Design and Implementation of a Comprehensive Insider Threat Ontology

James D. Lee

George Mason University

Design and Implementation of a Comprehensive Insider Threat Ontology

17th Annual Conference on Systems Engineering Research (CSER) 2019
Washington, D.C., April 3-4, 2019

Paper Session 13 (11:00 – 11:20 AM)

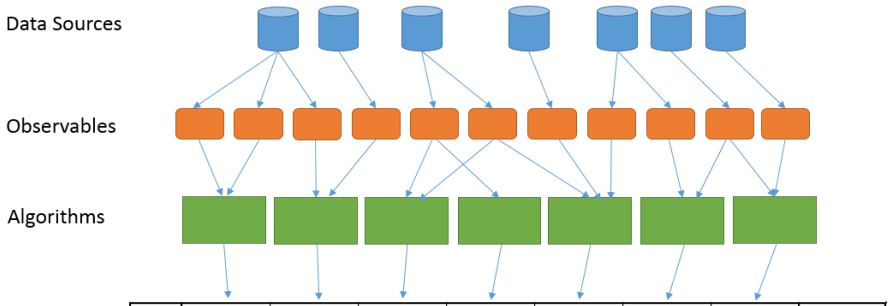
Dr. Frank L. Greitzer
James D. Lee (Presenter)
Justin Purl
Dr. Abbas K. Zaidi

Overview

- Background
  - Insider threat detection
  - Problem statement
- Sociotechnical and Organizational Factors for Insider Threat (SOFIT)
- Ontology Implementation
- Applications
- Conclusion

Background

- In 2016, 874 insider threat incidents across 54 organizations averaged $4.3M damage/organization [1]
- Organizations' response to mitigate insider threat risk varies widely from *reactive* to *proactive* and *predictive*
- Best practices employ a predictive approach that monitors a variety of technical and behavioral data:



	Indicator 1	Indicator 2	Indicator 3	Indicator 4	Indicator 5	Indicator 6	Indicator 7	Target Behavior
user1	**TRUE**	FALSE	**TRUE**	**TRUE**	FALSE	**TRUE**	**TRUE**	Yes
user2	FALSE	**TRUE**	FALSE	**TRUE**	**TRUE**	FALSE	**TRUE**	Yes
user3	FALSE	FALSE	**TRUE**	FALSE	**TRUE**	**TRUE**	FALSE	No
user4	FALSE	FALSE	FALSE	**TRUE**	FALSE	**TRUE**	**TRUE**	No
user5	FALSE	FALSE	FALSE	FALSE	**TRUE**	FALSE	**TRUE**	No

- Data processed to observables
- Collection of observables infer indicators
- Indicators infer target (threat) behavior

Problem Statement

Challenges:

- Making inferences based on incomplete and uncertain data
- Lack of completeness and accuracy of a single source knowledge base that informs such inferences
- Non-optimal data – data that are the most available may not always be the most useful for particular types of threat
- Lack of ground truth required for testing mitigation approaches
- Need for better understanding of:
  - Indicators that infer target (threat) behavior
  - Collection of observables that infer indicators
  - Necessary data given the observables of interest

Approach

- Adoption of comprehensive Insider Threat factor knowledge base as an ontology
  - To provide a **common structure** of the knowledge of the domain
  - To facilitate **sharing** of the knowledge base
  - To **enable** knowledge base to be **applied to a variety of missions**

Why Ontology?

- Formal description of concepts within domain
- Formal semantics and constraints provide computational properties
- Ability to draw inferences from asserted facts

Related Work

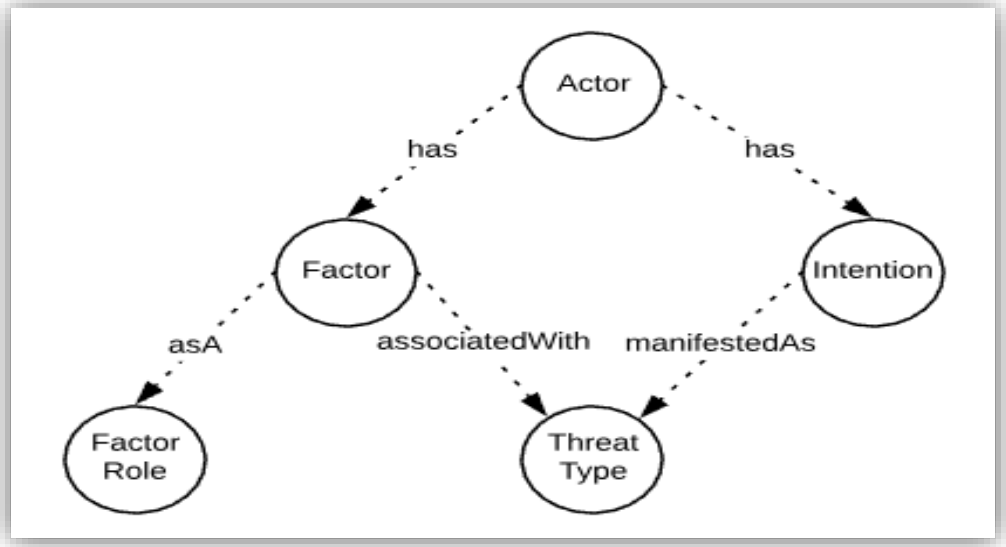
- This work derives from a large base of published research and case studies (especially CERT reports and publications, e.g. [2] and [3]; and research by Greitzer and colleagues [4])
- Development of SOFIT is documented in [5]-[7]

