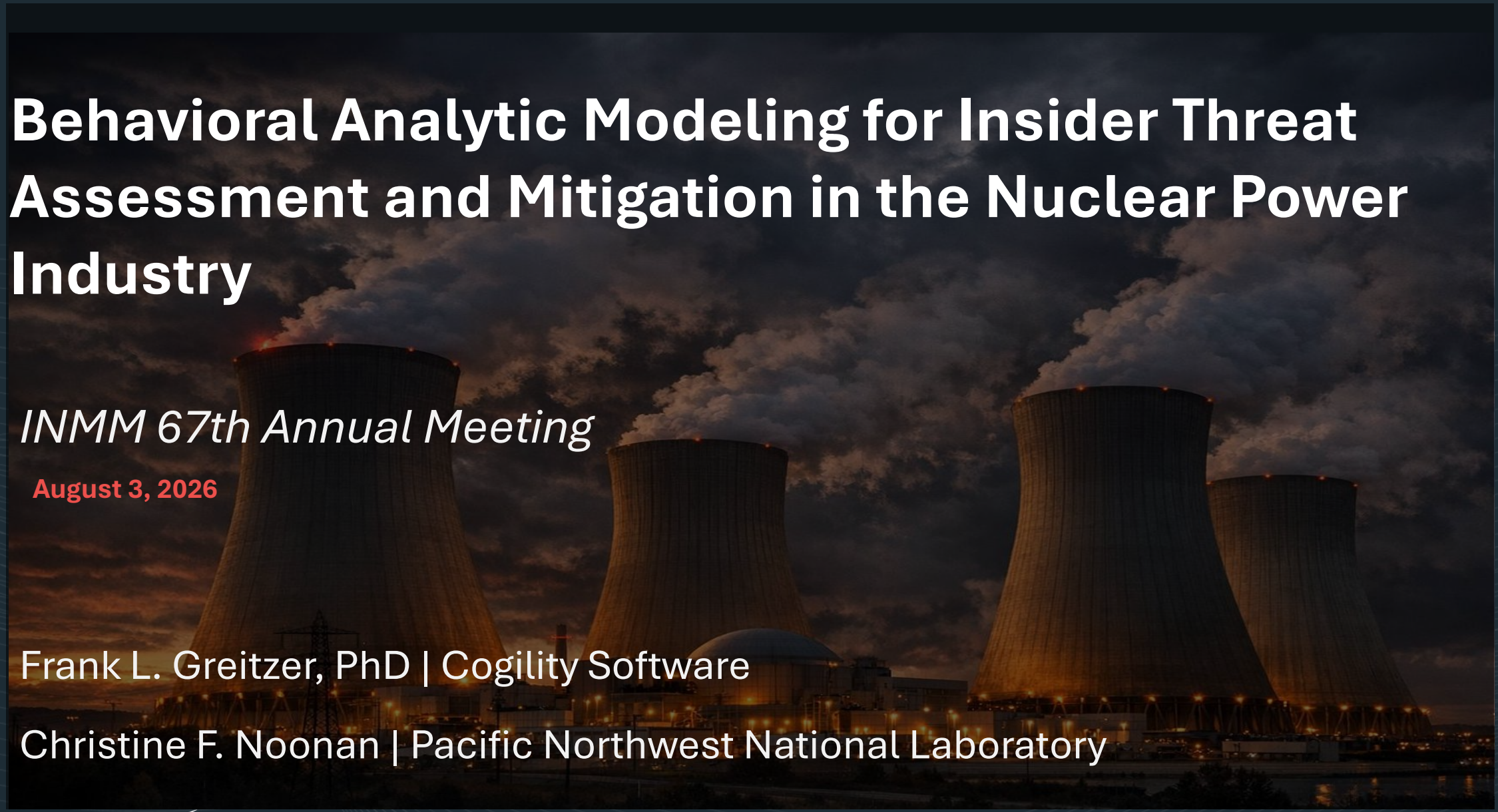
Behavioral Analytic Modeling for Insider Threat Assessment and Mitigation in the Nuclear Power Industry



