Human Factors in Cybersecurity, Vol. 91, 2023, 93–100
https://doi.org/10.54941/ahfe1003723

Enhancing Practical Cybersecurity Skills: The ECSF and the CyberSecPro European Efforts

Nineta Polemi[1,2] and Kitty Kioskli[2,3]

[1]Department of Informatics, University of Piraeus, Piraeus, Greece
[2]Trustilio B.V., Amsterdam, The Netherlands
[3]University of Essex, School of Computer Science and Electronic Engineering, Institute of Analytics and Data Science (IADS), Essex, United Kingdom

ABSTRACT

The accelerated digitalization of all business and industrial sectors (transport, government, health, finance manufacturing) will increase the number, complexity and scale of cybersecurity incidents and their impact on the economy and society. The digital transformation imposes Higher Education Institutions and training providers to enhance their role in preparing the new generation of workforce that will have the capabilities and skills to address the upcoming digital challenges. Training providers need to become the enablers of the digital transformation with the capacity to accommodate different skills needed by the market, to a variety of training specializations. Fostering collaboration with the private sector can be effective in attracting the necessary funding, state-of-the-art technological training tools needed and real-life based training material. In this paper, we describe two recent efforts coming from the European Union targeting to close the gap between the available cybersecurity training and cybersecurity marketing demands, and further analyse the human factors involved in these efforts.

Keywords: Cybersecurity incidents, Digital challenges, Higher education institutions, Training providers, Human factors

INTRODUCTION

As our daily lives and economies become increasingly dependent on digital technologies, we become more and more exposed to cybersecurity threats. Malicious cyber activities not only threaten our economies and the drive to the European Union (EU) Digital Single Market (DSM), but also the very function of our democracies, our freedoms, and our values. Public authorities and businesses in all sectors including vital ones for the economy and society such as automotive, transport, health, defense, telecom, finance, and energy need to be continuously equipped with the latest cybersecurity skills to protect their assets. Enhancing cybersecurity competencies is considered among the highest priorities in European strategies.

EU Higher Education Institutions (HEIs) have more than 142 cybersecurity programs (undergraduate, graduate, and professional). This is demonstrated in various databases, and mappings, such as the European Union Agency

for Cybersecurity (ENISA)/CyberHEAD, Joint Research Center (JRC)/Atlas, and recent European Commission (EC) funded projects (e.g., Sparta, CyberSec4Europe, ECHO, Rewire). Despite these efforts, the cybersecurity skills gap in the EU is increasing; the number of unfilled cybersecurity jobs grew by 350% in the past eight years, and an additional 2.7 million cybersecurity professionals are needed (ENISA report, 2022). Meanwhile, the World Economic Forum indicates the international shortage and highlights that 50% of all employees will need cybersecurity reskilling by 2025. As recommended by ENISA further collaboration among HEIs and the private sector is needed to address the cybersecurity market challenges and the associated industrial demands.

The existing EU programs are part of the academic rigid, static programs that cannot properly address hands-on dynamic capabilities, and emerging cybersecurity hard and soft skills needed in the market. Upskilling the existing workforce and developing a new one capable of promptly responding to future challenges in specialised industrial security domains and knowledge areas has become an urgent need. ENISA has recently published the European Cyber Security Skills Framework (ECSF) where 12 professional cybersecurity profiles have been identified and analysed in order to bridge the EU training supply with the marketing demands.

Building upon the traditional trust and societal respect of the HEIs, the enhanced, inclusive HEIs can become the main drivers towards digital transformation and the main contributors in putting into practice the new ECSF and the EU strategies (e.g., new EU Cybersecurity Strategy, Shaping Europe's Digital Future, the EU Security Union Strategy). Fostering collaboration of the HEIs with the private sector will provide the necessary boost to sustainable and effective practical cybersecurity training programs. This will be based on state-of-the-art technological training tools (e.g., simulation platforms, cyber ranges, cloud capabilities, large easily accessible computing power), real-life-based training material and digitally driven pedagogical approaches. This approach is adopted in CyberSecPro, a European project funded by the Digital Europe Programme (DEP) involving 16 HEIs and 12 SMEs from 14 EU Member States, Norway and Serbia.

