Journal of Cybersecurity Education, Research and Practice

Volume 2023 | Number 2 Article 1

2023

Editorial

Michael E. Whitman
Kennesaw State University, mwhitman@kennesaw.edu

Herbert J. Mattord
Kennesaw State University, hmattord@kennesaw.edu

Editorial

Abstract
Editorial for Volume 2023, Issue 2

Keywords
Editorial

FROM THE EDITORS:

Since 2016, it has been the mission of the Journal of Cybersecurity Education, Research, and Practice (JCERP) to be a premier outlet for high-quality information security and cybersecurity-related articles of interest to teaching faculty and students. This is the 15th edition of the (JCERP) and, as ever, we are seeking authors who produce high-quality research and practice-oriented articles focused on the development and delivery of information security and cybersecurity curriculum, innovation in applied scholarship, and industry best practices in information security and cybersecurity in the enterprise for double-blind review and publication. The journal invites submissions on Information Security, Cybersecurity, and related topics such as those found in this edition.

We also continue to have the need for additional reviewers for the Journal. Currently, we have about 30 reviewers that have steadfastly stuck with us, reviewing 3-4 articles per year. We'd rather keep the reviewer assignments closer to 2-3 per year, but with so few reliable reviewers, it's becoming more and more difficult. We tend to get 20-30 submissions per year, accepting 10-15, giving us an overall 50% +/- accept rate. We would love to have you join us as a reviewer, so please reach out and volunteer. We are seeing a significant increase in the submissions to our journals. However, we need more reviewers, as we count on their volunteer effort to ensure all papers accepted are of highest quality for the readers.

Editorial

All things change. That's our story and we're sticking to it. It was sad to see our colleague and friend, Dr. Hossain Shahriar leave Kennesaw State. Last May, we were notified that the university would be discontinuing the operations of the Institute for Cybersecurity Workforce Development. Since 2019, Dr. Mattord, Dr. Shahriar and I worked to build up the Institute, its outreach, and its degree programs. The BS-Cybersecurity reached 800 students. The MS-Cybersecurity reached 300. Things were going well. Now… things have changed. Dr. Mattord and I will be returning to the teaching faculty and Dr. Shahriar has accepted a position at the University of West Florida, which is the Southeast CAE Regional Hub. We wish him well and will miss him. I've been asked to stand up a center to continue to support KSU's CAE efforts – we're calling it the Center for Cybersecurity Education. The BS-Cybersecurity will move to the Coles College of Business, but be independent of the AACSB requirements, meaning it will remain a BS degree. The MS-Cybersecurity will move to the College of Computing and Software Engineering. I'll go back to what I was doing before. Things change.

Another thing changing is the Journal for Cybersecurity Education. After much discussion, we've decided to slightly change the format of the Journal. Many of you know we've changed the format of the actual papers to be in alignment with the CCERP/CISSE IEEE format. We were discussing the current practice of publishing two issues per year, with 6-8 papers per issue, when it occurred to me that we were still following the same model physical journals do, when we're an online/digital journal. Not only online, but open access - free to submit and to read. So why wait 6 months to a year to publish a paper, when there are no processes preventing doing so immediately? Lightbulb! So, we agreed that effective immediately (or at least as soon as the 2023, Issue 2 – this one, is published), we will begin publishing articles as soon as they are accepted and complete the formatting/QA review. This will make the articles available in a much timelier manner, benefiting both the reader and the author. I seem to remember we contemplated doing this when we first moved to the Digital Commons platform, but don't remember exactly why we didn't. Oh well, things change. Going forward, authors can list their accepted publication within one issue (e.g. Volume 2024, Issue 1), as all papers will be included in one issue per year.

Unfortunately, we're also going to have to ask our submitting authors to expect a slow-down in the review process. As I've been advising for some time, the lack of dedicated reviewers is negatively impacting on our original 45-day initial review decision policy. We want to get the submission under review within a week of submission, with reviews within 30 days, and feedback to the author within 45. Lately I've been inviting 4-5 reviewers, many of whom didn't explicitly agree to be reviewers but are authors automatically added by Digital Commons, to review a paper. Of those, we're lucky if 2 agree to review. This requires a new set of invitations to review, with another delay. We understand the time constraints on faculty, as we are faculty. We're lucky to have a group of about 30 reviewers that have stuck with us through thick and thin, diligently reviewing 3-4 papers a year. Now we're having to ask those reviewers to review 5 and 6 papers, just because we don't have anyone else. Even the editors are reviewing, as well as screening papers. We desperately need help. If you or a colleague could review, please email me.

