

The Human Centric AI Seminars
CSIRO Data 61 DSS Group



A **dventures in Insider Threat Predictive Analytics**

Frank L. Greitzer, PhD

PsyberAnalytix

www.PsyberAnalytix.com

March 23, 2022



Topics

[Whole Person Perspective](#)

[Insider Threat Ontology](#)

[Empirical Studies](#)

[Behavioral Analytics / Pattern Processing](#)

[Concluding Remarks and References](#)

[Addendum: Unintentional Insider Threats](#)





Whole Person Perspective

Definition of Insider Threat

Traditional Approach

Critical Pathway Framework

Getting “Left of Boom”

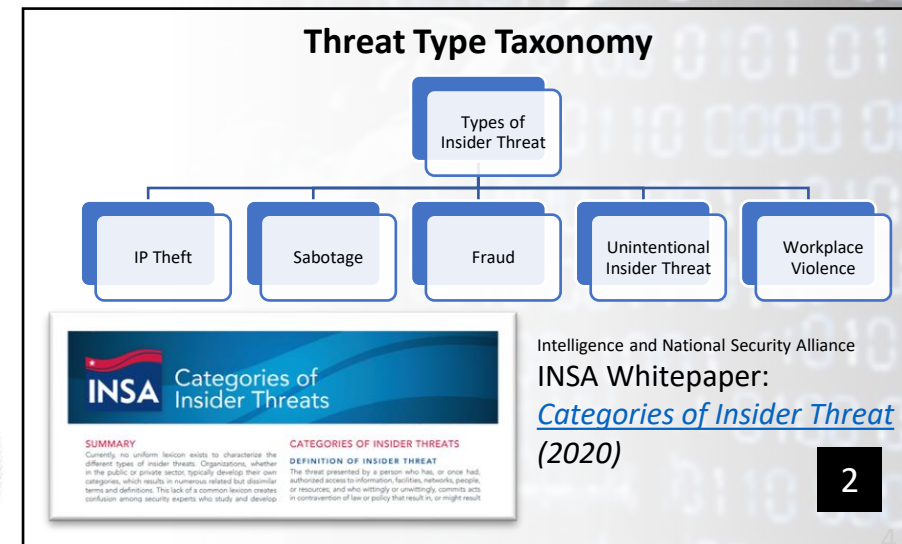
Integrating Technical and Behavioral Factors

Insider Threat Defined

- An **insider** is any person who has or had authorized access to, or knowledge of, an organization's resources, including personnel, facilities, information, equipment, networks, and systems.
- **Insider threat** is the potential for an insider to use their authorized access or understanding of an organization to harm that organization:
 - Individual uses their authorized access (maliciously or unintentionally) in a way that may harm the organization.



CERT (Cappelli et al., 2012) **1**



Typical Monitoring Approach...

Host/network logs

Intrusion
Detection
Systems

Data Loss
Prevention
Products

Cyber Data Collection

- Registry entries
- IDS events
- Firewall logs
- DNS logs/Internet sites accessed
- Host event logs
- Host print logs
- Network print logs
- Search engine query log data
- Physical security (prox-card data)
- Database server logs
- Web server Logs
- File permissions
- Access to account
- Digital signatures
- Local stored or cached file
- Applications installed
- Patch status
- Keystroke record

A typical network monitoring system can generate over 2 Billion events per week!

Typical Monitoring Approach...

“Streetlight Effect”

3 (Freedman, 2010)



Insider Threat Programs Miss the Human Side of the Problem

NEWS

EMERGING TECH

CYBERSECURITY

Mar 1, 2017 | 9:55 am

SHARE THIS STORY



“Where we’re missing the boat, oftentimes, is on the human resource side,” said Evanina. “The goal is to stop them before [they act]. We have to find a way to identify them ahead of time and say, ‘hey listen, I know things are rough, you’re having problems, but there’s other options.’ ”

Bill Evanina, national counterintelligence executive and director of the U.S. National Counterintelligence and Security Center, speaking at an *Intelligence and National Security Alliance (INSA)* event.

Stopping insider threats relies more on addressing human problems than technological ones, according

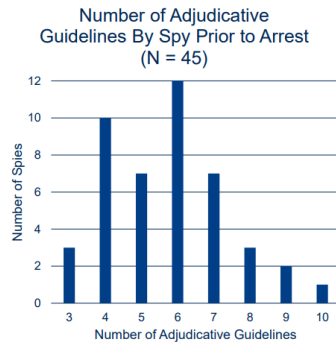
Trusted insiders who commit crimes do not just “pop-up.”

In 8 of 10 insider espionage/sabotage cases examined, social/organizational precursors were identified that could have been addressed before the attack. -- Shaw & Fischer (2005) **4**

Defense Personnel and Security Research Center

PRELIMINARY FINDINGS

- In 20 of the 45 cases, someone noticed the spy's concerning behavior or a change in behavior prior to arrest
 - In 15 of these 20 cases, someone went on to report the concerning behavior prior to arrest
- Hypothesis: There is a direct relationship between the number of adjudicative guidelines and the number of concerned others



U.S./DoD/OPA/PERSEREC | 18

PERSEREC-TR-19-02
Jaros et al. (March 2019). *The Resource Exfiltration Project: Findings from DoD Cases, 1985-2017.*
<https://www.dhra.mil/PERSEREC/Selected-Reports/#TR19-02> **5**



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

Critical Pathway to Insider Risk

(Shaw & Sellers, 2015) **6**

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



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

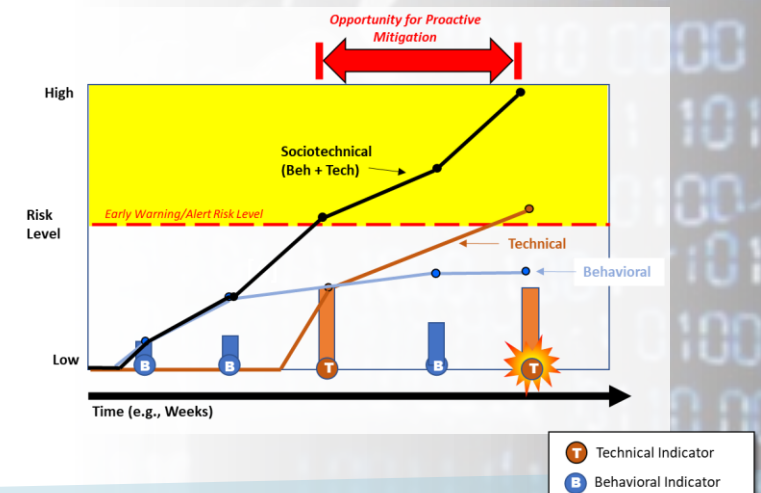
Need to incorporate behavioral and organizational “tripwires” into the insider risk mitigation process

- *Holistic*: Include *Behavioral*, *Psychosocial*, and *Organizational* indicators in addition to technical/cyber indicators
- *Proactive*: Anticipatory analysis instead of reactive/forensic approach
- Focus on staff and organizational “well-being” rather than a punitive “law enforcement” approach.

7 (Greitzer, 2019)

A holistic, proactive approach helps insider-threat analysts get “left of boom.”

8 (Greitzer et al., 2018)





