Insider Risk Behavioral Analytic Schema[1]

Historical Factors	Personal Predispositions	Pressures	Behaviors of Interest
Pre/post-employment events or circumstances, not proximate to the insider risk referral issue. **Static or dynamic factors** which may increase risk. These might include: medical, legal, financial, psychosocial issues, academic/ occupational history, vulnerable family members in employee's country of origin.	Tendencies to think or behave in a certain way, or to suffer from a given condition (identified or inferred from patterns of behavior). **Dynamic factors** which may increase risk. These might include: negative personality or behavioral tendencies, medical, psychiatric or substance use symptoms/ diagnoses, social network risks, or ideological bent.	Real or perceived stressors of internal and/or external origin, proximate to the insider risk referral issue. Pressures can be personal or professional; and may include organizational contributors like workplace mistreatment. Also encompasses pressure associated with administrative inquiries or other negative consequences of someone's disruptive or rule-breaking behavior.	Behaviors which can help gauge level of risk. Proximate to insider risk referral issue or identified during an inquiry. *Concerning:* e.g., interpersonal, technical, security-related, financial, social networks, foreign contacts, travel *Mitigating:* e.g., proactive self-reporting, remedial training, utilization of available support systems, efforts to remedy any harm or damage inflicted
Organizational Response	**Organizational Vulnerabilities**	**Attack-Related Ideation, Research, Planning or Preparation[2]**	**Execution**
Refers to how an organization does or does not respond to concerning behaviors or suspicious circumstance denoting increased risk. Encompasses a range of constructive or detrimental responses, e.g., inattention; inadequate investigation; protecting or enabling a problem employee or leader; retaliation or other abuses of power; disproportionate or denigrating responses that could escalate risk.	Gaps in policies, procedures, training, resources, or security mechanism which can be exploited by an insider to degrade, destroy, or expose organizational assets or operations.	Possibly detectable warning behaviors that might portend violent or destructive insider acts.	Specific behavioral measures taken to effect a destructive insider act or type of activity. Includes counter-measures to delay or avoid detection.

[1] This framework was adapted from the *Critical Path to Insider Risk* (Shaw & Sellers, 2015)

[2] Dimensions of "Pathway to Violence" warning behavior (Calhoun & Weston, 2003; Fein & Vossekuil, 1999, 1998; Meloy et al., 2012)

Victoria Balenger, PhD, CTM ~ www.behavioralriskmgmt.com