In this Issue

This will be the last "In this Issue" when we move forward with the just-in-time publishing model, it won't be feasible. I plan to periodically remind our constituents of the availability of the Journal and our need for reviewers. For the last issue, the following papers are included (presented in alphabetical order by title):

A Mixed-Method Study Exploring Cyber Ranges and Educator Motivation

By: Cheryl Beauchamp (Regent University), Holly M. Matusovich (Virginia Tech).

A growing number of academic institutions have invested resources to integrate cyber ranges for applying and developing cybersecurity-related knowledge and skills. Cyber range developers and administrators provided much of what is known about cyber range resources and possible educational applications; however, the educator provides valuable understanding of the cyber range resources they use, how they use them, what they value, and what they do not value. This study provides the cyber range user perspective of cyber ranges in cybersecurity education by describing how K-12 educators are motivated using cyber ranges. Using mixed methods, this study explored educator motivation associated with cyber range usage through the lens of Eccles' Situated Expectancy Value Theory. This research contributes to understanding how educators are motivated using academic cyber ranges for cybersecurity education. Overall, educators were motivated but professional development and preparation resources that do not assume any prior cybersecurity knowledge would contribute positively to their usage. Cybersecurity education stakeholders should continue to support cyber range integration to strengthen cybersecurity education programs and support educators' ability to become better cybersecurity educators.

Adoption of cybersecurity policies by local governments 2020.

By: Donald F. Norris PhD (University of Maryland, Baltimore County), Laura K. Mateczun JD (University of Maryland, Baltimore County).

This paper should be of interest to the readers of this journal because it addresses a subject that has received little scholarly attention; namely, local government cybersecurity. The U.S. has over 90,000 units of local government, of which almost 39,000 are "general purpose" units (i.e., municipalities, counties, towns and townships). On average, these governments do not practice cybersecurity effectively (Norris, et al., 2019 and 2020). One possible reason is that they do not adopt and/or implement highly recommended cybersecurity policies. In this paper, we examine local government adoption or lack of adoption of cybersecurity policies using data from three surveys. Norris, et al, 2019 & 2020; Hatcher, et al., 2020; and Norris and Mateczun, 2023. It will probably not be surprising that our first finding is that, by and large, local governments still do a poor good job of adopting and

implementing cybersecurity policies. Thus, our first recommendation is that these governments must take whatever actions are needed to ensure high levels of cybersecurity. If they do not, the consequences will be painful and costly, as demonstrated by examples presented in the text. Among these actions, we next recommend that local governments adopt and effectively implement the highly recommended cybersecurity policies discussed in the concluding section. Last, as we have recommended previously, we again call upon local governments to create and maintain within their organizations a culture of cybersecurity – one in which all parties in these governments fully understand and support cybersecurity at the highest levels in their governments.

Cybersecurity Challenges and Awareness of the Multi-Generational Learners in Nepal.

By: Raj Kumar Dhungana (Kathmandu University, School of Education), Lina Gurung Dr (Kathmandu University), Hem Poudyal (University of Bremen, Germany).

Increased exposure to technologies has lately emerged as one of the everyday realities of digital natives, especially K-12 students, and teachers, the digital immigrants. Protection from cybersecurity risks in digital learning spaces is a human right, but students are increasingly exposed to high-risk cyberspace without time to cope with cybersecurity risks. This study, using a survey (N-891 students and 157 teachers) and in-depth interviews (27 students and 14 teachers), described the students' cybersecurity-related experiences and challenges in Nepal. This study revealed that the school's cybersecurity support system is poor and teachers has very low awareness and competencies to protect students from cybersecurity-related challenges. To create a safe cyberspace for learners, it is urgent to enhance the cybersecurity awareness and skills of teachers, as the existing infrastructure is weak and there is a significant gap related to the cybersecurity awareness between students and teachers. Poor cybersecurity is one of the significant barriers to the quality of education in Nepal. In the age of information and technology, effective collaboration among parents, teachers, and students, the multi-generational learners, is the prerequisite for ensuring children's rights to learn in all settings including cyberspace.

