Behavioral Indicators of Insider Threat: Looking Forward

Dr. Robert Gallagher

Guardian Defense Group

NITSIG Board Member

Insider Threat Indicator Lists

- Everybody loves a list
  - If we had a single and comprehensive list of THE behavioral indicators of insider threat, all we would need to do is screen for or monitor those indicators and we could eliminate all insider threats
- Everybody has a list
  - Cursory search turned up more than 20 distinct lists of behavioral indicators
  - Lists vary from a handful to hundreds of items

Three Primary Approaches to List Development

- Reverse Engineering Cases
  - Study and identify precursors to action in known cases
- Rational Approach – SME
  - Rely on logic and experience
- Science
  - Those items that discriminate between good and bad actors

The Problem With Lists

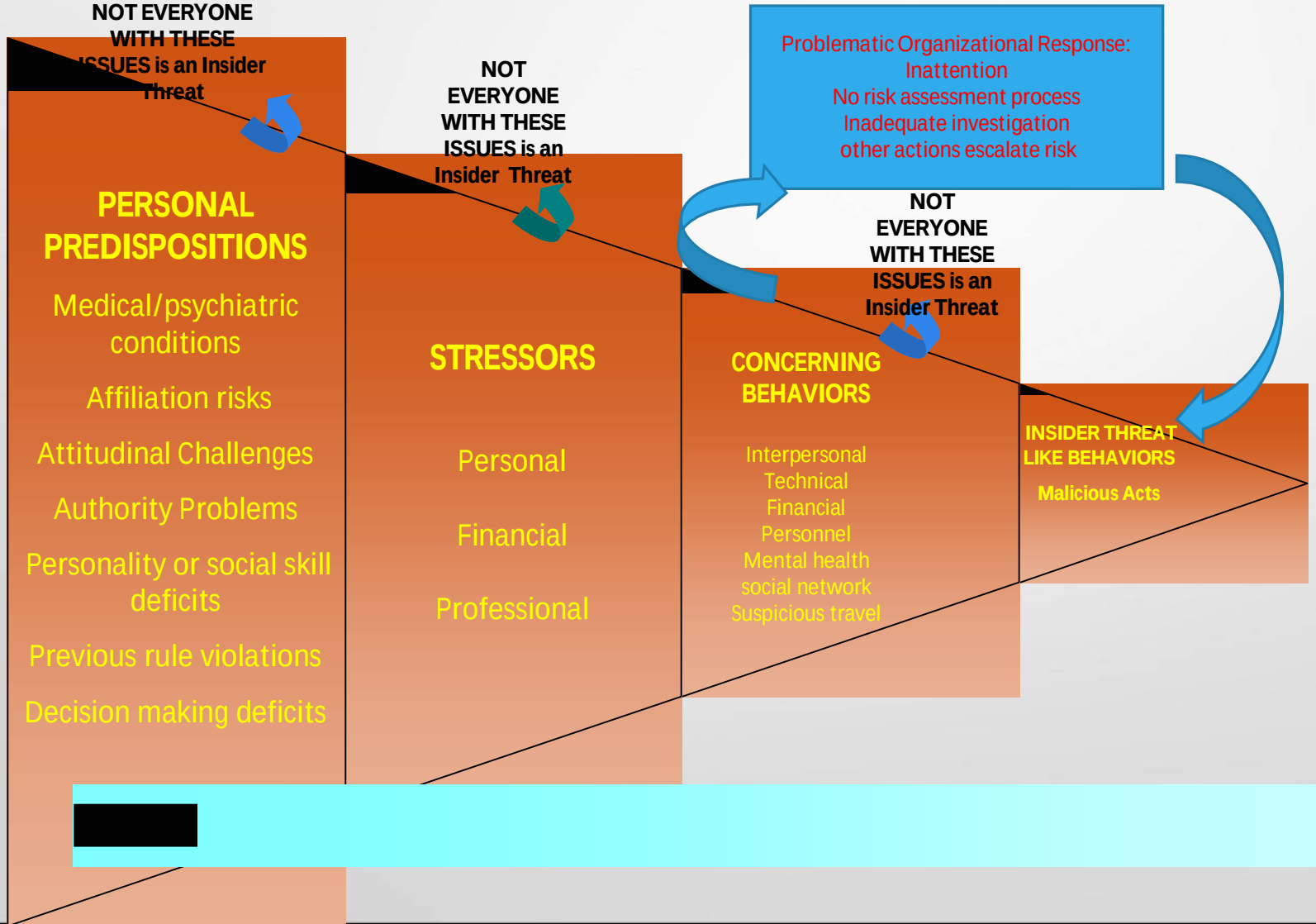
- Humans are Messy:
  - An indicator in one setting may not be an indicator in another
  - An indicator for one person may not be an indicator for another
  - An indicator for me one day may not be an indicator on another day
- False Positives:
  - The base rate of insider threat is very small
  - For almost any indicator there will be more non-malicious actors doing it than malicious actors
- General Flaws:
  - Reverse engineering of past events leads to a backwards orientation
  - Lists tend to treat all indicators as equally indicative
  - People tend to personalize and minimize selected items
  - Lists tend to reduce critical thinking

