White Paper: Behavioral Signs of Insider Threats

Kirk Lurie

Traditional approaches for identifying and mitigating insider threats often identify a breach after the fact. Effective security requires early recognition of warning signs often manifested in behavioral patterns. Individuals who commit insider threats consistently display behaviors such as criminal history, financial instability, foreign connections, and problematic conduct at work that manifests as policy violations, unexplained performance changes, secrecy, or disregard for rules.

This white paper advocates for the integration of behavioral science, personality assessment frameworks (Big Five, Dark Triad), and continuous monitoring. By combining behavioral indicators with identity and access data, organizations can detect risks before escalation, especially as hybrid work, global hiring, and AI-driven impersonation broaden the threat landscape.

Indicators of Insider Threat Risk

Insider risk encompasses malicious, negligent, and compromised insider behavior, exacerbated by hybrid/remote work, global hiring, and AI-driven impersonation. Abuse often occurs in critical sectors with direct access to sensitive systems.

Patterns of concerning behaviors are often manifested before incidents, such as criminal history, financial instability, foreign associations, or problematic work conduct (see the figure). Inadequate organizational policies and/or enforcement often allow these behavioral patterns to go unnoticed. Programs combining behavioral indicators with identity and access context help detect risk earlier than behavior-only approaches.

Behavioral Indicators of Insider Threat

Criminal History

Criminal history, especially individuals with backgrounds involving fraud, embezzlement, drug-related offenses, organized crime, or computer-related crimes (hacking, identity theft), is a reliable predictor (U.S. Department of Homeland Security [DHS], 2024). Further, a documented criminal history raises the risk of being susceptible to coercion or blackmail, especially if offenses are undisclosed. Malicious actors often leverage fear of exposure or legal consequences for serious offenses, such as fraud, embezzlement, sex crimes, or computer-

related crimes. Thorough background checks and continuous monitoring are critical for personnel security and insider threat mitigation.

Financial Problems

Foreign intelligence officers commonly exploit financial distress to recruit individuals for espionage or sabotage. Officers initiate contact under the guise of support, gather details about financial challenges, and then offer compensation in exchange for sensitive information. Manipulation is increasingly sophisticated, leveraging tailored offers and social engineering. Organizations should conduct regular financial risk assessments and provide support to mitigate exploitation risks.

Foreign Connections

Foreign connections, while not inherently suspicious, warrant monitoring when combined with other warning signs. Relationships with foreign nationals, ownership of foreign property, or overseas financial ties increase the risk of blackmail or bribery. Intelligence officers build rapport and trust over time, enabling exploitation of undisclosed affiliations or property ownership. Advanced social engineering, digital surveillance, and psychological strategies make coercion harder to detect. Organizations must educate employees, require disclosure of foreign contacts and holdings, and implement support mechanisms to address vulnerabilities.

Problematic Work Behavior

Habitual policy violations, irregular work hours, unexplained or unapproved absences, unauthorized computer conduct, and harassment signal unwillingness to comply with rules and may reflect deeper issues such as disgruntlement or isolation. These behaviors, especially when combined with chronic tardiness, insubordination, aggression, policy violations, or intentional slowdowns, increase risk of severe violations, including unauthorized disclosure or deliberate attempts to compromise security. Employees engaging in these behaviors often escalate over time, especially when grievances go unresolved.

Social Indicators

Personnel challenges and ongoing interpersonal conflicts provide clues about core personality traits and workplace conduct. They also are reliable indicators of future violations. Frequent arguments, repeated disputes, ineffective communication, withdrawal, and refusal to cooperate are warning signals. Patterns of workplace friction, online antagonism, and clashes with colleagues are especially telling when they coincide with policy breaches or improper data use. Organizational monitoring is needed to detect online harassment, doxxing, public criticism, and false information campaigns.

Personnel issues, such as unauthorized disclosures, bringing prohibited devices into secure areas, or ignoring security protocols, signal a willingness to escalate concerning behaviors. Regular review and intervention are essential, and organizations increasingly must emphasize proactive risk assessment, education, and robust reporting mechanisms.

Guidance from the U.S. Cybersecurity and Infrastructure Security Agency (2020) and research from the Center for Development of Security Excellence (n.d.) detail the significance of monitoring behavioral risk factors, including repeated violations of security protocols, conflicts with colleagues, and other patterns outlined above. These agencies emphasize proactive risk assessment and robust reporting mechanisms to address threats posed by individuals with a history of security violations.

Detection and Intervention

Organizations often become aware of problematic behaviors but lack timely or effective intervention due to delayed recognition, inadequate follow-up, or insufficient resources. Advanced technologies, user activity monitoring, behavioral analytics, and real-time alert systems enable earlier detection, but significant risk factors arise from gaps in personnel screening and unresolved workplace issues. Overlooked red flags in hiring, failure to assess behavioral risk, and neglecting psychological fit allow potential threats to remain in sensitive roles. Greitzer and Frincke (2010) offer insights on combining traditional cybersecurity audit data with psychosocial data.

Best practices emphasize robust behavioral screening during recruitment, ongoing assessments, and proactive management of workplace disputes. Multidisciplinary insider threat programs combining Human Resources, security, and mental health professionals are increasingly common. Regular manager training, clear reporting channels, and a culture of vigilance and support are critical for successful intervention.

