# Whole Person Approach to Insider Threat

Insider Threat Roundtable

October 2020

Frank L. Greitzer, PhD

PsyberAnalytix

# Trusted insiders who commit crimes do not just "pop-up."

In roughly 80% of insider espionage/sabotage cases, investigators have identified social/organizational precursors that could have been addressed before the attack.

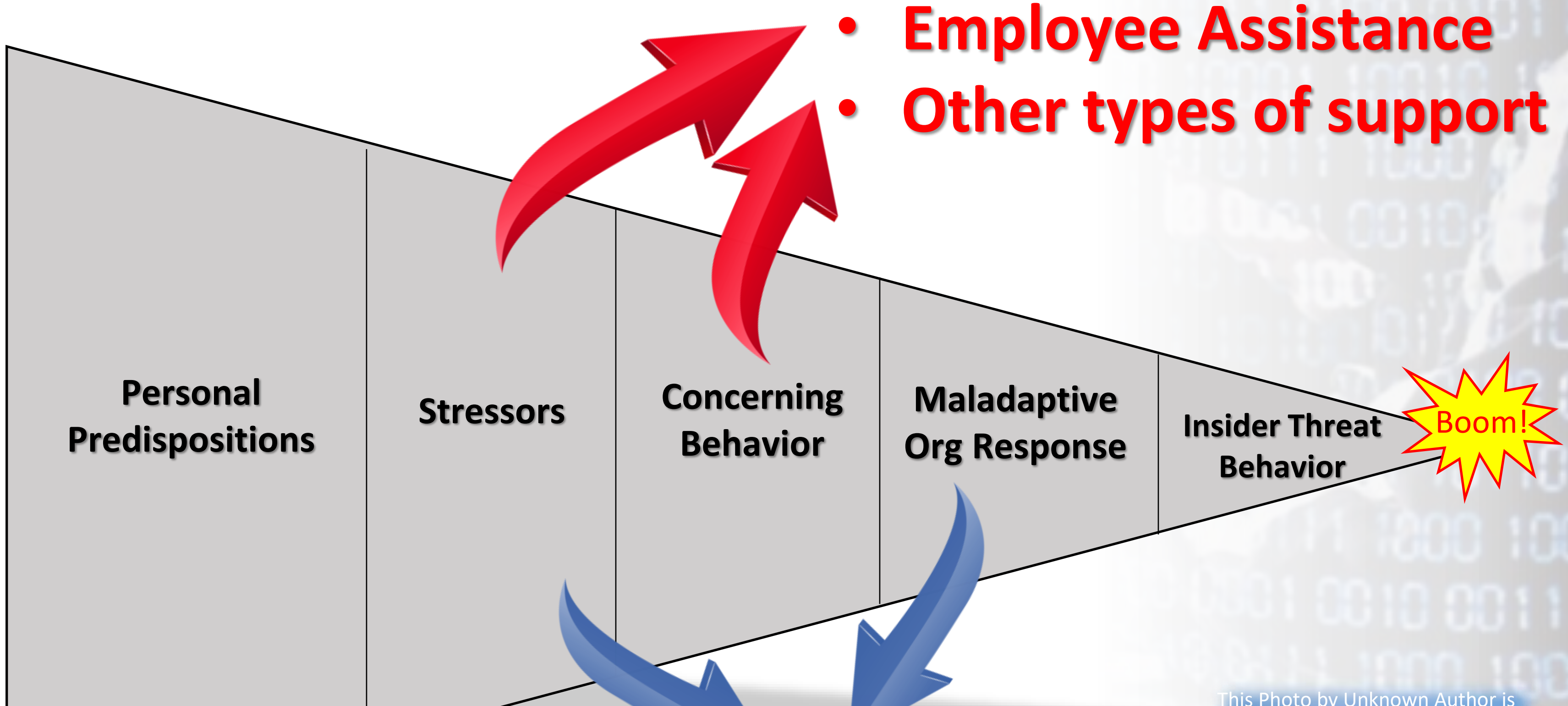
(Shaw & Fisher, 2005)

This Photo by Unknown Author is licensed under CC BY-SA

# Critical Pathway

This Photo by Unknown Author is licensed under CC BY-NC-ND

Critical Pathway to Insider Risk
(Shaw & Sellers, 2015)

