Journal of Cybersecurity Education, Research and Practice

Volume 2023 | Number 1 Article 1

2023

Editorial - 2023 - 1

Hossain Shahriar
Kennesaw State University, hshahria@kennesaw.edu

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

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

Editorial - 2023 - 1

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 14th 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.

Editorial

Cybersecurity Threats, Risks and Opportunities in the Post COVID time

There is a tremendous level of dialogues and events around the nation on cybersecurity – particularly how to develop cyber workforce. At the same time we are constantly seeing cyber infrastructure coming under attacks from insider threats and external nation states. Not long ago we saw the news of a low altitude balloon from a nation state flew over USA territory for so long that experts believe it gained much valuable information bypassing all other security measures in place – and there may be yet more examples we may not have been aware as of yet. Cybersecurity risks will keep evolving as our understanding of threats, risks keeps changing, and it must remain as a collective effort to defend our resources.

This issue covers a broader selection of articles – addressing the barriers for minority citizens to enter into cyber workforce, application of gaming based pedagogy to train cybersecurity, coping with cyberbullying by adults, if there is any effect on internet anonymity and gender differences for online trolling and cybervictimization, evaluating the effectiveness of security education, awareness and training programs, systematic mapping study to identify implementation and evaluation of gamification applications in undergraduate CSO education, and review of cybersecurity threats landscape for K-12 school districts.

Now we are seeing all in person conferences are being held, we are seeing slightly increase in the submissions to our journals. However, we need more reviewers and we count on their volunteer effort to ensure all papers accepted are of highest quality for the readers.
The Conference on Cybersecurity Education, Research, and Practice will be held jointly with the Colloquium for Information Systems Security Education in 2023 at KSU campus in the fall. We will host the event as a hybrid conference with CISSE, CCERP and one to two other conferences as a multi-venue event. We look forward to your further participation in the event. We hope our readers will consider submitting papers there as well.

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