Developing an Ontology for Individual and Organizational Sociotechnical Indicators of Insider Threat Risk

Frank L. Greitzer, *PsyberAnalytix*
Muhammad Imran, ***[Presenter]*** *George Mason University*
Justin Purl, *Human Resources Research Organization*
Elise T. Axelrad, *Innovative Decisions, Inc.*
Yung Mei Leong, *Independent Consultant*
D.E. (Sunny) Becker, *Human Resources Research Organization*
Kathryn B. Laskey, *George Mason University*
Paul J. Sticha, *Human Resources Research Organization*

Presented to:

The Eleventh International Conference on Semantic Technology for Intelligence, Defense, and Security (STIDS 2016)

November 15-16, 2016

Greitzer, FL, M Imran, J Purl, ET Axelrad, YM Leong, DE Becker, KB Laskey, and PJ Sticha. (2016). "Developing an ontology for individual and organizational sociotechnical indicators of insider threat risk." *The Eleventh International Conference on Semantic Technology for Intelligence, Defense, and Security (STIDS 2016),* Fairfax, VA, November 15-16, 2016.

Research reported here was supported under IARPA contract 2016-16031400006. The content is solely the responsibility of the authors and does not necessarily represent the official views of the U.S. Government.

Definition

Insider threat:

An individual (or individuals) who….

- is a current or former employee, contractor, or other business partner
- has or had authorized access to an organization's network, system, or data
- intentionally (or unintentionally) exceeds or misuses that access to negatively affect the confidentiality, integrity, or availability of the organization's information or information systems

[CERT, 2012]

Objectives

A major goal of this research is to develop a formal representation of our current understanding of factors underlying insider threats

Specific objectives:

- Extend current insider threat ontology frameworks by incorporating sociotechnical constructs reflecting both individual/behavioral and organizational factors
- Support modeling and reasoning approaches for insider threat assessment

There is a notable lack of standards within the insider threat domain to assist in developing, describing, testing, and sharing techniques and methods for detecting and preventing insider threats

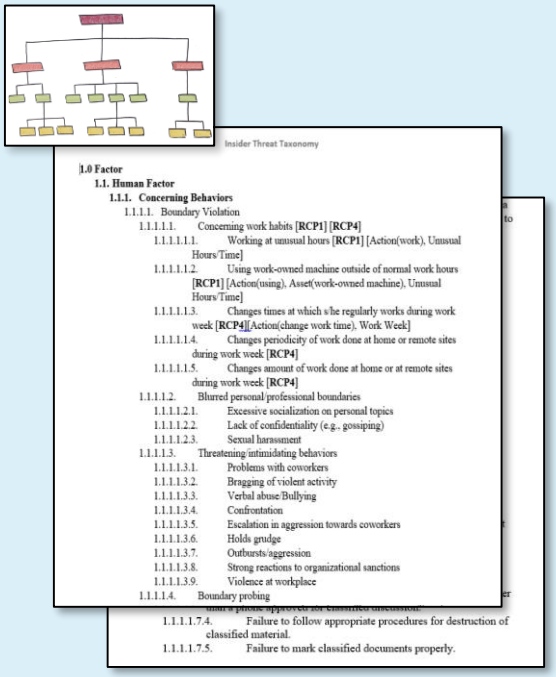
Approach

- Develop a hierarchical taxonomy for insider threat risk
- Migrate the taxonomy into a formal ontology for insider threat risk
- Ontology development methods include:
  - Methontology [Fernandez-Lopez et al. 1997] engineering methodology for development, re-use, re-engineering of existing ontologies

  - IDEF5 Ontology Description Method to acquire knowledge and develop graphical knowledge representation models
  - Implementation in Protégé software followed “Ontology 101” [Noy and McGuinness 2008]

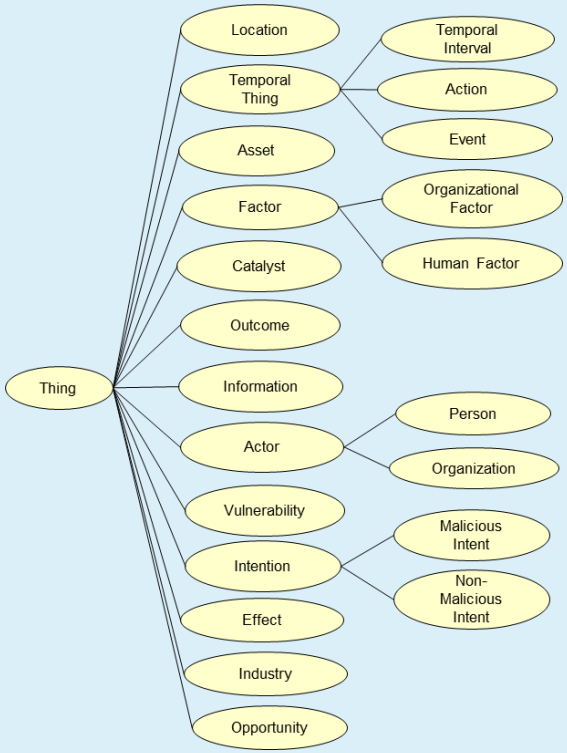
Migrating Taxonomy to Ontology

Insider Threat Taxonomy



(Organized hierarchy of Classes, factors, …)