Summary of Current Ontology Representations in Cybersecurity/Insider Threat				
Ontology/Reference	Domain/Scope	Types of Constructs Represented		
		Technical/ Cyber	Human/ Behavioral	Organizational
CERT ITIO	**Insider Threat**	✓	-	-
MITRE (STIX)	Cyber Security	✓	-	-
MITRE (CAPEC)	Cyber Security - Attack Patterns	✓	-	-
MITRE (CWE)	Cyber Security - Weaknesses	✓	-	-
MAEC	Cyber Security - Malware	✓	-	-
CRATELO	Cyber Security	✓	-	-
HUFO	Cyber Security - Trust	✓	✓	-
SOFIT	**Insider Threat**	✓	✓	✓

Design Objectives

- Use Case 1. Ontology capturing expert knowledge on insider threat factors that may be shared with research/operational communities.
- Use Case 2. Support development of a tool to evaluate the coverage of an organization's insider threat mitigation program compared to 'best practices'.
- Use Case 3. Support development of tools to assess insider threat risk for individuals in an organization.

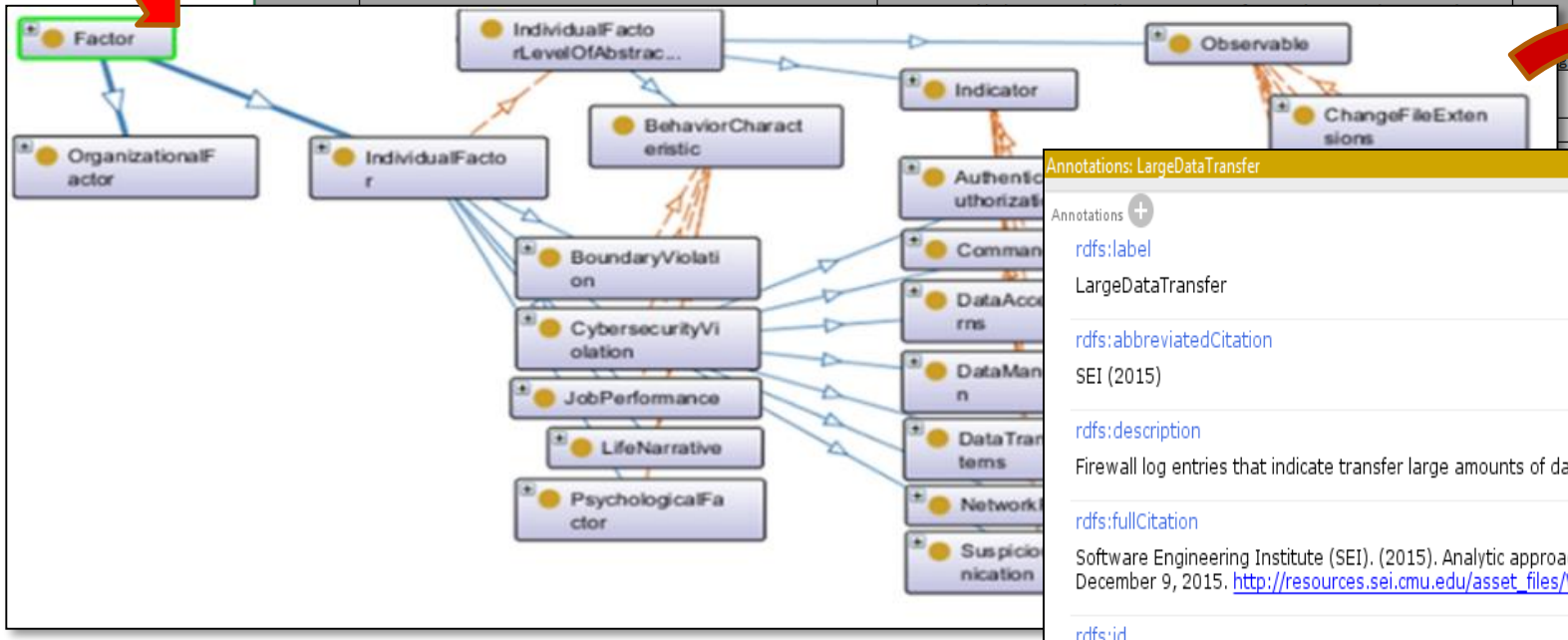
Ontology Overview

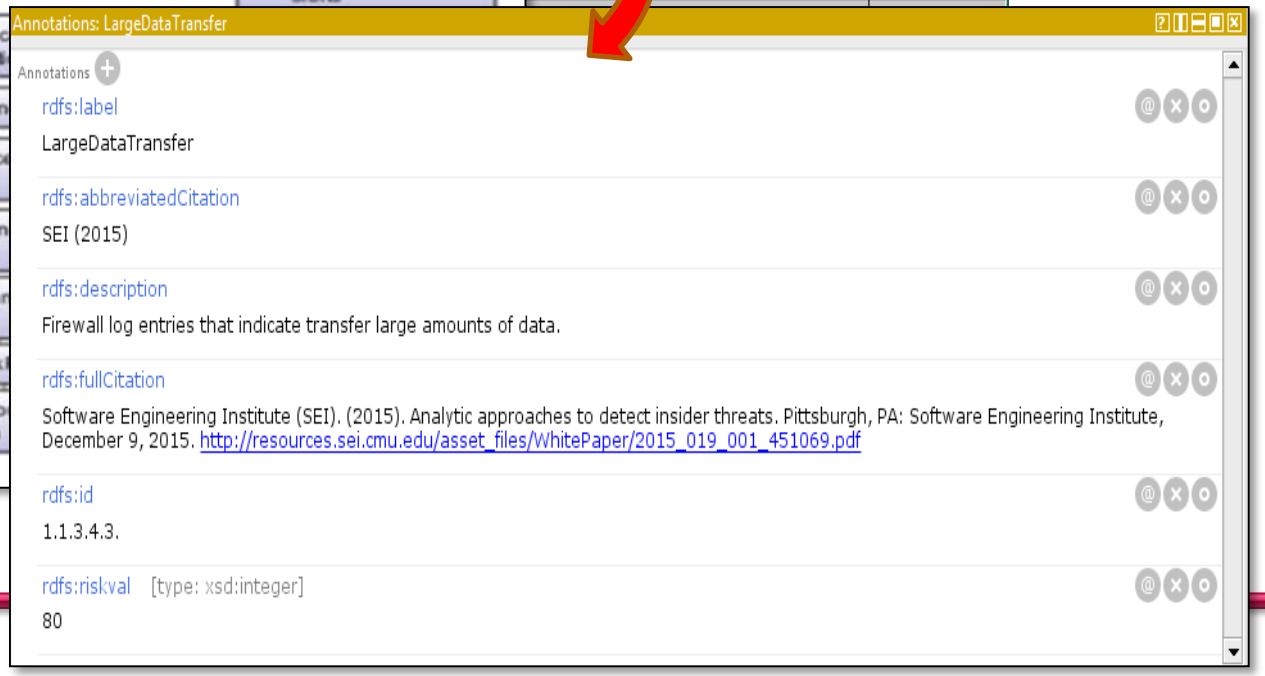


- Actor has Factor and Intention
- Intention is manifested as Threat Type
- Factor is associated with Threat Type and plays a role (Factor Role) in process of insider threat exploit