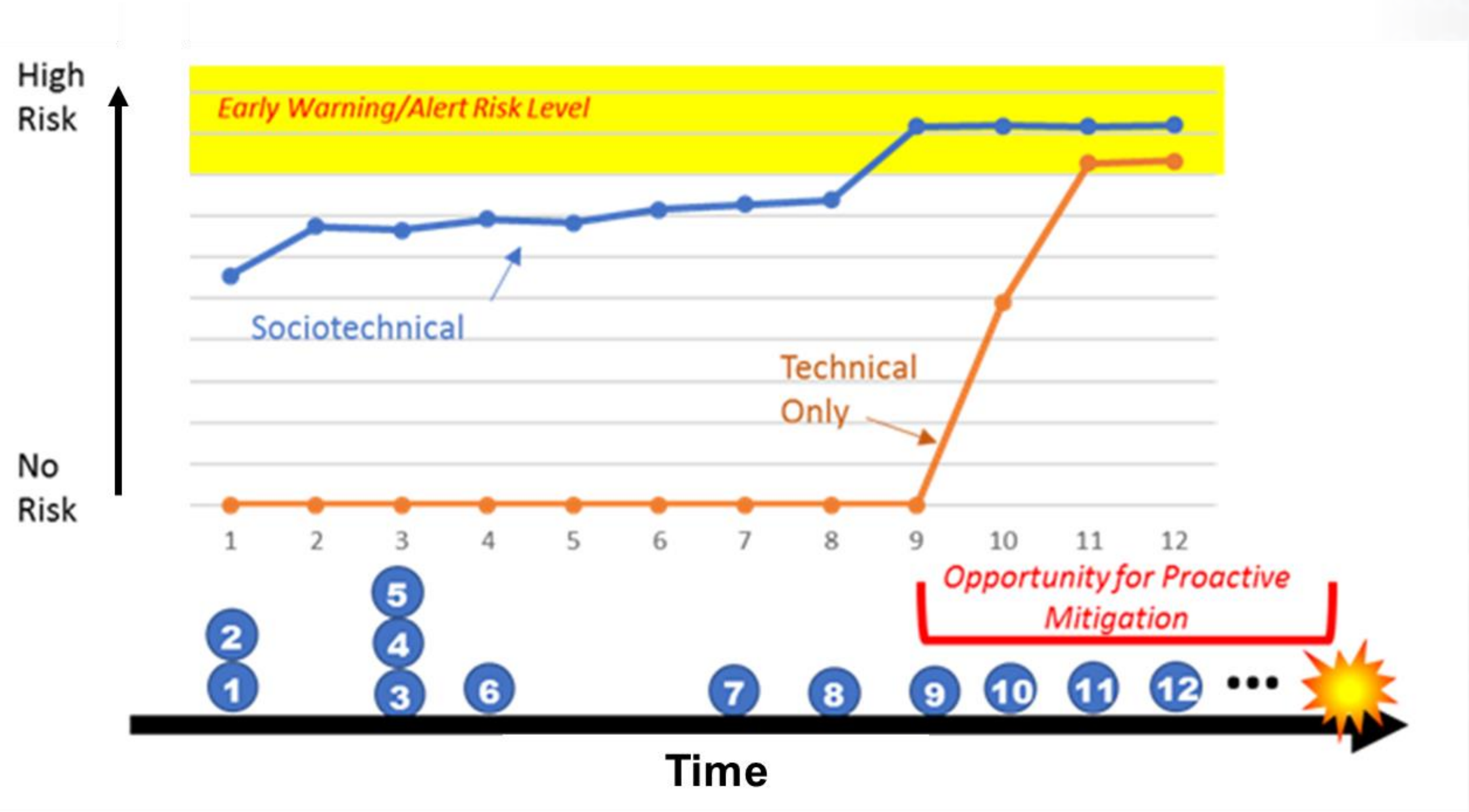


- **Counseling**
- **Employee Assistance**
- **Other types of support**

**Organizational Improvements**

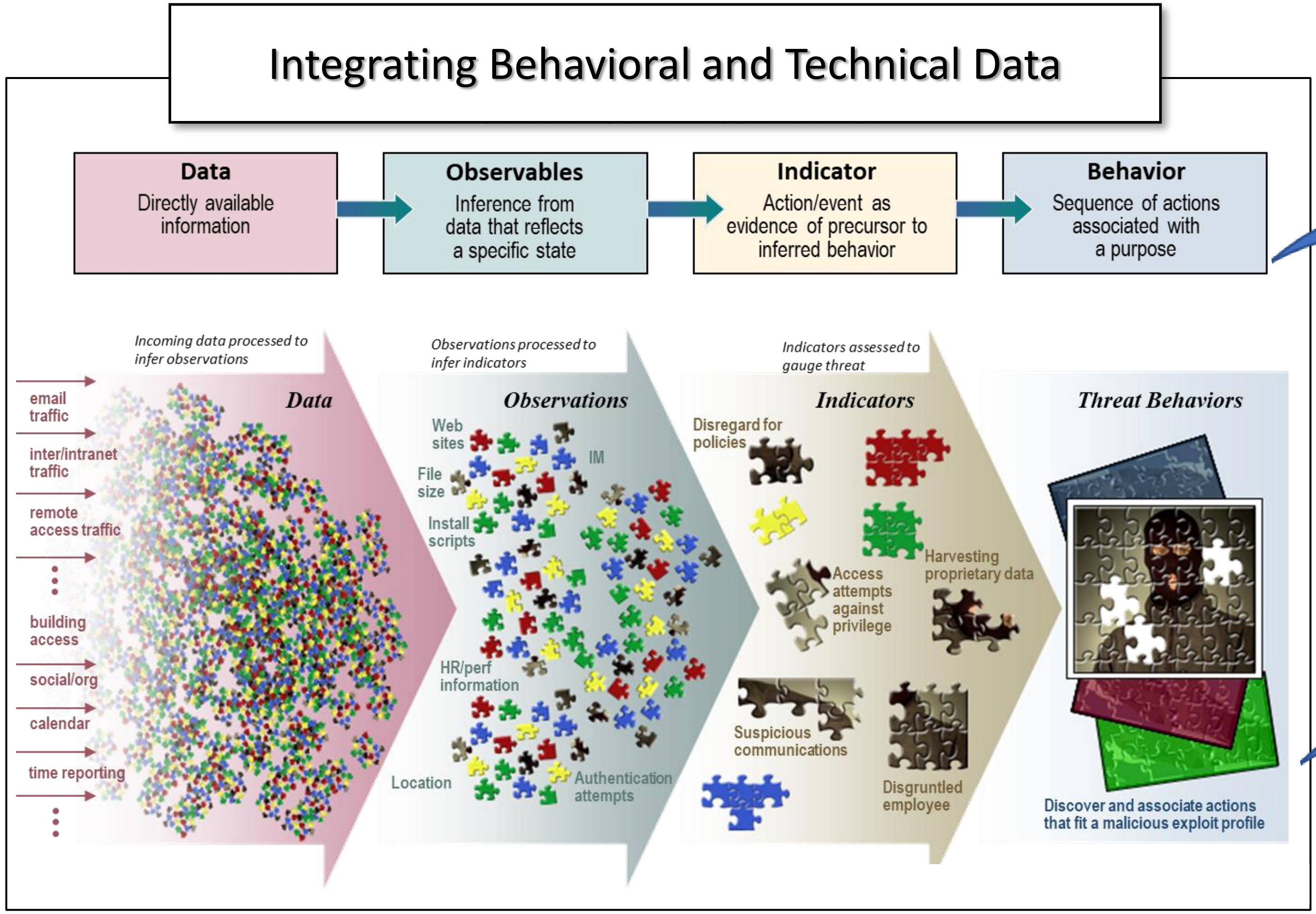
This Photo by Unknown Author is licensed under CC BY-NC-ND