Alternate Approaches

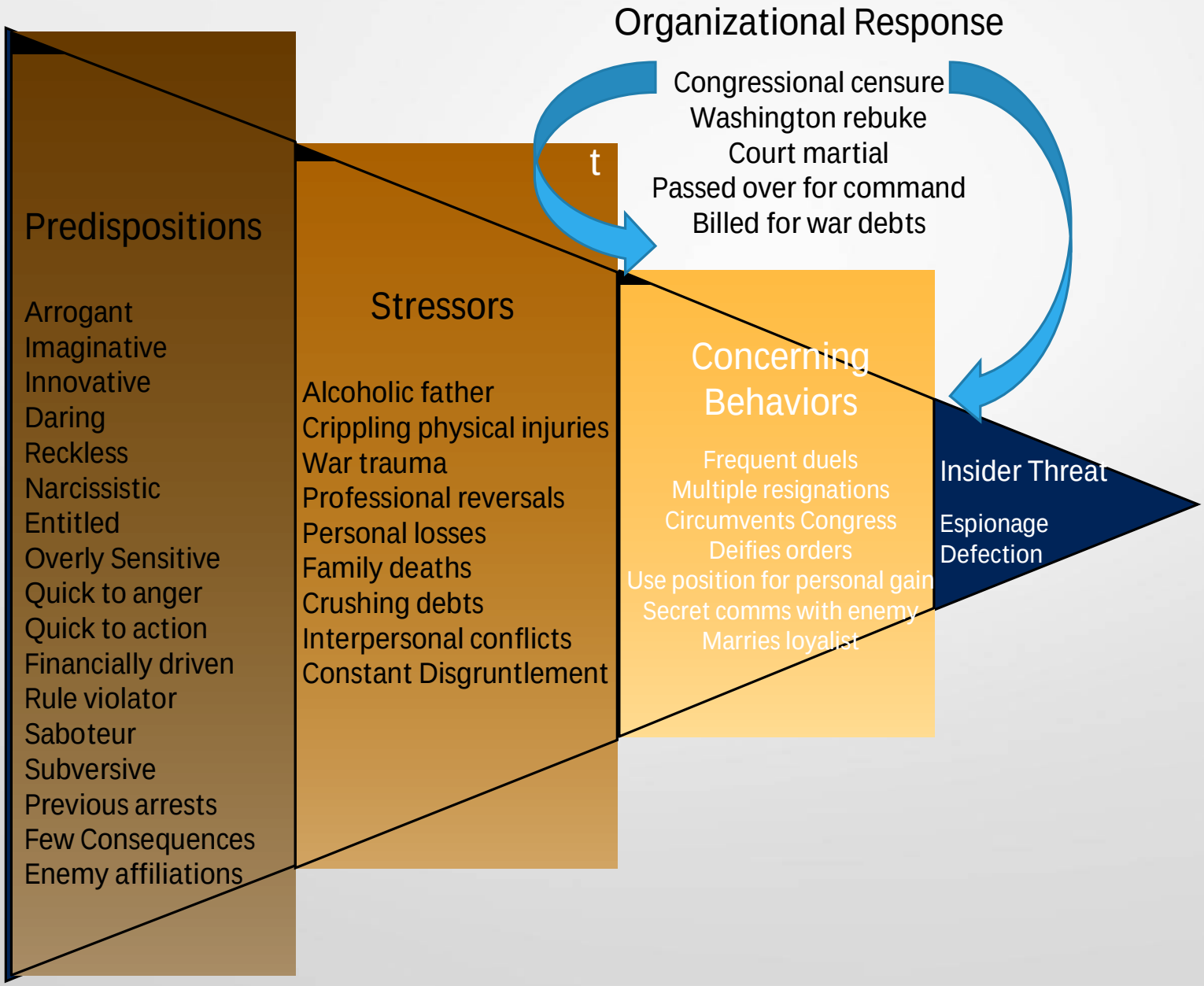
- Anomaly detection
  - Identify and assess any behavior that violates statistical norms
- Cultural and contextual aberrance
  - Identify and assess any behaviors that violate the behavioral norms of the organization
- Critical Pathway Modelling
  - Logical progression of risk from Precursors to full Insider Threat

The "Critical Path" to Insider Threat Risk: A Behavioral Model

Sources: Shaw, E. and Sellers, L. (2015); Carnegie Mellon Univ. (2006-present)



Case Example: Benedict Arnold



Conclusions

- There is no single definitive list of behavioral indicators of insider threat (and perhaps there never should be)
- Insider threat is a dynamic human problem and requires a dynamic human solution
- Overreliance on lists of behavioral indicators may cause us to focus on the wrong behaviors, suspend critical thinking, or reach inaccurate conclusions
- All concerning behaviors should be viewed within the individual, organizational and cultural context

Questions

Dr. Robert Gallagher
rgallagher@gdgllc.us
301-318-0245