Exploring Network Security Educator Knowledge

By: Jennifer B. Chauvot (University of Houston), Deniz Gurkan (University of Houston), Cathy Horn (University of Houston).

It is critical for nations to have trained professionals in network security who can safeguard hardware, information systems, and electronic data. Network security education is a key knowledge unit of the National Centers of Academic Excellence in Cybersecurity and various information systems security curricula at the master's and bachelor's levels in higher education. Network security units are components of computer science curricula in high school contexts as well. Educators who teach these concepts play a significant role in developing a skilled workforce of network security experts for both governmental and non-governmental organizations. Understanding the necessary knowledge and skills of network security educators serve to better inform institutes of higher education, educator preparation programs, and others who support educators in the field. This study describes knowledge constructs of a higher education faculty member who teaches networking and network security and was developing, and piloting innovative network security curriculum embedded in both undergraduate and graduate courses. Data were transcripts of recorded monthly meetings with the educator, fieldnotes taken during the meetings, and course artifacts. Existing teacher knowledge frameworks that have been applied in both K-12 and higher education contexts were used to deductively code the data. Examples of curricular knowledge and pedagogical content knowledge specific to the teaching of network security are provided. The affordances of using engagement within curriculum development to understand educator knowledge constructs and the existing teacher knowledge frameworks as tools for analyses are highlighted.

Integrating certifications into the cybersecurity college curriculum: The efficacy of education with certifications to increase the cybersecurity workforce
By: Binh Tran (Georgia Gwinnett College), Karen C. Benson (Georgia Gwinnett College), Lorraine Jonassen (Georgia Gwinnett College).
One only needs to listen to the news reports to recognize that the gap between securing the enterprise and cybersecurity threats, breaches, and vulnerabilities appears to be widening at an alarming rate. An untapped resource to combat these attacks lies in the students of the secondary educational system. Necessary in the cybersecurity education is a 3-tiered approach to quickly escalate the student into a workplace-ready graduate. The analogy used is a three-legged-stool, where curriculum content, hands-on skills, and certifications are equal instruments in the edification of the cybersecurity student. This paper endeavors to delve into the 3rd leg of the stool by developing the concept of vendor-specific and vendor neutral certifications to educate the cybersecurity student and test their capability of protecting the workplace. The research data was drawn from companies in the Atlanta, Georgia area, who employ and hire cybersecurity recruits. The data from the research proves certifications are necessary as an addition to the cybersecurity curriculum in the secondary education arena. The paper reviews the need for cybersecurity graduates, the balance between cybersecurity theory and applied skillsets, the difference between a certificate and a certification, benefits to the community, classifications of certifications, relevancy of a college degree in today's workforce, and recommendations for further study.

Like Treating the Symptom Rather than the Cause - the Omission of Courses over Terrorism in NSA Designated Institutions
By: Ida L. Oesteraas (Old Dominion University).?
The National Security Agency (NSA) awards Center of Academic Excellence (CAE) designations to institutions that commit to producing cybersecurity professionals who will work in careers that reduce vulnerabilities in our national infrastructure. A review of the curricula in the 327 institutions and their degree programs reveal that only two programs offer a required course about terrorism. Given the fluid nature of terrorism and its threat to national infrastructure, the omission is concerning. It is recommended that NSA-certified cybersecurity programs begin implementing educational content that aim to teach about this emerging crime and justice issue. One suggestion is to embrace the interdisciplinary nature of cybersecurity, as exemplified in the success of the Cybersecurity Living and Learning Community (CLLC). Designing courses that educate about the social processes that leads to the growing problem of violence and terror directed towards marginalized communities and our nation's technological infrastructure, is another.

