CALL FOR JOURNAL PAPERS:
MANAGING INSIDER RISK & ORGANIZATIONAL RESILIENCE (MIROR)

Editorial team: James Bluman, Ph.D., P.E., Jessica Baweja, Ph.D., Jessica Dawson, Ph.D., Stephanie Jaros, Jonathan W. Roginski, Ph.D.

Manuscript Submission: https://www.editorialmanager.com/mirorjournal/default2.aspx

**Contact: jonathan.roginski@westpoint.edu or insiderthreat@westpoint.edu

Background: Insider threat is dangerous to organizations and their people, intellectually, physically, and emotionally. For many years, those serving the purpose of protection sought to counter the insider threat by focusing on identifying individual threats among the thousands, tens of thousands, or more employees that did not present a threat. We expended tremendous time and resource to develop tools, models, and algorithms to identify these malicious or unintentional threats (with varying levels of efficacy). Certainly, these efforts have been productive, useful, and protective. Unfortunately, with all the resource leveraged against the problem, we continue to be largely reactive to threat activity that manifests while seeking a more proactive approach.

Recent research into the idea of insider *risk* has promise to be such a proactive approach. Rather than using a binary classification of “threat” or “no threat,” consideration of risk makes use of the entire spectrum in between “0” and “1.” The insider risk discussion enables a broader, “ecosystem” approach to countering damaging insider activity impacting an organization or its people before that activity is allowed to mature into a threat or a danger. We may finally move beyond a confrontational and punitive threat-based mindset to one of holistic individual and enterprise wellness that makes dangerous threat activity incompatible with existence.

It is likely that even with the most insightful and effective risk management and threat identification that procedures damaging insider actions will still occur. In this event, the ability of the enterprise to care for its personnel and mission is of paramount importance. This *organizational resilience* must be deliberately cultivated, it will not happen by accident. Fortunately, the very actions organizations take to increase wellness and resilience within its individuals and across the enterprise have been shown to reduce risk and threat behaviors.

The *Managing Insider Risk and Organizational Resilience (MIROR)* journal is a peer-reviewed online and print publication. MIROR will share research, best operational practices, leadership perspectives, and reviews of relevant work that further both the proactive practices of insider risk management and promotion of holistic wellness and resilience in organizations.

The editors will review content across those areas that move discussion forward concerning insider risk and organizational resilience, including but not limited to the following:

- Recruitment and pre-employment screening. How do we recruit and hire the right "fit" for our organization, setting the stage for longer term and higher quality retention?
- Development and/or implementation of policies and practices. How does an agency build policies and practices to accomplish its mission while maximally protecting against risks presented to mission accomplishment from the inside?
- Training and education. How do we effectively train the workforce on policies and practices (prepare for the known) and educate toward continuous improvement (prep for the unknown)?
- Continuous evaluation. How do we foster trust across the enterprise by thoughtfully and respectfully verifying the alignment of values between individual and organization extant at hiring continues to result in mutually supportive behaviors?
- Risk modeling and reporting. How do we leverage the tremendous suite of quantitative and qualitative mathematical, statistical, and mental models that exist (or will exist) against the challenge of keeping people and organizations happy, healthy, and safe? How are the results of those models communicated to leaders to facilitate decision making and change?
- Data science applications. Data science is arguably the most “in-demand” contemporary analytical field—how may we benefit from the groundbreaking knowledge and techniques in the insider risk and threat management field?
- Creation and maintenance of positive organizational culture. Employees that are connected to and invested in their organization are protective and constructive toward themselves, their peers, and the company. How do we make, keep, and foster such an environment?
- Employee intervention. How do we identify people and practices that increase risk of negative insider activity and align appropriate resources to protect people and the enterprise?

Article types and submission. Submissions in the following categories are welcome:

Professional Commentary (800+ words)
Professional commentaries seek to bring forward insight from leaders in the field and highlight recent developments, concerns, and bridge gaps between industry, government, and academia. A Professional Commentary includes references as embedded discussions in the text and no endnotes.

Original Research (1 500 – 5 000 words)
Traditional research article with findings and results up to 5 000 words. Short articles (1 500 – 2 500 words) with preliminary findings, early results, or responses to current developments are considered as Research Notes. Endnotes must be hyperlinked with the text referenced. Discursive endnotes are strongly discouraged; cite only direct quotations and paraphrases. No need for a bibliography. The journal’s formatting style is the Chicago Manual of Style (CMS), 17th edition, endnotes.

Lessons Learned, Case Studies, Vignettes (500 – 1 500 words)
Experiences from practitioners and professionals close to the developments in the field. The article type is a feedback loop from the field back to the community. A Lessons Learned, Case Studies, Vignettes article has needed references as embedded discussions in the text and no endnotes.

Book Review (1000 words)

Traditional academic book review with no endnote references.