Special Issue Call for Abstracts

Evidence-Based Capability: Results from Sponsored Research into Human Performance in Cybersecurity

The creation and adoption of any new technology or tool has direct impacts and consideration for the cybersecurity workforce, which includes practitioners, educators, and researchers. Investment in cybersecurity research in the last decade has resulted in many opportunities to consider the impact of new cybersecurity technologies to the broader cybersecurity workforce, from testing to planning for technology transfer. Beyond marketing, operationalizing new technology requires an understanding of how to train or educate practitioners and educators to effectively use the technology to achieve the positive outcomes promised by that technology.

Despite a critical call a decade ago for research on the human performance of cybersecurity[1] and various legislative attempts to spur research efforts to understand behavioral factors that affect cybersecurity technology and practice, there is still little published research into the role of the human practitioner in cybersecurity. Recent technical advances such as automation, ML and AI further highlight the gap in understanding human performance and knowing what knowledge or procedures are needed to optimize the interaction between practitioners and automated processes intended to protect and defend the nation.

The *Cybersecurity Skills Journal* is seeking ideas and drafts for Articles, Notes and Dialogues that impact cybersecurity practice, improve learning, and advance the state of the cybersecurity workforce's capability maturity and which arise from recent sponsored research.

Abstracts may address any aspect of research into cybersecurity but must align with the Journal's mission: emphasis should be placed on enhancing the capabilities of the cybersecurity practitioner, educator, or researcher, not on technology.

CSJ seeks submissions in the following areas (non-exclusive list):

- Theoretical/conceptual research with implications for capabilities of the cybersecurity workforce
- Systematic investigations that analyze, evaluate, improve, and measure the human operator's techniques, tactics and procedures (TTPs) including, but not limited to, the use of technologies
- In-depth, systematic reviews of the research and literature in specific areas of evidence-based practice of cybersecurity by practitioners, educators, and researchers

[1] Boyce, M. W., Duma, K. M., Hettinger, L. J., Malone, T. B., Wilson, D. P., & Lockett-Reynolds, J. (2011, September). Human performance in cybersecurity: a research agenda. In Proceedings of the Human Factors and Ergonomics Society annual meeting (Vol. 55, No. 1, pp. 1115-1119). Sage CA: Los Angeles, CA: SAGE Publications.

- Case studies or other qualitative analyses demonstrating the application of innovative tactics, techniques and protocols which highlight critical or often overlooked skill requirements for cybersecurity professionals
- Research on cybersecurity professional practice and performance requirements
- Unique challenges encountered by cybersecurity professionals in applying their knowledge, skill, and abilities
- Instructional designs or materials, assessments, or practice/challenge lab designs that may raise capability maturity in students or professionals
- Design and deployment of instructional systems that raise capability maturity

The *Cybersecurity Skills Journal* uses a two-step submission process designed to encourage submission of abstracts aligned with the Journal's mission. Prospective authors are encouraged to review the Overview Presentation for this Special Issue to understand the different paper types and submission requirements. Specifications for practice, instructional design, or research manuscripts are available in the Manuscript Content Guidelines.

Special Issue Timeline

November 12, 2021: Call for Abstracts released

December 1, 2021: Paper Development Workshops begin

April 1, 2022: Abstract submissions opens

July 31, 2022: Early abstract submission deadline (prioritized for publication)

October 31, 2022: Abstract submissions close

December 15, 2022: Accepted manuscript submissions due

Abstracts on technical solutions that lack a substantive contribution for improving or teaching skillful performance of cybersecurity job functions and roles do not align with the Journal's mission and will not be considered.

NATIONAL CYBERWATCH CENTER

Cybersecurity Skills Journal: Practice and Research is published by the National CyberWatch Center. Our authors benefit from exceptional support including but not limited to constructive advice received from 10-person peer review and mentoring panels. Through print and electronic access, articles published in the *Cybersecurity Skills Journal* are available to a global audience of over 400 institutions and 35,000 potential readers. Additional information about the *Cybersecurity Skills Journal* is available on the National CyberWatch web page at https://csj.nationalcyberwatch.org.