SOFIT Ontology

Origins

Individual Factors

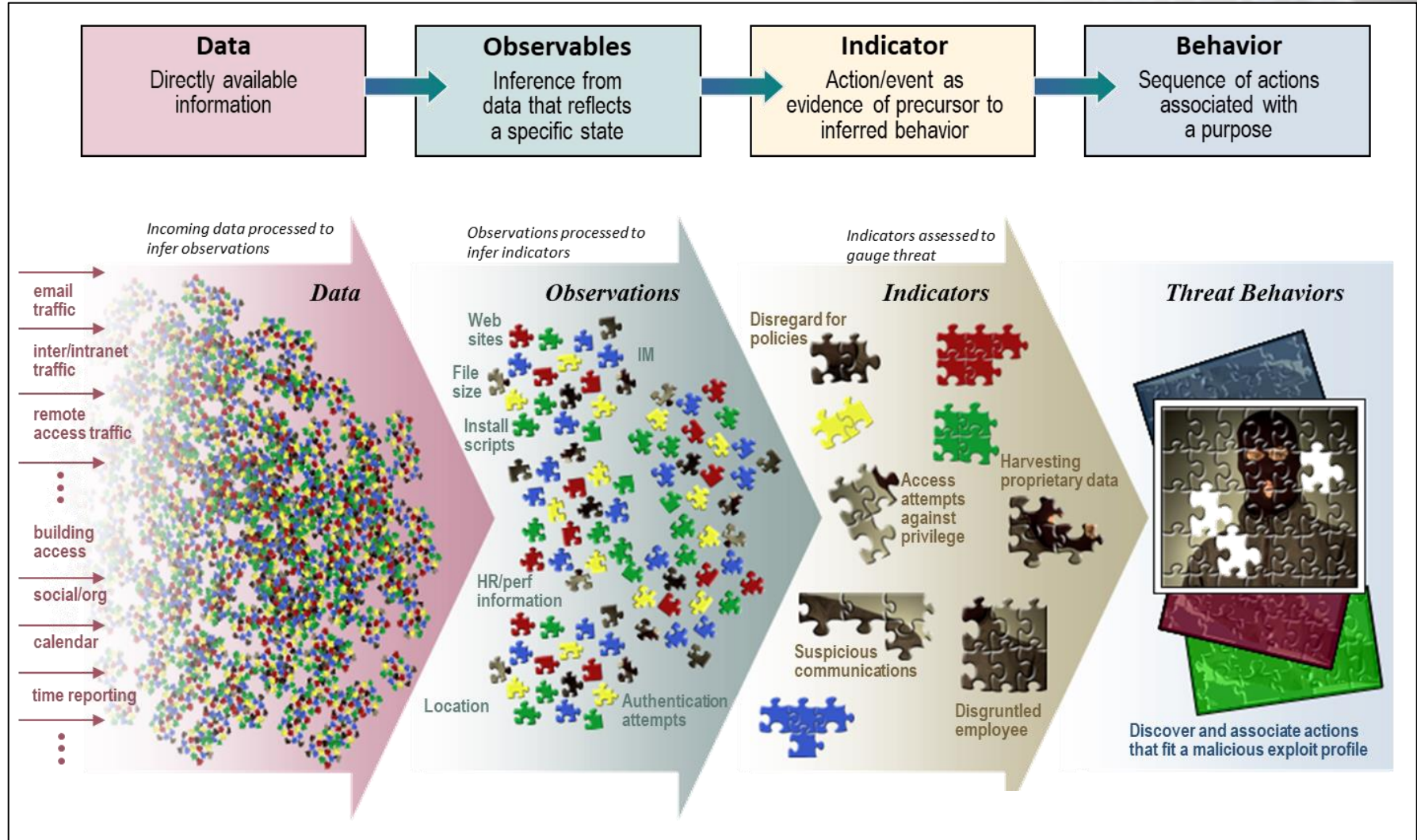
Ontology Overview

Sociotechnical and
Organizational
Factors for
Insider
Threat

Integrating Technical and Social/Behavioral Data

“Shredded Puzzle Metaphor”

(Greitzer & Frincke, 2011) 9



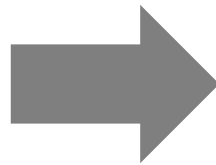
Why Ontology?

- Formal description of concepts within a domain
- Provides computational properties that support inferences from asserted facts
- Supports development of models for insider threat assessment.
- Defines concepts and relationships that may be applied consistently across organizations



Method/Approach for Developing Knowledge Base

Sources



Published Case Studies and Scientific Literature

Expert Knowledge Elicitation Surveys

Indicator Class/Factor	Range of Insider Threat/Risk Concern	Threat Risk Score	Description
Data Access Patterns	0 - 100	0 - 100	
Attempt unauthorized access to sensitive data	<	50	Seeking to gain undue access to files that are not backed up.
Granting unauthorized access to sensitive data	<	50	Granting access to sensitive documents to person(s) without a need to know.
Attempt unauthorized access to sensitive data	<	50	Seeking to gain undue access to sensitive data or documents without a need to know.
Attempts to access new workstation	<	50	Login to a new workstation (physically or remotely).
Attempts to change file permissions	<	50	Changing or attempting to change file permissions.
Circumvent document control	<	50	Defeating document control safeguards.
Request unauthorized access to sensitive data	<	50	Requesting unrequired access (e.g., access to documents for which one has no need to know, establishing an extra login account or access path).
Network Patterns	0 - 100	0 - 100	
Booting from local media	<	50	Using local media (e.g., CD or USB-drive) to boot a separate operating system from that installed on the work computer.
Compromised machine	<	50	An individual or network of work computers infected with malicious software (bot, botnet) that are remotely controlled by a malicious actor.
Duplicate log file backup	<	50	Duplicating log files.
Extra backups	<	50	Making extra backups of network files.
Failure to join machine to domain	<	50	Use or maintain a computer that is disconnected from domain.
High activity on high target machine	<	50	Unusually high activity on a machine containing sensitive data.
Printing documents of others	<	50	Printing documents that are owned by others.
Using multiple printers simultaneously	<	50	Concurrent use of multiple printers.
Use of unusual printer	<	50	Printing to locations unrelated to one's work location.
Search computer libraries	<	50	Unusual search of computer libraries.
Search own name	<	50	Searching logs or security data for own name.

(Greitzer et al., 2018, 2019)

8

10

Doc #	Title	Organization / Author(s)	Date	Comments
1	Understanding Insider Threat - Proceedings of a March 2004 Workshop	RAND corporation		
2	Advanced IC Information Assurance	ARDA		
3	Honeypots - Catching the Insider Threat	Lance Spitzner		
4	Advanced Countermeasure for Insider Threat, presolicitation notice	Boanerges Aleman-Meza, Phillip Burns, Matthew Epensson, Delvander Robert DelZoppo, Eric Brown, Matt Downe, Michael D'Erredita		
5	An Ontological Approach to the Document Access Problem of Insider Threat			
6	A Multi-Disciplinary Approach for Countering Insider Threats			
7	ACIT Workshop			
8	Lockheed Martin Omnicon and Authentica to Develop Solution to Mitigate Insider Threat Within the Intelligence Improved Information Systems Security in DoD Environments			
9	How the FBI Investigates Computer Crime			
10	CS/IFBI Computer Crime and Survey			
11	Ten Tales of Behavioral - Technology Insiders			
12				

2019 Lit search

Doc #	Title	Organization / Author(s)	Date	Comments			
	Costa, D. L., Albrethsen, M. J., & Collins, M. L. (2016). Insider Threat Indicator Ontology (No. CMU/SEI-2016-TR-007). CARNEGIE-MELLON UNIV PITTSBURGH PA PITTSBURGH United States.			Y	Y	Cybersecurity	page 70 has indicators -- page 23 talks about v
	Torres, J. M., Sarriegl, J. M., Santos, J., & Serrano, N. (2006, August). Managing information systems security: critical success factors and indicators to measure effectiveness. In International Conference on Information Security (pp. 530-545). Springer, Berlin, Heidelberg.			Y	N	Cybersecurity	indicators of critical success factors for effective security management, not person level indicators of cyber threat
	Hunker, J., & Probst, C. W. (2011). Insiders and Insider Threats-An Overview of Definitions and Mitigation Techniques. JoWUA, 2(1), 4-27.			Y	Y	Both	page 18
	Young, W. T., Goldberg, H. G., Memory, A., Sartain, J. F., & Senator, T. E. (2013, May). Use of domain knowledge to detect insider threats in computer activities. In 2013 IEEE Security and Privacy Workshops (pp. 60-67). IEEE.			Y	Y	Cybersecurity	Page 61 and 67
	Greitzer, F. L., Imran, M., Puri, J., Avelrad, E. T., Leong, Y. M., Becker, D. E., ... & Sitcha, P. J. (2016). Developing an Ontology for Individual and Organizational Sociotechnical Indicators of Insider Threat Risk. In STIDS (pp. 19-27). Bishop, M., Gates, C., Frincke, D., & Greitzer, F. L. (2009, May). AZALIA: an A to Z Assessment of the Likelihood of Insider Attack. In 2009 IEEE Conference on Technologies for Homeland Security (pp. 385-392). IEEE.			Y	Y	Psychology	table 1, figure 2,
	Huth, C. L., Chadwick, D. W., Claycomb, W. R., & You, I. (2013). Guest editorial: A brief overview of data leakage and insider threats. Information Systems Frontiers, 15(1), 1-4.			Y	N	?	editorial
	Baikalov, I. A., Gulati, T., Nayyar, S., Shenoy, A., & Patwardhan, G. H. (2017). Risk scoring for threat assessment. U.S. Patent No. 9,800,605. Washington, DC: U.S. Patent and Trademark Office.			N		Cybersecurity	from abstract alone, does not appear to have indicators
	Shaw, E. D., & Stock, H. V. (2011). Behavioral risk indicators of malicious insider theft of intellectual property: Misreading the writing on the wall. White Paper, Symantec, Mountain View, CA, 2011.			Y	Y	Psychology	A lot of indicators in this article: page 4, table 1, table 2, table 5
	Flynn, L., Huth, C., Trzeciak, R., & Buttles, P. (2012, October). Best practices against insider threats for all nations. In 2012 Third Worldwide Cybersecurity Summit (WCS) (pp. 1-8). IEEE.			Y	N	Cybersecurity	
	Sanzgiri, A., & Dasgupta, D. (2016, April). Classification of insider threat detection techniques. In Proceedings of the 11th annual cyber and information security research conference (p. 25). ACM.			N	N	Cybersecurity	
	Hashem, Y., Takabi, H., GhasemiGol, M., & Dantu, R. (2015, October). Towards insider threat detection using psychophysiological signals. In Proceedings of the 7th ACM CCS International Workshop on Managing Insider Security Threats (pp. 71-74). ACM.			Y	N	?	identifies physiological indicators using EEGs, but doesn't actually state what those indicators are
	Greitzer, F. L., & Ferryman, T. A. (2013, May). Methods and metrics for evaluating analytic insider threat tools. In 2013 IEEE Security and Privacy Workshops (pp. 90-97). IEEE.			Y	N	Both	
	Symonenko, S., Liddy, E. D., Yilmazel, O., Del Zoppo, R., Brown, E., & Downey, M. (2004, June). Semantic analysis for monitoring insider threats. In International Conference on Intelligence and Security Informatics (pp. 492-500). Springer, Berlin, Heidelberg.			Y	N	Both	Social network analysis and natural language
	Sheldon, F. T., Abercrombie, R. K., & Mill, A. (2009, January). Methodology for evaluating security controls based on key performance indicators and stakeholder mission. In 2009 42nd Hawaii International Conference on System Sciences (pp. 1-10). IEEE.			N	N	Cybersecurity	"This paper proposes a Cyberspace Security Ec
	Cole, E., & Ring, S. (2005). Insider threat: Protecting the enterprise from sabotage, spying, and theft. Elsevier.			N	Y	Cybersecurity	Book, indicators might be on page 295
	Guido, M. D., & Brooks, M. W. (2013, January). Insider threat program best practices. In 2013 46th Hawaii International Conference on System Sciences (pp. 1831-1839). IEEE.			N	N	Cybersecurity	
	Magklaras, G., & Furnell, S. (2010). Insider threat specification as a threat mitigation technique. In Insider Threats in Cyber Security (pp. 219-244). Springer, Boston, MA.			Y	N	Cybersecurity	focuses on development of a domain specific insider threat prediction language
	Cappelli, D. M., Moore, A. P., & Trzeciak, R. F. (2012). The CERT guide to insider threats: how to prevent, detect, and respond to information technology crimes (Theft, Sabotage, Fraud). Addison-Wesley.			N	Y	Cybersecurity	Book, page 33 has indicators (parts of the book are able to be previewed)
	Claycomb, W. R., Legg, P. A., & Gollmann, D. (2014). Guest Editorial: Emerging Trends in Research for Insider Threat Detection. JoWUA, 5(2), 1-6.			Y	N	Cybersecurity	Guest editorial