Comprehensive Ontology

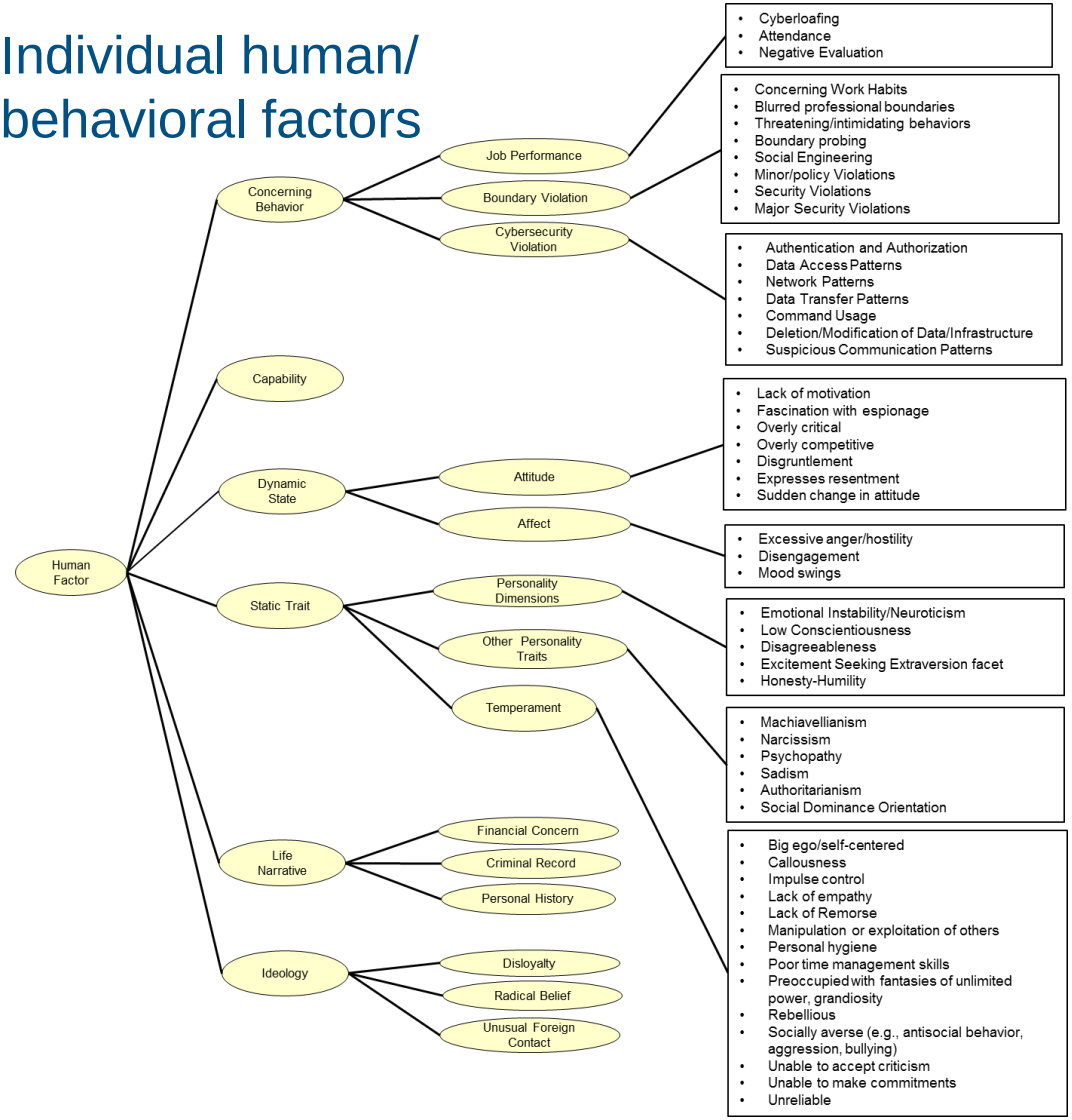


Incorporates class structures recently published by CERT (re-use of 125 classes of technical indicators)

Full ontology comprises >350 constructs within a framework 6-7 layers deep

Human Factor and Organizational Factor Branches

Individual human/ behavioral factors



Organizational factors

The human factor branch of the ontology provides a link between technical actions/exploits and key contributing factors such as personal predispositions (e.g., personality traits, dynamic states), ideology, capability, etc.

