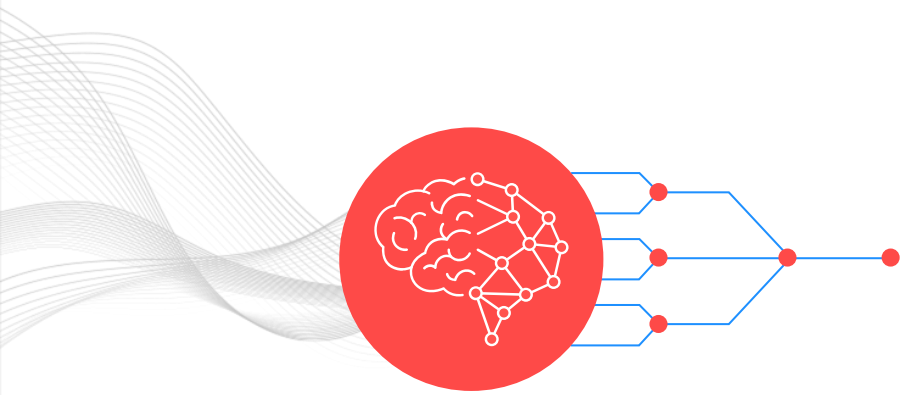
INMM 67th Annual Meeting

COGILITY



“Catch Me if You Can”

A Panel on Insider Threat Detection and Mitigation
Lessons for Advanced Nuclear Facilities

“15 minutes on Three Big Ideas”

Frank L. Greitzer, PhD

August 5, 2026

I. The Human-Centric Challenge for Nuclear Security

COGILITY

The Human-Centric Challenge

Nuclear MC&A programs remain vulnerable to human-centric risks that evade early detection.

Information Theft

Unauthorized access to sensitive nuclear data

Material Diversion

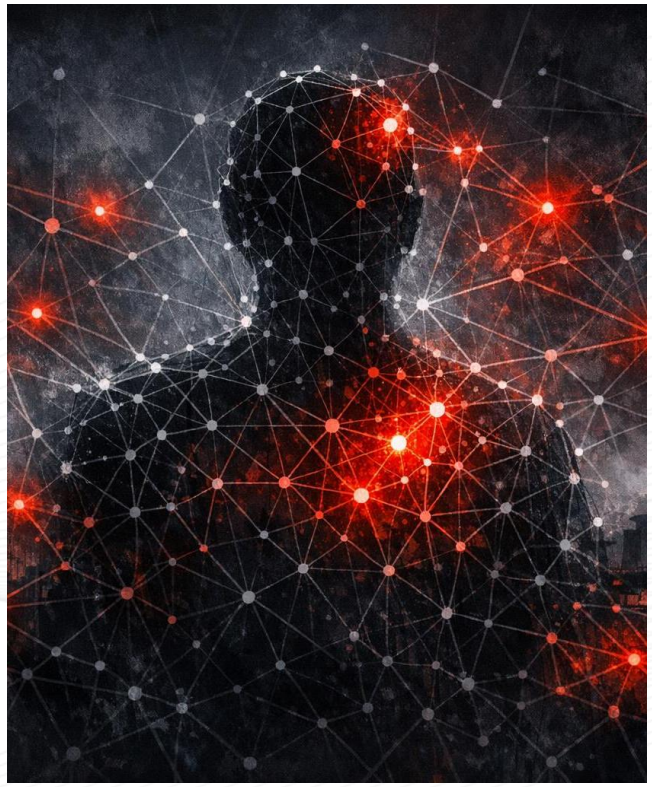
Theft or misrouting of nuclear materials

