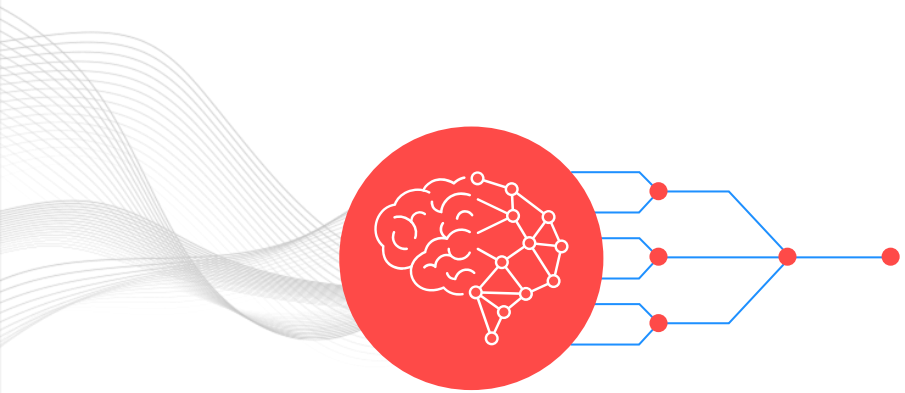


An Updated Insider Threat Potential Risk Indicator Knowledge Base

Workshop on Research for Insider Threat (WRIT)

Frank L. Greitzer, PhD

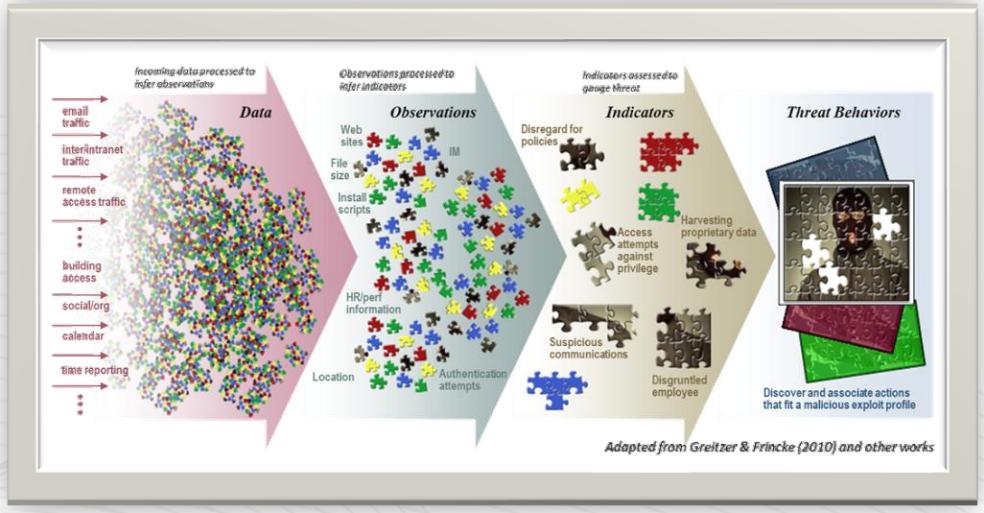
fgreitzer@cogility.com

June 5, 2025

COGILITY

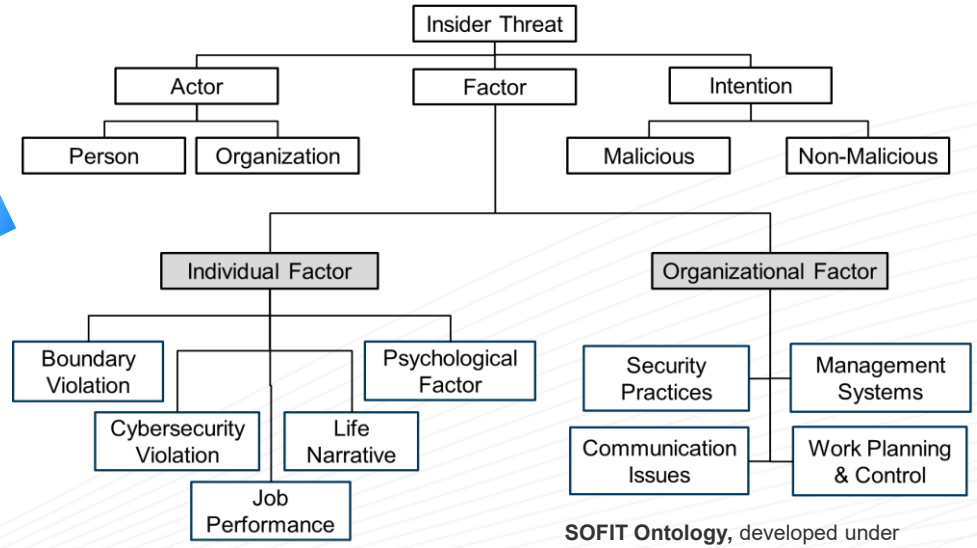
Potential Risk Indicators (PRIs)

My research emphasizes patterns of PRIS…



Framework for modeling insider risk based on behavioral, technical and organizational factors.

