Author Guidelines

The Cybersecurity Skills Journal (CSJ) is a double-blind peer-reviewed journal published by the National CyberWatch Center Digital Press. The goal of 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. The CSJ seeks to integrate and expand the methods, processes, and evidence of effective practices which underlie skilled performance. CSJ focuses on valued, measured results; considers the larger system context of people’s performance; and provides valid and reliable measures of effectiveness.

Types of Manuscripts Invited. CSJ emphasizes original work from the following communities of research and practice: process improvement; organizational design and alignment; analysis, evaluation, and measurement; performance management; instructional systems; and management of organizational performance. CSJ will consider literature reviews, experimental studies, survey research, and case studies with a scholarly base. An article should be primarily directed towards one of the three audiences of the journal: practitioners, instructors, and researchers.

Practice articles in CSJ should offer evidence-based guidance to practitioners in the form of techniques, tactics, procedures or tools that demonstrate substantial effectiveness in preventing, mitigating, or resolving cybersecurity threats, vulnerabilities, or attacks. A CSJ practice article sufficiently documents the practice such that a reader can follow the procedural guidance to execute the actions necessary for effective application. CSJ prefers practice articles that document a digital asset which can be downloaded by readers to support implementation of the practice.

Instructional design articles in CSJ should provide guidance to instructors as though you were “training the trainer” with the article. In other words, might there be observations or conclusions an instructor should be making about the learner as they proceed with each step to ensure their proficiency in understanding both the concepts involved and the procedure being applied. Some considerations might be:

- What conceptual understanding is a prerequisite for each step.
- What misunderstandings (confusion) or misconceptions (confidently held, but mistaken assumptions) may prevent a learner from fully comprehending or performing each step?
- How would you recommend assessing correct or incorrect understanding of prerequisite or instructed conceptual understanding?
- If incorrect understanding has occurred with students in the past, or you can imagine lack of prerequisite knowledge, confusion or mistakes that could occur, what additional instructional devices might you recommend should be applied to remediate learning?
- Are there conditions at any step that might suggest an alternative process or a decision on an approach that might be more effective or less effective at that stage?

Updated: July, 2019
If the procedure needs to be altered on some conditions, under what situations might these conditions arise?

What errors might be expected during the application of the principles and techniques in hands-on practice? How might these errors be detected or manifested? What remediation might be appropriate for each error?

How might the understanding and skilled application of the concepts and techniques you are developing through your instruction be further tested in simulations of real-world events, such as in designing an interactive competition?

What research is needed to adequately answer any of the above questions or to further improve your instructional design?

How might the processes and procedures taught through your instructional design be used to improve cybersecurity practices in the workplace?

Are there executable files (e.g., LMS packages, test questions, procedural guides) that have been or could be developed to assist with implementing your instructional design?

Research articles should provide evidence from the literature to clearly establish the severity and urgency of the problem being addressed by the practice that was empirically analyzed. The method of designing, implementing and/or evaluating the practice should be clearly specified, with discussion of the Population, Intervention, Comparative measurement, and Outcomes (PICO) achieved in an empirical analysis of effectiveness. Results should be reported with sufficient detail that a reader of the article can determine practice standardized effects, coefficient of determination, or variance explained. Discussion should conclude the article by summarizing the contribution made to cybersecurity practice, any limitations of the study design, and the implications for future research.

Editorial Policy. Authors are responsible for the accuracy of all submitted materials including references, quotations, and spellings. All materials other than specific quotations must be the author’s own work. If there is substantial use of copyrighted materials, the author is responsible for securing permission to use the material. The author agrees that any manuscript accepted for publication in CSJ will provide a non-exclusive right for CSJ to publish the article, including any derivative products, and permits CSJ to sublicense such rights. Authors are required to sign a Copyright Assignment Agreement. All manuscripts submitted for publication must conform to the Publication Manual of the American Psychological Association (APA), sixth edition. In addition, CSJ uses Merriam-Webster's Collegiate Dictionary, eleventh edition, as a standard reference for spelling, hyphenations, and definitions. CSJ will apply its own style guidelines to ensure consistency.

Permissions. Reproduction of an unaltered figure, table, or block of text from any non-federal government publication requires permission from the copyright holder. All direct quotations should have a source and page citation. Acknowledgment of source material cannot substitute for written permission. It is the author’s responsibility to obtain such written permission from the owner of the rights to this material. Authors must also receive permission to use figures that have been adapted.

Length. Although there is no fixed length, average articles (including tables and figures) are approximately 5,000 to 12,000 words. If you wish to submit a longer manuscript, discuss it with the CSJ editor prior to submission.

Manuscript Format and Author Information. CSJ articles, while scholarly, should be written to enhance readability. We prefer that articles be written in first person. Whether written in first person or third person, your point of view should be consistent throughout the manuscript.