# Conceptual Illustration: Getting "left of boom"…



Greitzer et al. (2018)

# *Whole Person Approach*



## Integrating Behavioral and Technical Data

**Data**
Directly available information

**Observables**
Inference from data that reflects a specific state

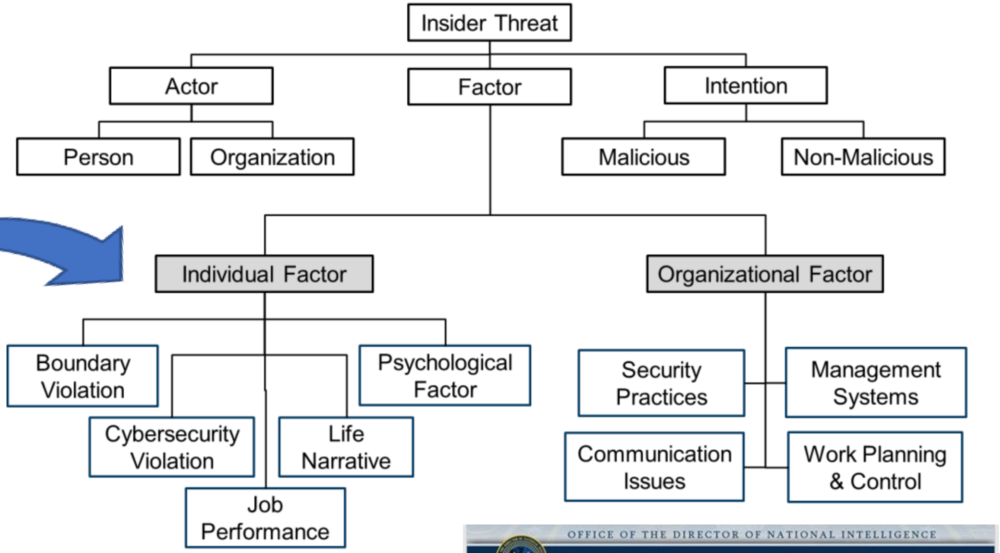
**Indicator**
Action/event as evidence of precursor to inferred behavior

**Behavior**
Sequence of actions associated with a purpose

Incoming data processed to infer observations
Observations processed to infer indicators
Indicators assessed to gauge threat
email traffic
inter/intranet traffic
remote access traffic
building access
social/org
calendar
time reporting
Data
Observations
Web sites
File size
Install scripts
IM
HR/perf information
Location
Authentication attempts
Indicators
Disregard for policies
Harvesting proprietary data
Access attempts against privilege
Suspicious communications
Disgruntled employee
Threat Behaviors
Discover and associate actions that fit a malicious exploit profile

(Greitzer & Frincke, 2010)

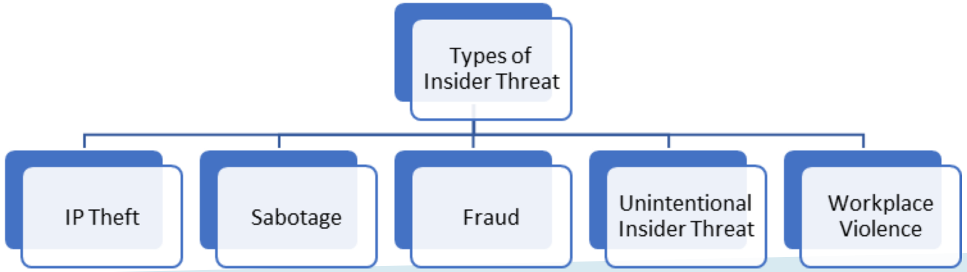
## Sociotechnical and Organizational Factors for Insider Threat (SOFIT)