Competency Questions

Representative CQs:

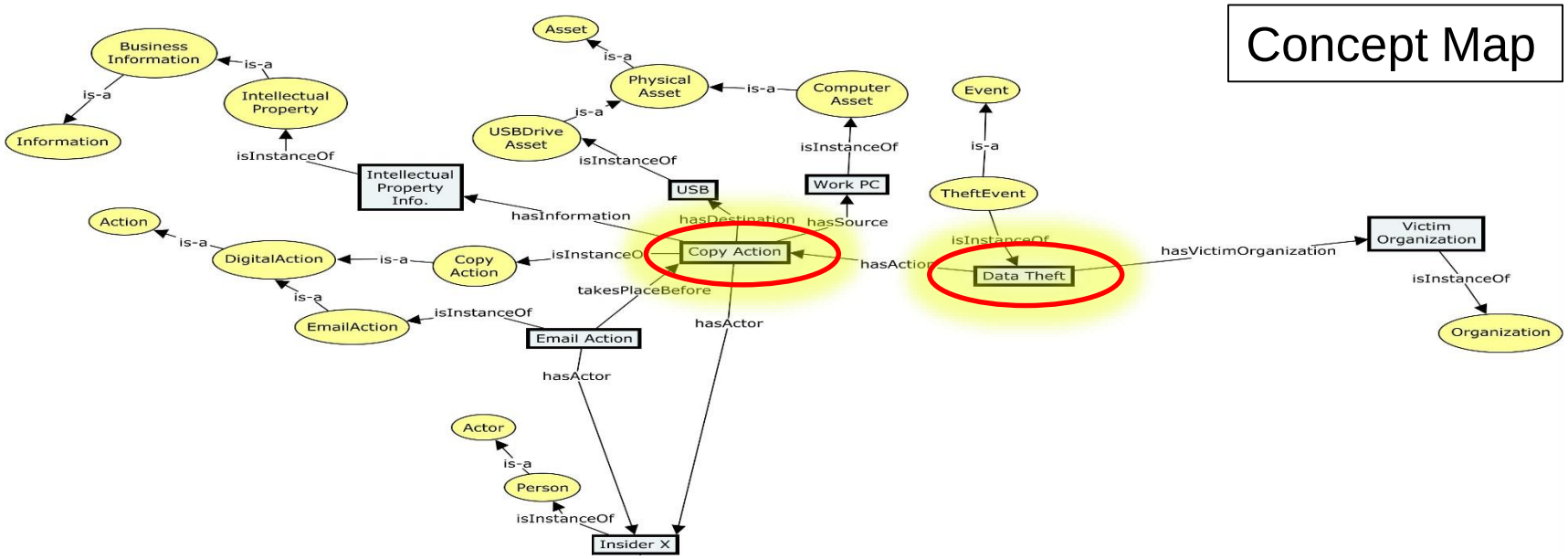
Competency Question	Concepts*		Relationships*
What are the components of the class, ATTITUDE?	• Attitude • Lack of Motivation	• Overly Competitive • Resentment	Resentment is instance of Attitude (etc.)
What factors (classes/sub-classes) are associated with the following observables? • *Attendance Problems* • *Unauthorized Personal use of Work Computer* • *Manipulative*, *Hostile*	• Human Factor • Concerning Behavior • Job Performance • Attendance Problems • Boundary Violation • Cyberloafing	• Dynamic State • Affect • Temperament • Manipulative • Hostility	• Dynamic State is a Human Factor • Temperament is a Dynamic State • Hostility is an Affect • Affect is a Dynamic State (etc.)
What factors (classes/sub-classes) are associated with the following observables: • *Heavy prolonged workload* • *Job instability* • *Unexplained affluence*	• Organizational Factor • Work Planning & Control • Heavy/Prolonged Workload • Work Setting • Job instability	• Human Factor • Life Narrative • Financial Concerns • Unexplained Affluence	• Work Planning is an Organizational Factor • Heavy workload is instance of Work Planning • Work Setting is an Organizational Factor (etc.)

**Representative list: not exhaustive*

Competency Questions are created to define scope of work and requirements of ontology

Scenario 1

Represents a typical insider exploit with technical/cyber activities



Use Case #1

John **[PERSON: Insider X]** *is a long-time system administrator* **[LIFE NARRATIVE: PERS HISTORY] [CAPABILITY]** *with access to sensitive and classified information* **[OPPORTUNITY]** *in a company that performs government-sponsored R&D* **[ORGANIZATION: Victim Organization]**.

John uses his personal web-based email account from his work computer to communicate with prospective employers **[DIGITAL ACTION/EMAIL ACTION]**. *Then he uses his administrative privileges to access some sensitive intellectual property information* [**BUSINESS INFORMATION: INTELLECTUAL PROPERTY**] *that will be of interest to a competitor. John saves these files to his computer* [**COMPUTER ASSET: WORK PC**] *and copies the files to a thumb drive* [**CONCERNING BEHAVIOR: TECH/CYBER VIOLATION–DIGITAL ACTION/COPY ACTION**] [**PHYSICAL ASSET: USB DRIVE**], *which he then sneaks out of the office with the intention of using the information to leverage a job offer with a competitor* [**THEFT EVENT: DATA THEFT**]. *Subsequently John resigns and accepts a job offer from a competitor.*

Scenario 2 Highlights Contribution of Human Factors

Scenario#2 adds realistic human/ behavioral factors to the scenario.

