Victim, Necessity for Sacrifice**
24	RIVALRY OF SUPERIOR AND INFERIOR	• Superior Rival, Inferior Rival, The Object
25	**ADULTERY**	• **Deceived Spouse, Two Adulterers**
26	CRIMES OF LOVE	• Lover, Beloved
27	**DISCOVERY OF THE DISHONOR OF A LOVED ONE**	• **Discoverer, Guilty One**
28	OBSTACLES TO LOVE	• Two Lovers, Obstacle
29	**AN ENEMY LOVED**	• **Beloved Enemy, Lover, Hater**
30	AMBITION	• Ambitious Person, Thing Coveted. Adversary
31	**CONFLICT WITH GOD**	• **Mortal, Immortal**
32	MISTAKEN JEALOUSY	• Jealous One, Object of Possession. Supposed Accomplice, Cause or Author of the Mistake
33	**ERRONEOUS JUDGMENT**	• **Mistaken One, Victim or Mistake. Cause or Author of the Mistake, Guilty Person**
34	REMORSE	• Culprit, Victim or Sin. Interrogator
35	**RECOVERY OF A LOST ONE**	• **Seeker, Found One**
36	LOSS OF LIVED ONES	• Kinsman Slain, Kinsman Spectator, Executioner

Simulated Threat Dramas by Background Extension



Background

0 Collect

u1

u2

u3

1 Extract

Casting

social, spatial, temporal features

uc1=(u2, c1)

uc2=(u3, c2)

3 Cast

Blending

Social. Temporal Blended Users

ua1

ua2

DB view

4 Release

casting preferences and constraints

2 specify

transfer

De-ID

Headlines, case files, background data

1 Author

Layoff Logic Bomb

Threat Scripts

2 compile

Simulated fictional characters in host monitored studio

(c1, s1)

(c2, s2)

Recording

threat window

u1

ua1

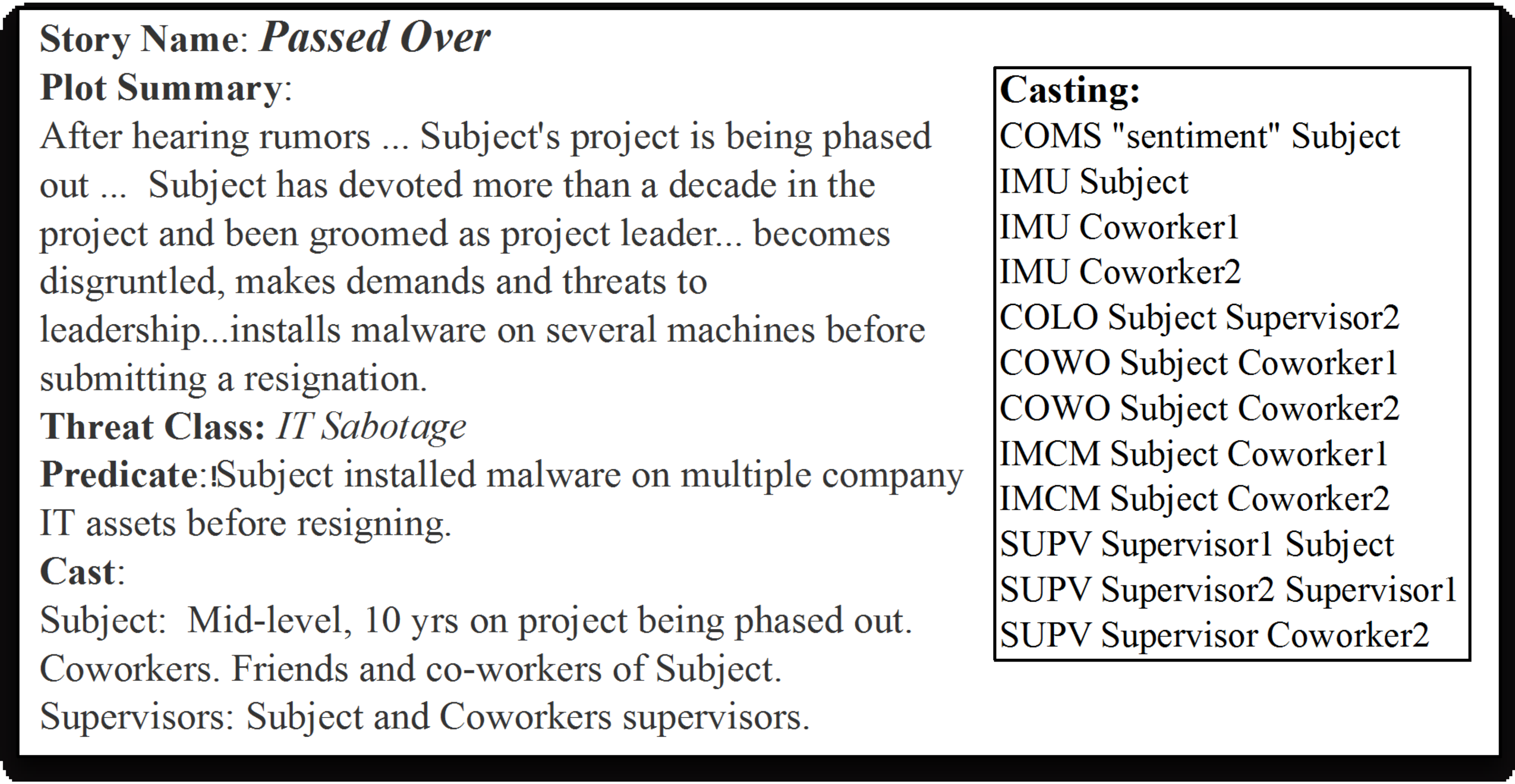
ua2

Scheduling

characters

DETAILS

Authoring: Passed Over (Story Summary)



Story Name: ***Passed Over***

Plot Summary:

After hearing rumors ... Subject's project is being phased out ... Subject has devoted more than a decade in the project and been groomed as project leader... becomes disgruntled, makes demands and threats to leadership...installs malware on several machines before submitting a resignation.

Threat Class: *IT Sabotage*

Predicate: Subject installed malware on multiple company IT assets before resigning.