Sabotage

Deliberate damage to systems or processes

Unintentional Errors

Human mistakes with safety consequences



The Human Factor: Behavioral Science Perspective

Negligent

- Careless policy violations
- Unsafe workarounds
- Poor cyber hygiene

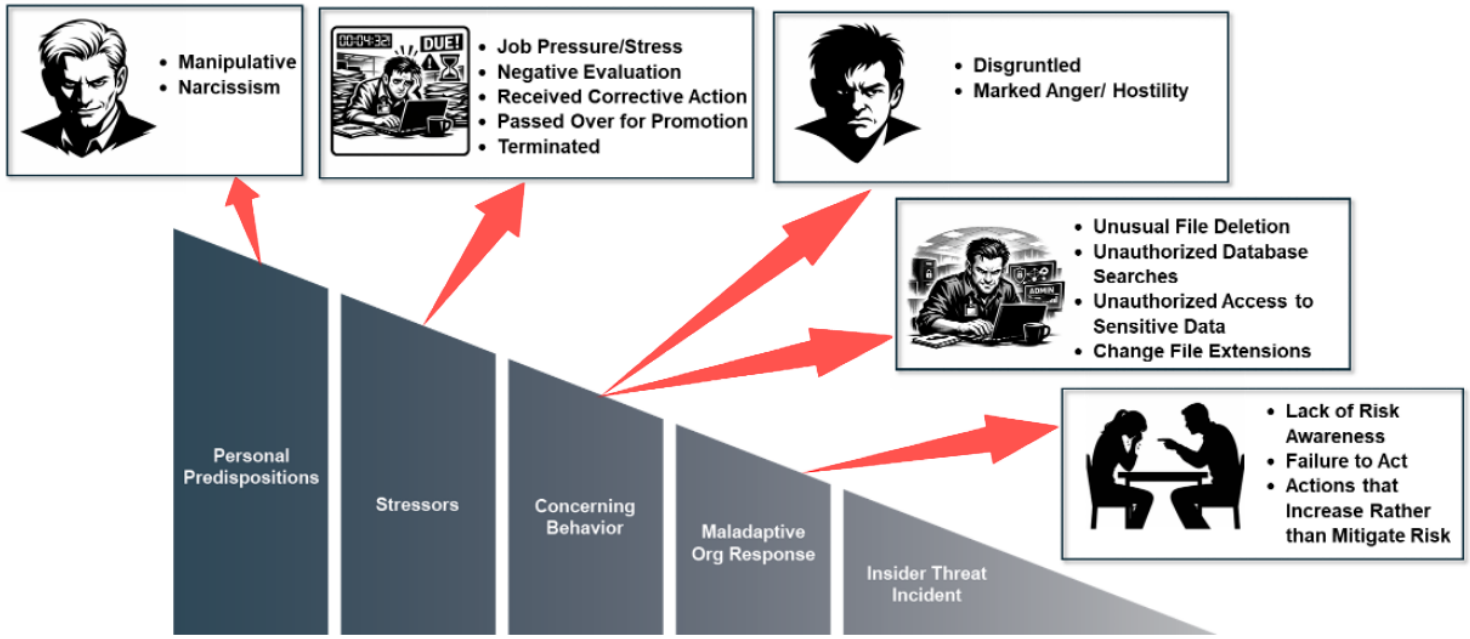
Misguided

- Testing systems to “help”
- Unauthorized tool introduction
- Well-intentioned shortcuts

Malicious

- Sabotage and theft
- Espionage facilitation
- External attack enablement

Drivers Down the “Critical Pathway”



COGILITY

Why Traditional Controls Fail

Training and compliance-focused approaches have limited lasting impact

- Training alone doesn’t change behavior
- Perimeter-focused defense (technical monitoring) often fails to identify precursors
- Reactive programs respond to alerts after the incident occurs rather than proactively addressing stressors and risky patterns
- Organizational silos prevent a unified view of risk across HR, IT, OT engineering, and security.

Whole-Person Approach to Insider Risk Mitigation

Fusing behavioral science, cyber-physical signals, and organizational context into explainable, auditable decision support.