Whole Person

Ontology

Studies

Beh Analytics

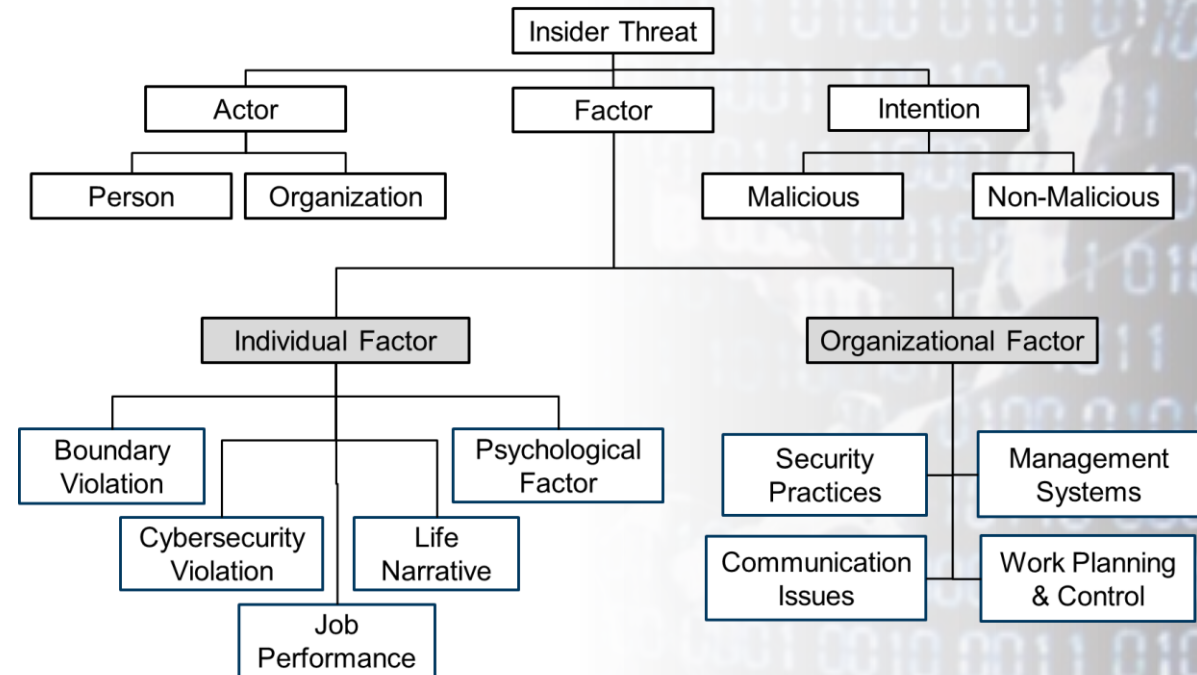
Conclusion

Addendum: UIT

SOFIT Ontology

- Individual (Human) Factor branch contains more than 270 technical and behavioral factors
- Organizational Factor branch includes roughly 50 contributing factors
- Developed in OWL [Web Ontology Language](#) – a Semantic Web language to represent rich and complex sets of knowledge

Sociotechnical and Organizational Factors for Insider Threat



(Greitzer et al., 2018, 2019, 2019, 2021)

8

10

11

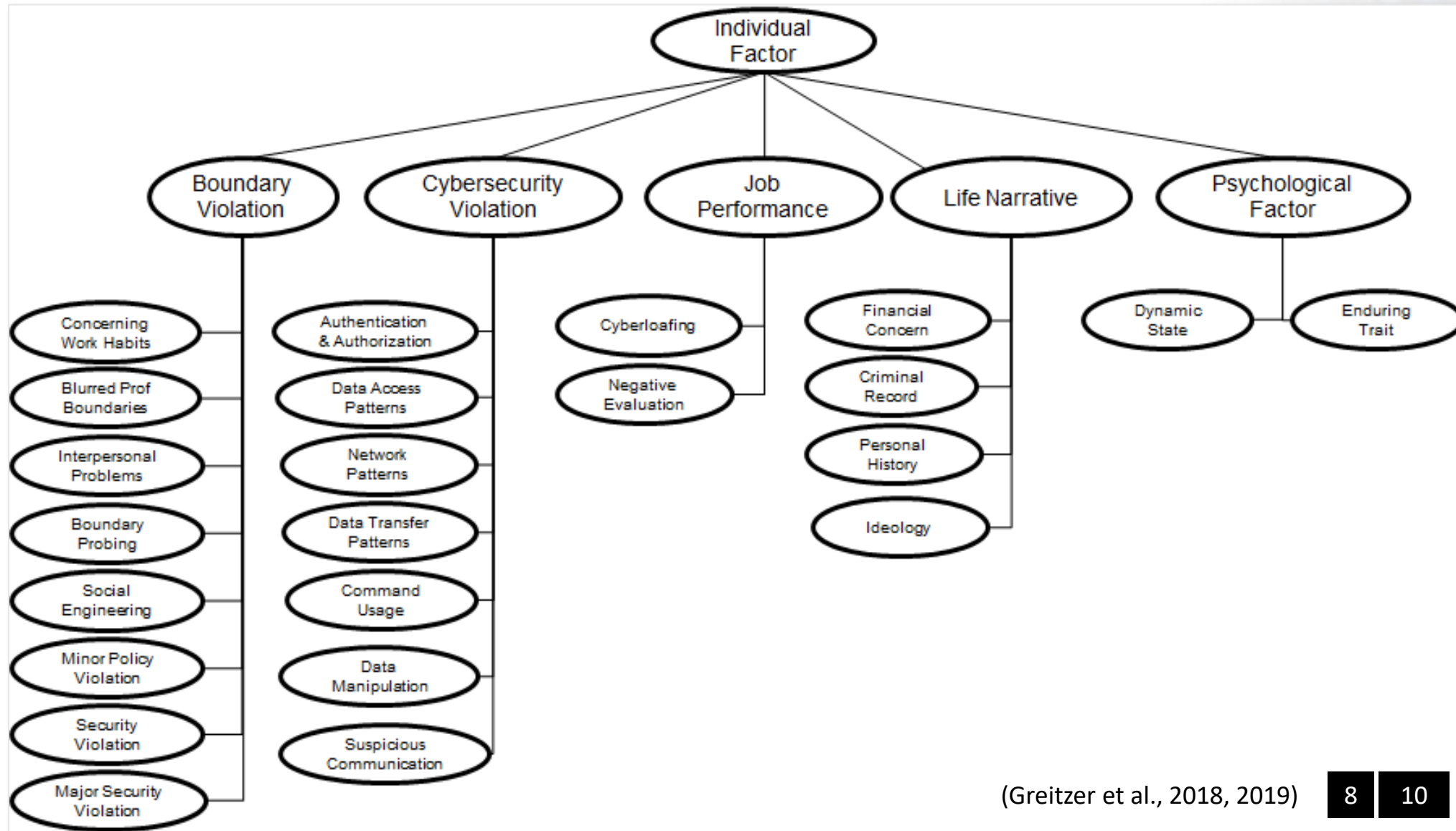
12

SOFIT developed under IARPA funding (2016-2019)