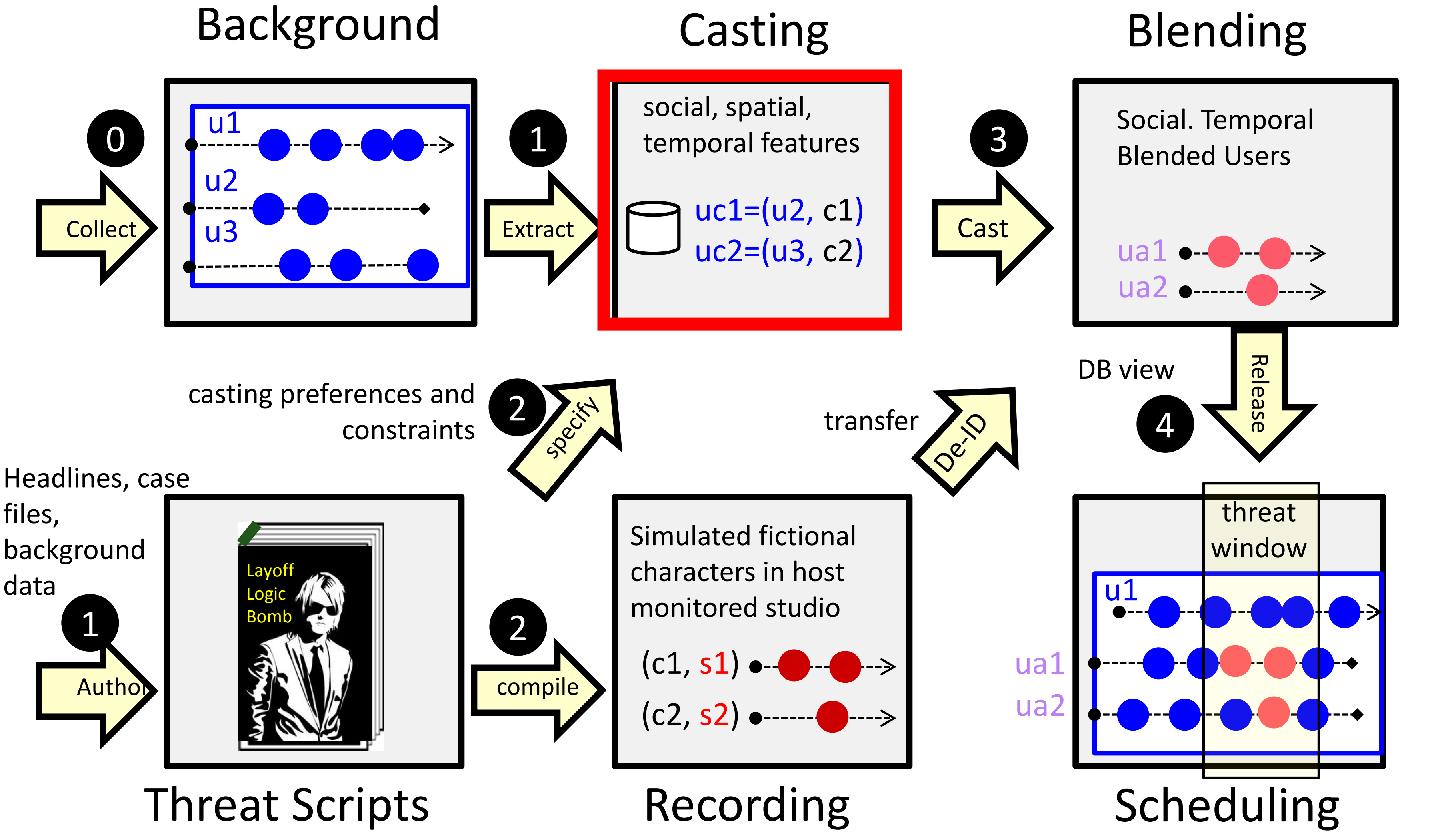
Cast:

Subject: Mid-level, 10 yrs on project being phased out.
Coworkers. Friends and co-workers of Subject.
Supervisors: Subject and Coworkers supervisors.

Casting:

COMS "sentiment" Subject
IMU Subject
IMU Coworker1
IMU Coworker2
COLO Subject Supervisor2
COWO Subject Coworker1
COWO Subject Coworker2
IMCM Subject Coworker1
IMCM Subject Coworker2
SUPV Supervisor1 Subject
SUPV Supervisor2 Supervisor1
SUPV Supervisor Coworker2

Simulated Threat Dramas by Background Extension



Background

0 Collect

u1

u2

u3

1 Extract

Casting

social, spatial, temporal features

uc1=(u2, c1)

uc2=(u3, c2)

3 Cast

Blending

Social. Temporal Blended Users

ua1

ua2

casting preferences and constraints

2 specify

transfer

De-ID

DB view

4 Release

Headlines, case files, background data

1 Author

Layoff Logic Bomb

2 compile

Simulated fictional characters in host monitored studio

(c1, s1)

(c2, s2)

