# Cyber Security Education for Industry and Academia - CSE4IA

Vita Santa Barletta [1], Danilo Caivano [1], Federica Caruso [2], Sara Peretti[2], and Veronica Rossano [1]

[1] *University of Bari Aldo Moro, 70121, Bari, Italy*
[2] *University of L'Aquila, 67100, L'Aquila, Italy*

**Abstract**

We propose the first edition of the workshop on Cyber Security Education for Industry and Academia (CSE4IA) to be co-located with the next edition of IS-EUD 2023. Cybersecurity education has become increasingly important in recent years due to the shortage of cybersecurity professionals in the international job market. To address this challenge, it is necessary to focus on three contexts and their interconnections: Industry, Academia, and Public Administration. This integration should result in the development of new education and professional training programs, as well as innovative teaching tools that can effectively train end-users (students and professionals) to handle real-world scenarios. In addition, their joint work will lead to the identification of the key elements of cybersecurity education that are relevant to end-users in the context of end-user development and provide examples of practical measures that end-users can take to protect themselves and their technology solutions from cyber-attacks. The aim of this workshop is to create a community for both researchers and practitioners to discuss new ideas and present new research contributions on cybersecurity education.

**Keywords**

Cybersecurity, Education, CSE4IA.

## 1. Introduction

The job market reflects a global supply and demand problem in the recruitment of cybersecurity professionals. Several factors are driving the growth of the cybersecurity workforce, foremost among them the increase in cyber-attacks.

The motivation for cyber-attacks is usually based on criminal intent to cause harm or financial gain. From Distributed Denial of Service (DDoS) attacks to ransomware, threat actors cause a danger to people's safety or lead to compromised intellectual property, either sold on the dark web or used as leverage for ransom.

Consequently, several challenges need to be addressed to increase end-user awareness and education about cybersecurity.

So, it is necessary to investigate how new training modalities and technologies can lead to the education of cybersecurity professionals who can respond to market needs but more importantly bridge the gap between training and business demand. For example, ENISA (European Union Agency for Cybersecurity) provides a common understanding of the relevant roles, competencies, skills, and knowledge required, facilitates recognition of cybersecurity skills, and supports the design of cybersecurity-related training programs. The goal is to help end-users make guided learning choices, understand possible career paths, and, in turn, bridge the gap between professional workplaces and

IS-EUD'23: 9th International Symposium on End-User Development, June 06--08, 2023, Cagliari, Italy

EMAIL: vita.barletta@uniba.it (A.1); danilo.caivano@uniba.it (A.2); federica.caruso1@univaq.it (A.3); sara.peretti@guest.univaq.it (A.4) ; veronica.rossano@uniba.it (A.5)
ORCID: 0000-0002-0163-6786 (A.1); 0000-0001-5719-7447 (A.2); 0000-0002-6167-3896 (A.3); 0000-0001-9784-5816 (A.4) ; 0000-0002-4079-9641 (A.5)

learning environments. In addition, these new training modalities and technologies will lead professionals to a better understanding of cybersecurity risks and the learning of skills required to build secure and resilient technology solutions.

Given these premises, the workshop aims to bring together a community of researchers and practitioners to discuss new ideas for improving cybersecurity training and addressing current market needs. In addition, a key point that should not be overlooked is the digital transformation we are experiencing and the need to be able to securely perform activities that deal with sensitive user data, and how training for public employees is needed to improve and securely perform these activities.

Therefore considering students, professors, and professionals as end-users to be educated in cybersecurity, the workshop intends to discuss a shared understanding between the demand (workplace, recruitment) and supply (qualification, training); increase end-user awareness; support the identification of the critical skills required from a workforce perspective; promote harmonization in cybersecurity education, training, and workforce development.

## 2. Objectives and Topics

In this section, we describe the objectives of the proposed workshop and the topics of interest.

### 2.1. Objectives

The aim of the workshop is to provide a forum for researchers and practitioners to present and discuss current challenges in cybersecurity education to train future cybersecurity professionals but also to be able to train employees of private and public industries on real-world cybersecurity scenarios.

