frontiers | Frontiers in Education

TYPE Editorial
PUBLISHED 27 October 2023
DOI 10.3389/feduc.2023.1277282

OPEN ACCESS

EDITED AND REVIEWED BY
Terrell Lamont Strayhorn,
Virginia Union University, United States

*CORRESPONDENCE
Ricardo G. Lugo
ricardo.g.lugo@ntnu.no

RECEIVED 14 August 2023
ACCEPTED 20 September 2023
PUBLISHED 27 October 2023

CITATION
Lugo RG, Sütterlin S, Knox BJ, Bukauskas L, Brilingaitė A and Maennel OM (2023) Editorial: The human factor in cyber security education. *Front. Educ.* 8:1277282. doi: 10.3389/feduc.2023.1277282

Editorial: The human factor in cyber security education

Ricardo G. Lugo[1,2]*, Stefan Sütterlin[3,4], Benjamin James Knox[1,5,6], Linas Bukauskas[7], Agnė Brilingaitė[7] and Olaf Manuel Maennel[3]

[1]Department of Information Security and Communication Technology, Faculty of Information Technology and Electrical Engineering, Norwegian University of Science and Technology, Gjøvik, Norway, [2]Estonian Maritime Academy, Tallinn University of Technology, Tallinn, Estonia, [3]Centre for Digital Forensics and Cyber Security, Tallinn University of Technology, Tallinn, Estonia, [4]Faculty of Computer Science, Albstadt-Sigmaringen University, Sigmaringen, Germany, [5]Faculty of Health, Welfare and Organization, Østfold University College, Halden, Norway, [6]Norwegian Armed Forces Cyber Defense, Oslo, Norway, [7]Faculty of Mathematics and Informatics, Institute of Computer Science, Vilnius University, Vilnius, Lithuania

KEYWORDS

human factor (HF), cyber defense exercises, cybersecurity (CS), cybersecurity training, cybersecurity education

Editorial on the Research Topic
The human factor in cyber security education

The significance of understanding the human component in cybersecurity cannot be overstated, as it extends well beyond mere technical proficiency. Comprehending human behavior and engaging with people through various methods such as modeling, gamification, and the application of neuroergonomic methodologies is essential in building a resilient cybersecurity infrastructure.

From Venables, one can understand that modeling cyberspace must include humans as an integral component. Acknowledging the human factor emphasizes the need for a multidimensional approach to cybersecurity. By focusing on aspects such as geography, politics, and time, and not just technology, a more comprehensive view of cybersecurity can be achieved. This helps to understand not only the terrain of cyberspace but also the human motivations that drive malicious intent.

Cybersecurity exercise design can incorporate approaches that can aid in the acceleration of learning and developing a soft skill toolset, which has been identified as a key area (European Union Agency for Cybersecurity, 2022), by using, for example, gamification (Canham et al.) or applying neuroergonomic approaches (Ask et al.). The use of gamification in cybersecurity is emerging as an effective tool for both engagement and education. Interactive methods such as the Phish Derby competition utilize competition and prizes to incentivize learning, turning it into a fun and engaging experience. Gamification techniques can be applied to enhance situational awareness, making learning more immersive and intuitive. This approach can be especially useful for educating non-experts or the general public about complex cybersecurity concepts. But as identified by European Union Agency for Cybersecurity (2022) technical skills alone are insufficient in today's complex cybersecurity landscape and developing soft skills, i.e., effective communication, collaboration, and situational awareness, are equally vital. Whether it's through the creation of a Recognized Cyber Picture (RCP; Ask et al.) or the implementation of neuroergonomic principles to improve interpersonal situational awareness, nurturing these soft skills is essential. Fostering a culture that values both hard and soft skills is critical to achieving proficient cybersecurity protocols.

In order to achieve and validate these educational milestones, Pirta-Dreimane et al. showed that paradigms from other domains (intervention mapping; health) can be applied and help cybersecurity education developments. The need for well-designed educational frameworks that incorporate stakeholders' input and address specific competency requirements is paramount. The application of Intervention Mapping in the design of cybersecurity education, for instance, allows for a more structured and evidence-based approach. This highlights the importance of using well-grounded methodologies in both development and execution.

To objectively rate cybersecurity competencies, a balancing scoring of Cybersecurity Exercises must be accomplished. Mäses et al. demonstrated the complexity of achieving appropriate balance in scoring cybersecurity exercises, as seen in the Locked Shields case study, and illustrated the nuances involved in creating an effective and fair evaluation system. Clarity and transparency are essential to maintaining engagement and learning. This adds another layer to the intricate task of training and evaluating individuals in cybersecurity.

Conclusion

The global health crisis has brought about unique challenges. The rapid shift to remote work and learning has increased the risks of security breaches, while also placing greater stress on employees. Education and training must adapt to address these evolving dynamics and provide support for the new workplace environment. Cybersecurity education must be inclusive, considering experts, workforce employees, and the general public. Tailoring strategies to meet the needs of different groups is crucial. Having a holistic approach ensures that education and awareness permeate all levels of society, thus enhancing overall cybersecurity resilience.

The complexities of cybersecurity education call for a multifaceted approach that recognizes the human factor at its core. The intertwining of technological, psychological, sociological, and pedagogical elements requires continuous research, collaboration, and innovation. The insights from gamification, the focus on soft skills, the need for comprehensive frameworks, and the importance of adapting to societal changes, such as the impact of the COVID-19 pandemic, highlight the intricate nature of this field. Together, these aspects forge a path toward a future where cybersecurity education is agile, inclusive, and robust, ready to meet the ever-changing challenges of the digital age.

Author contributions

RL: Writing—original draft, Writing—review & editing. SS: Writing—original draft, Writing—review & editing. BK: Writing—original draft, Writing—review & editing. LB: Writing—original draft, Writing—review & editing. AB: Writing—original draft, Writing—review & editing. OM: Writing—original draft, Writing—review & editing.

Funding

This work was supported through ACDICOM, and the research project was funded by the Research Council of Norway, through the SAMRISK program (#302941). This work was also supported by the EU Horizon2020 project MariCybERA (agreement No. 952360) and the Advancing Human Performance in Cybersecurity, benefits from nearly €1 million grant from Iceland, Liechtenstein, and Norway through the EEA Grants. Project contract with the Research Council of Lithuania (LMTLT) No. is S-BMT-21-6 (LT08-2-LMT-K-01-051).

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

European Union Agency for Cybersecurity, ENISA (2022). *European Cybersecurity Skills Framework*. Available online at: https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/ecsf-profiles-v-0-5-draft-release.pdf (accessed August 6, 2023).