threat window

u1

ua1

ua2

Threat Scripts

Recording

Scheduling

characters

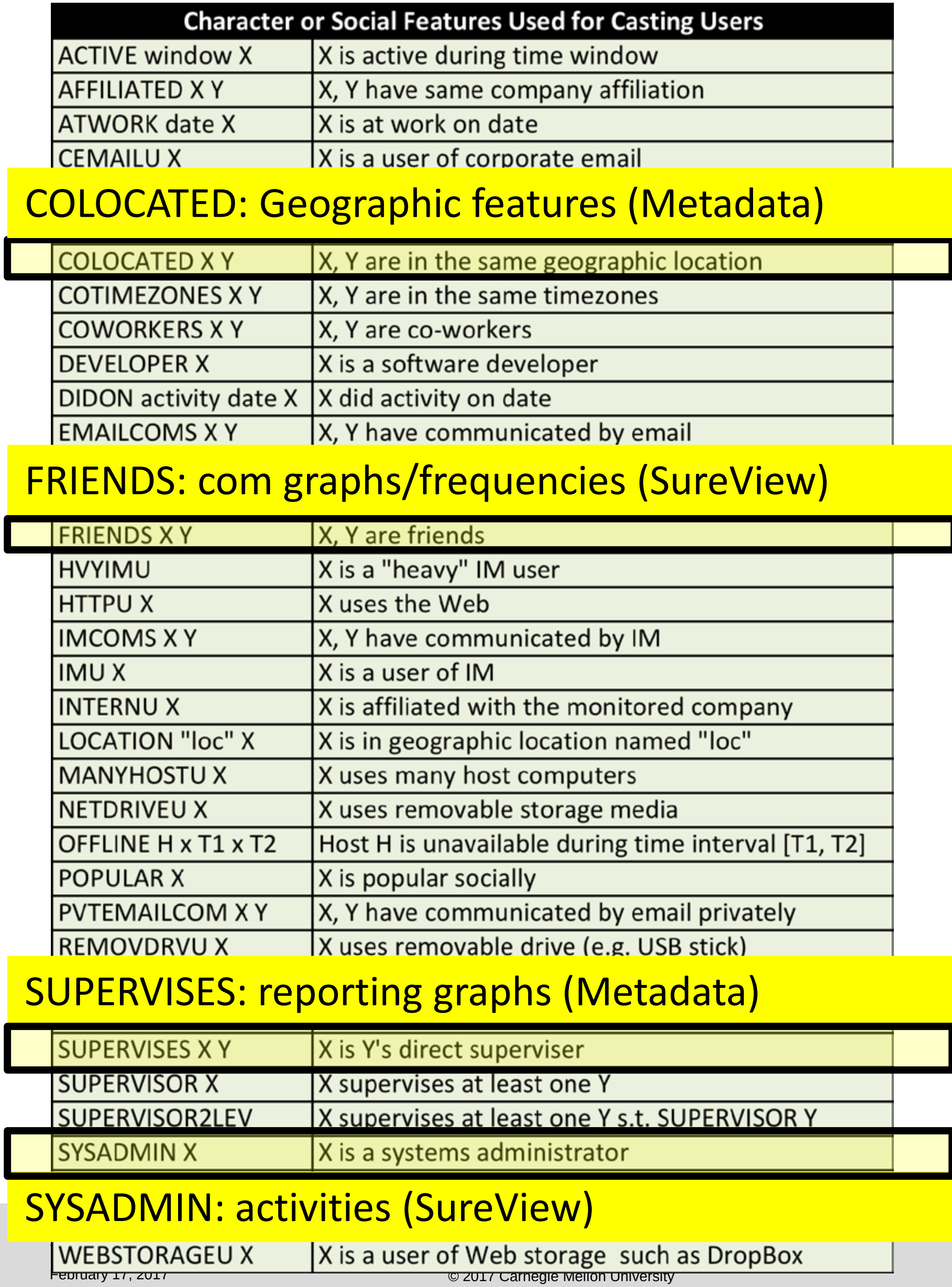
Casting

Goal: find the “right” users to perform dramatic simulations

- Character features: job roles, activity preferences
- Social features: friend and team graphs, reporting structure

> 70 casting features induced by narratives (not pre-defined)

- They reveal something about the underlying threat construct



Character or Social Features Used for Casting Users	
ACTIVE window X	X is active during time window
AFFILIATED X Y	X, Y have same company affiliation
ATWORK date X	X is at work on date
CEMAILU X	X is a user of corporate email
COLOCATED X Y	X, Y are in the same geographic location
COTIMEZONES X Y	X, Y are in the same timezones
COWORKERS X Y	X, Y are co-workers
DEVELOPER X	X is a software developer
DIDON activity date X	X did activity on date
EMAILCOMS X Y	X, Y have communicated by email
FRIENDS X Y	X, Y are friends
HVYIMU	X is a "heavy" IM user
HTTPU X	X uses the Web
IMCOMS X Y	X, Y have communicated by IM
IMU X	X is a user of IM
INTERNU X	X is affiliated with the monitored company
LOCATION "loc" X	X is in geographic location named "loc"
MANYHOSTU X	X uses many host computers
NETDRIVEU X	X uses removable storage media
OFFLINE H x T1 x T2	Host H is unavailable during time interval [T1, T2]
POPULAR X	X is popular socially
PVTEMAILCOM X Y	X, Y have communicated by email privately
REMOVDRVU X	X uses removable drive (e.g. USB stick)
SUPERVISES X Y	X is Y's direct superviser
SUPERVISOR X	X supervises at least one Y
SUPERVISOR2LEV	X supervises at least one Y s.t. SUPERVISOR Y
SYSADMIN X	X is a systems administrator
WEBSTORAGEU X	X is a user of Web storage such as DropBox

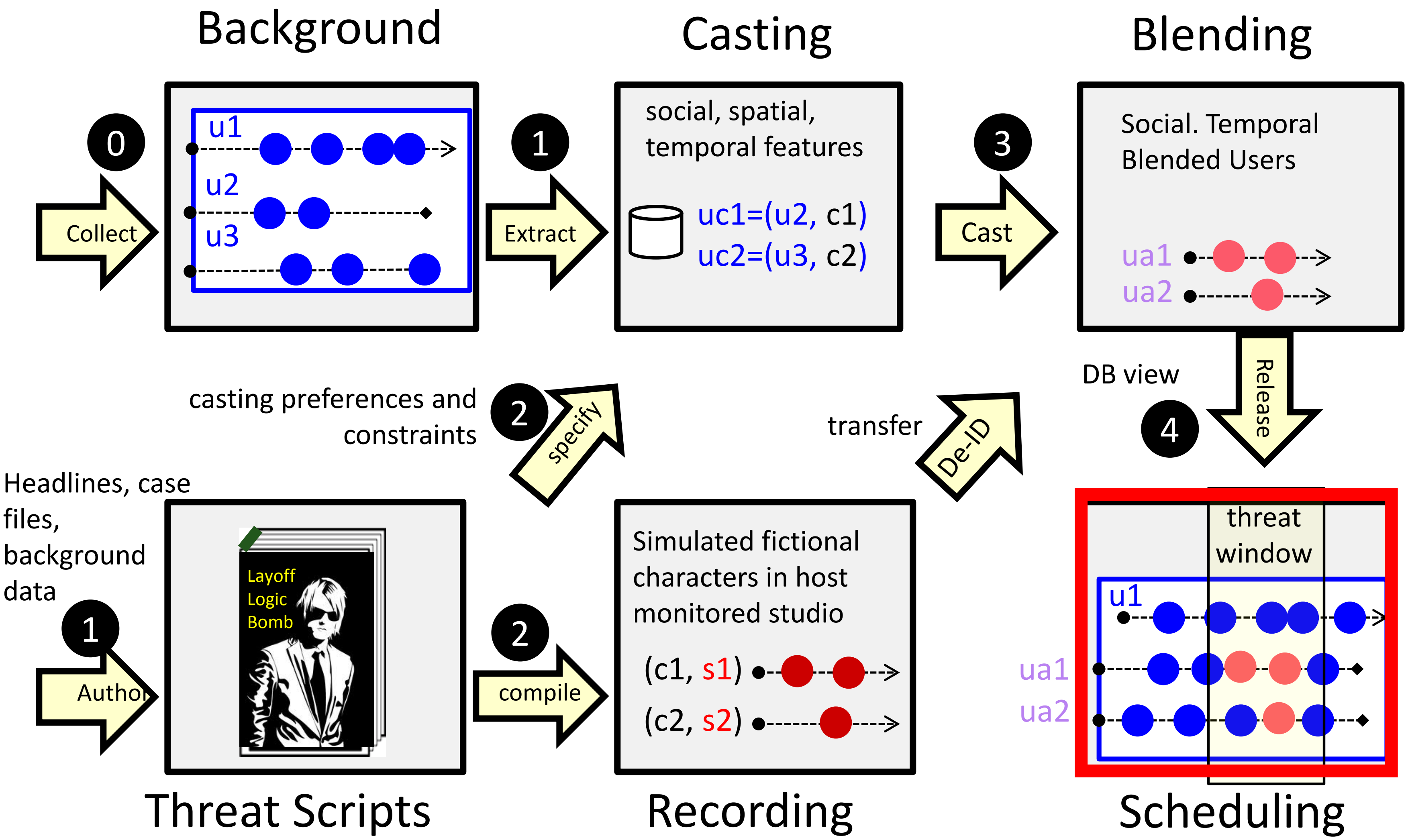
COLOCATED: Geographic features (Metadata)