- Insider Threat
  - Actor
    - Person
    - Organization
  - Factor
    - Individual Factor
      - Boundary Violation
      - Cybersecurity Violation
      - Job Performance
      - Life Narrative
      - Psychological Factor
    - Organizational Factor
      - Security Practices
      - Communication Issues
      - Management Systems
      - Work Planning & Control
  - Intention
    - Malicious
    - Non-Malicious

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
Scientific Advances to Continuous Insider Threat Evaluation (SCITE) Program
Intelligence Advanced Research Projects Activity

(Greitzer et al., 2016, 2018, 2019)

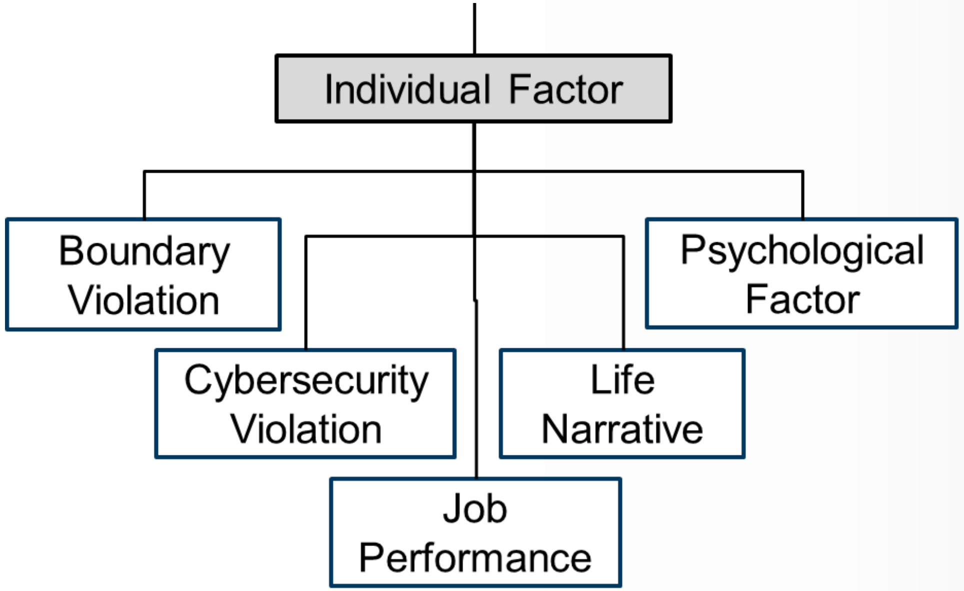


- Types of Insider Threat
  - IP Theft
  - Sabotage
  - Fraud
  - Unintentional Insider Threat
  - Workplace Violence

INSA Whitepaper: *Categories of Insider Threat*

*Whole Person Approach*

# Concerning Behaviors and Personal Stressors



- Disregard for security procedures
- Performance issues
- Bullying/harassment
- Disgruntlement
- Substance abuse
- Financial stress