SOFIT: *Sociotechnical and Organizational Factors for Insider Threat*



SOFIT Ontology, developed under IARPA funding [Greitzer et al (2018)]

Executive Order 13587 (2011)

COGILITY

Original SOFIT PRI Knowledge Base – Individual Factors

Classes

Sub-Classes

Boundary Violations

Concerning Work Habits

- Working unusual hours
- Exhibiting incidents of physical violence
- Persistent lateness
- Poor time management
- Past untruthful-ness
- Lack of attention
- High workload
- Illness
- Lack of knowledge, training

Policy/Compliance Violations

- Accessing classified information without need-to-know
- Violating security practices
- Ignore security norms
- Improper handling of classified material
- Possessing illegal weapons
- Possessing illegal drugs

Job Performance

HR Concerns

- Dismissal
- Failure to return company property
- Demotion
- New hire
- Resigned

Job Status

- Declining job performance
- Passed over for promotion
- Unexcused absences
- Disciplinary actions

Life Narrative Factors

Financial Concerns

- Unexplained affluence
- Failure to comply with regulations for reporting foreign contacts or foreign travel
- Financial concerns – excessive debts
- Bankruptcy

Foreign Ties

- Frequent personal travel
- Ties to Foreign defense contractor
- Frequent, unreported contact with foreign persons

Criminal Activities

- Restraining order
- Wage garnishment
- Engaged in criminal activity
- Lying to investigators

Ideology

- Associating with extremist group
- Expressing ill will toward U.S. Gov't
- Extremist views

