

ERIC D. SHAW

FROM RESEARCH TO PRACTICE AND BACK AGAIN:

IMPLICATIONS OF THE CRITICAL PATHWAY TO INSIDER RISK FOR CURRENT PERSONNEL SECURITY PRACTICES

Eric D. Shaw provides an overview of recent development of the Critical Pathway to Insider Risk™, highlighting the critical role that practitioners have had in its evolution.

INTRODUCTION

The Critical Pathway to Insider Risk™ (CPIR) describes the personal predispositions past insiders have brought to their organisations (personality and psychiatric issues, previous violations, social network risks), the triggers or stressors that have stimulated higher levels of insider risk, the concerning behaviours that signal observable behavioural indicators of increased insider risk in the workplace, the often maladaptive organisational responses that have failed to deter insider risks and the crime scripts that have accompanied insider actions.

It was described in detail by Shaws and Sellers and has been the focus of significant development and review by practitioners and researchers over the past 20 years. Since 2015, the CPIR™ has been frequently incorporated into discussions of insider actions and methods for detection of insider risk. Lenzenweger and Shaw (2022) summarised this development of the CPIR™, its strengths and weaknesses and reasons for its wide acceptance. This work summarises recent evolution of the framework and highlights direct implications for Personnel Security policies and practices.

FROM PRACTICE TO RESEARCH: THE EVOLUTION OF THE CPIR™

The CPIR™ framework is a living document. It has evolved as a direct result of feedback and engagement from insider risk professionals. Over 2,000 practitioners have participated in interactive CPIR™ training worldwide and have directly contributed to the framework's development based on their experience. Examples of these contributions, subsequent modifications, and questions include:

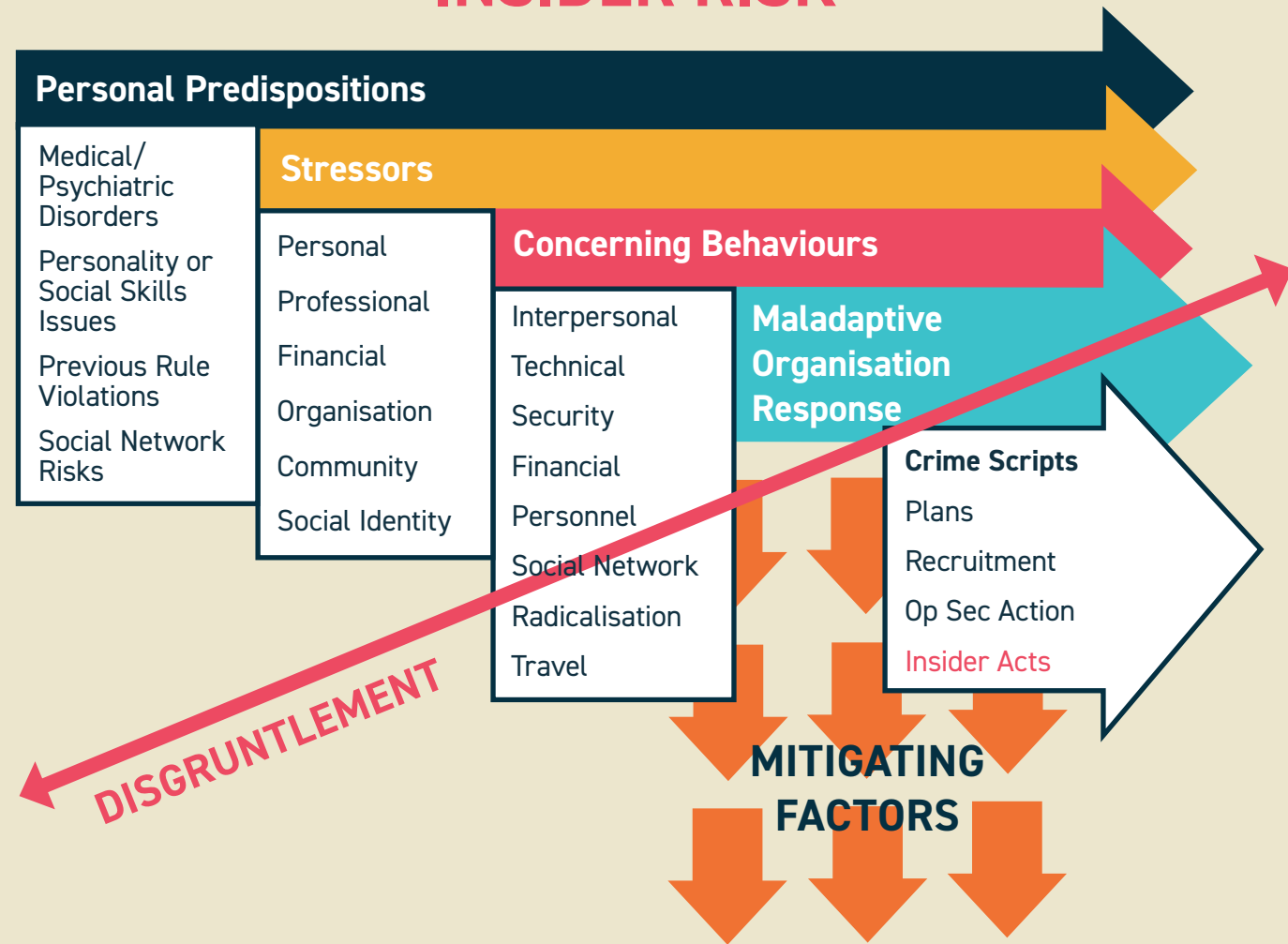
- The addition of Organisational Stressors to the Stressor Category as a trigger for heightened insider risk. Instead of concentrating on individual stressors alone, we have learned that leadership changes or controversy, mergers, redundancies, and other organisational changes often impact employee risk drivers;
- The addition of the Community Stressor category, which focuses on events impacting entire communities, also drives employee risk. No experience drove the important impact of these stressors home more than the COVID-19 Pandemic, which resulted in an increase in personal, family, financial, social, professional, and financial stressors to employees;