FRIENDS: com graphs/frequencies (SureView)

SUPERVISES: reporting graphs (Metadata)

SYSADMIN: activities (SureView)

Simulated Threat Dramas by Background Extension



Background

Casting

Blending

0 Collect

u1

u2

u3

1 Extract

social, spatial, temporal features

uc1=(u2, c1)
uc2=(u3, c2)

3 Cast

Social. Temporal Blended Users

ua1

ua2

DB view

Release

4

casting preferences and constraints

2 specify

transfer

De-ID

Headlines, case files, background data

1 Author

Layoff Logic Bomb

2 compile

Simulated fictional characters in host monitored studio

(c1, s1)

(c2, s2)

threat window

u1

ua1

ua2

Threat Scripts

Recording

Scheduling

characters

Results

39 threat dramas, performed 89 times in 26 month-long windows

- espionage, sabotage, IP theft, fraud
- greed, family crises, extortion, misplaced idealism, resentment
- conspiracies, lone wolves, foreign agents, victims, enablers
- from case files, headlines, and events occurring in background

Story	#Perf	Story	#Perf
Anomalous Encryption	5	Insider Startup	7
Blinded Me with Science	1	Job Hunter	1
Bollywood Breakdown	2	Layoff Logic Bomb	1
Bona Fides	2	Manning Up	2
Breaking the Stovepipe	3	Manning Up II	1
Byte Me!	2	Masquerading (Orig)	1
Byte Me! Middleman	2	Masquerading 2	2
Circumventing Sureview	2	Naughty by Proxy	4
Conspiracy Theory	2	Outsourcer's Apprentice	3
Credit Czech	1	Panic Attack	2
Czech Mate	1	Parting Shot	1
Exfil using Steganography	1	Parting Shot: Deadly Aim	1
Exfil Before Layoff	3	Passed Over	4
Exfil Using Screenshots	4	Selling Login Credentials	2
From Belarus With Love	2	Snowed In	6
Gift Card Bonanza	1	Stealing Login Credentials	1
Hiding Undue Affluence	4	Strategic Tee Time	1
Indecent RFP	1	Survivor's Burden	4
Indecent RFP 2	2	The Big Goodbye!	2
		What's the Big Deal?	2

K. Wallnau, B. Lindauer, M. Theis, S. Durst, T. Champion, E. Renouf and C. Petersen, “Simulating Malicious Insiders in Real Host-Monitored User Data,” *Usenix Workshop on Cybersecurity Experimentation and Test (CSET’14)*, San Diego, CA, August 2014.

Possible Implications

Localization:

- The technique is abstracted from collectors and collection policies
- Threats dramas can be written once, then cast and performed in local data

Scale:

- Thousands of performance variations of each threat data can be obtained quickly and automatically (different casts, temporal placement of scenes)
- End-to-end automation after the “creative” part (principally, threat authoring)

Realism and Validity:

- As real as any dramatic narrative and performance needs
- No “built-in” detector-technology bias in threat specifications

Contact Information

Kurt Wallnau, PhD

Principal Researcher

Software Engineering Institute

Telephone: +1 412-268-3265

Email: kcw@sei.cmu.edu

The Role of Positive Incentives in Reducing Insider Threats

Andrew Moore

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

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.

DM-0004494

Research Objective

Determine influence of workforce management practices on insider threat behaviors

Negative Incentives

Workforce management practices that attempt to *force* employees to act in the interests of the organization

Employee Constraints, Monitoring, Punishment

Positive Incentives

Workforce management practices that attempt to *attract* employees to act in the interests of the organization

Focus on Employee Strengths, Fair & Respectful Treatment

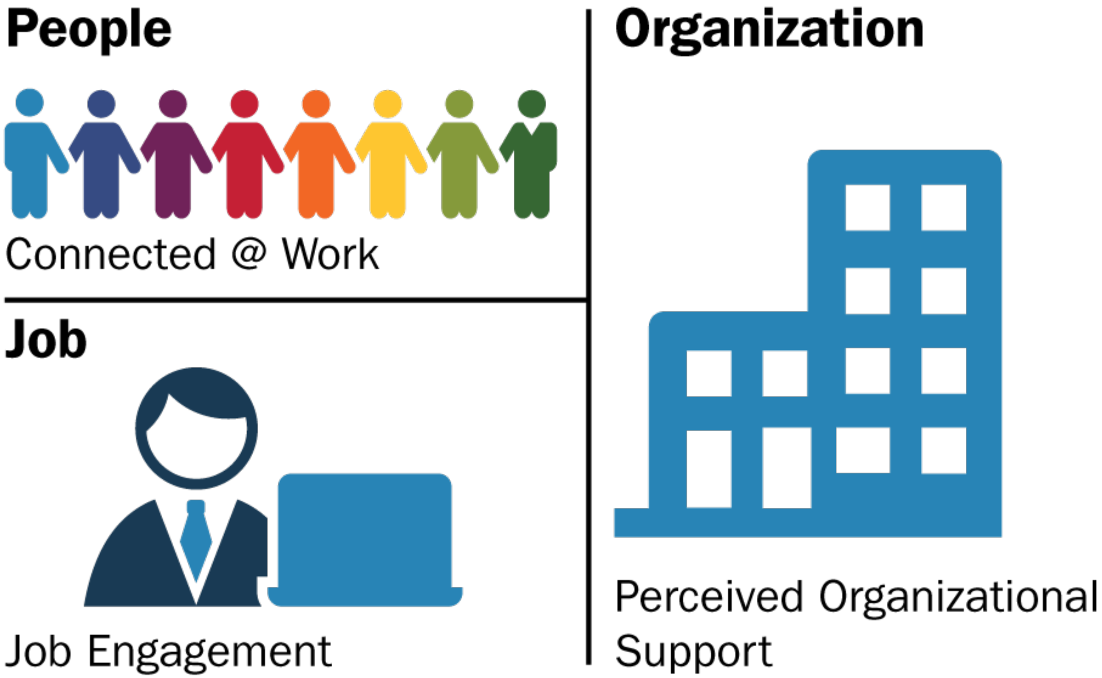
Negative incentives *alone* can *exacerbate* the threat they are intended to mitigate*