INMM 67th Annual Meeting

August 3, 2026

Frank L. Greitzer, PhD | Cogility Software

Christine F. Noonan | Pacific Northwest National Laboratory

Pacific Northwest NATIONAL LABORATORY

COGILITY

The Insider Risk Spectrum

Insider Risk: The potential for someone with legitimate, authorized access to an organization's systems, data, or facilities to misuse that access, causing harm to the organization

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

Why Nuclear Is Uniquely Vulnerable

IT/OT Convergence

- Connected digital systems span information technology and operational technology domains
- OT failures can cascade into real-world physical impacts

Safety-Critical Operations

- High-consequence physical outcomes demand zero tolerance for security failures
- Human performance variability—fatigue, cognitive overload, procedural drift

Insider Advantage

- Legitimate access rights and deep operational knowledge
- Awareness of workarounds, time pressures, and security gaps

Pacific Northwest NATIONAL LABORATORY

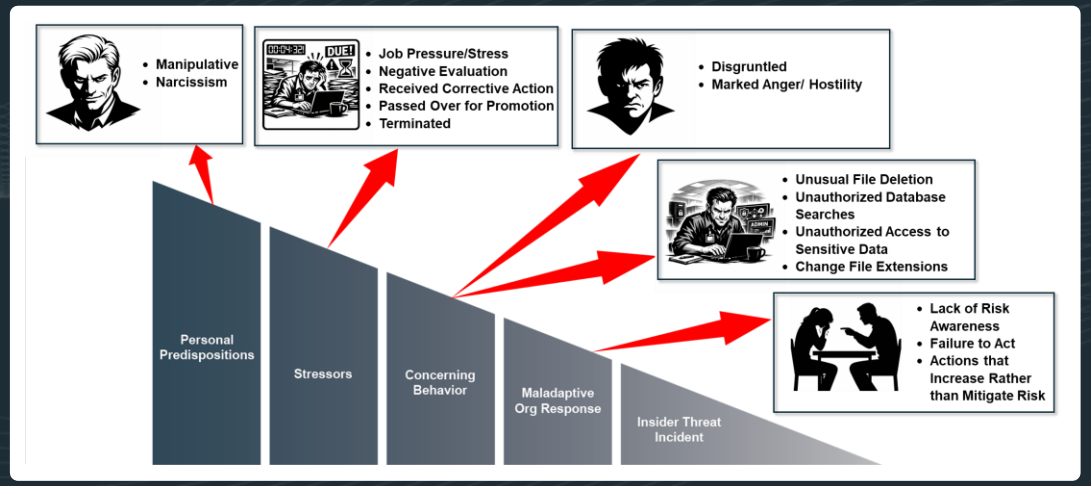
COGILITY

The Human Factor: Behavioral Science Perspective

Drivers Down the "Critical Pathway"

- Personal predispositions
- Stressors: Workload, insufficient tooling, unclear governance
- Maladaptive organizational responses

Organizational narratives treating employees as "deficient users" shift attention from systemic factors



Pacific Northwest NATIONAL LABORATORY

COGILITY

Why Traditional Controls Fail

Training and compliance-focused approaches have limited lasting impact

- **Training alone doesn't change behavior:** Rules-based training without addressing social norms, resource constraints, and perceived costs of compliance yields limited impact
- **Perimeter-focused defense:** Technical monitoring optimized to suppress noise often fails to escalate early insider activity
- **Reactive posture:** Programs respond to alerts after incidents rather than addressing stressors and risky patterns before harm
- **Organizational silos** prevent a unified view of risk across HR, IT, OT engineering, and security.

The Detection Gap

Structural Challenges

- Risk signals distributed across HR, physical security, IT, OT engineering, and management
- Organizations lack governance and tooling to integrate “whole-person” risk assessment

Practical Barriers

- Siloed departments and privacy concerns
- Lack of management buy-in/ ownership
- Budget constraints
- Employees resist monitoring perceived as punitive surveillance

Real-World Nuclear Insider Threat Cases

Case	Year	Key Behavioral Insight
San Onofre	2012	Disgruntlement and workplace tensions as risk amplifiers
Doel-4	2014	Insider sabotage within normal access privileges
Eccleston	2013	Contractor-enabled espionage via trusted relationships
GE Wilmington	1979	Probe-and-test boundary testing over time

An integrated behavioral analytic framework looks for COMBINATIONS of these patterns rather than isolated anomalies.