Your manuscript must be submitted with a separate file containing a cover sheet that includes a statement indicating that the manuscript is not currently being considered for publication by another journal and the following information: manuscript title, authors in order of preference with names listed as they should appear in the published article,
Structured Abstract. A second page, headed by the manuscript title, should provide a structured, extended abstract. The structured abstract should be less than 500 words. The purpose is to summarize the manuscript using the following section headers. You should answer the “what” and “why” questions below to indicate how your paper will make a substantial contribution to our understanding of skilled performance of cybersecurity practices.

1. **Problem Statement**: What is the primary problem that the study investigated? Why is this an urgent and/or severe problem?
2. **Research question(s)**: What questions related to the problem have not been answered by prior research? Why are practitioners or prior research lacking an understanding of the phenomenon being studied?
3. **Contribution**: What is the contribution made by this manuscript to a current conversation in the literature? Why are the method, findings, or conclusions surprising or contributing new and important insights?
4. **Theory propositions or hypotheses**: What is the paper’s argument? Why are the claims and propositions warranted by prior literature?
5. **Method**: What is the paper’s empirical rationale? Why is the method appropriate to develop or test the theoretical claims and propositions?
6. **Findings**: What are the primary findings from the study? Why might we expect a substantive impact on cybersecurity practice from the factors analyzed in this study?
7. **Implications for practice**: What advances in cybersecurity workforce capabilities are implied? Why is the study advancing cybersecurity workforce capabilities?
8. **Implications for research**: What advances in research are implied? Why will the study prompt new investigations of effective cybersecurity practices?

**Figures and Tables.** CSJ pages are 7” wide by 10” long. Figures and tables should be pre-sized to fit in a 5.5” x 8” space. Figures should be professionally rendered. The resolution of computer-generated images (figures) should be at least 300 dpi and scanned, created, or saved in TIFF or EPS format. Images copied from the World Wide Web are not acceptable. Each figure must be on a separate page at the end of the manuscript with its number and title at the top of the page. A placement indicator should appear in the text with a line above and below the figure title.

Tables should be clearly formatted using Microsoft Word’s table-making feature. They should appear in the body of the manuscript where they belong followed by the table number and title. Do not apply shading to the table unless doing so imparts information, in which case a legend must be supplied.

Please use the typeface Arial (light, regular, and bold) for all tables and figures. Do not use any type of background color (shading) behind the text of figures or tables. CSJ reserves the right to modify the size and shape of figures and artwork, provided their meaning is not substantially changed, and to reject any figures or artwork not meeting CSJ standards.

**Bibliography.** The bibliography, formatted in APA (sixth edition) style, should contain only those works cited in the text. The bibliography should be titled *References*.

**Submission and Review Process.** All manuscripts should be submitted electronically using the EasyChair review system. You may access the open Call for Papers here: [https://easychair.org/cfp/CSJ-2019](https://easychair.org/cfp/CSJ-2019). To maintain the strictest blind review practice, a manuscript must be submitted without any reference to an author. Author names must not appear on a title or cover page. Self-citation references to prior work by any author must be removed prior to
submission. Each manuscript is automatically scanned for author names and will be rejected immediately if references to author are found in the document.

The EasyChair system automatically assigns a manuscript to an associate editor for fit with editorial policies and the types of manuscripts invited for the journal issue. If a manuscript passes the associate editor review, a panel of ten (10) peer reviewers having expertise in the topic area will review the manuscript. The size of CSJ review panels enable reviewers to collaborate in providing detailed constructive reviews which aim to assist the authors in moving the manuscript towards publication, whether in CSJ or another journal. The review panel provides collegial support to authors during the revision process in the interest of creating the best possible manuscripts for readers. Only when a review panel has approved the manuscript for proof editing will it be forwarded to the Editorial Board, who remains blind to all editorial decisions prior to the final publication stage. Proofs are reviewed by the managing editor and up to three associate editors to ensure a high-quality proof is submitted for final publication after the corresponding author has approved any proof edits.

The goal of the CSJ Editorial Board is to provide the initial detailed and constructive review within six weeks of submission. Review decisions and peer reviewer comments and recommendations can be accessed by any registered author through the EasyChair review submission. Reviewer comments, decision status, and editorial proof reviews may be accessed up to the earliest of the publication date of the manuscript or four weeks after a decision has been sent to the corresponding author.

All questions in regard to editorial content should be directed to publications@nationalcyberwatch.org.

Copyright

If your paper is accepted, the author identified as the formal corresponding author for the paper will receive an email prompting them to login into the EasyChair manuscript review submission; where they will be able to complete the license agreement on behalf of all authors on the paper.

Note to Contributors on Deposit of Accepted Version

Authors are permitted to self-archive a version of the Contribution on the Contributor’s personal website, in the Contributor’s company/institutional repository or archive, and in certain not for profit subject-based repositories such as PubMed Central, subject to an embargo period of 12 months for scientific, technical and medical (STM) journals following publication of the final Contribution. If the article is accepted for publication, instructions on final submission will be sent to the corresponding author.