Technical Activity Monitoring

UEBA with personalized baselines for anomaly detection in access, timing, and data movement

Psychosocial / Behavioral Indicators

Behavioral science to anticipate noncompliance precursors and psychosocial risk

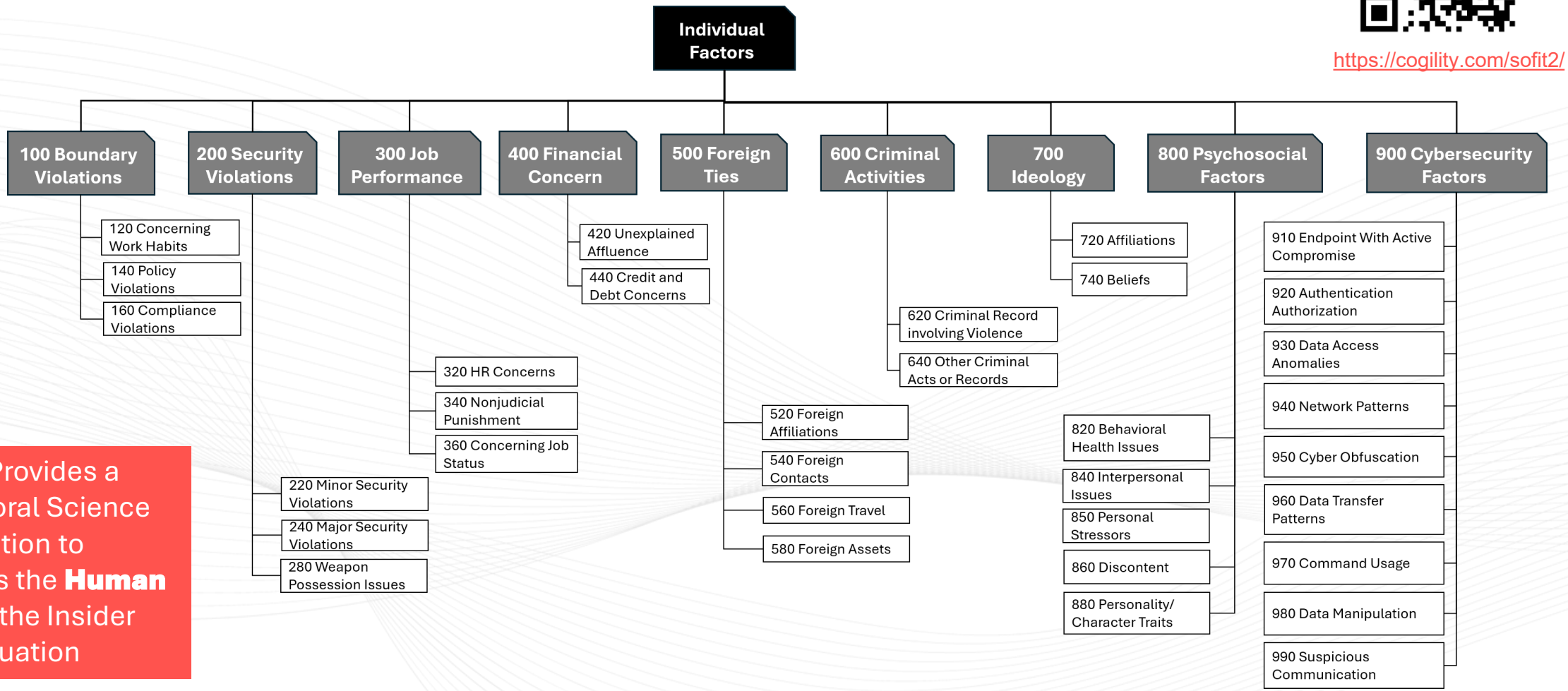
Organizational Factors

Security climate, reporting norms, and governance that shape risk expression

SOFIT: Sociotechnical and Organizational Factors for Insider Threat

Structured knowledge base of behavioral/psychosocial, organizational, and technical/cybersecurity contributors to insider risk

https://cogility.com/sofit2/



SOFIT Provides a Behavioral Science Foundation to Address the **Human** Side of the Insider Risk Equation

COGILITY

II. Predictive Risk Assessment Approaches

COGILITY

Comparing Risk Assessment Approaches

Legend

- Met
- Partially met
- Not met

Criteria:	Model expert	Scalability	Transparency	
Qualitative Models • Analyst Judgment/SPJ • "Counting" Models	✓	✗	✓	• Not scalable
Quantitative Models • Additive • Probabilistic (Bayesian)	–	✓	–	• May make simplifying assumptions
Machine Learning (ML)	–	✓	✗	• Limited by training set • "Black box" solutions
Expert AI Behavioral Analytics Integrating AI and Quantitative Modeling	✓	✓	✓	• Reflect expert knowledge