LEAKS • SPILLS / UIT

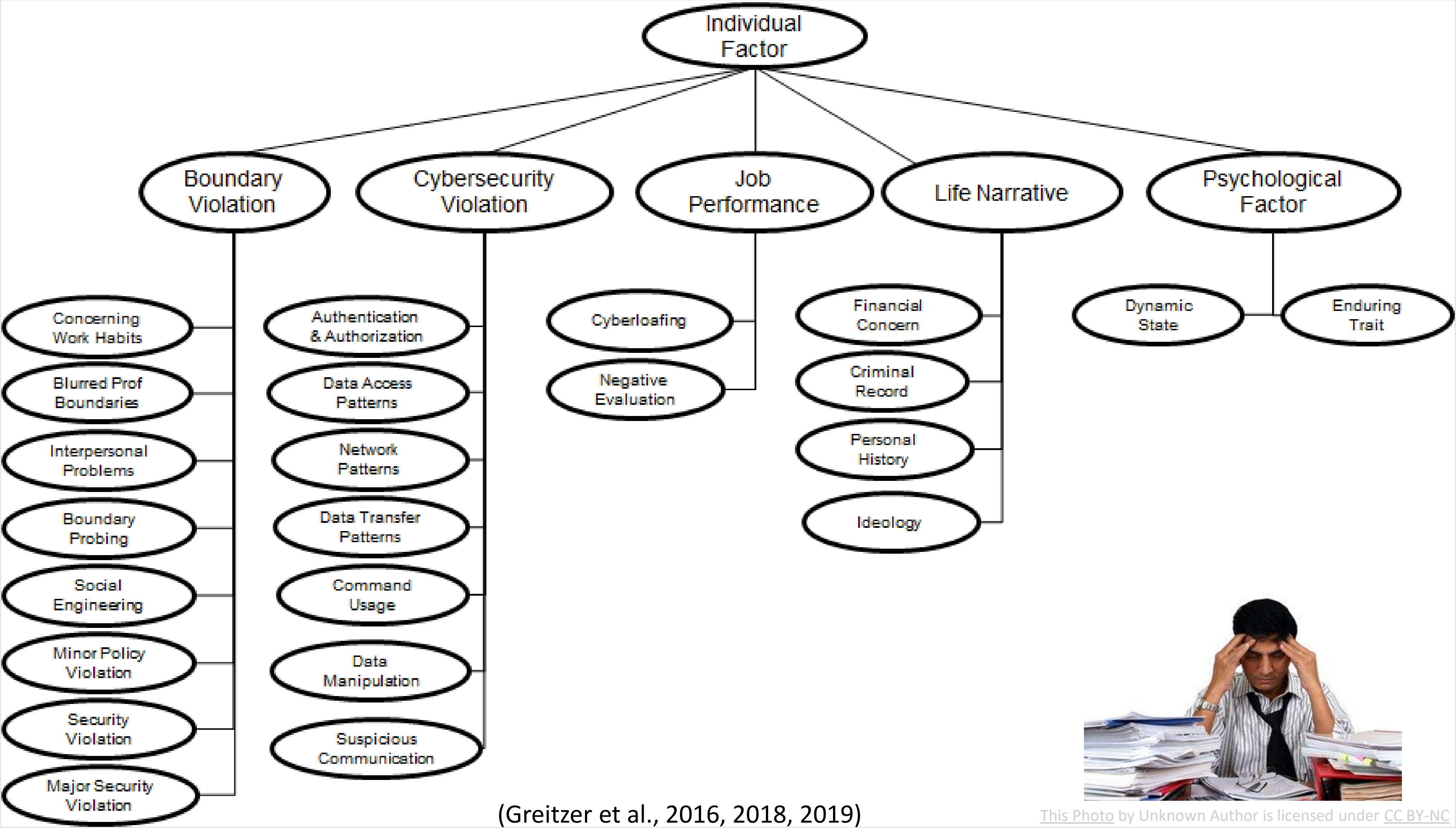
ESPIONAGE • THEFT

• SABOTAGE

• FRAUD

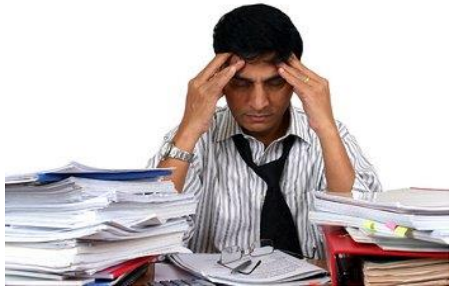
• WORKPLACE VIOLENCE

# SOFIT: Individual Factors



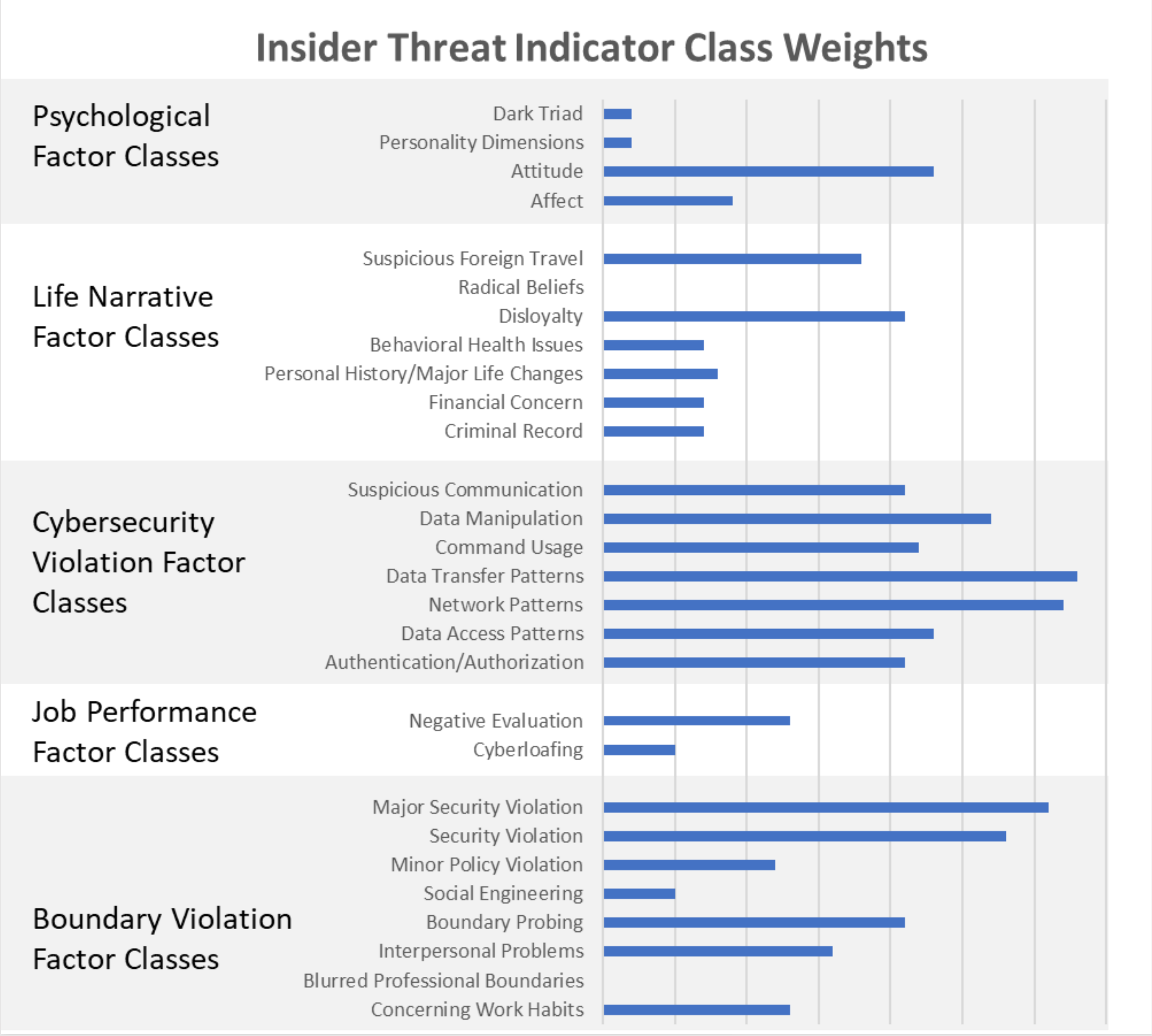
- Individual Factor
  - Boundary Violation
    - Concerning Work Habits
    - Blurred Prof Boundaries
    - Interpersonal Problems
    - Boundary Probing
    - Social Engineering
    - Minor Policy Violation
    - Security Violation
    - Major Security Violation
  - Cybersecurity Violation
    - Authentication & Authorization
    - Data Access Patterns
    - Network Patterns
    - Data Transfer Patterns
    - Command Usage
    - Data Manipulation
    - Suspicious Communication
  - Job Performance
    - Cyberloafing
    - Negative Evaluation
  - Life Narrative
    - Financial Concern
    - Criminal Record
    - Personal History
    - Ideology
  - Psychological Factor
    - Dynamic State
    - Enduring Trait