Adding **individual behavioral (human) factors**, and **organizational factors** enhances contextual knowledge of relationships among detected technical actions.

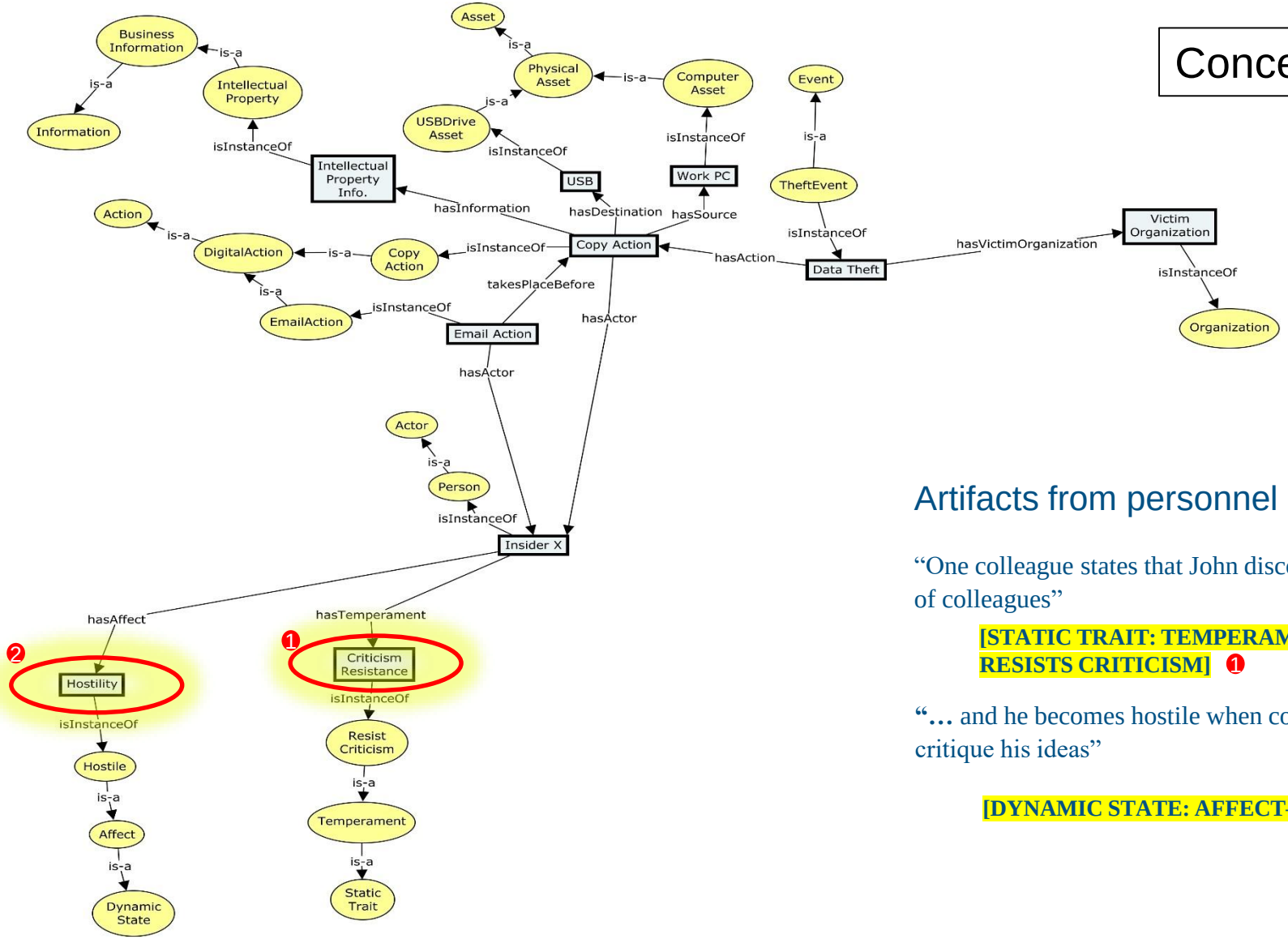
Use Case #2

*John **[PERSON: Insider X]** is a long-time system administrator **[LIFE NARRATIVE: PERS HISTORY] [CAPABILITY]** with access to sensitive and classified information **[OPPORTUNITY]** in a company that performs government-sponsored R&D **[ORGANIZATION: Victim Organization]**. The following input was recorded in his personnel file: (1) One colleague states that John discounts the opinions of colleagues and he becomes hostile when colleagues discuss and critique his ideas **[STATIC TRAIT: TEMPERAMENT: RESISTS CRITICISM] [DYNAMIC STATE: AFFECT—HOSTILE]**. (2) A different colleague states that John seeks to control all aspects of a project and often insists on dominating the conversation about project tasks and approach **[STATIC TRAIT: OTHER PERSONALITY DIMENSIONS—AUTHORITARIANISM]**. (3) His manager corroborates these inputs and adds that John tends to become argumentative and irritated, and defensively cites his superior knowledge of industry best practices when others criticize his rigid protocols **[DYNAMIC STATE: AFFECT–HOSTILE] [STATIC TRAIT: TEMPERAMENT—BIG EGO]**. Staff development/performance review assessment includes criticism by colleagues that portions of his protocols are idiosyncratic with weak rationale, and that his rigid protocols have impacted company projects **[CONCERNING BEHAVIORS: JOB PERF—NEGATIVE PERF EVALUATION]**.*