We expect that the workshop will help with:

- the adoption of methodologies, techniques, and tools that support cybersecurity education and the design of cybersecurity-related training programs;
- the identification of methods and tools to support Industry and Academia to collaborate in cybersecurity education;
- the identification of new processes, methods, and techniques to empower end-users development, to set, modify, and increase the security of their technological solutions;
- the proposition of reference taxonomies to characterize the common understanding of the relevant roles, competencies, skills, and knowledge required;
- the design of new techniques to develop cybersecurity competencies for professionals aligned with the European Cybersecurity Skills Framework.

### 2.2. Topics

Topics of interest include but are not limited to, the following:

- Technology-Enhanced Learning for Cyber Security
- Artificial Intelligence for Cyber Security Education
- Virtual reality environments for Cyber Security Education
- Game-based approaches for Cyber Security Education
- Quantum solutions for Cyber Security Education
- Artworks for Cyber Security Education
- Design and implementation of tools, frameworks, and methodologies for Cyber Security Education
- Methodologies for Cyber Security Education in formal and informal contexts
- Innovative technologies to support the identification and articulation of task, competencies, skills and knowledge for professionals cybersecurity
- Explainable Security in Public Administration
- Human, Economics, Ethical, and Legal Aspects in Cyber Security Education
- Innovative programs and training for Cyber Security Education

- Processes, methods and techniques for empowering users to create, modify and tailor technology artefacts taking into account Cyber Security issue
- Case studies and design implications on Cyber Security challenges and practices of end-user development

## 3. Workshop format

The workshop will be held in one single day with a number of sessions varying with respect to the number of accepted papers/talks. The workshop will start with an opening session, in which one of the organizers will introduce the workshop and its schedule. The opening session will be followed by a keynote, given by Luca Viganò (Professor at the Department of Informatics of King's College London and head of the Cybersecurity (CYS) group, and among the most active researchers in the field of Cybersecurity).

Accepted papers will have a different presentation schedule, according to the paper type: regular papers presenters will have 15 min for the presentation + 5 min of Q&A, vision papers 10 min + 5 min Q&A, and presentation abstracts 10 min + 10 min Q&A.

## 4. Paper selection procedure

We will consider three different types of submissions: regular papers, vision papers, and presentation abstracts. Regular papers will be up to 6 pages (not counting references) and will report original research on how cybersecurity and education can support Academia and Industry to reduce the gap between demand (workplace, recruitment) and supply (qualification, training). Vision papers, up to 4 pages (not counting references), will report novel ideas about the application of the role of cybersecurity education in Academia and Industry. Finally, presentation abstracts will report experiences from corporations or previously accepted papers that are relevant to the workshop. Regular and vision papers will be part of the proceedings, while presentation abstracts will not be included in the proceedings.

All papers should be submitted through Easychair in PDF format, using the "CEUR Template".

All papers will be subjected to a thorough peer-review process, with a focus on originality, quality, soundness, and relevance. The workshop will use a double-blind review process, with three members of the program committee reviewing each submitted paper.

Below, important dates for the first submission, notification, and camera-ready are reported:

- Papers submission: May 5th, 2023;
- Papers notification: May 13th, 2023;
- Papers camera-ready: May 17th, 2023.

The program committee members will be chosen from both senior and junior researchers working on the workshop's topics to ensure high review quality and, at the same time, support the integration of junior researchers in the community. We have invited 15 program committee members with a good background in cybersecurity and education. The detailed list of program committee members is reported in Appendix A.

## 5. Workshop Description

Cyber Security Education is gaining more and more importance over the last years. The exponential growth of cyber-attacks and the lack of cybersecurity professionals require new education and professional training programs and innovative teaching tools able to train end-users (students and professionals) on real-world scenarios.

In this scenario, researchers and practitioners are starting to identify new solutions to defend systems and society from cyber-attacks. The human factor is a key element of this context as most attacks are conducted utilizing user unawareness and poor cybersecurity training. Consequently, it is necessary to raise the level of awareness and identify new training programs that can be applied in different contexts

(Academia and Industry). Therefore, the adoption of innovative teaching modalities, tools and frameworks, innovative programs, and cybersecurity training, seems to be one of the most promising ways to reduce the gap between education (Academia) and real-word scenarios (Industry). In addition, these new training modalities and technologies will lead end-users to a better understanding of cybersecurity risks and the learning of skills required to build secure and resilient technology solutions.