Privacy Harm and Non-Compliance from a Legal Perspective
By: Suvineetha Herath (Dakota State University), Haywood Gelman (Dakota State University), Lisa McKee (Dakota State University).
In today's data-sharing paradigm, personal data has become a valuable resource that intensifies the risk of unauthorized access and data breach. Increased data mining techniques used to analyze big data have posed significant risks to data security and privacy. Consequently, data breaches are a significant threat to individual privacy. Privacy is a multifaceted concept covering many areas, including the right to access, erasure, and rectify personal data. This paper explores the legal aspects of privacy harm and how they transform into legal action. Privacy harm is the negative impact to an individual as a result of the unauthorized release, gathering, distillation, or expropriation of personal information. Privacy Enhancing Technologies (PETs) emerged as a solution to address data privacy issues and minimize the risk of privacy harm. It is essential to implement privacy enhancement mechanisms to protect Personally Identifiable Information (PII) from unlawful use or access. FIPPs (Fair Information Practice Principles),

based on the 1973 Code of Fair Information Practice (CFIP), and the Organization for Economic Cooperation and Development (OECD), are a collection of widely accepted, influential US codes that agencies use when evaluating information systems, processes, programs, and activities affecting individual privacy. Regulatory compliance places a responsibility on organizations to follow best practices to ensure the protection of individual data privacy rights. This paper will focus on FIPPs, relevance to US state privacy laws, their influence on OECD, and reference to the EU General Data Processing Regulation. (GDPR).

Understanding How to Diversify the Cybersecurity Workforce: A Qualitative Analysis
By: Maria Chaparro Osman (Florida Institute of Technology), Maureen Namukasa (Florida Institute of Technology), Cherrise Ficke (Florida Institute of Technology), Isabella Piasecki (Florida Institute of Technology), TJ OConnor (Florida Institute of Technology), Meredith Carroll (Florida Institute of Technology).
A robust cybersecurity workforce is critical for protection against a range of malicious attacks. However, it has been noted that there are many vacancies and a shortage of individuals entering the cybersecurity workforce. This workforce shortage has partly been attributed to the lack of diversity in the cybersecurity field, with women, African Americans, and Hispanics remaining underrepresented in educational and professional settings. Using a qualitative approach, this work sought to investigate what led underrepresented minorities currently involved in cybersecurity to the industry, with the goal of determining methods to attract and diversify the workforce. A thematic analysis was conducted using data collected during interviews with 23 participants including underrepresented minority students, underrepresented minority professionals, college instructors, and a high school administrator. The interview questions aimed to address (a) what attracted minorities to the field, (b) how they overcame educational and professional roadblocks, (c) how they built non-technical knowledge, skills, and attitudes, and (d) how they maintained engagement. Findings revealed 17 themes that were related to characteristics of (a) the learner, (b) the instruction, and (c) the environment. Based on these findings, recommendations are presented to illustrate how these themes can be implemented by instructors with the goal of increasing the participation and involvement of underrepresented minorities and fostering diversity in the cybersecurity field.

That's it for now. We welcome your submissions and feedback.

For the editors
Mike Whitman
Herb Mattord

In This Issue

For Volume 2023, Number 1 we are pleased to share the following scholarly articles:

1. **Sociocultural Barriers for Female Participation in STEM: A Case of Saudi Women in Cybersecurity**
Alanoud Aljuaid (*Marymount University*), Xiang Michelle Liu (*Marymount University*)

Abstract:
The participation of women in Science, Technology, Engineering, and Mathematics (STEM) workforces is overwhelmingly low as compared to their male counterparts. The low uptake of cybersecurity careers has been documented in the previous studies conducted in the contexts of the West and Eastern worlds. However, most of the past studies mainly covered the Western world leaving more knowledge gaps in the context of Middle Eastern countries such as Saudi Arabia. Thus, to fill the existing knowledge gaps, the current study focused on women in Saudi Arabia. The aim of the study was to investigate the factors behind the underrepresentation of Saudi women in the cybersecurity space by specifically targeting the existing socio-cultural barriers. The study used a qualitative design that entailed reliance on both primary interview data and additional evidence from prior literature to evaluate the barriers faced by Saudi women in cybersecurity. A sample of 15 Saudi women aged 18 – 30 years with a college education or still in college pursuing a course in IT (Information Technology) or had basic computer literacy skills was purposefully recruited as the most desirable participants. A thematic analysis process was conducted on the primary data to generate theory from the findings, further compared with and verified based on a critical literature review. The themes that were generated from the interviews include lack of autonomy, family responsibilities, female as the weaker gender, and child bearing and caring duties.