Intelligence Advanced Research Projects Activity
IARPA contract 2016-16031400006

SOFIT Individual Factors



(Greitzer et al., 2018, 2019)

8

10



Empirical Studies

Estimating “Severity” of Indicators

Evaluating Models

Dynamic Characteristics of Indicators

- **Temporal Factors**
- **Nonlinear Combinations**

Expert Knowledge Elicitation Studies (2018, 2019)

- Experts recruited from research and operational communities – email and online surveys
- Number of participants ranged from 8-35
- Surveys gathered expert judgments on:
 - Threat ratings of 202 *single* indicators (Greitzer et al., 2018, 2019) **8** **10**
 - Ratings for cases comprising *multiple* indicators
 - Temporal and Dynamic features (Greitzer & Purl, 2022) **13**

Estimating individual indicator level of concern

Ranking of cases

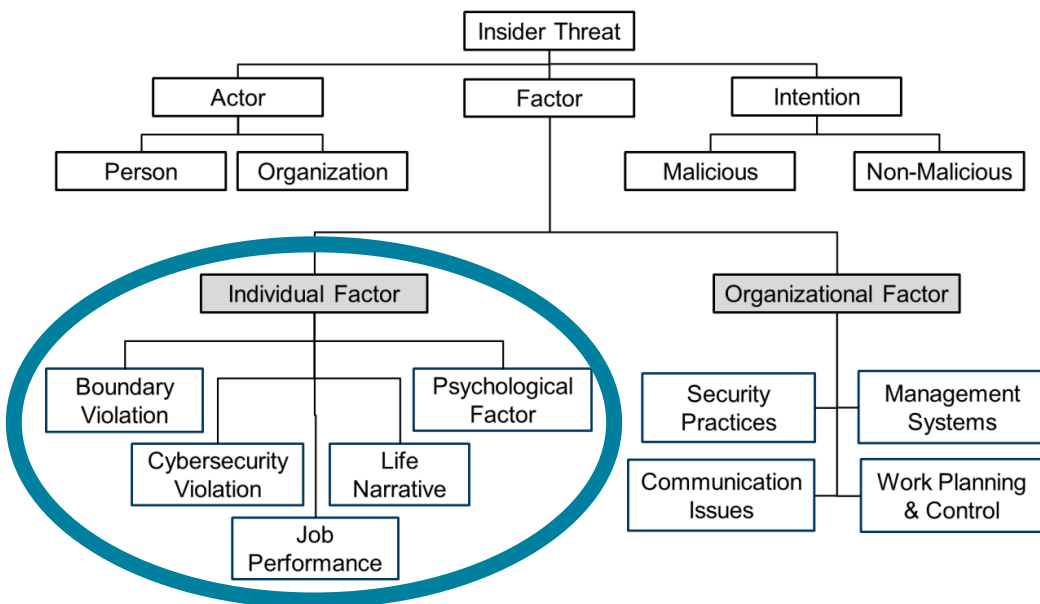
Temporal and dynamic relationships

The screenshot displays a survey interface for expert knowledge elicitation. It includes a table of indicators with columns for 'Indicator Class/Factor', 'Range of Indicator Threat/Risk Concern', and 'Description'. Below the table is a 'Cases to Assign' dialog box with a color-coded ranking scale from Low Concern to Extreme Concern. The main survey form, 'Case #2', shows a timeline of indicator reports from January to September, with specific counts for each month: Baseline: [0 indicators reported], Month 1: [1-3 indicators reported], Month 2: [0 indicators reported], Month 3: [0 indicators reported], and Month 4: [0-2 indicators reported].

Indicators Vary in Severity

[Greitzer et al., 2018]

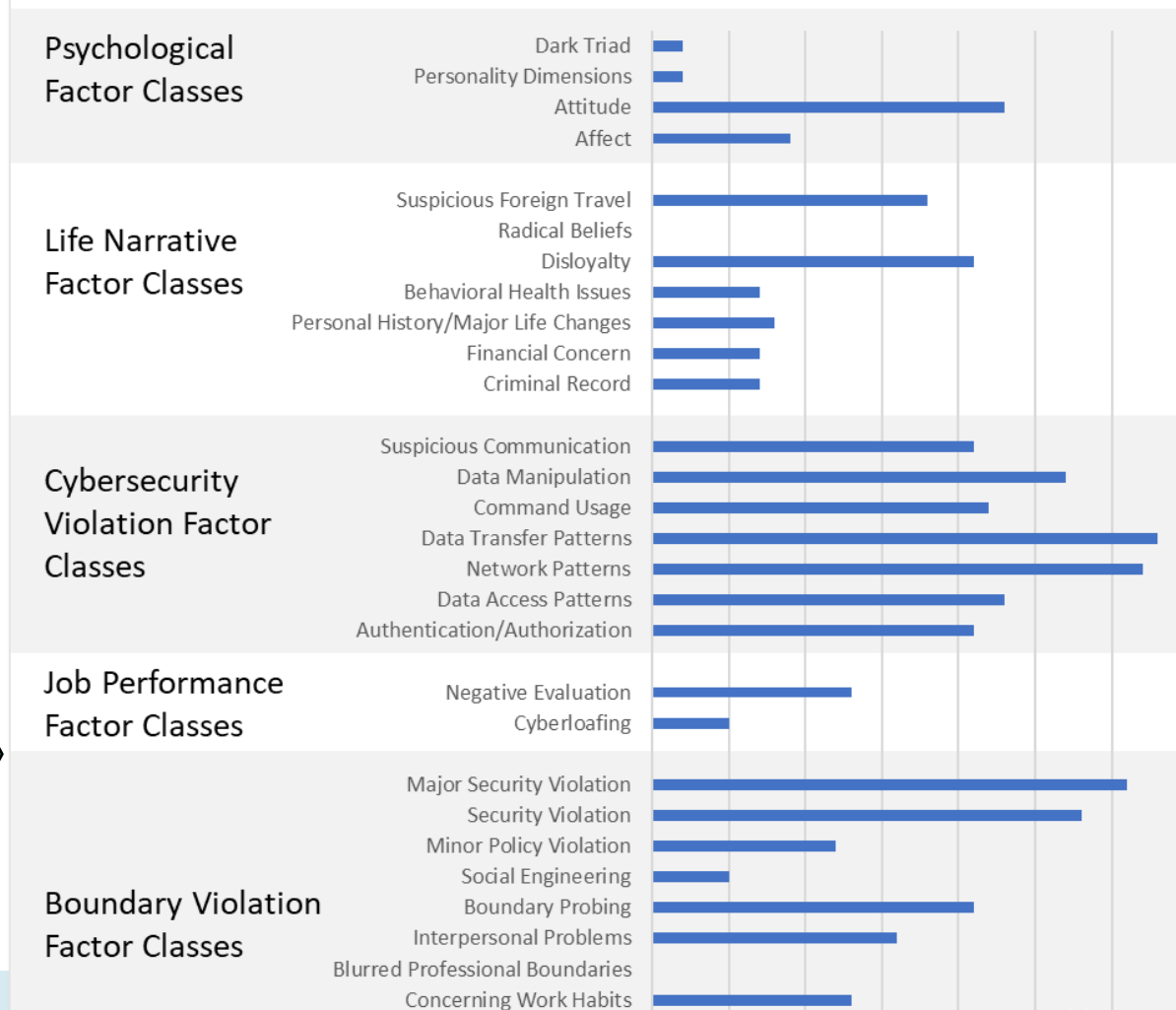
8



Not every factor is equally indicative of insider threat



Insider Threat Indicator Class Weights

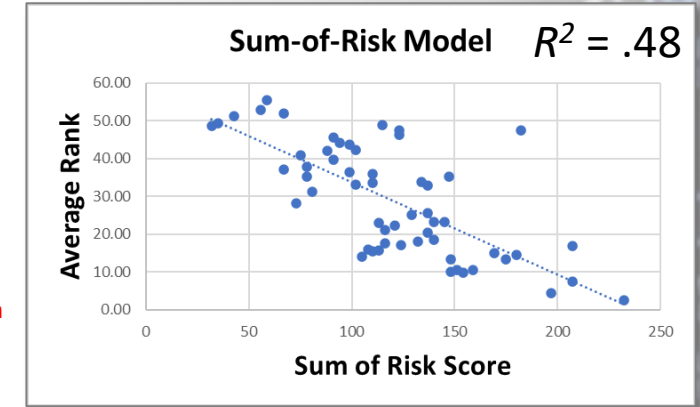
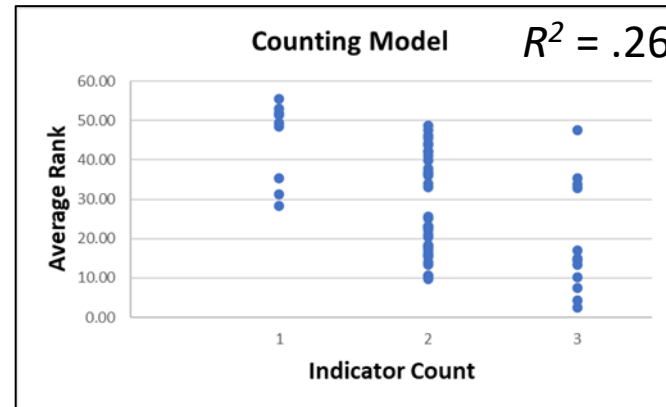


Modeling Severity Improves Prediction

We evaluated several alternative predictive models in accounting for expert judgments of insider threat risk. Experts assessed (ranked) threat of 57 hypothetical insider threat cases comprising combinations of one to three indicators.