*John was passed over for a promotion to manage a new, prestigious project **[LIFE NARRATIVE: PERS HISTORY: EMPLOYMENT–PASSED OVER FOR PROMOTION]**. He files a complaint with HR claiming unfair treatment and his manager, compelled to meet with him, comes away with the impression that John still harbors resentment over not being promoted. John's most recent evaluation cited a decline in performance **[CONCERNING BEHAVIORS: JOB PERF—NEGATIVE PERF EVALUATION]**; since being denied the promotion his attitude has been increasingly disgruntled **[DYNAMIC STATE: ATTITUDE—DISGRUNTLEMENT]**; and that there were multiple complaints from coworkers about frequent tardiness **[CONCERNING BEHAVIORS: BOUNDARY VIOLATION—ATTENDANCE]**. The attendance problem led to a formal, written warning **[CONCERNING BEHAVIORS: BOUNDARY VIOLATION–POLICY VIOLATION]**. After getting the warning, John talks to his manager and loses his cool--storming out of the office **[DYNAMIC STATE: AFFECT–HOSTILE]**. A colleague hears John's outburst and tells the manager about John's recent marital separation to provide some context to Johns behavior **[LIFE NARRATIVE: PERS HISTORY—MAJOR LIFE EVENTS/RECENT CHANGE IN MARITAL STATUS (MARITAL SEPARATION)]**. The incident prompts the manager to contact the company Security Office. The Security Office checks the local court records to learn that three weeks ago, John was arrested for allegedly driving under the influence (his first contact with the criminal justice system) **[LIFE NARRATIVE: CRIMINAL RECORD—DUI]**.*

*Faced with these job and personal stressors, John begins to seek work with a competitor. John contacts a competitor to see if they are interested in him and in the information he can provide. To avoid being noticed, John carries out email dialogue with the competitor by logging into his personal Yahoo web mail account from his work computer **[CONCERNING BEHAVIORS: JOB PERFORMANCE—CYBERLOAFING]**. Next, John carries out the insider threat attack and resigns, as described in second paragraph of Use Case #1.*

Incrementally Adding Human Factors to Concept Map…



Concept Map

Artifacts from personnel record:

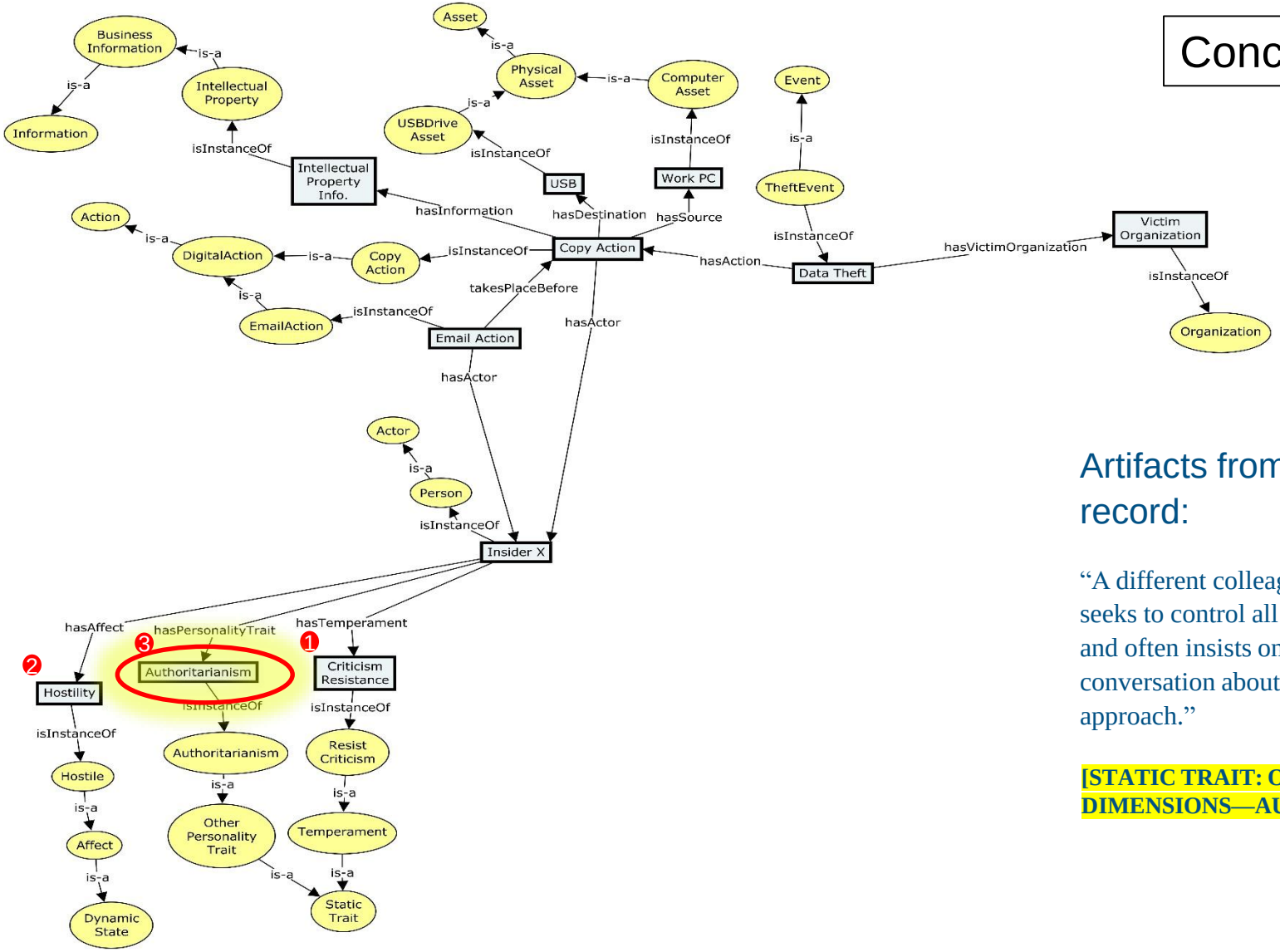
"One colleague states that John discounts the opinions of colleagues"

