WISE Workshops : Foundations for Collaborative Cyber Security Learning: Exploring Educator and Learner Requirements ; Reimaging Inclusive Pedagogy in Cybersecurity Education (A Workshop Proposal)

Jerry Andriessen, Steven Furnell, Gregor Langner, Gerald Quirchmayr, Vittorio Scarno, Teemu Tokola, Angela G. Jackson-Summers

WISE Workshops

Foundations for Collaborative Cyber Security Learning: Exploring Educator and Learner Requirements

Jerry Andriessen[1], Steven Furnell[2](✉), Gregor Langner[3], Gerald Quirchmayr[4], Vittorio Scarno[5], and Teemu Tokola[6]

[1] Wise & Munro, The Hague, The Netherlands
[2] University of Nottingham, Nottingham, UK
steven.furnell@nottingham.ac.uk
[3] Austrian Institute of Technology, Vienna, Austria
Gregor.Langner@ait.ac.at
[4] University, of Vienna, Vienna, Austria
[5] University of Salerno, Fisciano, Italy
[6] University of Oulu, Oulu, Finland

Abstract. This brief paper outlines the background to a workshop session at the 14th World Conference on Information Security Education (WISE 14), drawing upon early findings from the *Collaborative Cybersecurity Awareness Learning (COLTRANE)* project funded under the European Union ERASMUS + programme. It presents the background to the COLTRANE project and an outline of the workshop focus. The latter is based upon an investigation of current cyber security education delivery that has been conducted amongst existing educators and learners via prior survey-based data collection and follow-up workshop discussions within individual COLTRANE partner countries.

Keywords: Collaborative learning · Educators · Learners

1 Introduction

Cyber security is now an increasing area of focus within university-level educational provision, with related coverage within both undergraduate and postgraduate programme and encompassing programmes specifically addressing the topic and those that integrate it as a tangible thematic strand. However, while there is clearly a level of broad demand, few other fields require such a holistic and multidisciplinary view as cyber security. As such, it poses a challenge for institutions and educators to make effective provision, and for learners to feel they are receiving an appropriate experience.

L. Drevin et al. (Eds.): WISE 2021, IFIP AICT 615, pp. 143–145, 2021.
https://doi.org/10.1007/978-3-030-80865-5

2 The COLTRANE Project

COLTRANE aims to enhance cybersecurity education by introducing innovative concepts in the context of collaborative awareness education [1]. Traditional forms of education mainly focus on knowledge transmission, but in highly dynamic areas such as cybersecurity this does not lead to sufficient learning outcomes. We therefore need more innovative forms of education that aim at the development of joint action: being able to act in a variety of situations and knowing how to do this together.

The COLTRANE consortium consists of six partners, combining expertise in the areas of higher education learning and teaching, cybersecurity, state of the art technology, and collaborative learning and educational design:

- Austrian Institute of Technology, Austria
- University of Nottingham, United Kingdom
- University of Oulu, Finland
- University of Salerno, Italy
- University of Vienna, Austria
- Wise & Munro, The Netherlands

The work conducted within COLTRANE ultimately aims to contribute by:

- exploiting the affordances of cyber-ranges and collaborative learning platforms to create hands-on activities, as well as collaborative reflection;
- supporting the co-design of learning activities together with teachers, according to a framework for developing cybersecurity awareness education;
- developing a toolkit for teachers for evaluation of learning activities by students; and
- supporting managers and policy makers by co-designing toolkits for institutional implementation planning.

However, a starting point is to benchmark the current position and feelings of educators and students already operating in the space, determine the aspects that they already consider to be well-served, and the areas in which COLTRANE's intended approaches could offer opportunities for improvement.

3 Workshop Focus

The aim of the workshop is to share and further explore the current provision of cybersecurity education, based upon views collected from academics and students in current programmes. The project has conducted a series of data collection activities amongst educators and students in the partner countries. Specifically, a pair of online surveys (one targeting educators, the other addressing learners) were distributed to relevant participants in partner countries, followed by a series of related workshops (each with ~6–8 participants) to explore and discuss matters in more detail. The overall focus of these activities has been to establish:

- interpretations of cybersecurity (e.g. the extent to which it is seen as an interdisciplinary topic, drawing upon topic areas beyond computer science and IT);
- the existing content and coverage of cybersecurity education (e.g. in terms of knowledge coverage and skills development, with specific reference frameworks provided by the Cyber Security Body of Knowledge [2] and the CIISec Skills Framework [3]);
- the modes of learning and delivery (e.g. incorporation of activities such as coloration and problem-based learning, as well as the provision of facilities and practical experiences); and
- the extent of professional alignment (e.g. the extent of industry and professional body engagement within programme provision).