Model	R^2
Counting Model	0.26
Sum of Risk Model	0.48
Bayes Model	0.53

[Greitzer et al., 2018, 2019, 2021]



(Greitzer et al., 2018, 2019, 2021)

8 10 12

(Greitzer & Purl, 2022)

13

Room for Improvement in Assessing Insider Risk:

At best, these indicator-risk-based predictive models accounted for ~50% of the variance in expert judgments of threat/risk...

17 Indicators Organized by Role Type

Personal Predisposition

- Manipulative
- Big Ego/Self-Centered

Precipitating Event

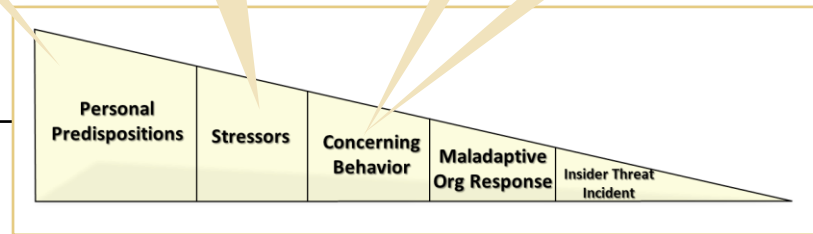
- Job Pressure/Stress
- Negative Evaluation
- Received Corrective Action
- Passed Over for Promotion
- Terminated

Behavioral Precursor

- Disgruntled
- Marked Anger/Hostility

Technical Precursor

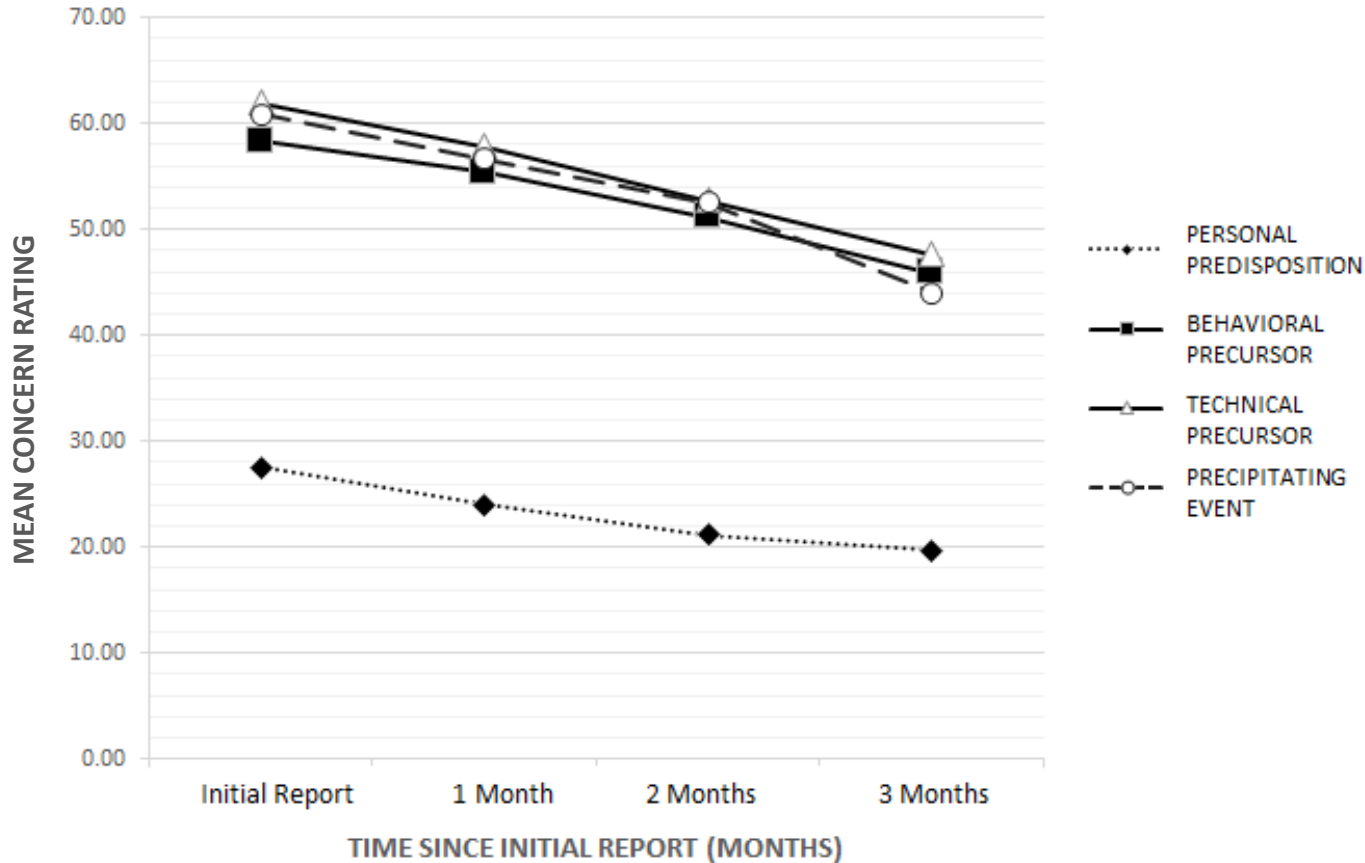
- Unusual File Deletion
- Excessive Unauthorized Database Searches
- Unauthorized Wireless
- Attempts Unauthorized Access to Sensitive Data
- Unusual Remote Access
- Using Multiple Printers Simultaneously
- Receiving Large Emails
- Change File Extensions



Temporal/Decay Effects by Role Type

All indicators showed some decay:

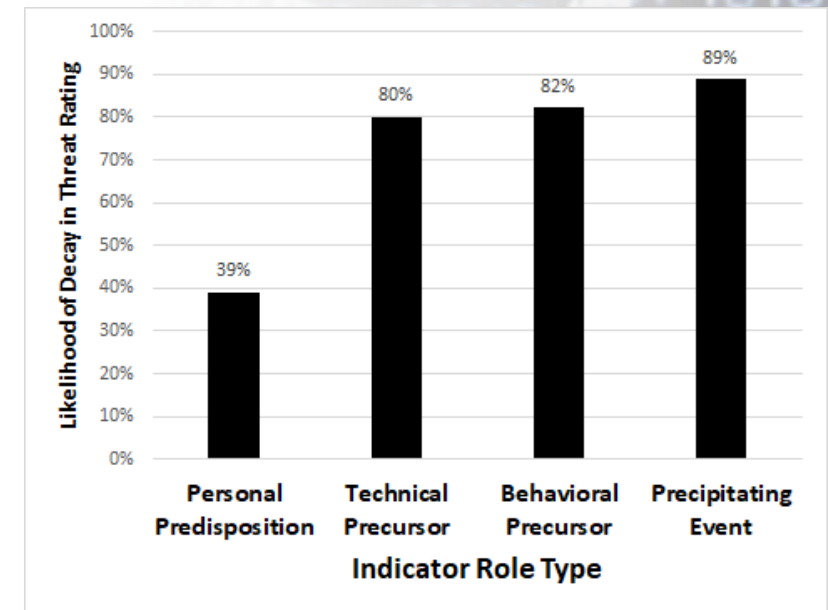
- Slight decrease in indicator threat/risk rating



Mean Concern Ratings from Baseline by Indicator Role Type

Personal Predispositions exhibited different decay characteristics:

- Started at a lower severity level
- Were significantly *less likely* to decay (39%) than any other indicator types



(Greitzer & Purl, 2022) 13

Indicator Interactions: Discrepant Cases

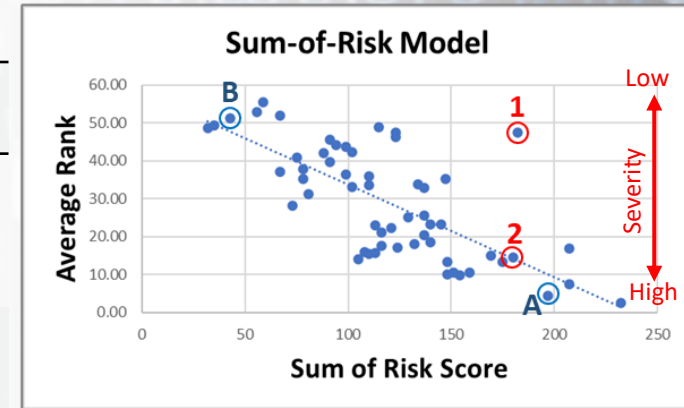
Threat Value scores were *expert judgments* of severity (0-100) for *individual indicators* (where 100 = most concerning). Case rankings were obtained by asking experts to sort (rank) 57 cases, producing ranks of 1-57, where 1 = most severe.