The present paper will first present the structure, objectives, and characteristics of the ECSF. Then the adopted approach of the 'Collaborative, Multi-modal and Agile Professional Cybersecurity Training Program for a Skilled Workforce In the European Digital Single Market and Industries' (CyberSecPro) project will be outlined in offering hands-on and working-life skills. The paper concludes by reporting future activities and directions in the EU's efforts to enhance cybersecurity capabilities in meeting market needs, while considering human factors in the training design decisions.

THE EUROPEAN CYBERSECURITY SKILLS FRAMEWORK (ECSF)

There are more than 142 cybersecurity training programmes offered in 26 EU Member States and there are various efforts to identify the training supply in the EU. For example, ENISA has developed and operates the Cyber

Higher Education Database (CyberHEAD) that most programmes have been registered with. CyberHEAD serves also as a tool that offers search possibilities and many filters to help students find the programme that suits their interests. The Digital Skills and Jobs Platform is the place where all European initiatives and policy actions on digital skills including cybersecurity skills can be found.

Most EC institutions and agencies (e.g., DG CONNECT, EEAS, DG GROW, DG MOVE, DG HOME, EASME JRC, ENISA, Europol) contribute towards enhancing cybersecurity capabilities. However, the training supply does not address the dynamic marketing demands on cybersecurity skills and capabilities. The existing EU training offers are fragmented and non-harmonised, for example, they do not have a common curriculum or comparable syllabus. Emerging technologies (e.g., IoT, AI, blockchain, satellite, 6G) are being adopted by the market at astonishing rates, finding employees unprepared to manage their new cybersecurity challenges. The training supply is not dynamic enough to process the deployment of the new technologies.

Notably, there are various international efforts in developing effective cybersecurity skills frameworks to contribute towards bridging the gap between training supply and market demand including:

- The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework developed by the National Institute of Standards and Technology in the US.
- The Cybersecurity Body of Knowledge (CyBOK) was developed by the UK National Cyber Security Program and the University of Bristol (Rashid, A. et al., 2018).
- The Cybersecurity Curricula framework (CSEC2017 Joint Task Force, 2017), developed by the Association for Computing Machinery (ACM) in collaboration with the IEEE Computer Society (IEEE-CS), the Special Interest Group on Information Security and Privacy of the Association for Information Systems (AIS SIGSEC), and the Committee on Information Security Education of the International Federation for Information Processing Technical (IFIP WG 11.8).
- The National Infocomm Competency Framework (NICF) - Singapore, that is part of the Singapore Workforce Skills Qualifications (WSQ) system and was developed by SkillsFuture Singapore (SSG), Infocomm Media Development Authority (IMDA) and other strategic stakeholders in the IT industry (Jones, K., et al., 2018, Cybersecurity Workforce Study, 2021).
- The SPARTA Cybersecurity Skills Framework, published by the EC project SPARTA in 2020, is a NICE-based framework (SPART Skills Framework, 2019).
- The ACM Skills framework entitled: "The Core Cyber-Defense Knowledge, Skills, and Abilities That Cybersecurity Students Should Learn in School: Results from Interviews with Cybersecurity Professionals" (Jones, K., et al., 2018)
- The "Cyber Security Skill Set Analysis for Common Curricula Development" (Yamin, M.M. and Katt, B., 2019).

However, these skills frameworks are not based on standards and do not address the specificities and structures of the national markets. ENISA assessed the above frameworks and has recently published the European Cyber Security Skills Framework (ECSF) where 12 professional cybersecurity profiles have been identified and analysed based on the EN 16234-1:2019 e-Competence Framework (e-CF) standard.