2. **Compete to Learn: Toward Cybersecurity as a Sport**
TJ OConnor (Florida Tech), Dane Brown (US Naval Academy), Jasmine Jackson, Bryson Payne (University of North Georgia), Suzanna Schmeelk (St. John's University)

Abstract:
To support the workforce gap of skilled cybersecurity professionals, gamified pedagogical approaches for teaching cybersecurity have exponentially grown over the last two decades. During this same period, e-sports developed into a multi-billion dollar industry and became a staple on college campuses. In this work, we explore the opportunity to integrate e-sports and gamified cybersecurity approaches into the inaugural US Cyber Games Team. During this tenure, we learned many lessons about recruiting, assessing, and training cybersecurity teams. We share our approach, materials, and lessons learned to serve as a model for fielding amateur cybersecurity teams for future competition.

3. **Cyberbullying: Senior Prospective Teachers' Coping Knowledge and Strategies**
Kürşat Arslan (*Dokuz Eylul University*), İnan Aydın

Abstract:
This study aimed to determine senior prospective teachers' coping knowledge and strategies for cyberbullying in terms of demographic variables. The sample consisted of 471 prospective teachers (324 female and 147 male) studying in the 4th grade in Dokuz Eylül University Buca Education Faculty in Izmir in the 2019-2020 academic year. It was a quantitative study using a causal-comparative research design to find out whether prospective teachers' coping knowledge

differed by independent variables. The "Coping with Cyberbullying Scale" developed by Koç et al. (2016) was employed to discover prospective teachers' coping strategies for cyberbullying. A "Personal Information" form was also prepared to collect demographic information. The data were analyzed with SPSS 25.0 program. Since the dependent variables did not have a normal distribution, the differences between the variables with two groups were analyzed with the Mann-Whitney U test, and the variables with three or more groups were analyzed with the Kruskal-Wallis H test. The findings suggested that the prospective teachers' cyberbullying coping knowledge level was moderate. Other findings were discussed in the discussion section.

4. **Anonymity and Gender Effects on Online Trolling and Cybervictimization**
Gang Lee (Kennesaw State University), Annalyssia Soonah (Kennesaw State University)

Abstract:
The purpose of this study was to investigate the effects of the anonymity of the internet and gender differences in online trolling and cybervictimization. A sample of 151 college students attending a southeastern university completed a survey to assess their internet activities and online trolling and cybervictimization. Multivariate analyses of logistic regression and ordinary least squares regression were used to analyze online trolling and cybervictimization. The results indicated that the anonymity measure was not a significant predictor of online trolling and cybervictimization. Female students were less likely than male students to engage in online trolling, but there was no gender difference in cybervictimization. In addition, the total hours spent on the internet increased the likelihood of the decision of college students to participate in online trolling, but not cybervictimization. Further implications for research related to online trolling and risk factors are discussed.

5. **How Effective are SETA Programs Anyway: Learning and Forgetting in Security Awareness Training**
David Sikolia (*Pittsburg State University*), David Biros (*Oklahoma State University*), Tianjian Zhang (*City University of Hong Kong*)

Abstract:
Prevalent security threats caused by human errors necessitate security education, training, and awareness (SETA) programs in organizations. Despite strong theoretical foundations in behavioral cybersecurity, field evidence on the effectiveness of SETA programs in mitigating actual threats is scarce. Specifically, with a broad range of cybersecurity knowledge crammed into in a single SETA session, it is unclear how effective different types of knowledge are in mitigating human errors in a longitudinal setting. This study investigates how knowledge gained through SETA programs affects human errors in cybersecurity to fill the longitudinal void. In a baseline experiment, we establish that SETA programs reduce phishing susceptibility by 50%, whereas the training intensity does not affect the rate. In a follow-up experiment, we find that SETA programs can increase employees' cybersecurity knowledge by 12-17%, but the increment wears off within a month. Furthermore, technical-level knowledge decays faster than application-level knowledge. The longer "shelf-life" of application-level knowledge explains why training intensity makes no difference within a month. This study reveals a (relatively) more effective component of SETA programs and cast doubts on the overall effectiveness of SETA programs in the long run.