[Based on data from Greitzer et al. (2018)]

Case 1 [Lower Severity]

Case 2 [Higher Severity]

Indicators	Threat Value	Indicators	Threat Value
(1) Big ego/self-centered	59	(1) Working unusual hours on work machine	35
(2) Callousness	56	(2) Failed attempts to exercise privilege	78
(3) Manipulative	67	(3) Manipulative	67
Sum of Risks	182	Sum of Risks	180
Average Risk Score	61	Average Risk Score	60
Rank in Sorting Task	47	Rank in Sorting Task	14



➔ *A hierarchical linear modeling analysis yielded statistically significant interaction effects for different combinations of indicators.*

(Greitzer & Purl, 2022) 13

Summary of Results for Series of Studies: 2010-2019

Indicator Severity

- Indicator threat values (severity/level of concern) vary – it's not sufficient merely to “count” the number of observed indicators

Indicator Decay

- Expert judgments of threat values generally tend to decrease over time at a relatively slow and approximately linear rate
- Threat ratings of Personal Predispositions are more stable and less likely to decay than other indicator role types

Indicator Interactions/Patterns

- Threat rating of a collection of indicators in a case is not simply a linear combination of intrinsic individual indicator threat values
- Suggests that incorporating *patterns* into the analysis may improve prediction.



Behavioral Analytics/ Pattern Processing

Hard Problems Require Innovative Solutions

Where AI Can Help

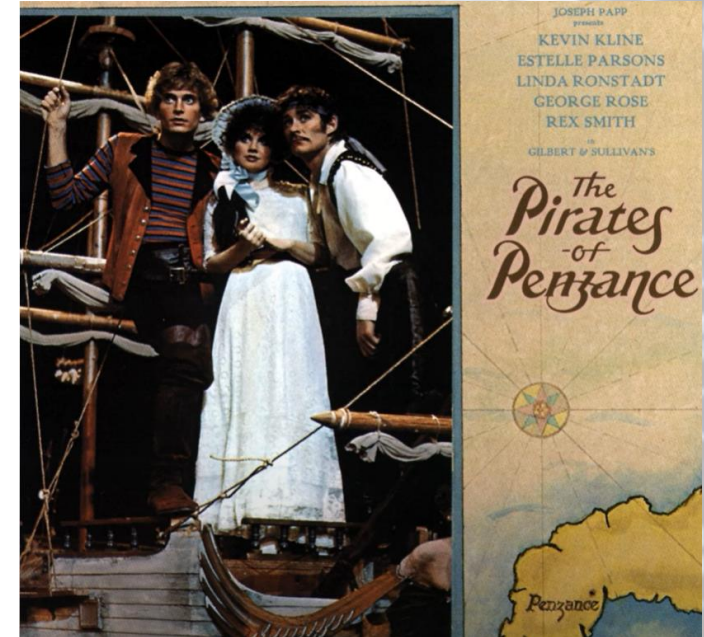
Insider Threat – “Hard” Problem



- *Lack of data and Ground Truth...*
- ***Most of the time the malicious insider behaves and looks much the same as innocent individuals...***

“When a felon is not engaged in his employment
Or maturing his felonious little plans-
His capacity for innocent enjoyment
Is just as great as any honest man's”

POLICEMAN'S SONG From the Gilbert & Sullivan opera
"Pirates of Penzance" (1879)

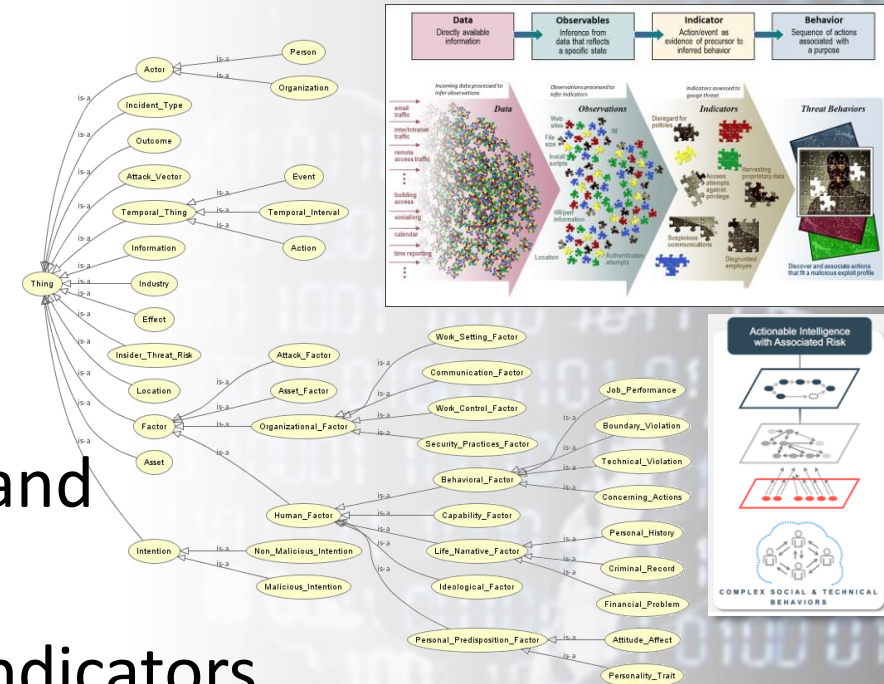


William Schwenk Gilbert / Sir Arthur Sullivan

Where AI can help:

Artificial Intelligence approaches may help address threat anticipation challenges...

- **Apply knowledge engineering methods** to understand and represent patterns of insider threat indicators
- **Capture emergent, dynamic relationships** among indicators beyond their individual, intrinsic characteristics
- **Model time dependencies** and the span of influence or “half-life” of insider risk indicators
- **Assimilate diverse data** representing...
 - The “whole person”
[sociotechnical + capability-motivation-opportunity]
 - Organizational culture/climate



... to support both individual and enterprise insider risk assessments



Concluding Remarks

Parting Thoughts

Contact Information

References

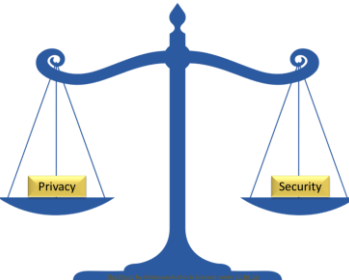
Parting Thoughts... Some Challenges / Needs:



- Data! [and ground truth!]
- **Holistic approach:** Monitor **Cyber + Human Behavioral + Organizational Factors**
- **It takes a village:** Coordination among *Cybersecurity, Management, HR, Security* stakeholders



• **Positive Deterrence:** *Supportive* rather than the more traditional *punitive* programs for mitigating insider risk (Moore et al., 2016) **14**



• **Ethical/privacy issues:** Aim for *transparency and buy-in* at all levels.

(Greitzer et al., 2011) **15**



• **AI technology:** Helping analysts find the “hidden needles in stacks of needles.”