Psychosocial Issues

Beh Health

- Depression
- Anxiety/ Sleep disturbances

Interpersonal

- Aggression, intimidation
- Disgruntled

Personality

- Manipulative
- Lack of empathy
- Narcissism
- Mental health counseling

Technical Violations

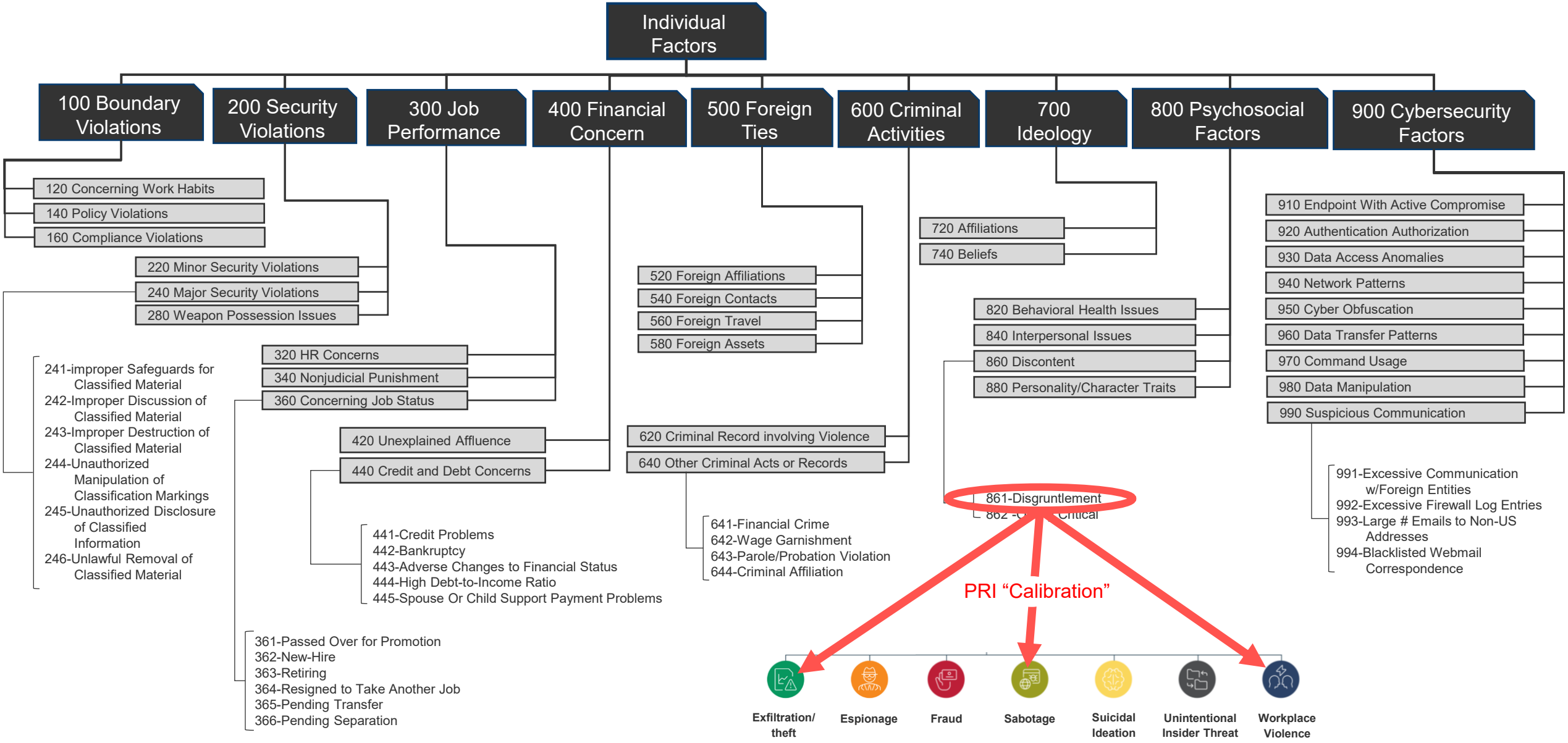
Cybersecurity Violations

- Attempts to access files without authorization
- Manipulation or destruction of sensitive information
- Access other users' credentials
- Misuse of U.S. Government information systems
- Unauthorized storage device
- Large data transfer

[This is a subset representing approximately 15% of the entire SOFIT PRI Framework]

COGILITY

SOFIT 2.0 PRI KNOWLEDGE BASE



4

Three “D’s” Behind SOFIT 2.0

1. Difficulty **Differentiating PRIs** → Consolidation/ ”pruning”

2. PRI **Decay model concerns** → Hierarchy restructuring

3. **Dependencies** at higher-order abstractions → Incorporating higher-level patterns

1. Consolidation / Pruning of PRI Hierarchy

Difficulty Differentiating PRIs

Criteria for merging PRIs:

- Same/similar definitions
- Same data / means of detecting the PRIs
- Same/similar mappings to threat behaviors

Example
(cyberloafing)

- Original SOFIT: **1.1.2. Job Performance**
  1.1.2.1. Cyberloafing

1.1.2.1.1.	Excessive Personal Use Of Work Computer	Non-productive or personal use of computer at work.
1.1.2.1.2.	Excessive Use Of Personal Webmail At Work	Unsanctioned or excessive use of personal webmail at work.
1.1.2.1.3.	Excessive Personal Use Of Work Email	Unsanctioned or excessive use of work email for personal use.
1.1.2.1.4.	Excessive Browsing To Non-Work Related Websites	Excessive access to non-work related websites.
1.1.2.1.5.	Playing Computer Games	Unsanctioned or excessive use of computer games at work.
1.1.2.1.6.	Using Social Media	Personal use of social media (e.g., Facebook, Twitter, messaging) at work.
1.1.2.1.7.	Watching Online Videos	Viewing online videos (e.g., YouTube) for personal use.
1.1.2.1.8.	Online Shopping Or Gambling	Accessing online shopping sites or online gambling sites.
1.1.2.1.9.	Managing Finances	Accessing online financial sites for personal use.
1.1.2.1.10.	Job Search	Unsanctioned (e.g., excessive) use of work time/resources in job search.

- SOFIT 2.0: **100 Boundary Violations**
  120. Concerning Work Habits
  127. Cyberloafing

127	Cyberloafing	Excessive or unsanctioned use of Internet during working hours for personal purposes. [e.g., computer games, social media, online videos, online shopping, online gambling] .

COGILITY

2. Improving PRI Decay Model

Initial model: PRIs decay based on ***role type…***

Greitzer et al. (2022)

- **Personal Predispositions**
- **Precipitating Events**
- **Behavioral Precursors**
- **Technical Precursors**

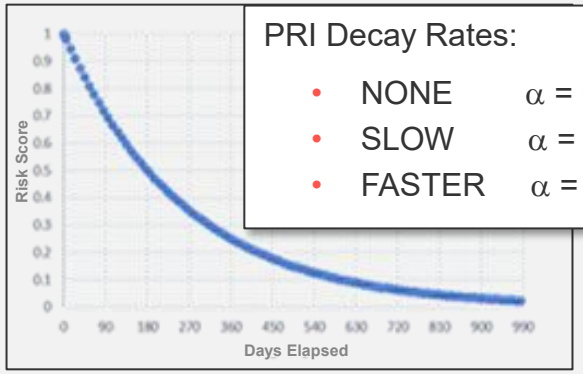
Inconsistencies were revealed in our research:

- Technical Precursors were assumed to exhibit relatively **high** decay rates, e.g.:
  - ***Printing to Anomalous Location***
  - ***Login failures***

  But:
  - ***Introduction of Malicious Code*** is a Technical Precursor with **low/no decay**
- Behavioral Precursors have mixed decay rates:
  - ***Attendance Issues***: **moderate** decay
  - ***Associating w/Extremist Group***: **low/no** decay
- Also: **SMEs reluctant to assign high decay rates.**

Updated PRI Decay Model

Exponential decay: The amount that a variable decays from one time to the next is proportional to the original value of the variable.