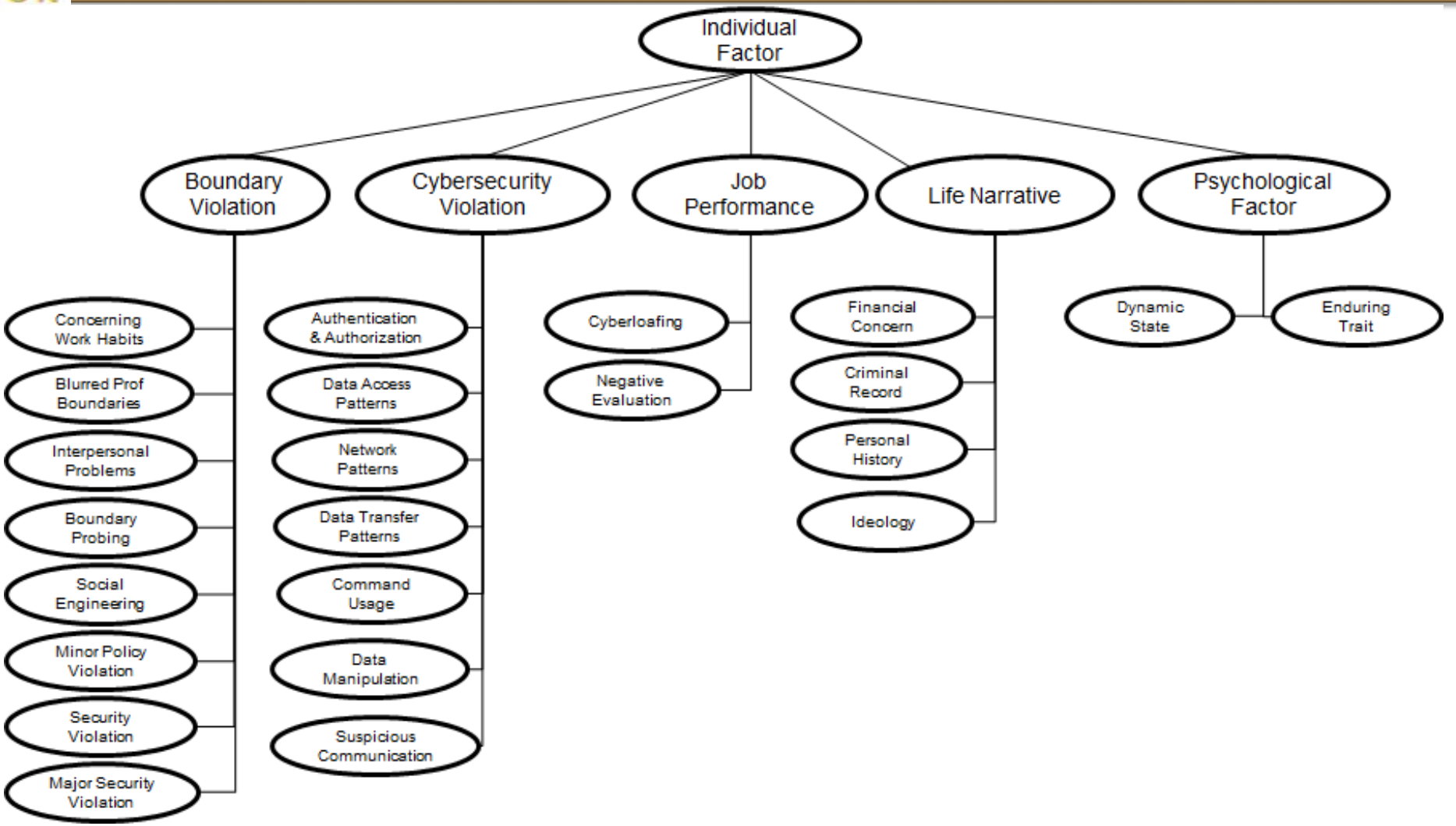
Taxonomy of Factors

ID	Factor Label	Description	Abbreviated Citation	Risk Value
1.	Factor	Characteristic relevant to assessment of insider threat.		
1.1.	Individual Factor	Individual human factors pertaining to human characteristics or behaviors in insider threat domain.	Band et al. (2006); Keeney et al. (2005)	
	Boundary Violation	Action by a person that is outside of normal or accepted behaviors. This may include actions up to the level of organizational policy violations.	Bulling et al. (2008)	
1.	Concerning Work Habits	Work habits and patterns that are potentially of concern for an enterprise.	Bulling et al. (2008)	
1.1.1.1.1.	Working At Unusual Hours	Working at hours markedly different from peers.	Bulling et al. (2008)	43
1.1.1.1.1.1.	Odd Hours Work Machine	Using work-owned machine outside of normal work hours.	IARPA SCITE Program	35
1.1.1.1.1.2.	Odd Hours Work Week	Changes times at which s/he regularly works during work week.	IARPA SCITE Program	30
1.1.1.1.1.3.	Odd Hours Work Week Offsite	Changes periodicity of work done at home or remote sites during work week.	IARPA SCITE Program	32
1.1.1.1.2.	Change Work Performed Offsite During Week	Changes amount of work done at home or at remote sites during work week.	IARPA SCITE Program	30
			et al. (2008)	
				22
				29