Basic Belief: Organizations should *explicitly* consider a *mix of positive and negative incentives* to build insider threat programs that are a net positive for employees

Initial Scope: Disgruntlement-spurred threat

* See “Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls,” SEI Digital Library, March 2015. http://resources.sei.cmu.edu/asset_files/WhitePaper/2015_019_001_446379.pdf

Three Dimensions of Employee-Organization Alignment



People

Connected @ Work

Job

Job Engagement

Organization

Perceived Organizational Support

Two-Pronged Exploratory Research Approach

1. Insider Incident Case Study Analysis

- How engaged, connected, and supported are insider threat actors?

2. Organizational Survey

- How much does organizational support influence insider cyber misbehavior?

Extension of previous work by focusing on

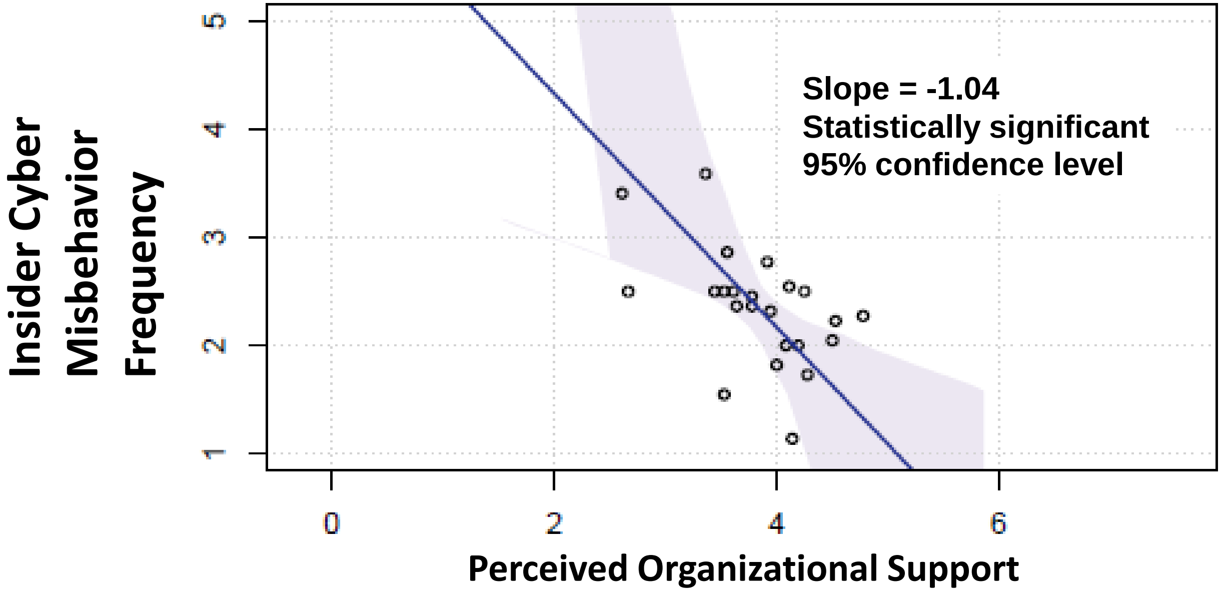
- Cyber-related insider threat behaviors
- Organizations actively establishing insider threat programs

Organizational Survey

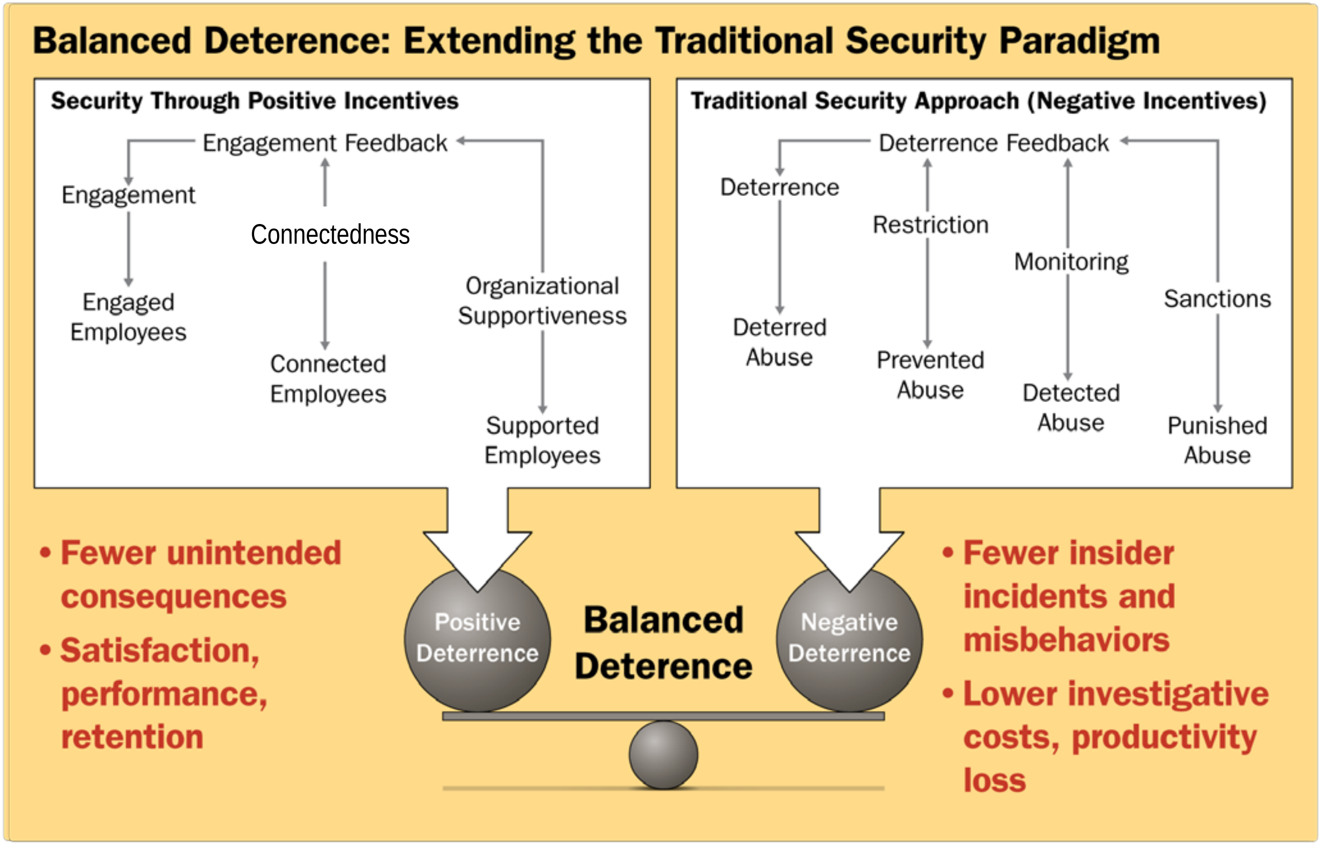
How much does organizational support influence insider cyber misbehavior?