Pacific Northwest NATIONAL LABORATORY

COGILITY

SOFIT: Behavioral Science Foundation

- **Sociotechnical and Organizational Factors for Insider Threat (SOFIT)**

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

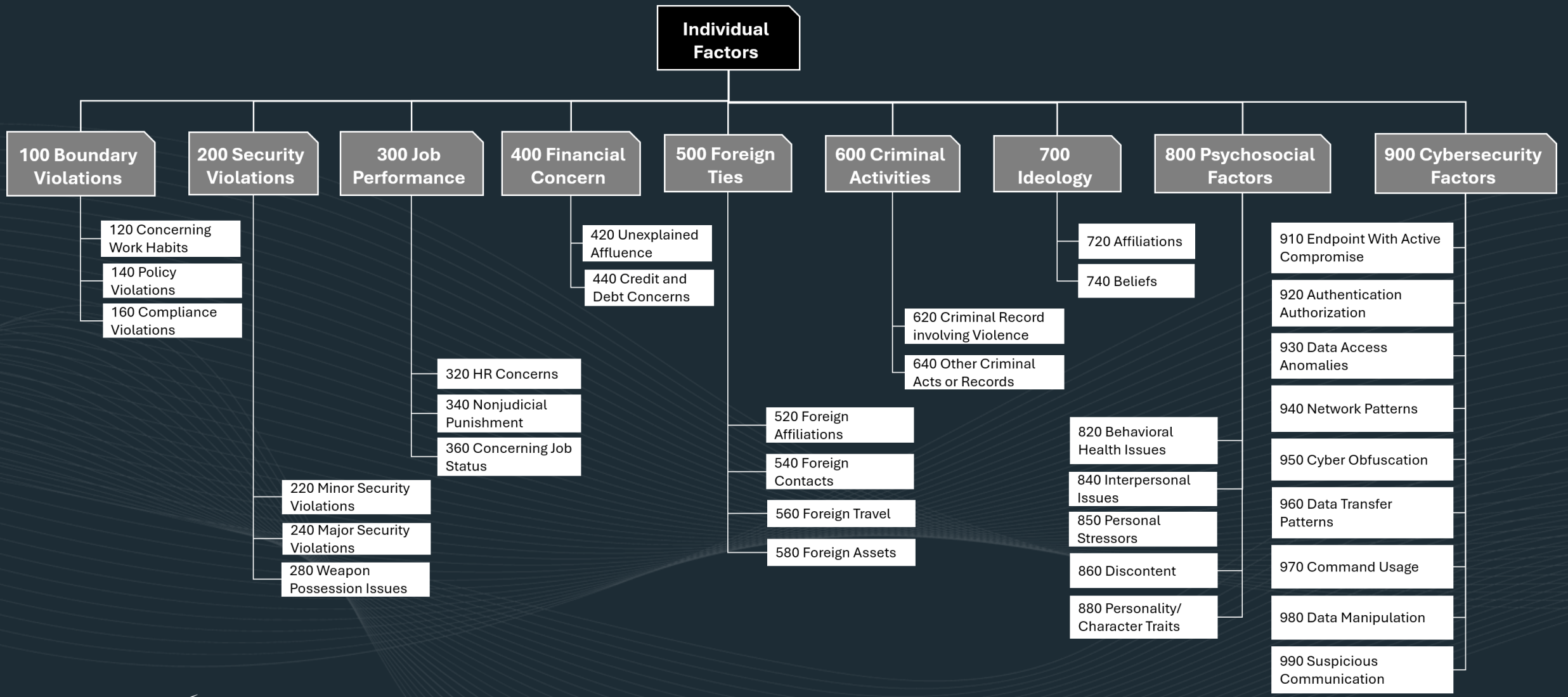
- **Potential Risk Indicators (PRIs):**

  Basic observables at the lowest level of the hierarchy, detected from varied ingested and recorded data

- **“Left of harm”:**

  Psychosocial and behavioral indicators often occur earlier in the attack lifecycle and offer opportunities to intervene