PRI Decay Rates:

- NONE $\alpha = 0.000$
- SLOW $\alpha = 0.004$ half-life = 6 mos., dissipates in 3 years
- FASTER $\alpha = 0.012$ half-life = 2 mos., dissipates in 1 year

PRI weight $p(t_1) = p(t_0)\,(1 - \alpha)^{(t_1 - t_0)}$

Examples

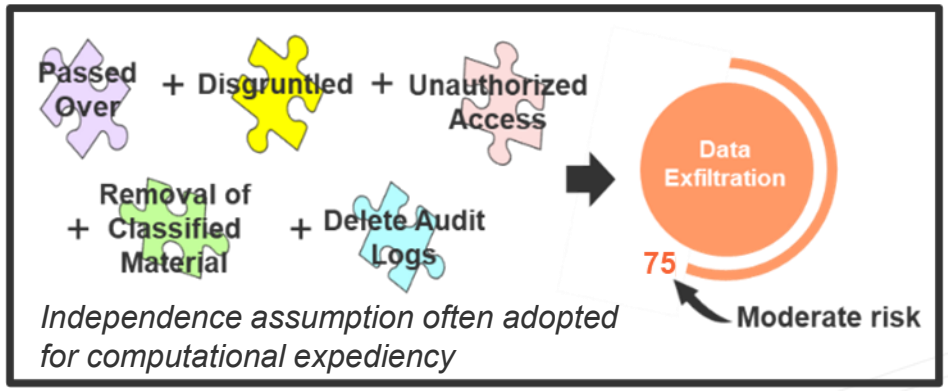
Decay Rate	Class	Sub-Class	PRI Examples
NONE	600 Criminal Activities	620 Criminal Record involving Violence	623. Exhibiting Violence at Work
	700 Ideology	740 Radical Beliefs	745. Express ill-will toward U.S.
	800 Psychosocial Factors	880 Personality or Character Traits	886. Narcissism
SLOW	400 Financial Concerns	440 Credit/Debt	442. Bankruptcy
	800 Psychosocial Factors	840 Interpersonal Issues	843. Anger/Aggression
FASTER	300 Job Performance	320 HR Concerns	324. Negative Evaluation – poor performance
	900 Cybersecurity Violation	940 Network Patterns	942. Use of unusual printer

COGILITY

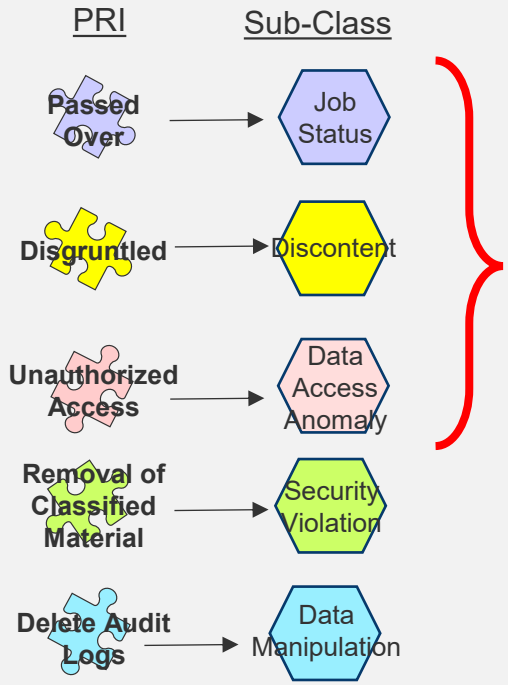
3. PRI Dependencies: Higher Level Patterns

Most models assume that individual indicators contribute independently to the risk analyst's judgment of threat…

Greitzer & Purl (2022)



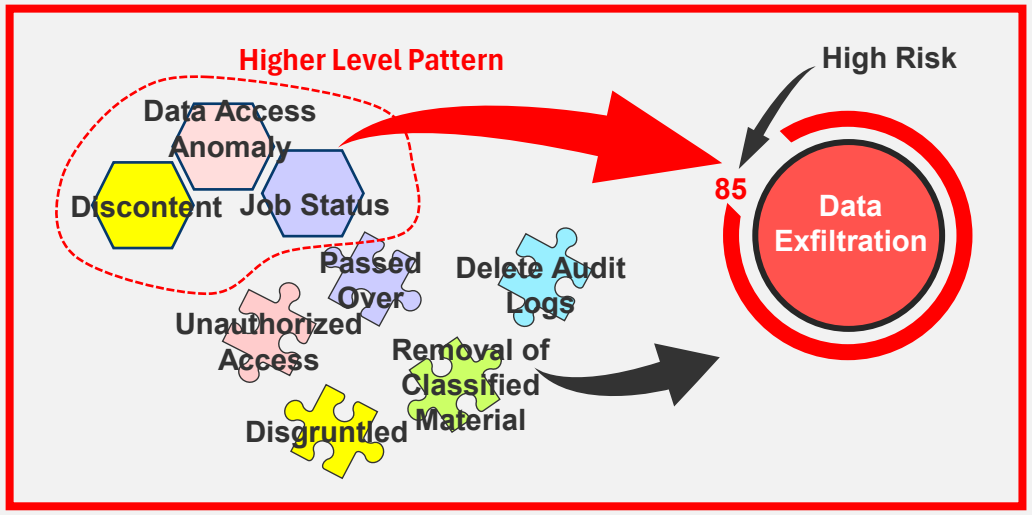
The SOFIT model incorporates higher abstractions…