References

- 1 Cappelli, D, AP Moore & RF Trzeciak. (2012). *The CERT® Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)*. Addison-Wesley.
- 2 Intelligence & National Security Alliance (INSA). (2020). *Categories of Insider Threat*
- 3 Freedman, DH. (2010). Why Scientific Studies Are So Often Wrong: The Streetlight Effect. Discover, December 9, 2010. Available online at: <https://www.discovermagazine.com/the-sciences/why-scientific-studies-are-so-often-wrong-the-streetlight-effect>
- 4 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>
- 5 Jaros et al. (March 2019). *The Resource Exfiltration Project: Findings from DoD Cases, 1985-2017*. <https://www.dhra.mil/PERSEREC/Selected-Reports/#TR19-02>
- 6 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>
- 7 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>
- 8 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>
- 9 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. http://dx.doi.org/10.1007/978-1-4419-7133-3_5
- 10 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.
- 11 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>
- 12 Greitzer, FL, J Purl, PJ Sticha, MC Yu, & J Lee. (2021). Use of Expert Judgments to Inform Bayesian Models of Insider Threat Risk. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, 12(2), 3-47. June 2021. DOI:10.22667/JOWUA.2021.06.30.003 <https://dx.doi.org/10.22667/JOWUA.2021.06.30.003>
- 13 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>.
- 14 Moore, AP, SJ Perl, J Cowley, ML Collins, TM Cassidy, N VanHoudnos, P Buttles, D Bauer, A Parshall, J Savinda, EA Monaco, JL Moyes & DM Rousseau. (2016). *The Critical Role of Positive Incentives for Reducing Insider Threats*. CERT Division, Software Engineering Institute, Carnegie Mellon University.
- 15 Greitzer FL, DA Frincke, and MM Zabriskie. (2011). "Social/Ethical Issues in Predictive Insider Threat Monitoring." In: MJ Dark (Ed.), *Information Assurance and Security Ethics in Complex Systems: Interdisciplinary Perspectives*. Hershey, Pennsylvania: IGI Global. Chapter 7, pp.132-161.
- 16 Dekker, S. 2002. *The Field Guide to Human Error Investigations*. Ashgate.
- 17 Greitzer, FL, J Strozer, S Cohen, J Bergey, J Cowley, A Moore, and D Mundie. (2014). "Unintentional insider threat: contributing factors, observables, and mitigation strategies. *47th Hawaii International Conference on Systems Sciences (HICSS-47)*, Big Island, Hawaii. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&number=6758854>
- 18 Greitzer, FL, J Strozer, S Cohen, A Moore, D Mundie, and J Cowley. 2014. "Analysis of unintentional insider threats deriving from social engineering exploits." *IEEE Security and Privacy Workshop on Research for Insider Threat (WRIT)*, San Jose, CA, May 17-18, 2014. <http://www.ieee-security.org/TC/SPW2014/papers/5103a236.PDF>
- 19 Li, W, J Lee, J Purl, FL Greitzer, B Yousefi, & KB Laskey. (2020). Experimental investigation of demographic factors related to phishing susceptibility. *53rd Hawaii International Conference on Systems Sciences (HICSS-53)*, Maui, Hawaii, January 2020. <https://scholarspace.manoa.hawaii.edu/bitstream/10125/64015/1/0221.pdf>
- 20 Greitzer, FL, W Li, KB Laskey, J Lee, & J Purl. (2021). Experimental Investigation of technical and human factors related to phishing susceptibility. *ACM Transactions on Social Computing*, 4(2), Article No. 8, June 2021, pp.1-48. <https://doi.org/10.1145/3461672>

Other Resources

1. Schultz, EE. (2002). A framework for understanding and predicting insider attacks. *Computers & Security, 21*, 526–531.
2. Gelles, M (2005). Exploring the mind of the spy. In Online Employees' Guide to Security Responsibilities: Treason 101. Retrieved from Texas A&M University Research Foundation website: <http://www.dss.mil/search-dir/training/csg/security/Treason/Mind.htm>
3. 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.
4. Carroll, TE, FL Greitzer, and A Roberts. (2014). "Security informatics research challenges for mitigating cyber friendly fire." *Security Informatics, 3:13* (25 September 2014) <https://security-informatics.springeropen.com/articles/10.1186/s13388-014-0013-5>
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. National Insider Threat Task Force (NITTF). (2017). *Insider Threat Guide: A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards*. Available online: <https://www.dni.gov/files/NCSC/documents/nittf/NITTF-Insider-Threat-Guide-2017.pdf>
7. Greitzer, FL, JD Lee, J Purl, & AK Zaidi. (2019). Design and implementation of a comprehensive insider threat ontology. *CSER Conference*, Washington, DC, April 2019.
8. Ponemon Institute. (2022). *2022 Cost of Insider Threats Global Report*. Sunnyvale, CA: Proofpoint. Available online: <https://www.proofpoint.com/uk/resources/threat-reports/cost-of-insider-threats>
9. Verizon (2020). *Data Breach Investigation Report*. <https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf>

See also:

- **PsyberAnalytix Blog:** <https://psyberanalytix.com/franks-blog>
- **INSA Whitepaper: Categories of Insider Threats.** https://www.insaonline.org/wp-content/uploads/2019/10/INSA_WP_Categories_of_Insider_Threats-1.pdf
- **INSA Whitepaper: Human Resources and Insider Threat Mitigation: A Powerful Pairing.** https://www.insaonline.org/wp-content/uploads/2020/09/INSA_InT_Sept252020.pdf
- **Psychology Today post:** "Why hostile work climates provoke insider risk." Scott Dust & Elsie Van Os (Jan 4, 2021). <https://www-psychologytoday-com.cdn.ampproject.org/c/s/www.psychologytoday.com/us/blog/what-we-really-want-in-leader/202101/why-hostile-work-climates-provoke-insider-risk?amp>
- **RAND Australia Research Report: Insider Threat and White-Collar Crime in Non-Government Organizations and Industries (2022).** https://www.rand.org/pubs/research_reports/RRA1507-1.html

Thank You for Your Attention!

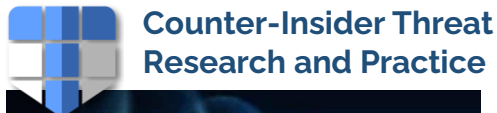
Frank L. Greitzer, PhD

PsyberAnalytix

Richland, WA, USA

<http://www/PsyberAnalytix.com>

Frank@PsyberAnalytix.com



Counter-Insider Threat
Research and Practice



***The Adventure Continues...
Stay tuned!***



Unintentional Insider Threats (UIT)

Human Factors Perspective

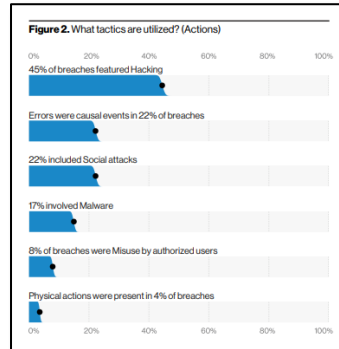
Phishing Study

Organizational Factors



Human Error Contribution to Security Breaches...

2020 Verizon *Data Breach Investigation Report*

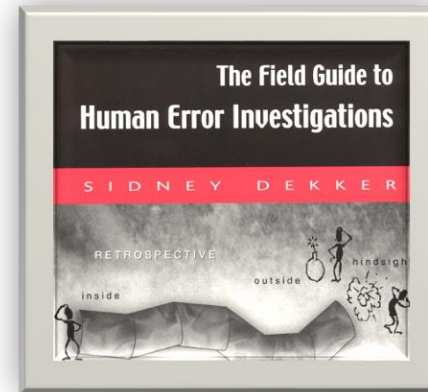


- 22% of breaches were social attacks (Phishing)
- **22% reported as direct causes of errors**

Revealed through decades of research in mid 20th century...

“Human error is a symptom of trouble inside a deeper system.”

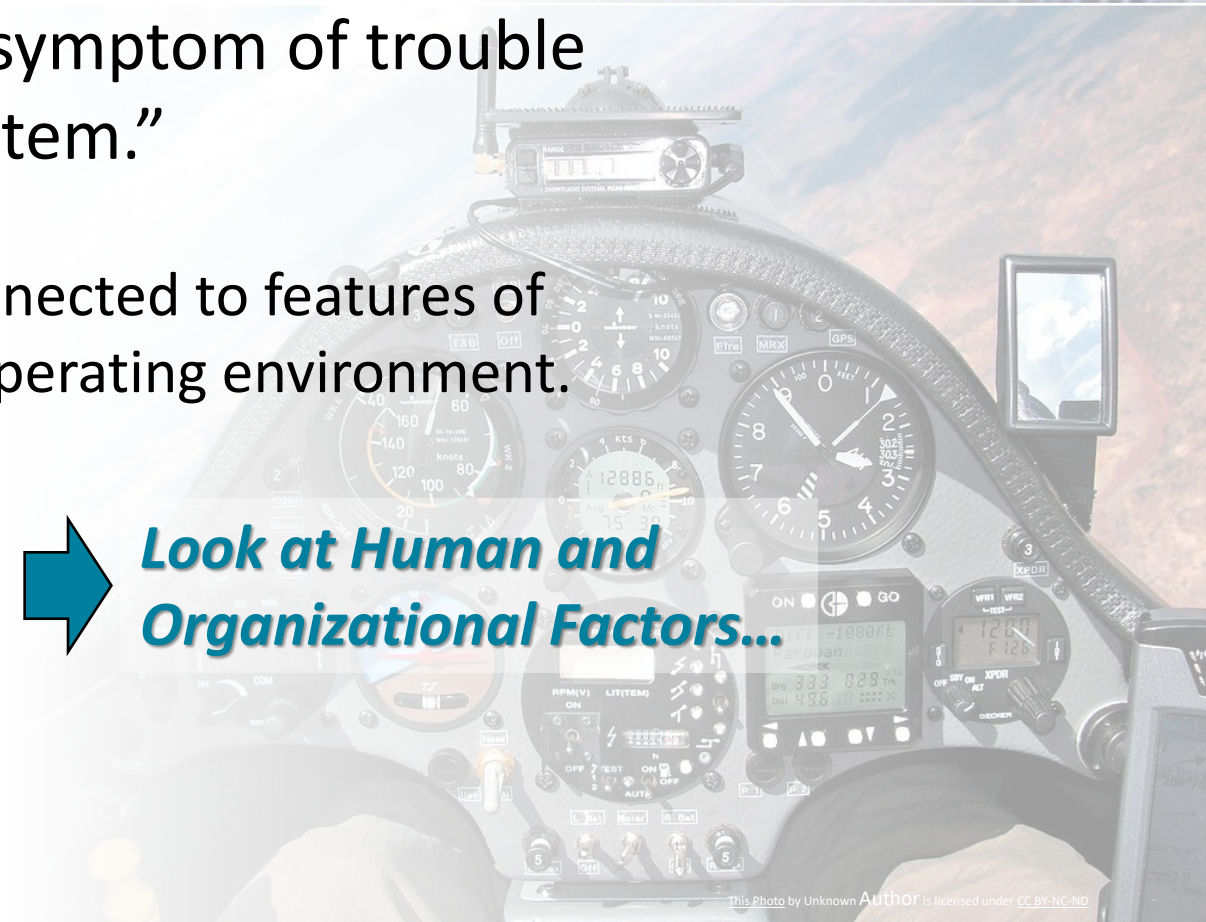
- Not random
- Systematically connected to features of tools, tasks, and operating environment.