Personality Indicators and Psychopathology

The Big Five

The Big Five personality framework assesses openness, conscientiousness, extraversion, agreeableness, and neuroticism, providing nuanced understanding of behavior. Its predictive power for insider risk is enhanced when combined with contextual variables such as stressors and job responsibilities. For instance, high neuroticism plus elevated work stress may increase risk, as can low agreeableness or conscientiousness with high system access.

Validated models like the Big Five and Dark Triad (narcissism, Machiavellianism, psychopathy) comprise an important part of risk assessment frameworks. Psychometric data help identify elevated risk profiles and monitor changes over time. However, effectiveness is limited by contextual interpretation and the need for ongoing validation to avoid false positives.

Psychopathology and psychological and behavioral disorders play critical roles in insider risk. Mood disorders, anxiety, personality disorders, and trauma can influence judgment and impulse control, increasing vulnerability. Untreated depression, anxiety, or personality disorder may lead to violations of security protocols. Recognizing the intersection of psychopathology and insider risk underscores the need for holistic assessments and early support.

The Critical Pathway to Insider Risk

The Critical Pathway to Insider Risk (CPIR) framework Shaw Model (Lenzenweger & Shaw, 2022) explains how personal predispositions interact with stressors and organizational environment, leading to concerning behaviors and potential insider incidents. Stages include:

- Personal Predispositions: Enduring traits or conditions increasing vulnerability (e.g., narcissism, poor impulse control, risky networks).
- Triggering Stressors: Acute personal, organizational, or community stressors (financial hardship, leadership changes, etc.).
- Emotional Fallout & Cognitive Bias: Grievance, entitlement, rationalization, or ethical distancing.
- Concerning or Counterproductive Behaviors: Policy violations, data hoarding, unauthorized tool use, lateral movement.
- Maladaptive Organizational Response: Ineffective intervention, weak oversight, failure to enforce safeguards, poor offboarding.
- Preparation & Crime Scripts: Staging activities, credential gathering, testing exfiltration, contacting external parties
- Insider Act: Theft, sabotage, espionage, fraud, and major misuse.
- Aftermath & Mitigation: Detection, response, and lessons learned; risk of recurrence if causes unaddressed.

Mapping risk indicators to CPIR stages enables early and proportional intervention.

Implications and Mitigation Strategies

Proactive, multi-layered mitigation strategies are essential. Supervisor and peer reporting must be supported by targeted training that emphasizes nuanced behavioral indicators and intervention pathways. Training should address organizational stressors and foster supportive environments. CPIR-informed interventions provide structured frameworks for identifying and mitigating insider threats, integrating technical monitoring, personnel records, and peer observations. Tailored support for at-risk employees, such as counseling and workload adjustments, address root causes.

Integrated, context-aware defenses, robust reporting channels, advanced training, and CPIR-guided risk management, substantially increase organizational resilience. Combining behavioral, identity, and access indicators with continuous monitoring and multidisciplinary engagement is critical for early detection and effective intervention.

Conclusion

Insider threats are complex and evolving constantly, driven by a mix of personal, financial, social, and organizational factors. Effective mitigation requires early recognition of behavioral signs, integration of personality and contextual indicators, advanced analytics, and a culture of

vigilance and support. By adopting proactive, multidisciplinary approaches, organizations can reduce the risk of insider incidents and protect their critical assets and personnel.

Contact Us

To learn more information about Electrosoft and our capabilities, contact us at info@electrosoft-inc.com.

About Electrosoft

Specializing in cybersecurity, Electrosoft supports federal civilian and military organizations in advancing cyber resilience, achieving digital transformation and adopting agile approaches that improve operational efficiency and security. With a focus on innovation and excellence, the award-winning company is recognized for its expertise, top workplace and leadership excellence. Electrosoft is headquartered in Reston, Virginia. www.electrosoft-inc.com

References

Center for Development of Security Excellence (CDSE). (n.d.). *Insider threat: Behavioral indicators.* https://www.cdse.edu.

Cybersecurity and Infrastructure Security Agency (CISA). (2020). *Insider threat mitigation.* https://www.cisa.gov/topics/physical-security/insider-threat-mitigation.

Greitzer, F. L., & Frincke, D. A. (2010). Combining traditional cyber security audit data with psychosocial data: Towards predictive modeling for insider threat mitigation. https://www.researchgate.net/profile/Frank-Greitzer/publication/227064429_Combining_Traditional_Cyber_Security_Audit_Data_with_Psychosocial_Data_Towards_Predictive_Modeling_for_Insider_Threat_Mitigation/links/551db73d0cf213ef063e9495/Combining-Traditional-Cyber-Security-Audit-Data-with-Psychosocial-Data-Towards-Predictive-Modeling-for-Insider-Threat-Mitigation.pdf

Lenzenweger, M. F., & Shaw, E. D. (2022). The critical pathway to insider risk model: Brief overview and future directions. *Counter-Insider Threat Research and Practice*, 1, 1-11. https://www.insiderriskgroup.com/the-cpir-certification-course/cpir-index-cpir-i

U.S. Department of Homeland Security (DHS) & National Insider Threat Task Force (NITTF). (2024). *Insider threat guide*. https://www.dni.gov/files/NCSC/documents/nittf/20240926_NITTF-Insider-Threat-Guide.pdf.

About the Author

Kirk Lurie is a Task Order Program Manager with Electrosoft Services, LLC. He possesses over 21 years of experience supporting the intelligence community, the National Institute of Standards and Technology, and reviewing risk and risk mitigation activities.