Method: Survey Open Source Insider Threat (OSIT) Information Sharing Group

Results: based on 23 out of ~90 organizations



Vision: Extending the Traditional Security Paradigm



Balanced Deterence: Extending the Traditional Security Paradigm

Security Through Positive Incentives

Engagement Feedback

Engagement

Connectedness

Engaged Employees

Organizational Supportiveness

Connected Employees

Supported Employees

Traditional Security Approach (Negative Incentives)

Deterrence Feedback

Deterrence

Restriction

Monitoring

Sanctions

Deterred Abuse

Prevented Abuse

Detected Abuse

Punished Abuse

- Fewer unintended consequences
- Satisfaction, performance, retention

Positive Deterrence

Balanced Deterence

Negative Deterrence

- Fewer insider incidents and misbehaviors
- Lower investigative costs, productivity loss

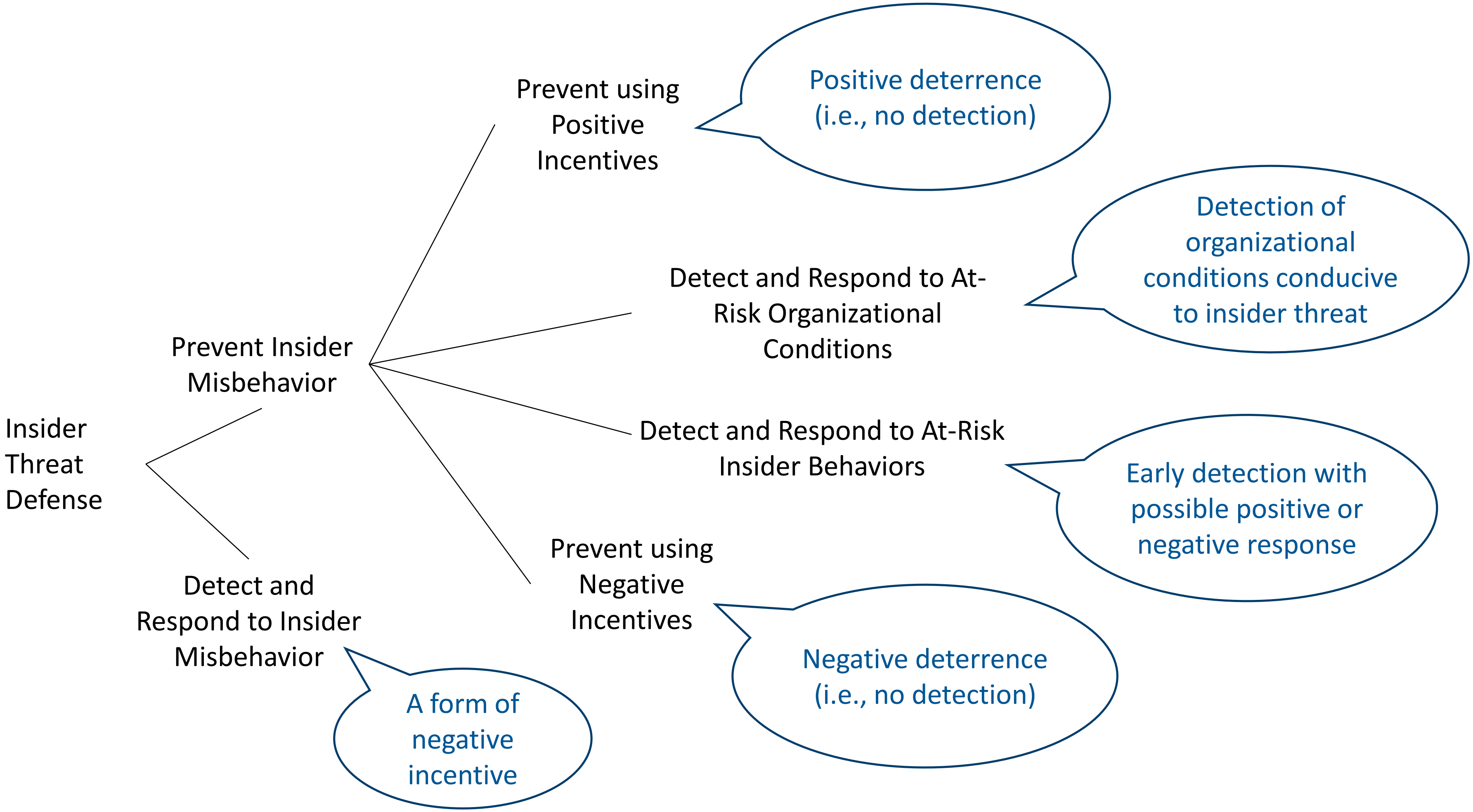
Backups

Categories of Negative Unintended Consequences in Insider Threat Programs (InTP)*