6. **A Systematic Mapping Study on Gamification Applications for Undergraduate Cybersecurity Education**

Sherri Weitl-Harms (University of Nebraska at Kearney), Adam Spanier (University of Nebraska at Omaha), John Hastings (University of Nebraska at Kearney), Matthew Rokusek (University of Nebraska - Lincoln)

Abstract:
Gamification in education presents a number of benefits that can theoretically facilitate higher engagement and motivation among students when learning complex, technical concepts. As an innovative, high-potential educational tool, many educators and researchers are attempting to implement more effective gamification into undergraduate coursework. Cyber Security Operations (CSO) education is no exception. CSO education traditionally requires comprehension of complex concepts requiring a high level of technical and abstract thinking. By properly applying gamification to complex CSO concepts, engagement in students should see an increase. While an increase is expected, no comprehensive study of CSO gamification applications (GA) has yet been undertaken to fully synthesize the use and outcomes of existing implementations. To better understand and explore gamification in CSO education, a deeper analysis of current gamification applications is needed. This research outlines and conducts a methodical, comprehensive literature review using the Systematic Mapping Study process to identify implemented and evaluated GAs in undergraduate CSO education. This research serves as both a comprehensive repository and synthesis of existing GAs in cybersecurity, and as a starting point for further CSO GA research. With such a review, future studies can be undertaken to better understand CSO GAs. A total of 74 papers were discovered which evaluated GAs undergraduate CSO education, through literature published between 2007 and June 2022. Some publications discussed multiple GAs, resulting in a total of 80 undergraduate CSO GAs listing at https://bit.ly/3S260GS. The study outlines each GA identified and provides a short overview of each GA. It also provides a summary of engagement-level characteristics currently exhibited in existing CSO education GAs and discusses common themes and findings discovered in the course of the study.

7. **Case Study: The Impact Of Emerging Technologies On Cybersecurity Education And Workforces**

Austin Cusak (Robert Morris University)

Abstract:
A qualitative case study focused on understanding what steps are needed to prepare the cybersecurity workforces of 2026-2028 to work with and against emerging technologies such as Artificial Intelligence and Machine Learning. Conducted through a workshop held in two parts at a cybersecurity education conference, findings came both from a semi-structured interview with a panel of experts as well as small workgroups of professionals answering seven scenario-based questions. Data was thematically analyzed, with major findings emerging about the need to refocus cybersecurity STEM at the middle school level with problem-based learning, the disconnects between workforce operations and cybersecurity operators, the distrust of Non-Traditional Training Programs, and the need to build digital security generalists' curriculum and training. Recommendations are also made for possible next steps.

8. **Examination of Cybersecurity Technologies, Practices, Challenges, and Wish List in K-12 School Districts**

Florence Martin (North Carolina State University), Julie Bacak (University of North Carolina Charlotte), Erik Jon Byker (University of North Carolina at Charlotte), Weichao Wang (University of North Carolina Charlotte), Jonathan Wagner (University of North Carolina Charlotte), Lynn Ahlgrim-Delzell (University of North Carolina Charlotte)

Abstract:
With the growth in digital teaching and learning, there has been a sharp rise in the number of cybersecurity attacks on K-12 school networks. This has demonstrated a need for security technologies and cybersecurity education. This study examined security technologies used, effective security practices, challenges, concerns, and wish list of technology leaders in K-12 settings. Data collected from 23 district websites and from interviews with 12 district technology leaders were analyzed. Top security practices included cloud-based technologies, segregated network/V-LAN, two-factor authentication, limiting access, and use of Clever or Class Link. Top challenges included keeping users informed, lack of buy-in from staff and decision-makers, lack of expertise to implement modern best practices, and cost of resources. Top concerns included possible cyberattacks, leaked student data, and lack of user awareness. Finally, their wish list included technology personnel, access to Clever of Class Link, external system diagnostic checks, professional development for staff, and replacing aging infrastructure. The findings have implications for K-12 administrators, technology leaders, and teachers.

We hope you enjoy this issue, and as always, please consider submitting a manuscript of your own to JCERP.

Dr. Mike Whitman
Dr. Herb Mattord
Dr. Hossain Shahriar

KSU Institute for Cybersecurity Workforce Development