Cogynt.ai Solution

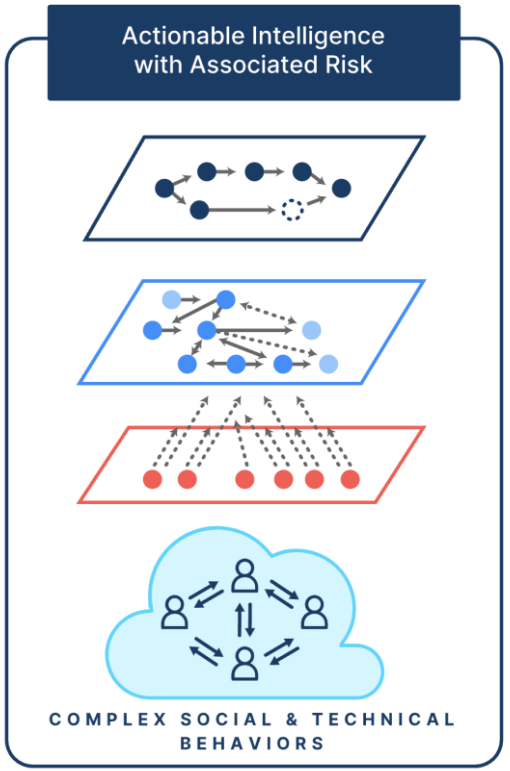
COGILITY

Cogynt.ai Decision Intelligence Platform

Powered by HCEP Hierarchical Complex Event Processing

- Integrates qualitative and quantitative analytics
- Provides triage support for safety personnel
- Scales from individual assessments to broader population screening
- SOFIT framework provides Behavioral Science foundation
- HCEP Risk Assessment
- Full transparency/ explainability with human oversight.

HCEP Abstraction Hierarchy



Pattern-based inference at increasing levels of abstraction

COGILITY

III. Changing Insider Risk Landscape

The Insider Risk Spectrum Has Changed

As AI agents become embedded in enterprise and mission systems, they introduce a new class of insider risk that traditional security tools are not designed to manage.

Human Insiders

Negligent

Misguided

Malicious

AI Agent

AI Agent(s)

AI Tools & Services

- Privilege abuse / Counterfeit agents
- Opaque reasoning degrades human oversight
- Anomalous delegation
- Orchestrated/multiple agents