Exfiltration

Analyze Contribution of higher-level patterns

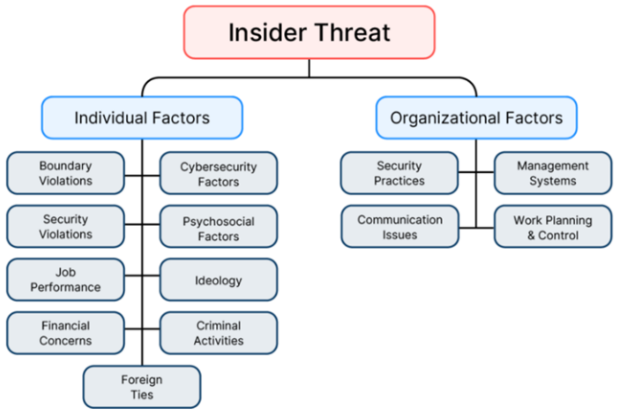
"The Whole is Greater Than the Sum of Its Parts"



COGILITY

SOFIT 2.0

https://cogility.com/sofit2/



cogility.com/sofit2

INDIVIDUAL FACTORS

SOFIT 2.0 Insider Risk Indicator Taxonomy		UPDATE DEVELOPED BY: Frank L. Greitzer, PhD			March 2025	MAPPING TO THREAT BEHAVIORS -- X = associated, Blank = unrelated						
SOFIT 2.0 ID	**SOFIT 1.0 ID**	**PRI Label**	**PRI Description**	**Abbreviated Citation**	**DECAY RATE**	**Fraud**	**WP Violence**	**Exfiltration**	**Espionage**	**Sabotage**	**UIT**	**Dom Terror**
100	1	Boundary Violations	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)								
120	1.1	Concerning Work Habits	Work habits and patterns that are potentially of concern for an enterprise.	Bulling et al. (2008)								
121	1.1.1	Working At Unusual Hours	Working at hours markedly different from peers.	Bulling et al. (2008)	MEDIUM	X		X	X	X		
122	1.1.2	Poor Time Management	Poor skills in planning and controlling how one spends the hours in the day to effectively accomplish tasks; may be manifested by procrastination.		MEDIUM			X			X	
123	1.1.3	Blurred Professional Boundaries	Interpersonal behavior, with colleagues or in professional setting, that is overly intrusive and/or overly personal, thus disrupting team morale/trust or mission focus; includes idle talk/rumors, especially about the personal affairs of others.	Bulling et al. (2008)	MEDIUM		X	X	X	X	X	
124	1.1.4	Nonproductive Socialization	Excessive idle talk, socializing, or gossiping about private affairs of others during working hours		MEDIUM			X			X	
125	1.1.5	Lack Of Confidentiality	Idle talk, rumors, gossiping---especially about personal or private affairs of others.		MEDIUM						X	

COGILITY

Computing Risk: Cogynt Decision Intelligence Platform

Hierarchical Complex Event Processing (HCEP)