[STATIC TRAIT: TEMPERAMENT: RESISTS CRITICISM] ❶

"**…** and he becomes hostile when colleagues discuss and critique his ideas"

[DYNAMIC STATE: AFFECT–HOSTILE] ❷

Incrementally Adding Human Factors to Concept Map…



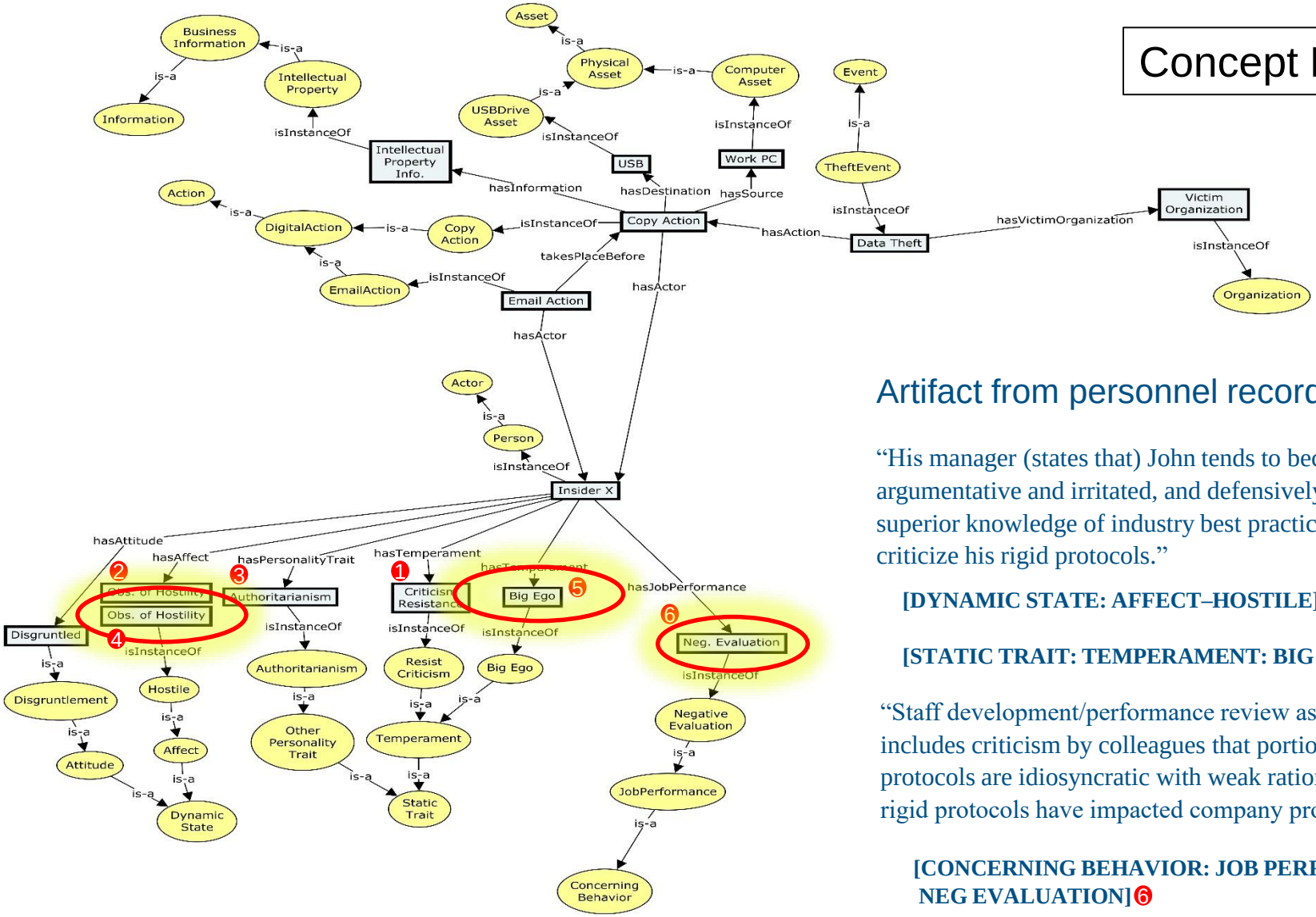
Concept Map

Artifacts from personnel record:

"A different colleague states that John seeks to control all aspects of a project and often insists on dominating the conversation about project tasks and approach."

[STATIC TRAIT: OTHER PERSONALITY DIMENSIONS—AUTHORITARIANISM] ❸

Incrementally Adding Human Factors to Concept Map…



Artifact from personnel record:

"His manager (states that) John tends to become argumentative and irritated, and defensively cites his superior knowledge of industry best practices when others criticize his rigid protocols."