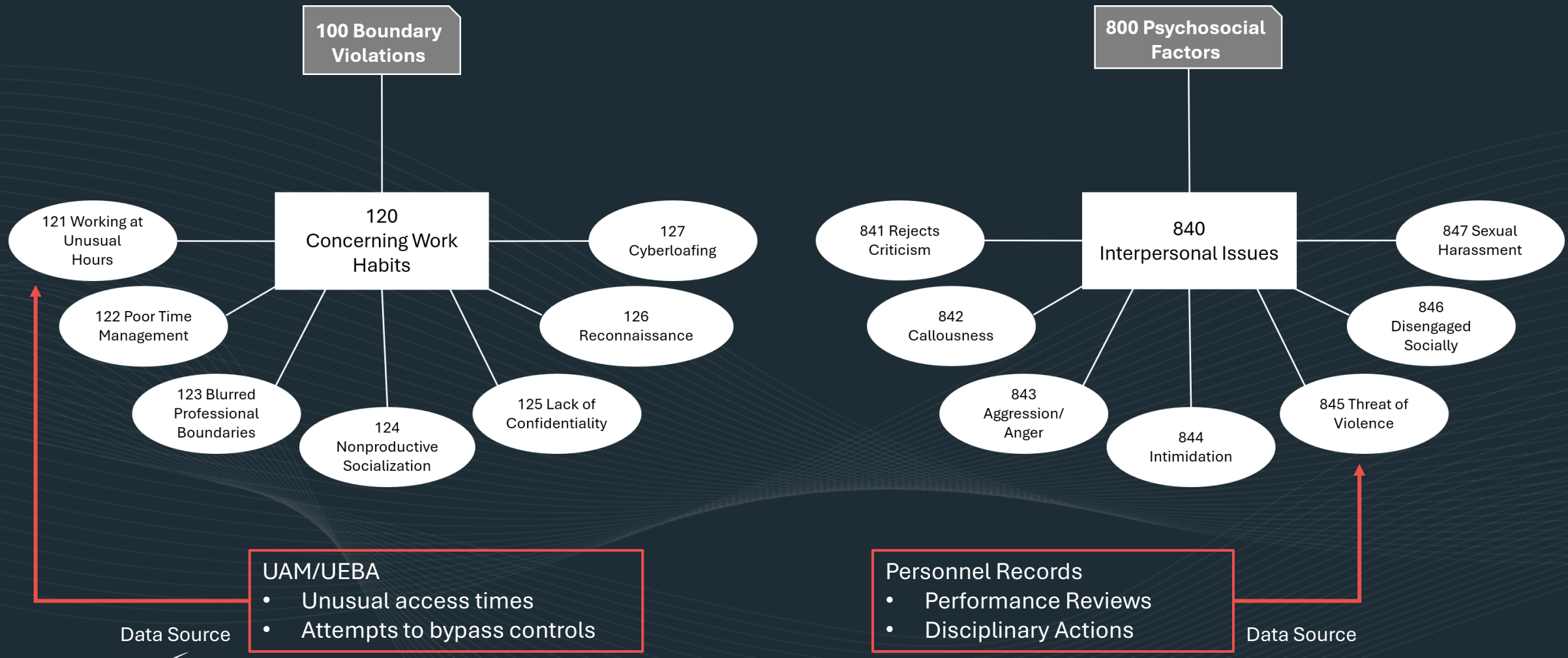
SOFIT Individual Factors Branch



Pacific Northwest NATIONAL LABORATORY

COGILITY

PRI Drill-Down Examples



Pacific Northwest NATIONAL LABORATORY

COGILITY

Nuclear-Specific Calibration

Tailoring the SOFIT framework for nuclear power environments

- **Role-specific monitoring:** Operators, engineers with OT access, system administrators, contractors, and physical security personnel
- **PRI calibration:** Define new indicators, modify existing ones, and adjust PRI mappings and weights for nuclear threat behaviors
- **Nuclear-specific analytics:** Abnormal control-room patterns, dynamic fatigue/workload models, risk scoring for high-impact remote access paths
- **Cross-domain integration:** Unified view across HR, IT, OT engineering, and physical security to overcome organizational silos