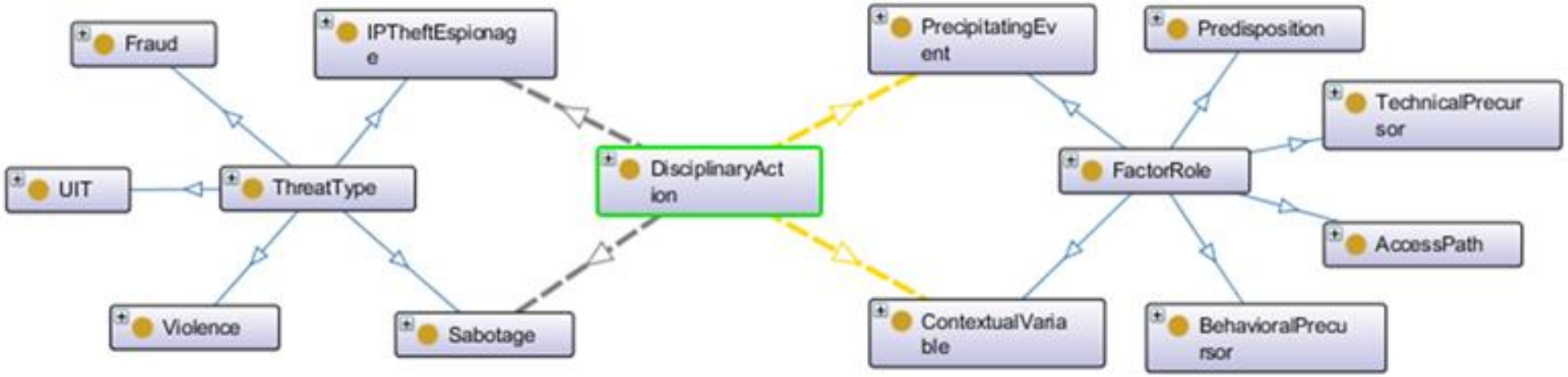




Individual Factor Class



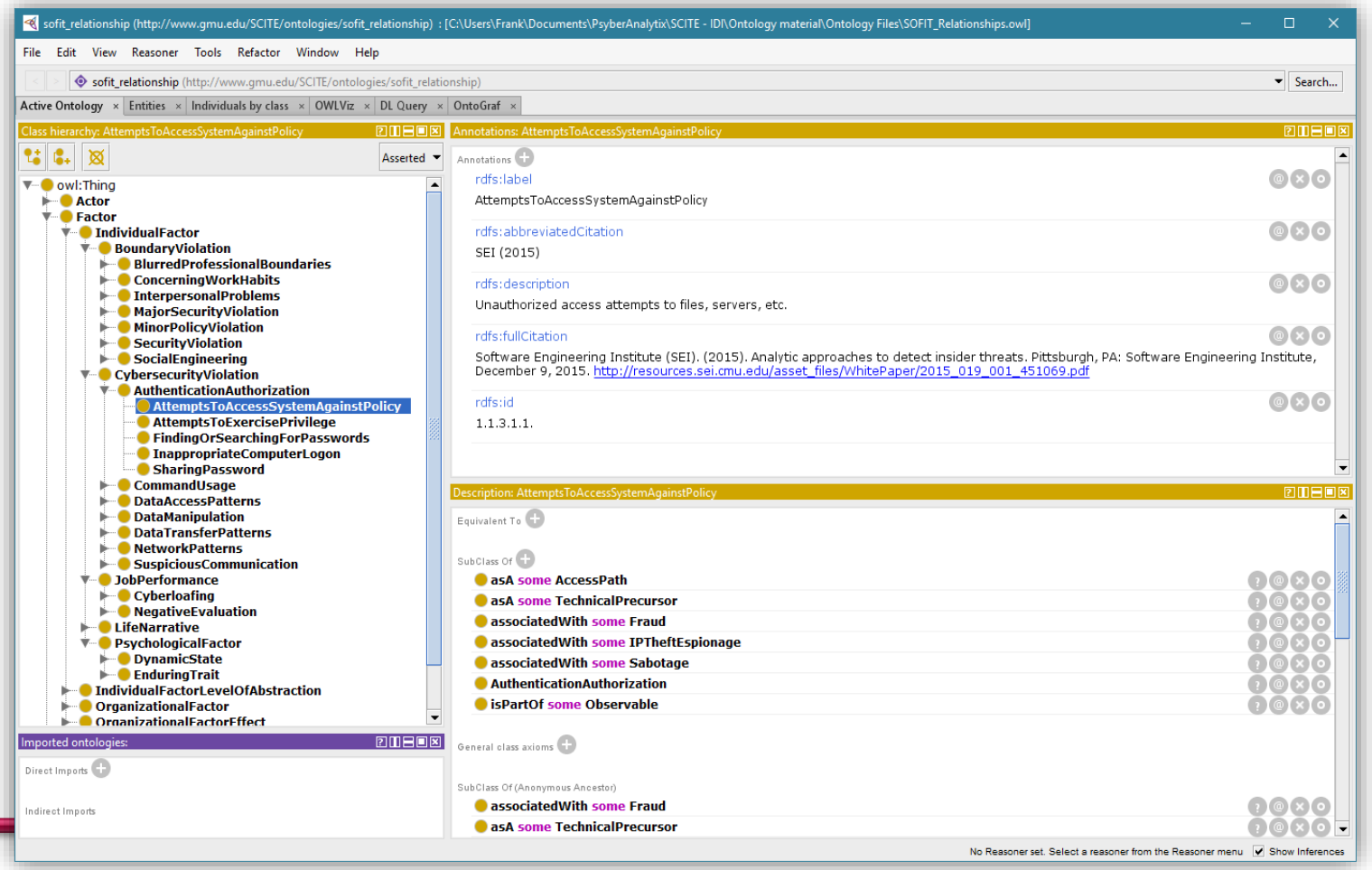
Threat Type and Factor Role



Use Case 1: Knowledge Base to Inform