[DYNAMIC STATE: AFFECT–HOSTILE] ❹

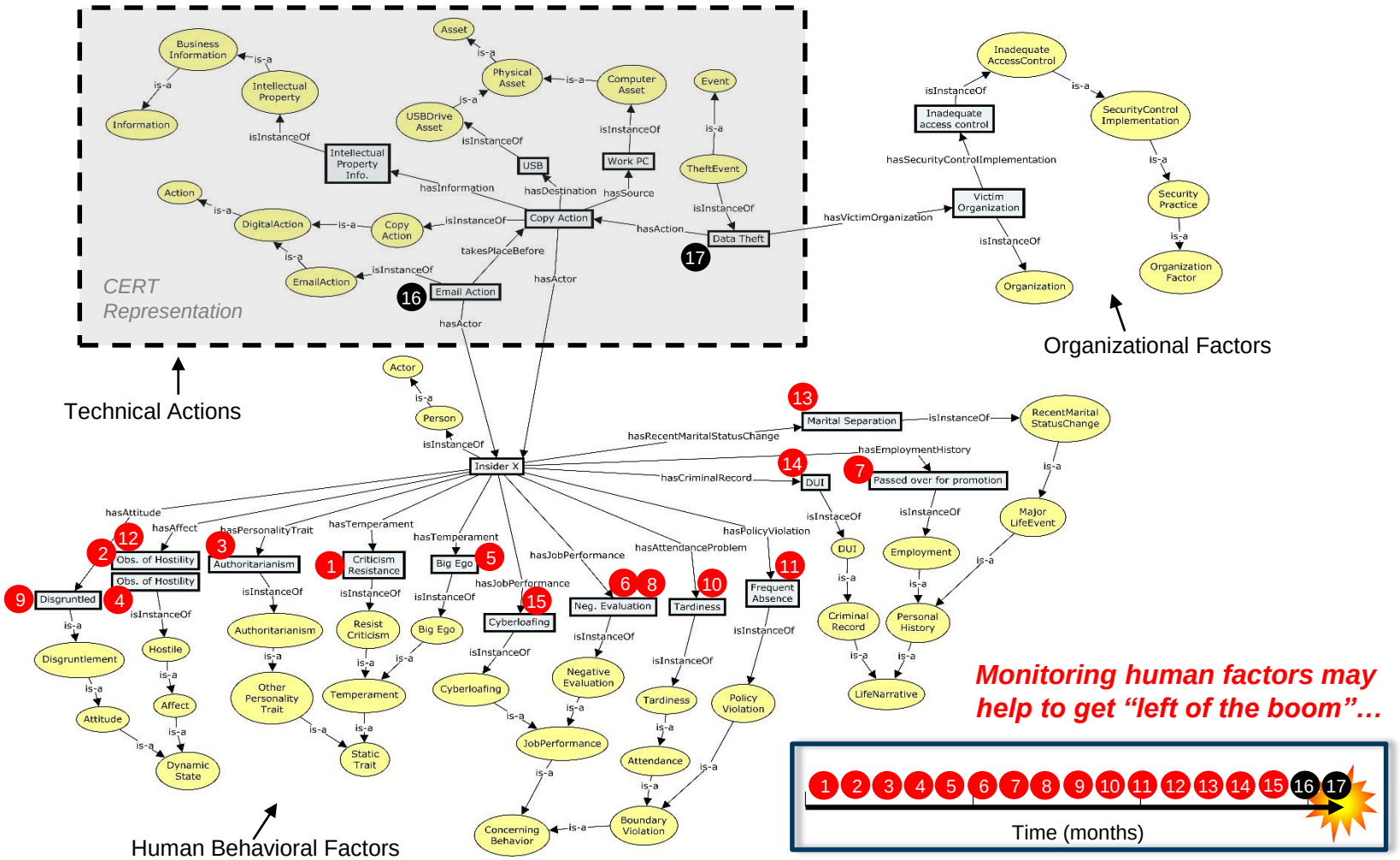
[STATIC TRAIT: TEMPERAMENT: BIG EGO]. ❺

"Staff development/performance review assessment includes criticism by colleagues that portions of his protocols are idiosyncratic with weak rationale, and that his rigid protocols have impacted company projects."

[CONCERNING BEHAVIOR: JOB PERFORMANCE—NEG EVALUATION] ❻

Full Concept Map Reveals Richer Representation

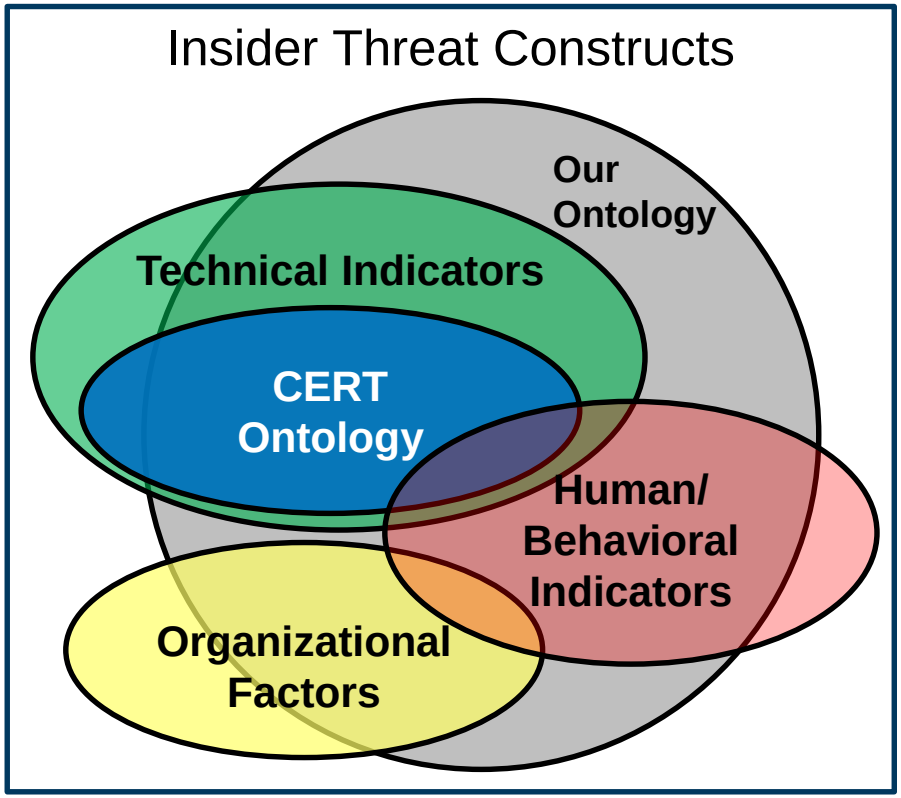
Our Ontology incorporates contextual knowledge of relationships among detected **technical actions**, **individual behavioral (human) factors**, and **organizational factors**



Comparison with Related Work

- Class structure in CERT's insider threat ontology defines 125 constructs
  - Focus is on technical/cyber events
  - Defines 31 actions (e.g., *copy*), in four major behavior classes (e.g., *digital*, *financial*, *job-related* insider threat behavior) associated with exploits on 26 assets (e.g., USB drive) and 16 types of information (e.g., password).

- The CERT ontology provides a foundation for representing technical/cyber actions – we have fully incorporated the CERT ontology
- Our ontology is substantially broader and deeper than the CERT ontology
  - We defined branches of the knowledge base for individual and organizational socio-technical constructs
  - Our ontology is 6-7 levels deep and includes more than 350 constructs



Future Plans

Future R&D focuses on:

- Continuing to populate individual and organizational classes of ontology with relevant instances
- Share these results with the research community and organizations so that they can actually start working towards collecting such behavioral data and analyzing it using our proposed solution.
- Extend our ontology into a probabilistic ontology to support reasoning under uncertainty, by incorporating information about uncertainty in the insider threat domain.

Conclusions

This research addressed two major challenges:

- Facilitating model development
- Establishing a common terminology and shared understanding of insider threat domain

Contributions:

- Knowledge representation more fully characterizes insider threat indicators, from perspective of human behavior as well as cyber/technical indicators
- Knowledge base is shareable to facilitate reuse and collaboration
- Product of the work will facilitate model development and inform operational risk management practice
- Ontology can inform scenario generation to support testing of insider threat tools