COGILITY

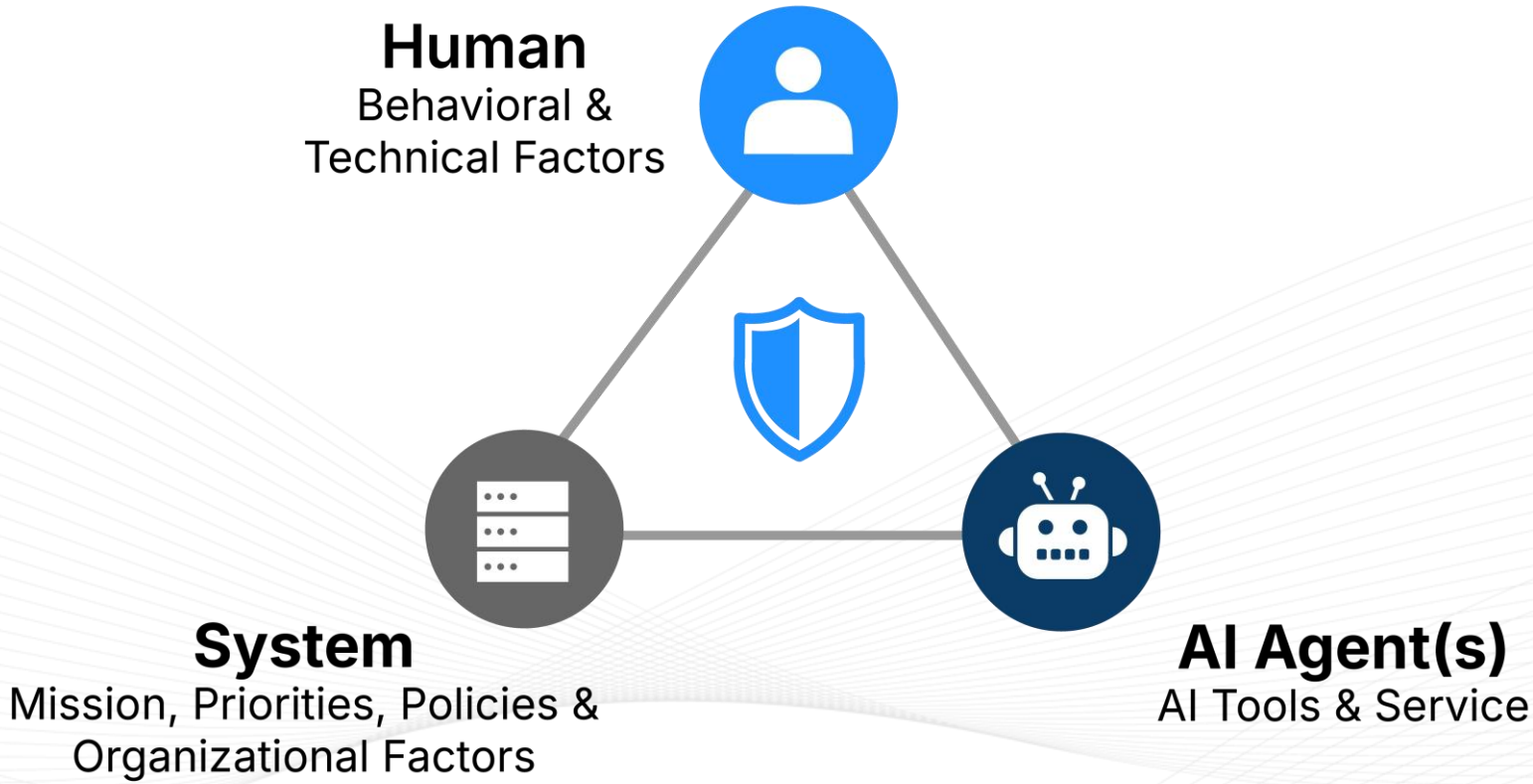
The Human-Agent-System Triad

Enterprises need governance across the **human-agent-system triad**

Human
- Sponsorship
- Delegation
- Approvals
- Role and accountability

Agent – *Digital Insider*
- Actions
- Tools
- Permissions
- Memory
- Behavior over time

System
- Policy constraints
- Data access
- Mission context
- Workflow boundaries



Core message:
Risk often emerges from the interaction among all three.

COGILITY

Core Capabilities for Agentic AI Risk Management

COGILITY

Agentic AI Guardrail Operations Concept

Investigative Intelligence Sequence

1. Map incoming log streams into stateful, in-memory representations
2. HCEP continuously generates composite events, linking each human actor's baseline risk profile to the agent's structural data access
3. When a composite pattern's risk weight crosses the threshold, the HCEP engine issues an alert

Risk posture shifts: Observer → Interdictor

triggers

Remediation Controls

State Isolation
Locks the active session

Control Execution
Trips the "circuit breaker"

Credential Revocation
Pauses the agent's execution queue

Real-Time Notification
Alerts a human analyst (human-on-the-loop)

COGILITY

Three Big Ideas/Challenges for Effective Insider Risk Management…

Download Cogility Materials for INMM Conference

See the following papers in INMM Proceedings:

- Greitzer, F.L. & Noonan, C.F. "Behavioral Analytic Modeling for Insider Threat Assessment and Mitigation in the Nuclear Power Industry." (*INMM 2026 Proceedings*)
- Greitzer, F.L. (2026). "Trusted AI Decision Intelligence Support for Nuclear Material Accountability and Control" (*INMM 2026 Proceedings*)

COGILITY