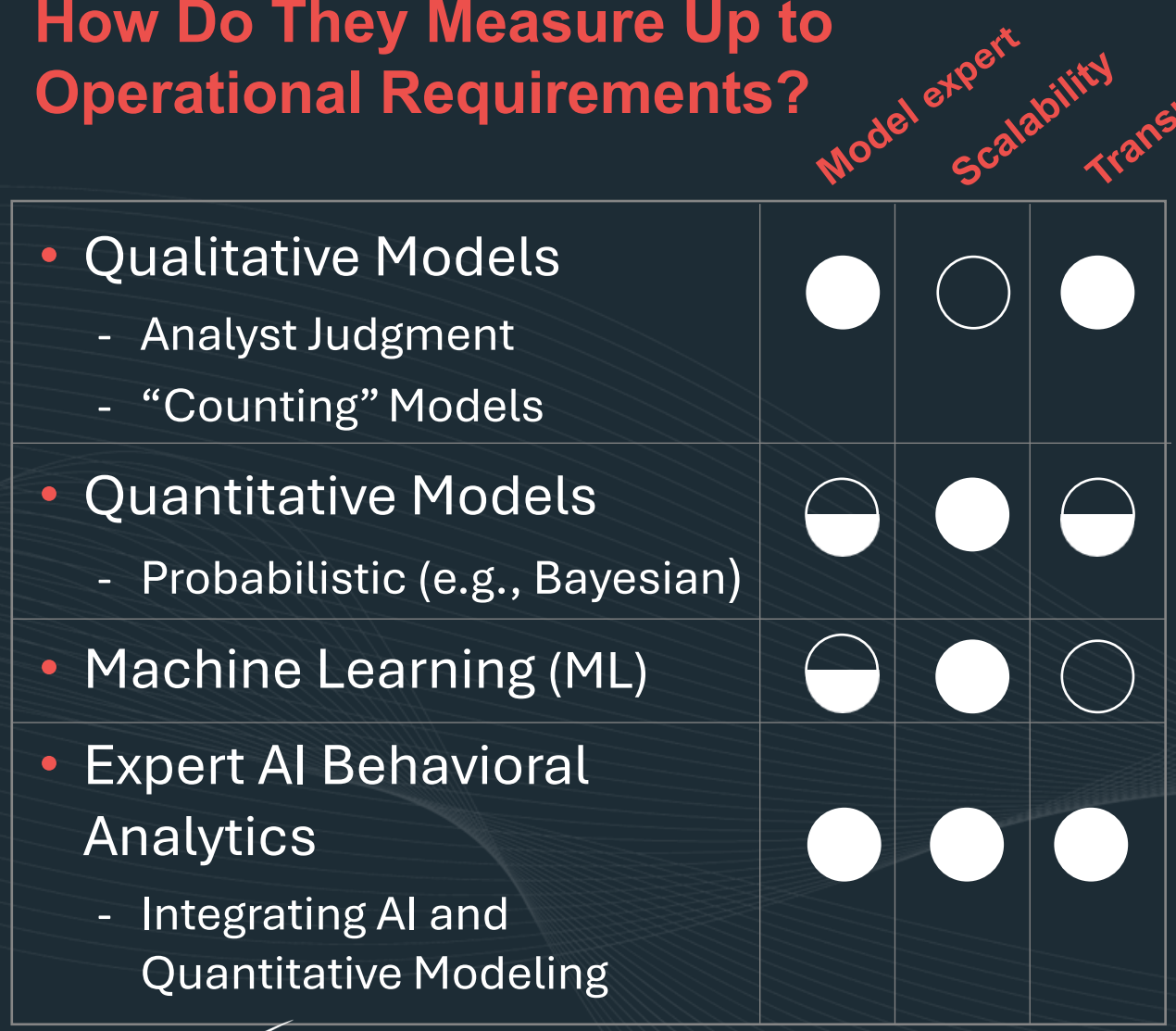
Operational Requirements: Behavioral Analytic Modeling for Nuclear Insider Risk

Key: Whole-Person Behavioral Analytics to get Left of Harm

- **Decision Intelligence**
  - Model expert decision processes for high-consequence, human-in-the-loop decision making
  - Continuous monitoring and data ingest across all risk domains
- **Scalability**
  - Integrated, interoperable open-architecture solution
  - Rapidly adapt to emerging threats while remaining future-proof
- **Transparency**
  - Full provenance and visualization of supporting information
  - Explainable rationales for every alert and recommendation

Comparing Threat Assessment Approaches

How Do They Measure Up to Operational Requirements?