Research and Operational Communities

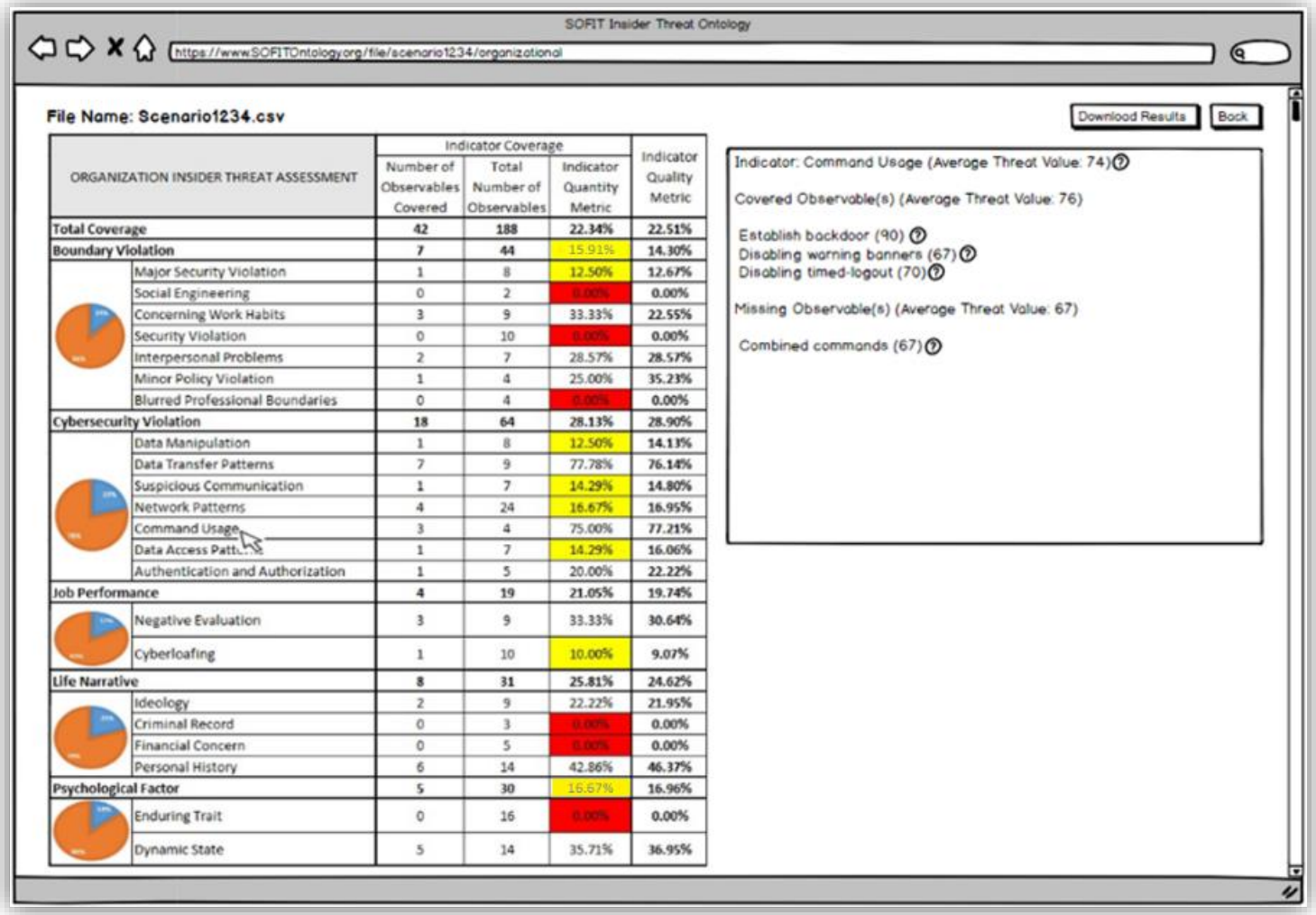
SOFIT is a comprehensive knowledge base for insider threat technical and behavioral indicators