INTEGRATED CASE MANAGEMENT

Tracks analytic throughput and generates tailorable reports

THREAT BEHAVIOR RISK COMPUTATION

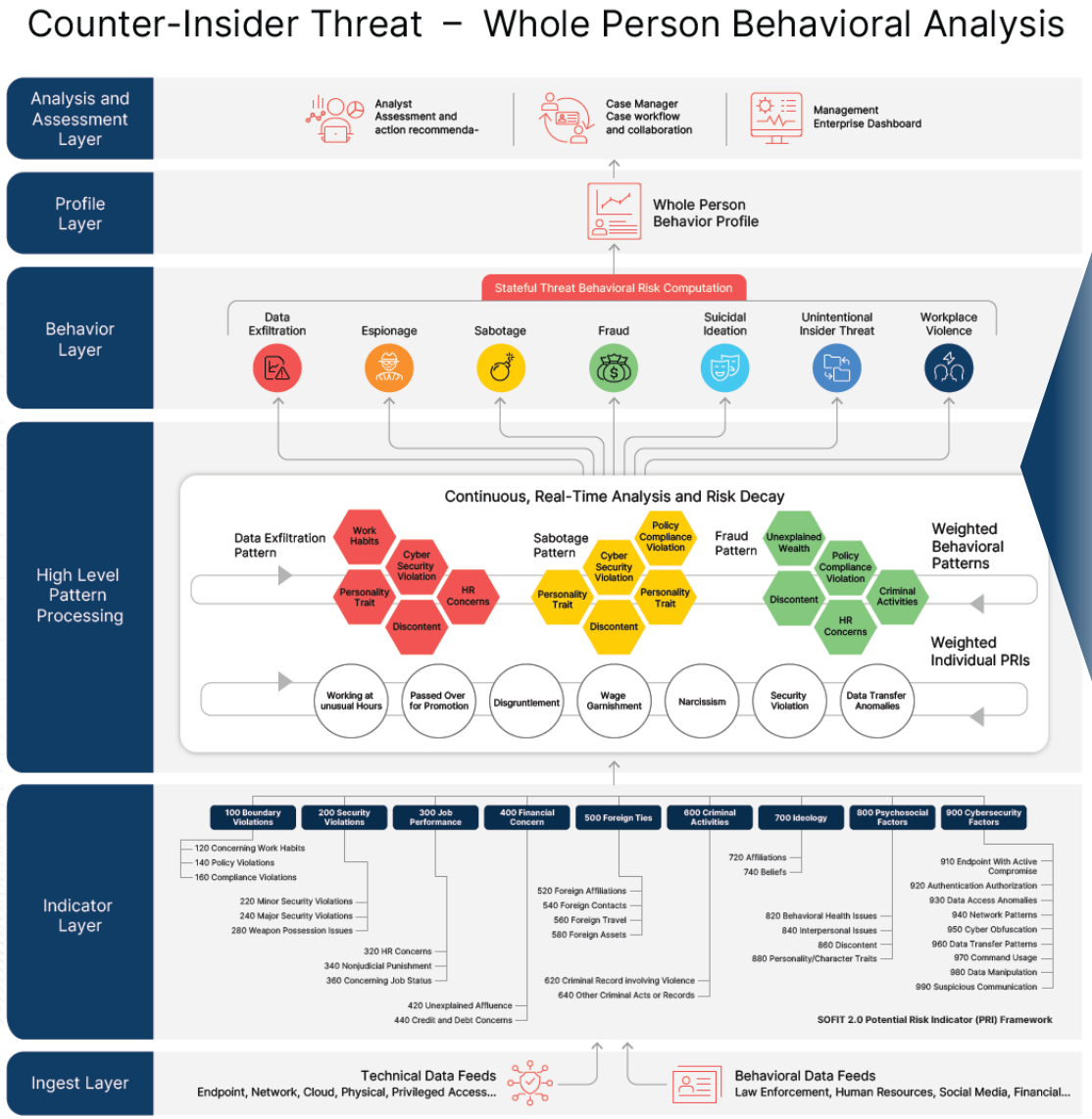
Cogynt model Accounts for Varying Threat Types

HIGHER-LEVEL PATTERN PROCESSING

Cogynt HCEP Captures Interactions Among PRIs

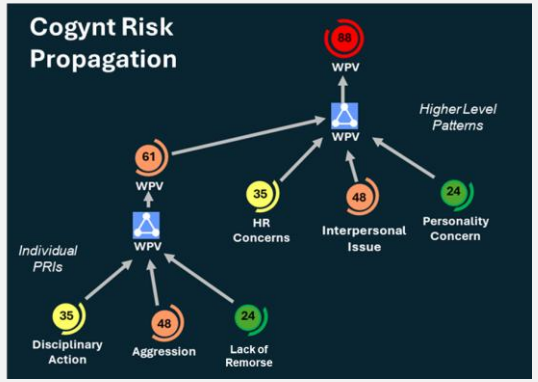
Data Ingested and Processed Within SOFIT Framework