- Within the category of Community Stressors, the addition of Social Identity Stress (SIS). Based on the work of Veenstra, which focusses on normative conflicts between employees and their organisations increasing insider risk (such as employee disgruntlement regarding Pandemic public health interventions at work);
- The improved development of SIS and its implications for Social Network Risks, Concerning Behaviours, Problematic Organisational Responses, and the Mitigator of Enlightened Management. SIS can increase the likelihood of Social Network Risks as Concerning Behaviours, managers can over-react to non-threatening network risks causing risk escalation, and Enlightened Management must now understand and communicate with employees regarding potential SIS, in addition to their personal risk issues. Our team are currently working on ways to better identify and assess SIS;
- Despite the relative strength of controlled research demonstrating the relationship between personality disorder traits and insider risk, the addition of immaturity (divided into naivete, as in the case of Clayton Lonetree, and gullibility, as in the case of Sharon Scrange) into the Personal Predispositions category;
- While therapy often succeeds in reducing risk, we have also highlighted many cases in which therapy did not deter or prevent insider acts, and without information on its effectiveness, may not prove a risk mitigator. Security managers are urged not to assume that an employee in therapy is no longer a potential insider;
- Attention to the possibility that suicidal ideation, marking a period of intense hopelessness, despair and need for relief, may prove a gateway into increased insider risk among the estimated 90% of persons who experience suicidal ideation but do not go on to take their lives. We have begun to collect data on insiders who experienced suicidal ideation prior to their violations and noted the relative frequency of such ideation in targeted and domestic violence, as well as in espionage subjects. We are also increasingly focused on better ways to detect suicide risk in the complex communication patterns of the estimated 50% of persons who kill themselves without overt references to self-harm in their communications.

These are currently useful hypotheses regarding the causes, motives, and pathways of insider risk, but may be immediately relevant for practitioner consideration. We welcome feedback from reader's own observations.

“ Over 2,000 practitioners have participated in interactive CPIR™ training worldwide and have directly contributed to the framework's development based on their experience. ”

THE CRITICAL PATHWAY TO INSIDER RISK™



FROM RESEARCH TO PRACTICE: THE DEVELOPMENT OF INVESTIGATIVE TOOLS

The CPIR™ has contributed to the development of several tools designed to assist analysts to locate persons at-risk, assess and measure their risk level, characterise their personality and decision-making processes for managers and help analysts evaluate their organisation’s vulnerability to insiders. These tools have included:

- The Insider Evaluation and Audit which takes managers through policies and practices designed to surface insider risk in employees through each step of the CPIR™ to allow them to assess their organisation’s insider risk vulnerability. For example, the Audit uses Personal Predispositions to determine how well an organisation’s screening and selection methods could detect such risks. It systematically reviews policies and practices designed to detect employee stressors or risk triggers, detect, and intervene in Concerning

Behaviours without committing Problematic Organisational Responses, and detect emerging insider crime scripts. We frequently use the Risk Audit to demonstrate how an insider or group of insiders penetrated the different layers of organisational risk detection and management protections, revealing weaknesses.

- The Pathfinder™ application operationalises the CPIR™ as an analyst risk database, directing analyst information search using the Pathway through a series of questions derived from each CPIR™ category. It uses a series of algorithms to produce an overall CPIR™ score, as well as a rating in each category, while comparing a subject to group and “known bad” scores. The application takes about two hours to score a new case, is sensitive to risk changes over time and has good interrater reliability.
- Based on colleague complaints that the Pathfinder™ application was too time-consuming, Lenzenweger

“...malicious insider activities are not isolated but instead result from a series of events.”

and Shaw produced the CPIR-Index™, a simpler operationalisation of the CPIR™ designed to produce similar risk score estimates within 20 minutes. The Index correlates closely with the Pathfinder™ risk score. The CPIR-Index™ provides a handy field screening tool and a common language for concerned security personnel to communicate about a case.

- Cognition communications software is designed to locate individuals at-risk for insider acts from their communications by identifying signs of Disgruntlement. Disgruntlement, defined as levels of Anger, Blame and Victimization significantly different than peers, has been found to differentiate unhappy employees from those that have demonstrated insider risk indicators. Based on this earlier work, Cognition’s psycholinguistic algorithms also provide an assessment of other risk areas (substance abuse, violence risk, religious extremism, dehumanisation, suicide, etc.) as well as characterisation of an author’s psychological state, personality, and decision-making preferences.

While we never conceived of the CPIR™ as the definitive analytical approach to insider risk assessment, it has served as a useful heuristic for analysts and managers within insider risk programs. According to Mitre, the CPIR™ has “benefited the insider threat community by motivating security analysts and law enforcement to consider the whole person, recognise risk factors beyond concerning behaviors, and realize that malicious insider activities are not isolated but instead result from a series of events.” The CPIR’s™ utility may lie in its’ ability to tell a story about the evolution of insider risk that makes sense to practitioners, produces testable research hypotheses, and remains consistent with the available empirical research on insider actions.

Dr Eric D. Shaw is a clinical psychologist and former intelligence officer who has spent the last 25 years performing consultations, training, assisting in investigations and conducting research on insider issues while helping organisations manage insider risk. He is the founder and CEO of Insider Risk Group.

“The CPIR™ has contributed to the development of several tools designed to assist analysts to locate persons at-risk...”