(Greitzer et al., 2016, 2018, 2019)



# Varied Weights of Indicators

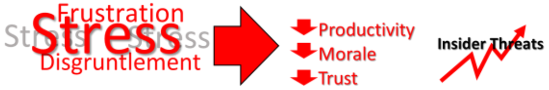
Not every factor is equally indicative of insider threat.

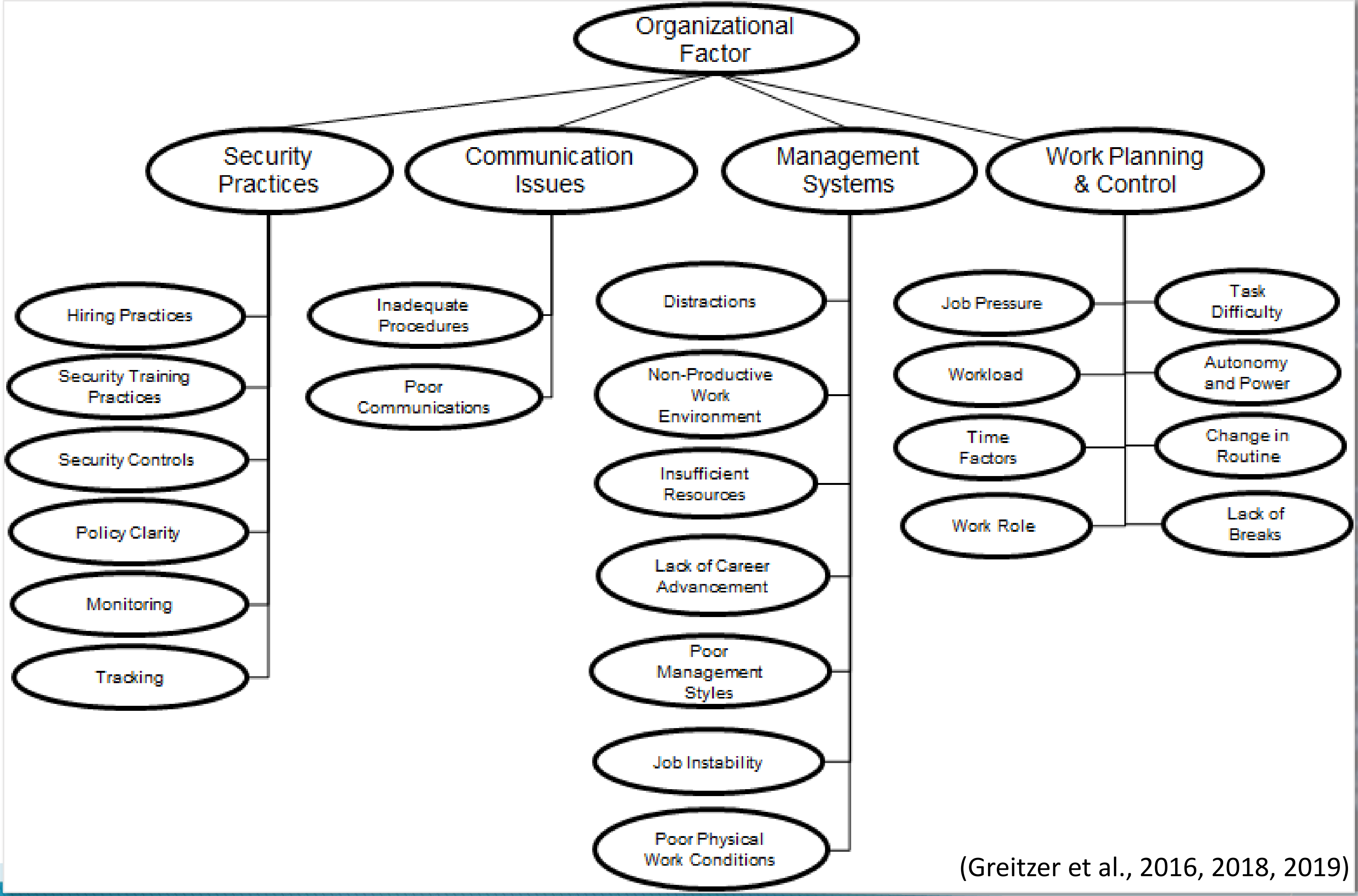


Greitzer et al. (2019)

