CYBERSECURITY SKILLS JOURNAL: PRACTICE AND RESEARCH

Call for Proposals: Facilitated Virtual Focus Groups

Encouraging dialogues about challenges, opportunities, and effective practices

The goal of the *Cybersecurity Skills Journal: Practice and Research* (*CSJ*) is to stimulate professional discussion and advance the interdisciplinary field of cybersecurity through the publication of scholarly works of value and interest to the profession. To encourage the community in critical discussions surrounding the cybersecurity workforce, *CSJ* invites practitioners, scholars, and educators to propose and lead virtual Focus Groups that will explore specific challenges and persistent problems related to issues in the cybersecurity workforce.

The next Focus Group event will be on Wednesday, January 11, 2023. Individual discussion sessions will run between 90 and 120 minutes, with different sessions starting at 10:30 AM (Eastern) and 3:00 PM (Eastern). Registration for the event will open in December 2022.

Proposals for individual Focus Group sessions must be submitted by December 1, 2022, to Track 1 in Easy Chair.

Proposers must identify the topic area for their Focus Group session, e.g., the specific problem and questions to be explored, and should also identify key stakeholders who will participate in that Focus Group. Focus Groups are not panel discussions or one-way webinars: registered attendees for the Focus Group will join in the real-time discussion on each question and share their expertise. *CSJ* will provide moderators for each session to facilitate the session and participation.

Focus Groups 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. Submissions related to cybersecurity technology or tools should emphasize the human factors involved in the technology design, development, use, or support.

Focus Group proposals might explore areas such as:

1) What should the role of industry be in funded research into cybersecurity skills?
   a) Students graduate with degrees but lack the skills local industry needs for open jobs; how might we change this dynamic? What degree or curriculum changes can we envision?
   b) Given workforce constraints, how might industry be more involved in funded research into cybersecurity skills?
   c) How might educational institutions more directly engage industry – how have you approached the challenges and what does success look like to you?
2) What is evidence-based research in cybersecurity?
3) What are the critical research gaps related to cybersecurity skills and how could the cybersecurity community address them? Who might fund this research?
4) What are potential innovative, long-range funded research programs into cybersecurity skills (acquisition, assessment, etc.) that could be game-changers for the maturity of the cybersecurity workforce?

5) What questions are YOU or YOUR ORGANIZATION wrestling with regarding funded research and cybersecurity skills in the workforce - recognizing that educators are part of the workforce?
6) Specific challenges or contributing factors to building (or retaining) a more diverse and/or larger pipeline of career entrants, and better prepared career entrants.
7) What research is needed to empirically identify shortfalls in cybersecurity workforce skills?
8) Is there empirical evidence that cybersecurity competitions actually improve or provide accurate assessment of specific technical skills or problem solving? How could this evidence be collected?
9) What are achievable measures of success for NICE Strategic Plan, or for Implementation Plans from the NICE Working Groups or Communities of Interest?
10) What life factors do students believe are impeding their abilities to devote enough time (i.e., the Carnegie Unit) to learning for their courses? What approaches might increase engagement for them?
11) What should be the scope of a cybersecurity course, given the amount of time students actually have available? How can faculty streamline the concept list to just the most essential content that will enable students to continue learning after the course?

All ideas submitted will be reviewed by the *CSJ* Editorial Board. Submissions must include at least three invited participants that are subject matter experts or stakeholders (e.g., practitioners, hiring managers, CISOs, learners, educators, government, academia, industry, K12, higher ed, etc.) impacted by the topic of the Focus group. Preference will be given to submissions that align with any of our open Calls for Proposals.

Each proposer may choose to pursue publishing the discussion from their Focus Group as a research manuscript in the form of a *CSJ* Dialogue. *CSJ* facilitates the creation of Dialogues by recording all sessions in the virtual platform; individual session proposers will receive both an audio recording and an automatic transcription of their group discussion. Proposers must review and edit the transcript, and provide an introduction and summary remarks before submitting the Dialogue for publication in a Special Issue from *CSJ*.

Timeline for the Focus Group

- October 15, 2022: Call for Proposals published
- December 1, 2022: Submission deadline for Focus Group session proposals
- December 15, 2022: Notification sent to all Focus Group proposers
- December 16, 2022: Registration for Focus Group Event opens
- January 11, 2023: Focus Group Event

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 *Cybersecurity Skills Journal* is available on the National CyberWatch web page at https://csj.nationalcyberwatch.org.