Qualitative models reflect analyst biases, hard to validate

Quantitative models can miss contextual factors

ML approaches tend to be opaque "black boxes" and are limited by training data

Hierarchical pattern-based structured reasoning with human oversight is explainable by design

Pacific Northwest NATIONAL LABORATORY

COGILITY

Cogynt.ai: Decision Intelligence Platform

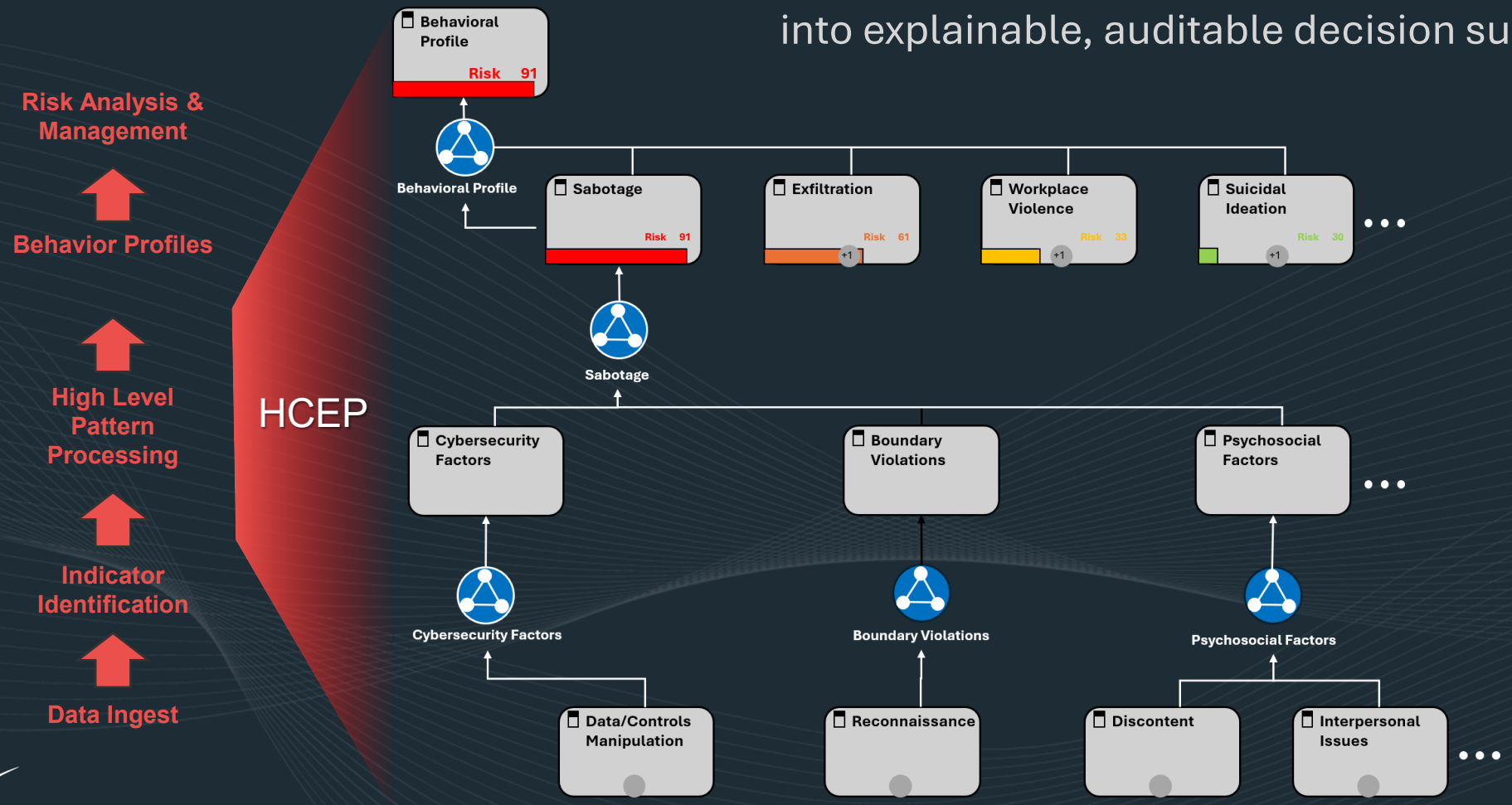
Expert AI behavioral analytic decision intelligence for insider risk