## 6. Publicity plans

To encourage people to attend our workshop, we'll send out a call for papers to mailing groups in the cybersecurity and human-computer interaction communities. We also so created a Twitter account (@Cse4ia) to publicize the workshop and reach as many researchers as possible. Additionally, we set up a website (https://sites.google.com/view/cse4ia-23) reporting all the most important information about the workshop.

All IS-EUD participants are welcome to attend the workshop. To assist in the wide dissemination of the accepted contributions as well as the discussion among the participants, we will nominate a person in charge of public relations and content dissemination during the workshop.

Finally, to attract more submissions, we aim to invite all the accepted papers to submit an extended version in the Multimedia Tools and Applications special issue: Cyber Security Education for Industry and Academia (https://www.springer.com/journal/11042/updates/25237732).

## A Program Committee

The confirmed program committee members are:

1) Mario Angelelli, University of Salento
2) Lerina Aversano, University of Sannio
3) Mauro Giuseppe Camporeale, Polytechnic of Bari
4) Dajana Cassioli, University of L'Aquila
5) Enrico Ciavolino, University of Salento
6) Fernando De La Prieta Pintado, University of Salamanca
7) Giuseppe Desolda, University of Bari
8) Roberto Di Bisceglie, EY, Italy
9) Tania Di Mascio, University of L'Aquila
10) Ilenia Fronza, University of Bolzano
11) Antonio Piccinno, University of Bari
12) Giuseppe Pirlo, University of Bari
13) Manuel A. Serrano, Universidad de Castilla-La Mancha
14) Giorgia Specchia, University of Salento
15) Walter Tiberti, University of L'Aquila

## B Organizing Committee

All the organizers have a background in Cybersecurity and Education.

**Vita Santa Barletta** is an Assistant Professor at the Software Engineering Research Laboratory (SERLAB) of the University of Bari Aldo Moro. She received a Ph.D. in Computer Science from University of Bari in 2021. Her research interests include cybersecurity, quantum computing, quantum software engineering, secure software engineering, and secure project management. She contributed to the creation of The Hack Space, the cyber security laboratory of the University of Bari. Contact her at vita.barletta@uniba.it.

**Danilo Caivano** is a Full Professor at the Department of Computer Science of the University of Bari Aldo Moro, and a consultant for companies and organizations, especially in the field of research and development projects. He is the head of SERLAB research laboratory (serlab.di.uniba.it), the director of the Short Master in Cyber Security; he contributed to the creation of The Hack Space, the cyber security laboratory of the University of Bari. He is a member of the Technical Scientific Committee of the Apulian Information Technology District and of the IT Strategic Steering Committee.

**Federica Caruso** is a post-doc research fellow at the Department of Information Engineering, Computer Science and Mathematics (DISIM) of the University of L'Aquila (Italy). She obtained the Ph.D. degree in Information and Communication Technologies (in 2022) and the master's degree in Computer Engineering (in 2018) from the University of L'Aquila. Her primary research interests are in Assistive Technology and Technology-Enhanced Learning. In particular, she is working on methodologies for designing Serious Games and Immersive Virtual Reality-based systems.

**Sara Peretti** is a post-doc fellow at the Center of Excellence DEWS of the University of L'Aquila. She obtained PhD in Neuroscience at the Department of Biotechnological and Applied Clinical Sciences of the University of L'Aquila. She is a psychologist with a long experience in the diagnosis and rehabilitation of children and adolescents with autism. Her main research activity concerns developmental psychology in both typical development and clinical populations, mainly autism spectrum disorders. In particular, she is working on tools, technologies, and methodologies for the evaluation of children and adolescents learning abilities, learning systems, and immersive virtual reality solutions.

**Veronica Rossano** is Associate Professor at the Department of Computer Science at the University of Bari. Her research activities focus on educational technology, to define and validate new IT methods and techniques to support learning and teaching processes, in formal and informal contexts. She is a co-founding member of the TELL (Technology Enhanced Learning Lab) of the UNIBA where she is coordinator of the research on Serious Games and Smart Education technologies. She has been involved in several research projects to coordinate activities on design and develop serious games to address specific problems, the most recent are: Regional Project C-LAB 4.0 – "Competences Lab for Industry 4.0", National Project TALIsMAn: "Personalised care technologies for improving quality of life", National project L.I.F.T.: "Learning Intelligent Factory based on Information Technologies".