# SOFIT: Organizational Factors

## Professional Stressors





- Organizational Factor
  - Security Practices
    - Hiring Practices
    - Security Training Practices
    - Security Controls
    - Policy Clarity
    - Monitoring
    - Tracking
  - Communication Issues
    - Inadequate Procedures
    - Poor Communications
  - Management Systems
    - Distractions
    - Non-Productive Work Environment
    - Insufficient Resources
    - Lack of Career Advancement
    - Poor Management Styles
    - Job Instability
    - Poor Physical Work Conditions
  - Work Planning & Control
    - Job Pressure
    - Task Difficulty
    - Workload
    - Autonomy and Power
    - Time Factors
    - Change in Routine
    - Work Role
    - Lack of Breaks

(Greitzer et al., 2016, 2018, 2019)

# Requires Coordination and Information Sharing Among Diverse Stakeholders

- Cybersecurity
- Security
- Management
- May include Human Resources

**Incident Response Team**

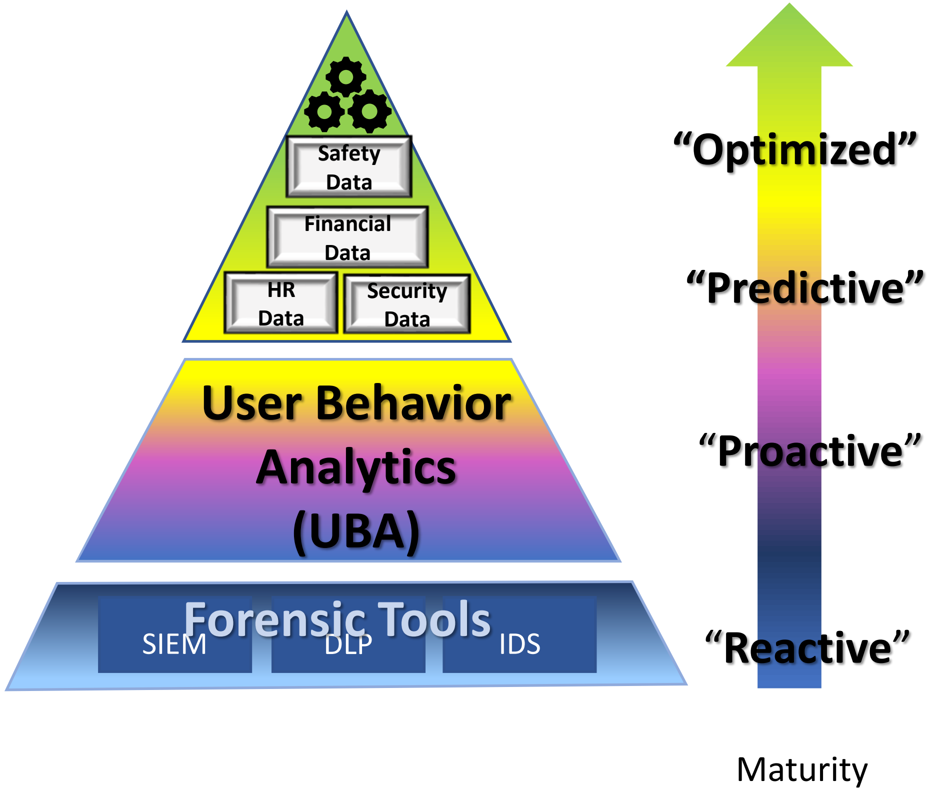
Trusted Workforce TW2.0

- Behavioral indicators define "Attributes of Trust"
- Informed by Critical Pathway model