The workshop at WISE 14 shares the related findings as a basis for discussion and further sharing of experience amongst the attendees. For COLTRANE this provides a valuable opportunity to share, validate and extend the findings before the project moves into further design and development phases, while for WISE attendees it provides an insight into current challenges and approaches that could help to inform participants' own initiatives and future developments.

References

1. COLTRANE Homepage. https://coltrane.ait.ac.at. Accessed 15 April 2021.
2. Rashid, A., Chivers, H., Danezis, G., Lupu, E., Martin, A.: The Cyber Security Body of Knowledge. Version 1.0, 31 October 2019 (2019). https://www.cybok.org/media/downloads/cybok_version_1.0.pdf
3. CIISec. CIISec Skills Framework, Version 2.4, Chartered Institute of Information Security, November 2019. https://www.ciisec.org/CIISEC/Resources/Capability_Methodology/Skills_Framework/CIISEC/Resources/Skills_Framework.aspx

Reimaging Inclusive Pedagogy in Cybersecurity Education (A Workshop Proposal)

Angela G. Jackson-Summers(✉)

U.S. Coast Guard Academy, New London, CT 6320, USA
Angela.G.Jackson-Summers@uscga.edu

Abstract. Cybersecurity education programs have steadily been working to meet the increasing global demand for cybersecurity professionals. However, academic institutions are often faced with meeting such demand, because of the lack of enrollment and retention of students from varying backgrounds and reflecting other differences (i.e. cultural, gender, age, racial). Minimal literature exists relating to inclusive pedagogy in cybersecurity education. The goal of this proposed workshop is to rethink inclusive pedagogy in cybersecurity education programs and develop a future research agenda that promotes inclusive pedagogy in cybersecurity education program delivery.

Keyword: Inclusive pedagogy · Inclusive pedagogical practices · Inclusive communications · Curricular design · Cybersecurity education

1 Introduction

1.1 Overview

To support cybersecurity workforce needs, academic institutions [6], governmental agencies [4], and researchers [1] have been working to develop and continuously enhance cybersecurity education programs. In recognizing the need to support cybersecurity workforce growth, the need to focus on diversity and inclusion in our pedagogical approaches has been a concern in recent literature [3]. Reimaging Inclusive Pedagogy in Cybersecurity Education is a workshop that proposes to foster collaborative discussion and continued growth in inclusive pedagogical practices and future research efforts supporting cybersecurity education delivery.

The Center for the Integration of Research, Teaching and Learning (CIRTL) offers an Inclusive Pedagogy Framework (Inclusive Pedagogy Framework (2) (cirtlincludes.net)) involving three core competencies as depicted in Fig. 1 below that will help frame the workshop into three (3) separate segments. Each segment will correspond and address a specific core competency, including related skills, strategies, and practices.

Angela G. Jackson-Summers, is an Assistant Professor of Information Systems at the U.S. Coast Guard Academy. The views here are her own and not those of the Coast Guard Academy or other branches of the U.S. government.

L. Drevin et al. (Eds.): WISE 2021, IFIP AICT 615, pp. 146–149, 2021.
https://doi.org/10.1007/978-3-030-80865-5

The objective in addressing each segment separately is to provide a common understanding of each core competency among workshop participants.

During each segment, the collective audience will be divided into smaller breakout sessions where participants can participate in brainstorming activities. These brainstorming activities will be designed to capture challenges and desired outcomes in achieving each core competency. Additionally, workshop participants will help define a forward-thinking research strategy and tactical action plan that offers continued research efforts in inclusive pedagogy in cybersecurity education. At the close of the workshop, the facilitator looks to establish a draft future research initiative that drives an inclusive pedagogy in cybersecurity education agenda supported by interested workshop participants.

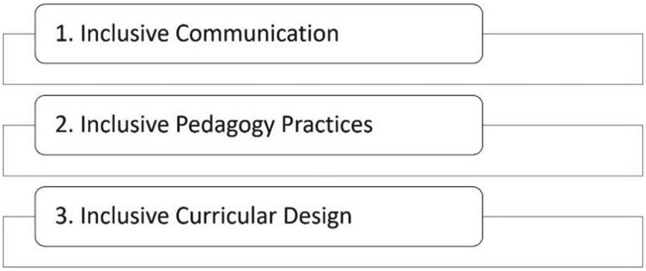
1. Inclusive Communication
2. Inclusive Pedagogy Practices
3. Inclusive Curricular Design

Fig. 1. Adapted depiction of CIRTL's Inclusive Pedagogy Framework.