1. Interference with legitimate whistleblower processes and protections
2. InTP management/employee relationships
3. InTP management's lack or loss of interest in the InTP
4. Purposeful Misuse of the InTP by its staff or other employees
5. Accidental Misuse of the InTP by its staff or other employees

* See "Effective Insider Threat Programs: Understanding and Avoiding Potential Pitfalls," SEI Digital Library, March 2015. http://resources.sei.cmu.edu/asset_files/WhitePaper/2015_019_001_446379.pdf

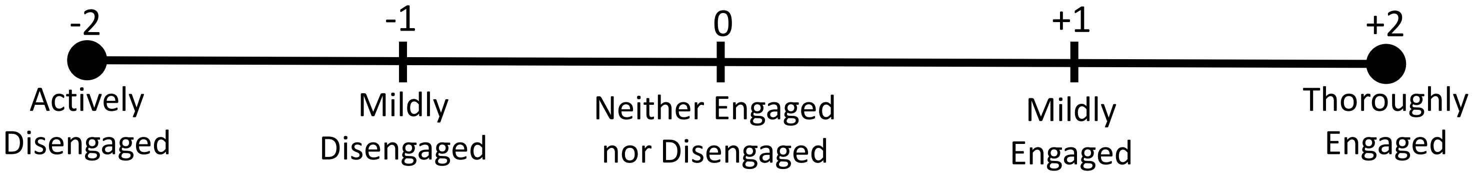
Research Context


Insider Threat Defense
Prevent Insider Misbehavior
Detect and Respond to Insider Misbehavior
Prevent using Positive Incentives
Detect and Respond to At-Risk Organizational Conditions
Detect and Respond to At-Risk Insider Behaviors
Prevent using Negative Incentives
Positive deterrence (i.e., no detection)
Detection of organizational conditions conducive to insider threat
Early detection with possible positive or negative response
Negative deterrence (i.e., no detection)
A form of negative incentive

Insider Incident Case Study Analysis

How engaged, connected, and supported are insider threat actors?

- **Method:** Rate dimensions on 5-point Likert scales over three time periods
  - For example, for Job Engagement



-2 Actively Disengaged

-1 Mildly Disengaged

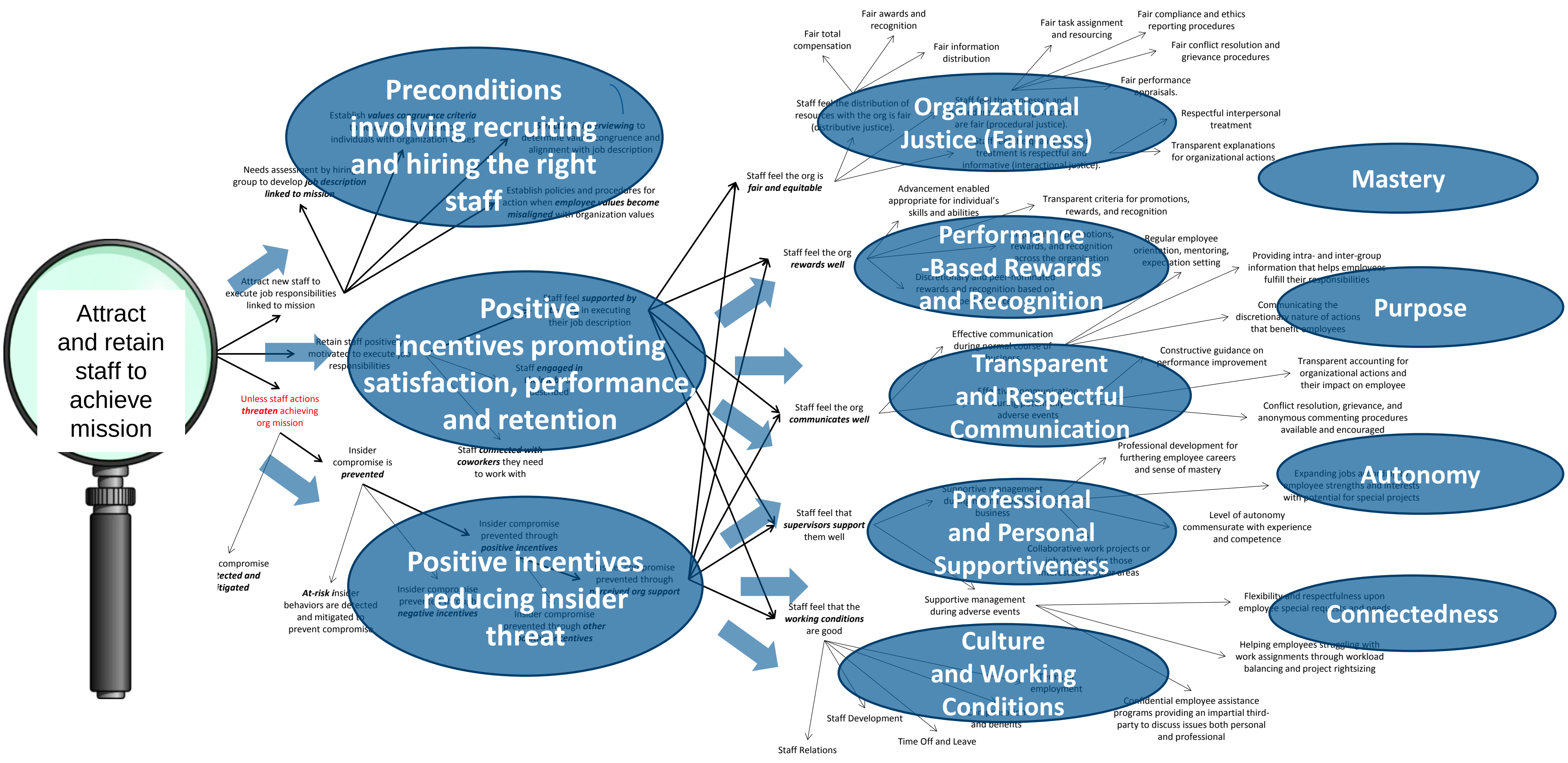
0 Neither Engaged nor Disengaged

+1 Mildly Engaged

+2 Thoroughly Engaged

- **Challenge:** Assessing insider perceptions through observables (w/o interview)
- **Results:** (3 prominent incidents)
  - Dimensions became increasingly negative over time, with some fluctuation
    - *Organizational Support* most strongly negative in all 3 incidents
    - *Job Engagement* negative in 2 out of 3 incidents
    - *Connectedness at Work* negative in 1 out of 3 incidents
- **Initial Decision:** Focus on perceived organizational support as foundation.

