Editor's Comments ▬▬▬▬▬▬▬▬▬▬

JCAE Editorial Policies and Practices ▬▬▬▬▬▬▬

JCAE editorial policies and practices gain their foothold with modeling from MISQ and other premier journals. As details develop: changes, additions, or enhancements will be recorded and announced through editorial comments and/or web pages. The editor of this inaugural issue, Dr. Derek J. Sedlack, provided a guide indicating the journals current editorial policies and practices. A template to help guide design elements to remove additional burdens from already nervous pre-publication authors can be found at (https://www.scholarlyexchange.org/ojs/index.php/JCEA/about/submissions).

Editorial and Research Mission

In the broadest sense of policy, the JCAE mission is to serve as a forum for higher education students to develop their research foundations through a better understanding of core cybersecurity elements that underpin our National Infrastructure and a global technological integration. The journal aims to encourage student research to address cybersecurity challenges and, in the process, engage them in scholarly activities to instill the value of research as a critical component of the cybersecurity profession. The scope of this journal is multi-disciplinary with a broad focus on cybersecurity education, training and awareness. We encourage secondary research with an emphasis on identifying particularly vexing cybersecurity issues.

As editor-in-chief, I speak on behalf of our editorial board members who review, edit, and contribute to the advancement of cybersecurity awareness and education in the highest of callings: serving students. I am proud of the efforts of the team in identifying, reading, and commenting on the large number of submissions that led to our first publication. It is their work that highlights and details the efforts of higher education students across the globe providing a venue for their voices to be heard.

What JCAE Publishes

JCAE considers and publishes papers in the following realms: Secondary Research Articles, Research Essays, Literature Reviews, and Case Studies.

A Secondary Research Article is a full-length, graduate research paper that generally covers existing theory and/or evidence with a focus on overview instead of the inquisition commonly found in primary research.

A Research Essay, in the genre of Research Articles, covers a topic narrowly, but with a point, thesis, or perspective. This paper should open a new area of discourse, examine shifting areas of public interest, and/or offer fresh, insightful views on topics of

importance to industry or government that can be applied by leadership to reduce overhead, mitigate cybersecurity-related risks, or improve effectiveness.

Literature Reviews provide a broad perspective on a current topic of interest to the general public through terms more consumable by business and relative newcomers to the field of cybersecurity. Insight should be gleaned by the reader, through the authors passion, as a byproduct of natural curiosity driven through normal coursework.

The Case Study should be a focused solution based on a well-documented data breach, incursion, or other cybersecurity-related issue that would benefit business or government through: general warning, resolution or mitigation steps, or population awareness where training aids in improved effectiveness.

What JCAE Does Not Publish

JCAE is not direct competition for publications of original works, new theory, or rigorous scientific debate. While JCAE would not refuse such submission, our mission is coupled with the National Security Agency demand for more cooperative efforts between business, government, and academia. As student-focused academicians, Dr. Gurvirender P. S. Tejay and I were frustrated that our colleagues expected doctoral candidates to immediately absorb higher quality publication skills through osmosis, proximity or, more commonly, the verbal firehose exchange during an advisement meeting. We do not want to discourage graduate students with ontological, methodological, or philosophical alignment requirements, instead, offer a stepping stone toward becoming the next great scientist and researcher that understands how to simplify, combine, and reduce their complex thoughts into explicit words that can inspire, excite, and educate another reader interested in the field of Cybersecurity.

I would like to personally thank Dr. Tejay and Ms. Julia Costin for their perseverance through our efforts to establish a name, find a home, design and test the publication software, and create promotion literature that developed our appearance of a much larger team. As we expand our Editorial Review team, we will never lose sight of our charter in student enablement and the distribution and dissemination of Cybersecurity Information leading toward a better tomorrow.

Derek J. Sedlack, Editor-in-Chief