Objectives. This online event is intended to exercise this "workshop as a research methodology" that offers workshop participants an opportunity to address their own research interests and promote future research in cybersecurity education. Workshop as a research methodology [5] has been described as a means of advancing and negotiating a topic, such as inclusive pedagogy in cybersecurity education, among workshop attendees (i.e. researchers, teachers). Additionally, workshop participants will share in the following takeaways.

- Build knowledge in an existing framework used for promoting inclusive pedagogy
- Gain insights on existing literature related to inclusive pedagogy and cybersecurity education needs
- Share their own challenges and desired outcomes in achieving more diverse and inclusive classrooms in cybersecurity education delivery
- Engage with other instructors and researchers having like interests in promoting inclusive pedagogy in cybersecurity education
- Participate in future collaborative-based dialogue and research-driven events that promote inclusive pedagogy in cybersecurity education

Workshop Length and Format. This online workshop is expected to be conducted as a collaborative group event in 2 to 2 ½ hours and is intended for a small audience of 12–15 attendees.

Audience/Participants. Attendees should include instructors and researchers who have a focal interest in the topics of inclusive pedagogy and cybersecurity as well as the use of varying theories and research methods. Additionally, the workshop welcomes attendees who are willing to share prior pedagogical practices that were intended to foster diversity and inclusiveness in cyber education programs or more specifically, cyber education course delivery.

Workshop Agenda. This online workshop is expected to be conducted as a collaborative group event in 2 to 2 ½ hours and is intended for a small audience of 12–15 attendees.

- Give an introduction from each workshop participant (i.e. affiliation, research interest).
- Revisit workshop objectives.
- Address the CIRTL Inclusive Pedagogy Framework and its three (3) core competencies.
- Share existing literature relating to inclusive pedagogy (i.e. inclusive communications, inclusive pedagogical practices, curricular design) and cybersecurity education.
- Present the approach to conducting the break-out sessions, capturing feedback, and presenting results.
- During each break-out session, brainstorm challenges and improvement opportunities to inclusive pedagogy.
- Identify next steps, including those attendees interested in actively engaging with colleagues to address specific research efforts.

Outcomes. To help foster and improve inclusive pedagogical practices in cybersecurity education through faculty development and research, the primary outcome of this workshop is as follows.

- A research working group of 2–3 teams (i.e. 3–5 individuals per team), which represent interested participants in future periodic forum discussions and collaborative research efforts.

Deliverables. To promote future research and efforts towards strengthening diverse and inclusive cybersecurity education, and related inclusive pedagogical practices, the following three workshop deliverables are expected as follows.

- Draft Inclusive Pedagogy in Cybersecurity Education strategy and high-level tactical action plan that shares proposed next steps in future research efforts and continued dialogue on inclusive pedagogical best practices.
- A summary of initial challenges and improvement opportunities to inclusive pedagogy in cybersecurity education.

References

1. Cabaj, K., Domingos, D., Kotulski, Z., Respício, A.: Cybersecurity education: evolution of the discipline and analysis of master programs Comput. Secur. **75**, 24–35 (2018)
2. Center for the Integration of Research, Teaching, and Learning. Inclusive pedagogy framework. Retrieved from Inclusive Pedagogy Framework (2) (cirtlincludes.net) (2018)
3. Mountrouidou, X., Vosen, D., Kari, C., Azhar, M.Q., Bhatia, S., Gagne, G., ... Yuen, T.T.: Securing the human: a review of literature on broadening diversity in cybersecurity education. Proceedings of the Working Group Reports on Innovation and Technology in Computer Science Education, pp. 157–176, Aberdeen, Scotland UK (2019)
4. Newhouse, W., Keith, S., Scribner, B., & Witte, G.: NIST special publication 800–181: National initiative for cybersecurity education (NICE) cybersecurity workforce framework. Gaithersburg, MD USA: U.S. Department of Commerce and the National Institute of Standards and Technology (2017)
5. Ørngreen, R., Levinsen, K.: Workshops as a research methodology Electron. J. e-Learning **15** (1), 70–81 (2017)
6. Schneider, F.B.: Cybersecurity education in universities IEEE Secur. Priv. **11**(4),3–4 (2013)

Author Index