- Implemented as an **ontology** with over 320 constructs (factors), including
  - **Individual (Human) Factor** branch contains more than 270 technical and behavioral factors
  - **Organizational Factor** branch includes roughly 50 contributing factors
- Current work focuses on applying the ontology to support modeling and inferences about insider threat.



Use Case 2: Foundation for Tools to Assess an Organization's Insider Threat Monitoring Program

Compare the indicators detectable by the organization's system against indicators identified in SOFIT and/or best practices



ORGANIZATION INSIDER THREAT ASSESSMENT		Indicator Coverage: Number of Observables Covered	Indicator Coverage: Total Number of Observables	Indicator Coverage: Indicator Quantity Metric	Indicator Quality Metric
Total Coverage		**42**	**188**	**22.34%**	**22.51%**
Boundary Violation		**7**	**44**	15.91%	**14.30%**
	Major Security Violation	1	8	12.50%	**12.67%**
	Social Engineering	0	2	0.00%	**0.00%**
	Concerning Work Habits	3	9	33.33%	**22.55%**
	Security Violation	0	10	0.00%	**0.00%**
	Interpersonal Problems	2	7	28.57%	**28.57%**
	Minor Policy Violation	1	4	25.00%	**35.23%**
	Blurred Professional Boundaries	0	4	0.00%	**0.00%**
Cybersecurity Violation		**18**	**64**	**28.13%**	**28.90%**
	Data Manipulation	1	8	12.50%	**14.13%**
	Data Transfer Patterns	7	9	77.78%	**76.14%**
	Suspicious Communication	1	7	14.29%	**14.80%**
	Network Patterns	4	24	16.67%	**16.95%**
	Command Usage	3	4	75.00%	**77.21%**
	Data Access Patterns	1	7	14.29%	**16.06%**
	Authentication and Authorization	1	5	20.00%	**22.22%**
Job Performance		**4**	**19**	**21.05%**	**19.74%**
	Negative Evaluation	3	9	33.33%	**30.64%**
	Cyberloafing	1	10	10.00%	**9.07%**
Life Narrative		**8**	**31**	**25.81%**	**24.62%**
	Ideology	2	9	22.22%	**21.95%**
	Criminal Record	0	3	0.00%	**0.00%**
	Financial Concern	0	5	0.00%	**0.00%**
	Personal History	6	14	42.86%	**46.37%**
Psychological Factor		**5**	**30**	16.67%	**16.96%**
	Enduring Trait	0	16	0.00%	**0.00%**
	Dynamic State	5	14	35.71%	**36.95%**

Conceptual Illustration

Use Case 3: Foundation for Qualitative and Quantitative Insider Threat Assessment Tool

Ongoing research to estimate quantitative threat/risk values for individual indicators that can inform threat assessment models…

Qualitative Assessment

Case #1
- Depression
- Misses or late for meetings
- Recent change in marital status
- Receiving large email attachments
- Requires excessive oversight

Case #2
- Terminated
- Extreme discontent
- Establish backdoor
- Transfer large amount of data
- Strong reaction to organizational sanctions

```
SELECT DISTINCT ?Property ?Value
WHERE {
  ?a rdfs:label "DisciplinaryAction".
  ?a rdfs:subClassOf ?b.
  ?b owl:onProperty ?c; owl:someValuesFrom ?d.
  {?c rdfs:label "asA"} UNION {?c rdfs:label "associatedWith"}.
  ?c rdfs:label ?Property.
  ?d rdfs:label ?Value
}
```

	Property	Value
1	"asA"	"ContextualVariable"
2	"associatedWith"	"IPTheftEspionage"
3	"associatedWith"	"Sabotage"
4	"asA"	"PrecipitatingEvent"

Characterization of Case #1	Characterization of Case #2
Precipitating Event • Recent change in marital status Behavioral Precursor • Misses or late for meetings Contextual Variable • Depression • Receiving large email attachments • Requires excessive oversight Indication of Insider Threat: None While there are contextual factors of concern about this employee that may indicate a need for follow-up, there is no indication that this person represents an insider threat risk.	Precipitating Event • Terminated Behavioral Precursor • Extreme discontent • Strong reaction to organizational sanctions Technical Precursor • Establish backdoor • Transfer large amount of data Indication of Insider Threat: Strong The presence of both behavioral and technical precursors, as well as a precipitating event associated with insider threat risk, yields a high level of concern that justifies further analysis by insider threat team.