It was realised that the main reason for the cybersecurity skills gap is the lack of common terminologies and taxonomies. ECSF provides a taxonomy of terms; in particular, all 12 profiles hold a main label where synonymous labels found in the market reflecting the same capabilities are merged.

ECSF addresses the needs of the EU DSM since it adopts a simple structure. The main characteristic of the DSM that ECSF considered was the fact that the majority (99%) of the enterprises in the DSM are SMEs and MEs (23 million were reported in 2022 EU Statistics on SMEs/MEs) with minimum resources and cybersecurity awareness as reported in (EU SMEs cybersecurity awareness - ENISA report). That was a main requirement considered in the design of ECSF and it was addressed by providing a simple structure of the framework aligning the main activities in securing an enterprise with the professional profiles.

In particular, the 12 profiles follow the lifecycle of the cybersecurity practices that consists of the following four (4) phases (see Figure 1):

- **Plan**: Where the cybersecurity management (e.g., governance, risk assessment/management) is set up. In this phase four (4) professional profiles are mapped: CISO, Compliance Officer, Risk Manager, and Architect.
- **Implement**: Where cybersecurity mitigation actions (controls, procedures, actions) are being developed, implemented and trained. In this phase two (2) profiles are being mapped: Architect and Educator.

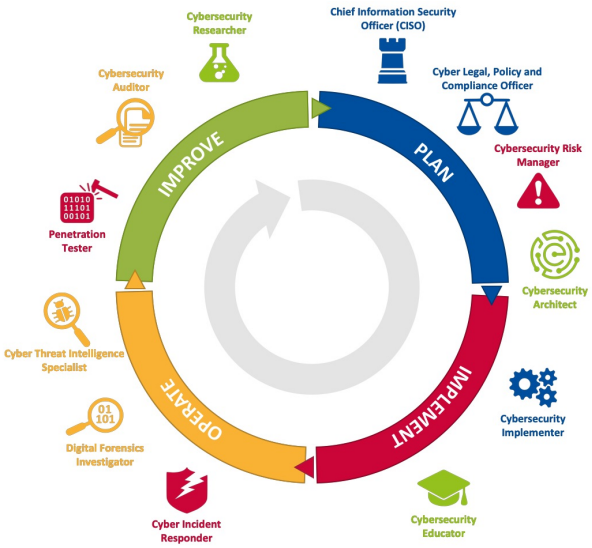

Figure 1: Cybersecurity phases and profiles (European cybersecurity skills framework).

- **Operate**: Where cybersecurity procedures/controls/functions/mechanisms are being operated. In this phase three (3) profiles are being mapped: Cyber threat intelligence specialist, Digital forensic investigator, and Cyber incident responder.
- **Improve**: Where actions take place in order to improve cybersecurity. In this phase the three (3) profiles are mapped: Auditor, Tester, and Researcher.

The description of every profile has two (2) parts (see Figure 2) that connect the marketing needs (left hand side) with the training offer (right hand side).

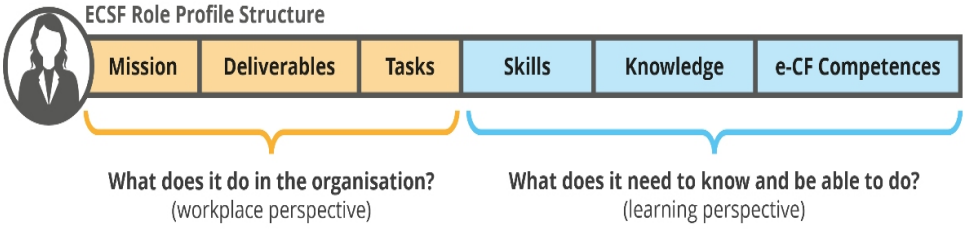

Figure 2: Cybersecurity profile structure (European cybersecurity skills framework).

The role profiles described in ECSF will be used to develop a comprehensive, flexible, and homogeneous curriculum guidance for academic institutions and training providers. The latter will encourage the mobility of expertise and it will help students to make guided learning choices and understand the possible career paths, and so bridge the gap between a professional workplace and learning environments.