Cogynt builds on the SOFIT Knowledge Base



Risk Calculation

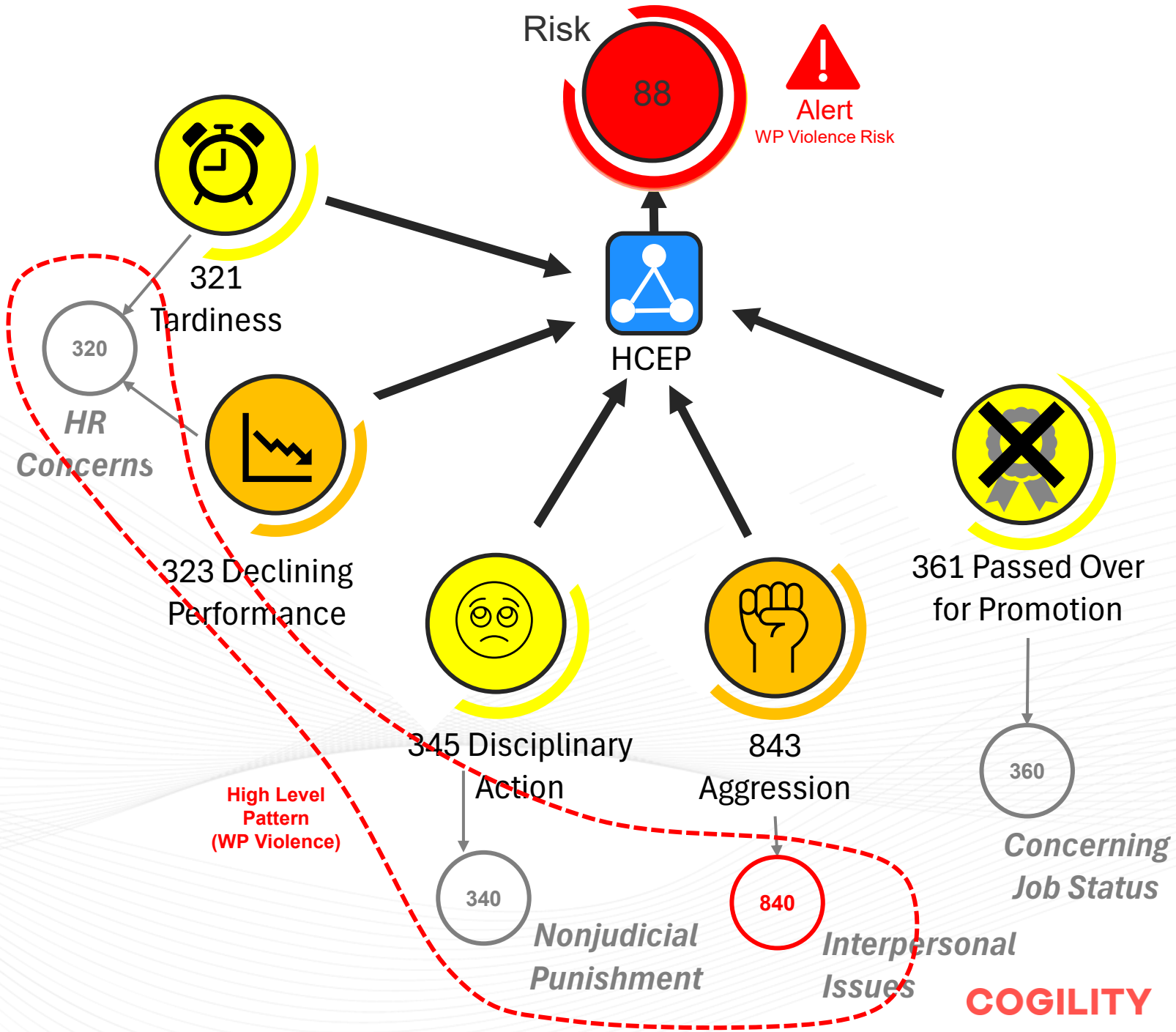
*Cogility's patented **HCEP** propagates the PRI probability weights through the SOFIT behavioral analytic hierarchy at increasing levels of abstraction.*



COGILITY

Example Scenario

Cited for chronic tardiness [321 Tardiness]	*320 HR Concerns*
Performance review [323 Declining Performance]	*320 HR Concerns*
Disciplined for performance deficiencies [345 Disciplinary Action]	*340 Nonjudicial Punishment*
Yells at colleague and punches locker [843 Aggression]	*840 Interpersonal Issues*
Employee did not get promotion [361] Passed over for promotion	*360 Concerning Job Status*



COGILITY

Conceptual Illustration of Cogynt Model: Workplace Violence Incident

Based on Gabriel Romero Case [2019]

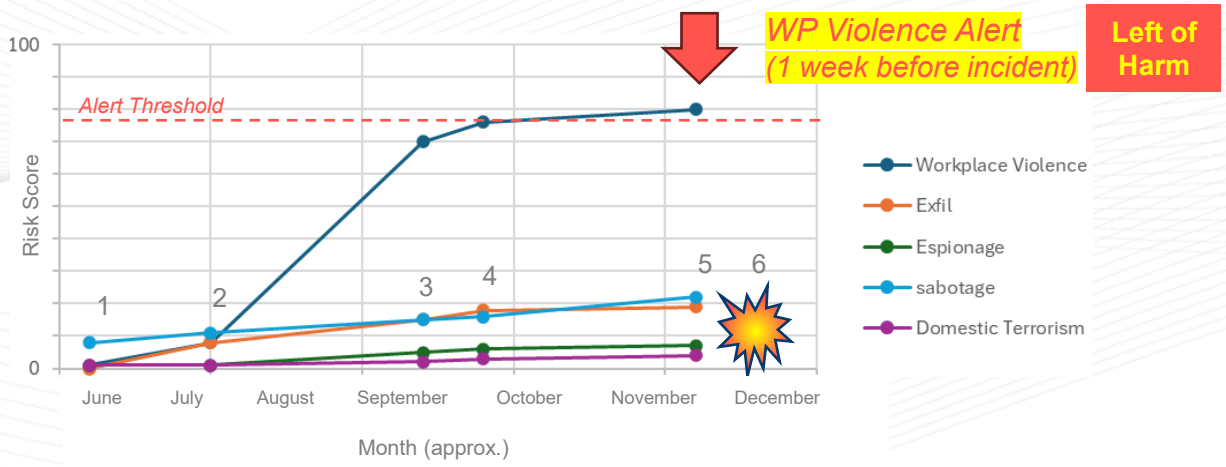
Sources:
CDSE case study
Military.com article