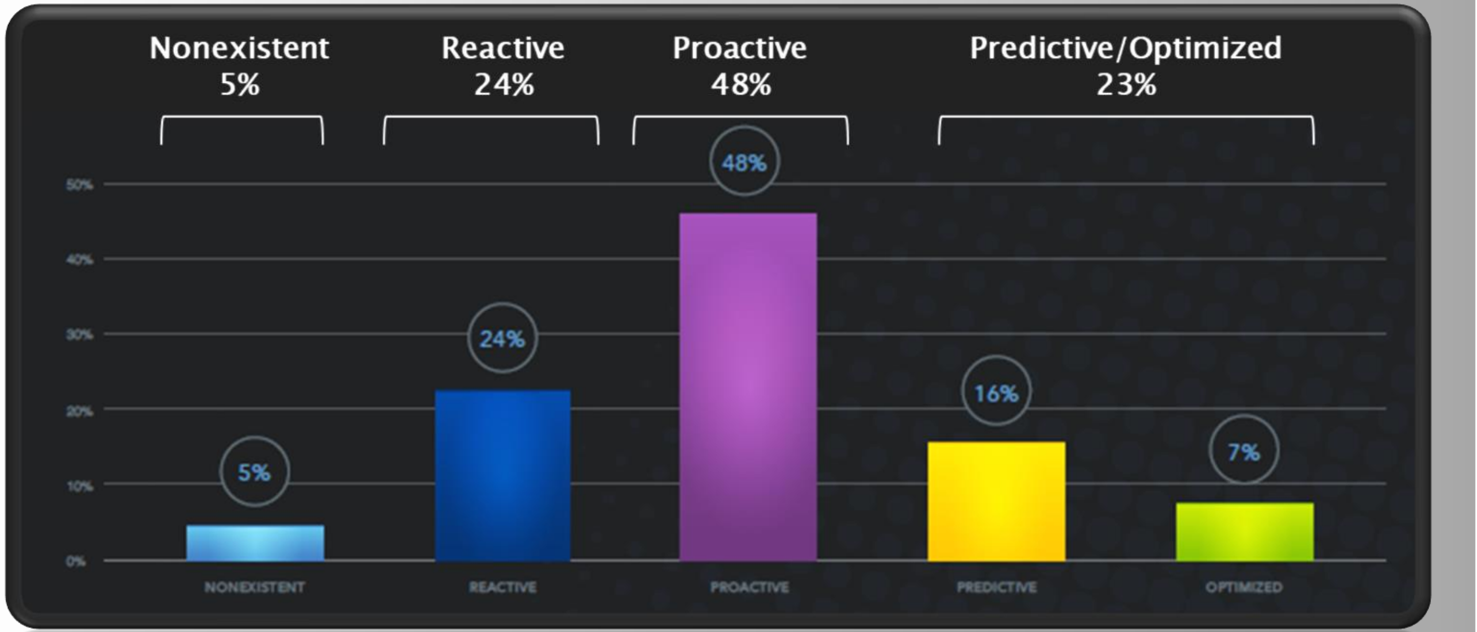
INSA Whitepaper: *Human Resources and Insider Threat Mitigation: A Powerful Pairing*

*Need: Greater involvement by Human Resources, Worker Representatives, Privacy Advocates to establish a proactive Insider Threat program*

# *Whole Person Approach*



## Insider Threat Program Maturity



Henderson & Cavalanca (2019)

# Summary: Insider Threat Program Should be…

- Comprehensive
  - Whole Person + Organizational Self-Assessment
- Inclusive
  - Engagement across departments/stakeholders and all levels of Organization
- Proactive
  - Cyber/technical monitoring to provide cyber defense and forensic data
  - Human behavioral data to identify at-risk individuals
  - Organizational assessment to identify contributing systemic factors
- Supportive
  - Mitigation is not just punitive—address individual risk factors and correct adverse organizational factors that increase risk and vulnerabilit

Greitzer (2019)

# References and Further Reading

- 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.
- 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. http://ceur-ws.org/Vol-1788/STIDS_2016_T03_Greitzer_etal.pdf
- 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. https://ieeexplore.ieee.org/document/8424651
- Greitzer, FL. (2019). “Insider Threat: It’s the HUMAN, Stupid!” *Proceedings of the Northwest Cybersecurity Symposium*, April 8-10, 2019. Article No. 4, pgs 1-8. ACM ISBN 978-1-4503-6614-4/19/04. https://dl.acm.org/doi/10.1145/3332448.3332458
- Greitzer, FL, J Purl, YM Leong, & PJ Sticha (2019). Positioning your organization to respond to insider threats. *IEEE Engineering Management Review, 47(2)*, 75-83. https://ieeexplore.ieee.org/document/8704879
- Henderson, J & N Cavalanca: *2019 Insider Threat Program Maturity Model Report*. https://cdn2.hubspot.net/hubfs/5260286/PDFs%20-%20%20Whitepapers,%20Case%20Studies,%20%20Datasheets/Whitepapers/insider-threat-maturity-report-2019.pdf
- Shaw, ED & LF Fischer. (2005). *Ten tales of betrayal: The threat to corporate infrastructures by information technology insiders Analysis and Observations*. PERSEREC Technical Report 05-13, September 2005. https://www.dhra.mil/Portals/52/Documents/perserec/tr05-13.pdf
- Shaw, ED & L Sellers. (2015). Application of the critical-path method to evaluate insider threats. *Studies in Intelligence, 59(2)*, 1-8. https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-59-no-2/pdfs/Shaw-Critical%20Path-June-2015.pdf

See also:

PsyberAnalytix Blog:
https://psyberanalytix.com/franks-blog

INSA Whitepaper: Human Resources and Insider Threat Mitigation: A Powerful Pairing
https://www.insaonline.org/wp-content/uploads/2020/09/INSA_InT_Sept252020.pdf

INSA Whitepaper: Categories of Insider Threat
https://www.insaonline.org/wp-content/uploads/2019/10/INSA_WP_Categories_of_Insider_Threats-1.pdf

# Thank You for Your Attention!

**Frank L. Greitzer, PhD**

**PsyberAnalytix**

**Richland, WA**

http://www/PsyberAnalytix.com

Frank@PsyberAnalytix.com