- Automated support + human-in-the-loop expert oversight
- Pattern recognition approach identifies complex behavioral patterns that traditional approaches often miss
- Complete transparency with clear provenance linking observed signals to plausible hypotheses—critical for safety-regulated environments
- Integrates behavioral, psychosocial, organizational, and technical indicators
- Scalable, interoperable open-architecture solution
- Reduces false positives and analyst overload while enabling earlier intervention "left of harm"

See companion paper in INMM Proceedings:
Greitzer, F.L. (2026)/ "Trusted AI Decision Intelligence Support for Nuclear Material Accountability and Control" (*INMM 2026 Proceedings*)

Cogynt.ai Hierarchical Complex Event Processing (HCEP)

The **HCEP** framework fuses behavioral science, cyber-physical signals, and organizational context into explainable, auditable decision support.



Pacific Northwest NATIONAL LABORATORY

COGILITY

Summary & Conclusions

- **Insider threat mitigation must evolve** from reactive, technically centered monitoring toward proactive, human-centric risk management
- **Expert AI behavioral analytics** offers earlier detection, fewer false positives, and stronger accountability
- **Success requires** cross-functional governance, privacy-preserving design, and trusted transparent analytics
- **Steps to Implement this Concept:**
  - Refine nuclear-specific indicator taxonomies
  - Develop the expert AI OT risk model (Cogynt.ai implementation)
  - Define evaluation metrics for detection, prevention, trust, and operational resilience
  - Validate models in OT environments

Cybersecurity is as much a human issue as a technical one.

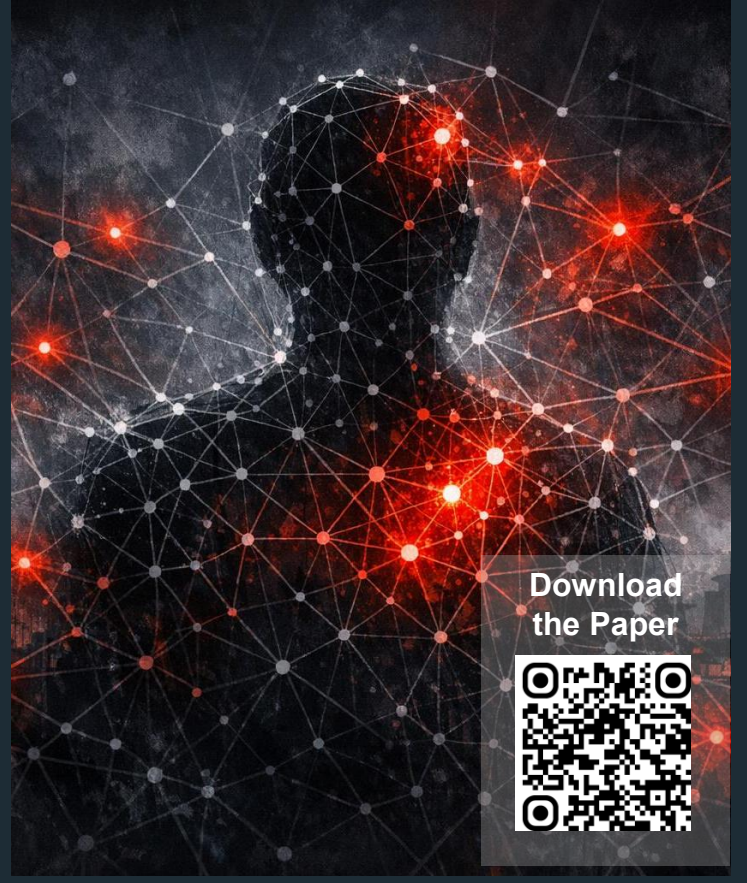
Durable improvements require cultural and organizational reinforcement alongside technical controls.

Thank You

Questions?

fgreitzer@cogility.com

Christine.noonan@pnnl.gov



Resources – 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.”
Greitzer, F.L. (2026)/ “Trusted AI Decision Intelligence Support for Nuclear Material Accountability and Control” (*INMM 2026 Proceedings*)

Pacific Northwest NATIONAL LABORATORY
PNNL-SA-223987
COGILITY