In December 2019, Machinist Mate Auxiliary Fireman Gabriel Romero reported for watch turnover aboard dry-docked Fast Attack Submarine USS Columbia at Pearl Harbor Naval Shipyard, taking possession of an **M-4 rifle** and **M-9 pistol** for his roving Dry Dock patrol.

Without provocation, he began firing his M-4 rifle at civilians, killing two and wounding a third, before shooting himself with his M-9 pistol.

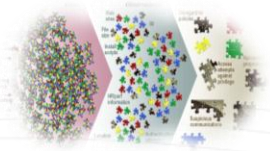
The incident only lasted a few seconds from beginning to end.

#	Event	SOFIT PRI	SOFIT Sub-Class
1 [June-Oct]	Tardiness	321 Attendance Issues: Tardiness	320 HR Concerns
2 [June-Oct]	Poor/declining performance	323 Negative Evaluation: Declining Performance	320 HR Concerns
3 [June-Oct]	Disciplinary action	341 Received Corrective Action	340 Nonjudicial Punishment
4 [June-Oct]	Yells at colleague, punches locker	843 Aggression	840 Interpersonal Issues
5 [November]	Employee passed over for promotion	361 Passed Over for Promotion	360 Concerning Job Status
6 [December]	Murder/Suicide		



COGILITY

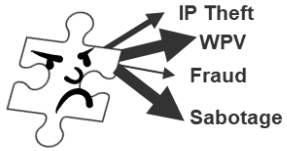
Conclusions: Best Practices for Whole-Person Approach



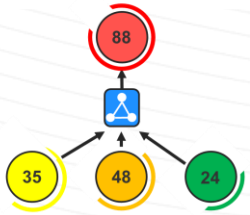
The **SOFIT PRI knowledge base** provides a solid framework for characterizing behavioral, technical, and organizational insider risk indicators and contributing factors

cogility.com/sofit2

PRIs should include not only the most egregious violations, but also **concerning events, behaviors, and characteristics** that help to identify at-risk individuals and proactive opportunities for positive mitigation providing an “offramp” from critical pathway



Map the PRIs to **all threat behavior types** of concern



Behavioral analytic models should reflect high-level **patterns of PRIs** to provide greater insights than would be derived from merely aggregating the PRI weights independently

COGILITY

Questions?

Thank you for your attention

Frank L. Greitzer, PhD
Chief Behavioral Scientist

COGILITY

fgreitzer@cogility.com

Founder, PsyberAnalytix

PsyberAnalytix

Frank@PsyberAnalytix.com

Cogility Insider Risk Management Academy

www.cogility.com

Works Cited:

Greitzer, FL, R Kliner, & S Chan. (2022). Temporal effects of contributing factors in insider risk assessment: Insider Threat indicator decay characteristics. *ACSAC WRIT Workshop*, December 2022, Austin, TX. https://www.acsac.org/2022/workshops/writ/WRIT_2022_paper_4765-Greitzer.pdf

Greitzer, FL, & J Purl. (2022). The dynamic nature of insider threat indicators. *Springer Nature Computer Science*, *3(102)*. https://doi.org/10.1007/s42979-021-00990-1.

Greitzer, FL, J Purl, YM Leong & DE Becker. (2018). SOFIT: Sociotechnical and Organizational Factors for Insider Threat. IEEE Security and Privacy Workshops (SPW), Workshop on Research for Insider Threat (WRIT), San Francisco, CA, May 24, 2018, pp. 197-206. DOI: 10.1109/SPW.2018.00035 http://conferences.computer.org/sp/2018/Resources/spw/2018/SOFITSociotechnicalandOrganizationalFact.pdf

Other Resources:

Greitzer FL & 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*, CW Probst, J Hunter, D Gollmann & M Bishop (Eds.), pp. 85-113. Springer, New York. https://link.springer.com/chapter/10.1007/978-1-4419-7133-3_5

Shaw, ED, & LF Fischer. (2005). *Ten Tales of Betrayal: The Threat to Corporate Infrastructures by Information Technology Insiders.* PERSEREC-TR-05-04

Jaros *et al*. (2019). *The Resource Exfiltration Project: Findings from DoD Cases 1985-2017*. PERSEREC Technical Report PERSEREC-TR-19-02. Seaside, CA: Defense Personnel and Security Research Center, Office of People Analytics

COGILITY