Quantitative Assessment

"additive" model example

Indicator	Score	Indicator	Score
Case #1		**Case #2**	
Depression	52	Terminated	69
Misses or late for meetings	38	Extreme discontent	66
Recent change in marital status	35	Establish backdoor	90
Receiving large email attachments	55	Transfer large amount of data	80
Requires excessive oversight	39	Strong reaction to organizational sanctions	69
Threat Value for Case #1:	**219**	**Threat Value for Case #2:**	**374**

Ongoing Research Supporting the Use Cases

Over the last 2 years we have conducted several expert knowledge elicitation surveys to support our objectives for Use Cases 1, 2 and 3:

- Helped to populate the ontology with expert judgments of threat/risk level for individual indicators
- Helped to test various quantitative models that describe how experts assess collections of observed indicators to determine overall threat/risk of insider threat cases

Because there was no access to operational test data with ground truth, these studies used expert judgments as "proxies" in evaluating models.

Conclusion

Contributions:

- Development of a comprehensive insider threat ontology that may be shared with operational and research communities
- Foundation for development of applications for
  - Assessing an organization's insider threat program
  - Individual insider threat assessment tools (qualitative & quantitative)
- Empirical studies obtained expert judgments to inform the ontology and to test proposed models of individual threat assessment

Limitations:

- While the knowledge base has been informed by expert judgments, the ontology and associated threat models have not been validated against operational data with ground truth.

References Cited in Talk

1. '2016 Cost of Insider Threats'. Ponemon Institute/Dtex Systems,Sept 2016. Accessed April 2018.
2. Band, SR., DM Cappelli, LF Fischer, AP Moore, ED Shaw, & RF Trzeciak. (2006). *Comparing insider IT sabotage and espionage: a model-based analysis*. Carnegie-Mellon University, SEI/CERT Coordination Center. CMU/SEI-2006-TR-026.
3. Costa, DL, M Collins, JS Perl, JM Albrethsen, JG Silowash, & D Spooner. (2014). An Ontology for Insider Threat Indicators. In K. B. Laskey, I. Emmons and P C.G. Costa (Eds.), *Proceedings of the Ninth Conference on Semantic Technologies for Intelligence, Defense, and Security* (STIDS 2014), 2014, 48–53.
4. Greitzer FL, and DA Frincke. (2010). "Combining Traditional Cyber Security Audit Data with Psychosocial Data: Towards Predictive Modeling for Insider Threat Mitigation." In *Insider Threats in Cyber Security*, ed. CW Probst, J Hunter, D Gollmann & M Bishop, pp. 85-113. Springer, New York. http://dx/doi.org/10.1007/978-1-4419-7133-3_5.
5. Greitzer, FL, M Imran, J Purl, ET Axelrad, YM Leong, DE Becker, KB Laskey, & 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.
6. Greitzer, FL, J Purl, YM Leong & DE Becker. (2018). SOFIT: Sociotechnical and Organizational Factors for Insider Threat. *IEEE Symposium on Security & Privacy, Workshop on Research for Insider Threat (WRIT)*, San Francisco, CA, May 24, 2018.
7. Greitzer, FL, J Purl, DE Becker, P Sticha, & YM Leong. (2019). Modeling expert judgments of insider threat using ontology structure: Effects of individual indicator threat value and class membership. *52nd Hawaii International Conference on Systems Sciences (HICSS-52)*, Big Island, Hawaii, January 2019.

Contact Information

- For more information, please contact:

Frank L. Greitzer, *PsyberAnalytix*
Frank@PsyberAnalytix.com

- Acknowledgments:

SOFIT: SOCIOTECHNICAL AND ORGANIZATIONAL FACTORS FOR INSIDER THREAT

Development Team/Knowledge Base Design:

Frank L. Greitzer, PsyberAnalytix
Justin Purl, Human Resources Research Organization
Yung Mei Leong, Independent Contractor
D.E. (Sunny) Becker, Human Resources Research Organization
Paul J. Sticha, Human Resources Research Organization

Ontology Implementation:

James Lee, George Mason University
Abbas Zaidi, George Mason University
Kathryn Laskey, George Mason University

This research 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.