Positive Incentive-Based Principles and Practice Areas



Attract and retain staff to achieve mission

Attract new staff to execute job responsibilities linked to mission

Retain staff positively motivated to execute job responsibilities

Unless staff actions *threaten* achieving org mission

Needs assessment by hiring group to develop *job description linked to mission*

Preconditions involving recruiting and hiring the right staff

Establish *values congruence criteria* to [illegible] individuals with organization values

[illegible] *interviewing* to determine values congruence and alignment with job description

Establish policies and procedures for action when *employee values become misaligned* with organization values

Positive incentives promoting satisfaction, performance, and retention

Staff feel *supported by* [illegible] in executing their job description

Staff *engaged in* [illegible] described

Staff *connected with coworkers* they need to work with

Insider compromise is *prevented*

[illegible] compromise [illegible]*tected and* [illegible]*itigated*

*At-risk i*nsider behaviors are detected and mitigated to prevent compromise

Positive incentives reducing insider threat

Insider compromise prevented through *positive incentives*

Insider compromise prevented through *negative incentives*

Insider compromise prevented through *perceived org support*

Insider compromise prevented through *other positive incentives*

Staff feel the org is *fair and equitable*

Staff feel the org *rewards well*

Staff feel the org *communicates well*

Staff feel that *supervisors support* them well

Staff feel that the *working conditions* are good

Organizational Justice (Fairness)

Fair total compensation

Fair awards and recognition

Fair information distribution

Fair task assignment and resourcing

Fair compliance and ethics reporting procedures

Fair conflict resolution and grievance procedures

Fair performance appraisals.

Respectful interpersonal treatment

Transparent explanations for organizational actions

Staff feel the distribution of resources with the org is fair (distributive justice).

Staff feel the processes and procedures in the organization are fair (procedural justice).

Staff feel the quality of their treatment is respectful and informative (interactional justice).

Performance-Based Rewards and Recognition

Advancement enabled appropriate for individual’s skills and abilities

Transparent criteria for promotions, rewards, and recognition

Alignment of promotions, rewards, and recognition across the organization

Discretionary and peer-nominated rewards and recognition based on performance

Regular employee orientation, mentoring, expectation setting

Transparent and Respectful Communication

Effective communication during normal course of business

Effective communication during potentially adverse events

Providing intra- and inter-group information that helps employees fulfill their responsibilities

Communicating the discretionary nature of actions that benefit employees

Constructive guidance on performance improvement

Transparent accounting for organizational actions and their impact on employee

Conflict resolution, grievance, and anonymous commenting procedures available and encouraged

Professional and Personal Supportiveness

Supportive management during normal course of business

Professional development for furthering employee careers and sense of mastery

Level of autonomy commensurate with experience and competence

Collaborative work projects or job rotation for those interested in other areas

Supportive management during adverse events

Flexibility and respectfulness upon employee special requests and needs

Helping employees struggling with work assignments through workload balancing and project rightsizing

Confidential employee assistance programs providing an impartial third-party to discuss issues both personal and professional

Culture and Working Conditions

Terms of employment

Compensation and benefits

Staff Development

Time Off and Leave

Staff Relations

Mastery

Purpose

Autonomy

Expanding jobs according to employee strengths and interests with potential for special projects

Connectedness

Future Research

Theory Development

- Experiment-based determination of cause-effect relationship between perceived organizational support and insider threat

Technology Development

- Detection of
  - at-risk organizational conditions associated with organizational support
  - insider alienation through indicative changes in insiders’ network of workplace relationships

Adoption

- Determine how organizations can
  - determine an appropriate mix of positive and negative incentives
  - transition to that from their current state

Contact

Presenter / Point of Contact :
Andrew Moore
Lead Insider Threat Researcher
Telephone: +1 412.268.5465
Email: apm@cert.org

***Contributors* :**

SEI CERT:
Samuel J. Perl
Jennifer Cowley
Matthew L. Collins
Tracy M. Cassidy
Nathan VanHoudnos

SEI SSD:
William Novak
David Zubrow

***Contributors* :**

SEI Directors Office:
Palma Buttles

SEI Human Resources:
Daniel Bauer
Allison Parshall
Jeff Savinda

SEI Organizational Effectiveness Group:
Elizabeth A. Monaco
Jamie L. Moyes

CMU Heinz College and Tepper School of Business:
Professor Denise M. Rousseau

Special thanks to the Open Source Insider Threat (OSIT) Information Sharing Group for their responses to our survey.

For more details on this research see “The Critical Role of Positive Incentives in Reducing Insider Threat,” *SEI Technical Report CMU/SEI-2016-TR-014*, December 2016.
http://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484929.pdf

Q & A

Open Source Insider Threat (OSIT) Information Sharing Group

Community of Interest for insider threat program practitioners across government and industry organizations

Over 230 members from ~100 organizations

Special interest groups around sectors (banking/finance) and sub-topics(data analytics)

Monthly Telecons

- Tool Vendor Demos

Bi-annual In-Person Meetings

- Hosted by various members of the group

To join, contact:

dlcosta@sei.cmu.edu
rft@cert.org

Presenter Contact

Robert Binder Senior Engineer +1 412 268 1549 rvbinder@sei.cmu.edu	Jim Northey Principal Services Consultant, Itiviti +1 906 482 0633 jim.northey@itiviti.com
Randy Trzeciak Director, CERT Insider Threat Center +1 412 268 7040 rft@sei.cmu.edu	Dan Costa, CISSP Technical Solutions Team Lead, CERT Insider Threat Center +1 412 268 8006 dlcosta@sei.cmu.edu
Kurt Wallnau, PhD Principal Researcher +1 412 268 3265 kcw@sei.cmu.edu	Andrew Moore Lead Insider Threat Researcher +1 412 268 5465 apm@cert.org

Insider Threat Blog https://insights.sei.cmu.edu/insider-threat/

Presenter Contact

U.S. Mail

Software Engineering Institute
Customer Relations
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
USA

Web

www.sei.cmu.edu
www.sei.cmu.edu/contact.cfm

Customer Relations

Email: info@sei.cmu.edu

Telephone:	+1 412-268-5800
SEI Phone:	+1 412-268-5800
SEI Fax:	+1 412-268-6257

Q & A