(Dekker, 2002) 16



Look at Human and Organizational Factors...

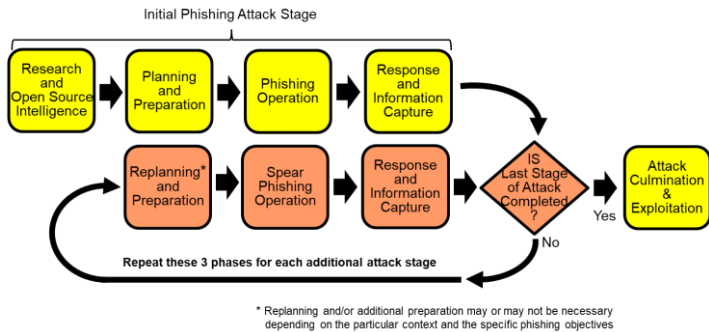


This Photo by Unknown Author is licensed under CC BY-NC-ND

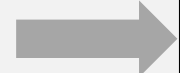
UIT and Human Factors

CERT Categorization of UIT contributing factors
 Greitzer et al. (2014) **17**  **Informed SOFIT**

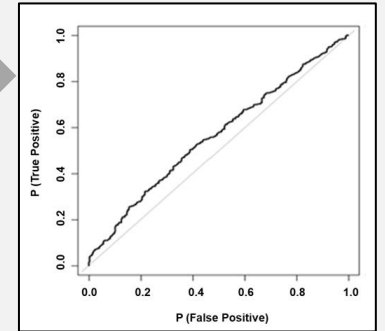
CERT Anatomy of a phishing attack
 (Greitzer et al., 2014) **18**



Major findings:

- 24 Technical indicators were of no value in predicting “clickers” 
- Sex/age variables alone were not useful predictors
- Phished before → more likely to succumb subsequently
- “Clickers” scored higher on impulsivity than non-clickers
- Participants with more appropriate online “security hygiene habits” were less susceptible
- Personality traits of Conscientiousness, Agreeableness, Neuroticism/Anxiety were not significant predictors of phishing susceptibility

ROC for Technical Indicators



20

GEORGE MASON UNIVERSITY Phishing study at GMU

-- Li et al. (2020) **19**

-- Greitzer et al. (2021) **20**

SOFIT Organizational Factors

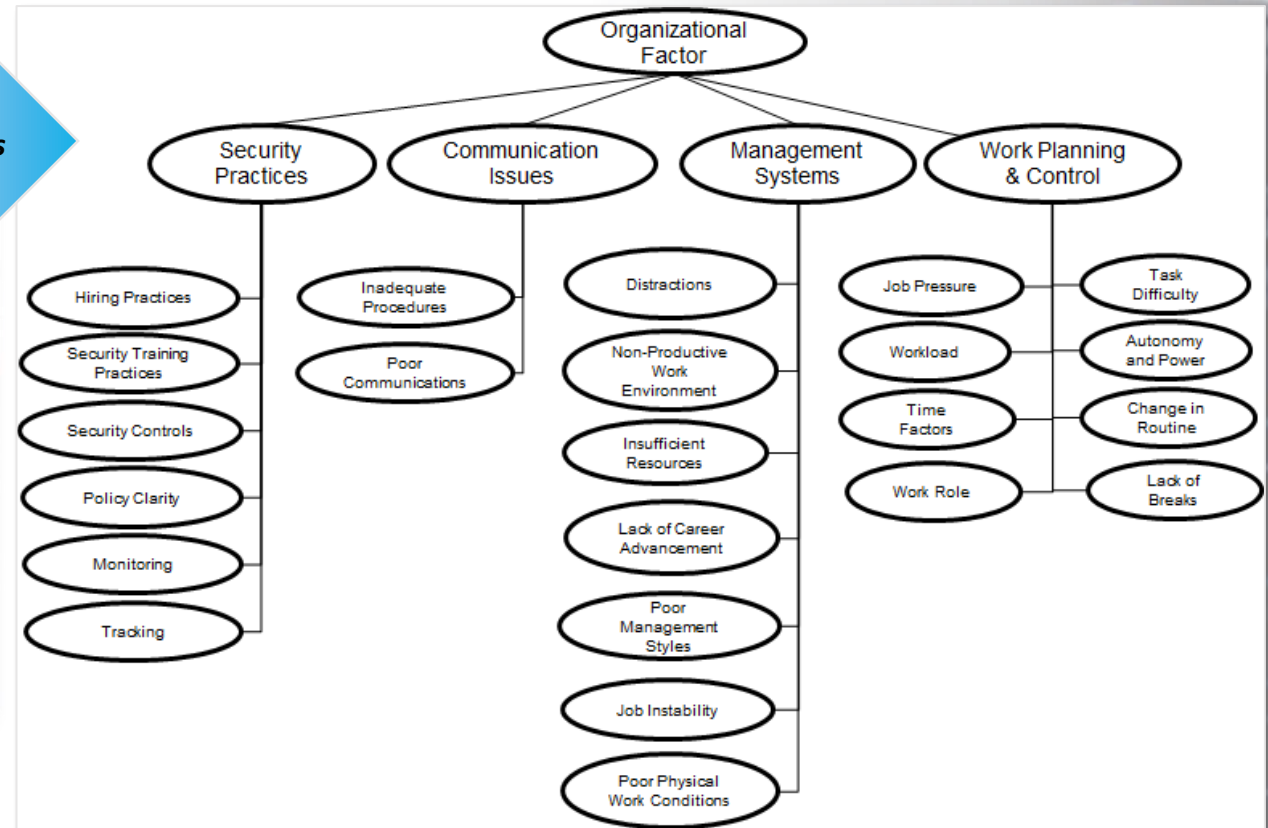
In addition to evaluating individual behavioral antecedents of insider threats...

More attention needs to be paid to assessing **potential stressors in the work environment** that affect worker motivations, behaviors and attitudes.

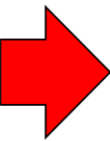
Professional Stressors



SOFIT Organizational Factors



Frustration
Stress
Disgruntlement



↓ Productivity
↓ Morale
↓ Trust

Insider Threats

UIT and Organizational Factors



March 28, 2020 | Insider Threat

Insider Threat Origins: Organizations Should Look Inward

PsyberAnalytix Blog:

<https://psyberanalytix.com/franks-blog>



September 1, 2020 | Insider Threat

Organizational Resiliency and Insider Threat

2020 DoD Counter Insider Threat Social and Behavioral Sciences [SBS Research Summit](#), hosted by the PERSEREC [Threat Lab](#).

Psychology Today

Find a Therapist (City or Zip) Verified by Psychology Today

Scott Dust, Ph.D.
What We Really Want in a Leader

Why Hostile Work Climates Provoke Insider Risk

When employees go rogue, hostile work climates might be part of the cause.

Posted Jan 04, 2021

f t e

One year ago, Mohammed Alshamrani, a 21-year-old Saudi aviation student studying at the Naval Air Station in Pensacola, FL, shot and killed three U.S. Navy Sailors. Last week, the [260-page investigation](#) was released, revealing an important yet overlooked impetus of this unfortunate event.

As dictated by Chief of Naval Operations, Adm. Michael Gilday, Alshamrani was primarily motivated by anti-American sentiment, but "the organizational environment inherent in the aviation pipeline, likely increased his probability of committing an insider attack."

"Why hostile work climates provoke insider risk." *Psychology Today*, online [post](#) by Scott Dust & Elsie Van Os (Jan 4, 2021).