THE CYBERSECPRO PROJECT

The implementation of the ECSF framework requires further analysis, scaling and harmonisation of the skills, knowledge areas and competencies reported and needed for each profile and CyberSecPro aims to contribute towards these needs. The EC funded project entitled "Collaborative, Multi-modal and Agile Professional Cybersecurity Training Program for a Skilled Workforce in the European Digital Single Market and Industries" (CyberSecPro) is a three-year project started on December 1st, 2022. The ambition of the project is to enhance the role of the HEIs to dynamic innovative training hubs offering skills to undergraduate and graduate, students, professionals, lifelong learners, and comebacks.

CyberSecPro project intends to drive a trustworthy digital transformation and equip the workforce with the necessary capabilities, and hard and soft skills to address the digital challenges and be able to meet the requirements of the ECSF cybersecurity professional profiles. Sixteen (16) HEIs and twelve (12) SMEs from fourteen (14) EU countries, Norway and Serbia are the members of the consortium that propose the agile CyberSecPro professional cybersecurity practical and hands-on training program that will complement, support, and advance the existing academic programs by linking innovation,

Figure 3: CyberSecPro human-centric solution approach to key challenges.

research, industry, academia, and SME support. CyberSecPro aims to bridge the gap between degrees, working life and marketable cybersecurity skill sets necessary in the digitalization efforts and become the best practice for all cybersecurity training programs. The project adopts a human-centric approach as described in Figure 3.

The members of the consortium will utilise their existing experience in cybersecurity training, and they will reach a consensus on formulating a common syllabus for the various training modules (e.g., courses, summer schools, hackathons, seminars, cyber exercises) that will be formulated during the project. The cybersecurity tools offered by the SMEs of the project will become part of the syllabus, pedological methodology, and training offerings.

The HEIs and SMEs involved in the CyberSecPro consortium will build Public Private Partnerships (PPPs) to ensure the sustainability of the practical CyberSecPro training modules that will be developed and offered. The project has identified the knowledge areas that the training modules will cover and the tools that will be considered for using during the trainings (described in Table 1).

This bundle of CyberSecPro training modules that will be developed will help the HEI and training providers to adopt them, all of them or individual modules, to enhance their cybersecurity curricula. The harmonisation of the syllabus will lead to harmonised curricula and enable the mobility of cybersecurity expertise in the EU.

CONCLUSION AND FUTURE WORK

ECSF and CyberSecPro described in this paper are recent EU efforts that aim to better prepare individuals for a trustworthy digital transformation while serving people, businesses and working life communities preserving their democratic, cultural, ethical values and rights. The implementation and trials of the applicability of ECSF will start in the second quarter of 2023. Already ENISA has invited experts from all EU Member States to assist ENISA in the integration and future development of the ECSF involving EU communities to further promote the alignment of the cybersecurity competencies by adopting

Table 1. Sample CyberSecPro training areas and tools.

CyberSecPro Knowledge Areas	CyberSecPro interactive e-tools
Practical, human-centric risk assessment/treatment, conformity assessment	CTM, CSAM, SIRA, Human-SM, CTM
Compliance with regulations and standards	C2M and open-source tools for compliance developed by the Sentinel, Cyrene and Cyberwatching.eu projects
Human Factors/Societal Security	Human-RM, Digital TORC
Privacy & Accountability Practice by Design (Including AI, IoT, Blockchain)	CodeWeTrust, CSAM
Malware & Attack Technologies	Cuckoo sandbox, FP_TTX, FP_CDX,
Security Operations & Incident Management in Practice	Digital TORC, SIRA, FP_TTX
Digital Forensics Investigations	SANL-CR
Operating Systems/ Virtualization & Connection Security	Digital TORC, AIT-IEA
Distributed Systems Security	nmap, IDA, Cuckoo,
Software Security and Privacy by Design	ICA, Codewetrust, FP_CDX,
Web & Mobile Security	Axiom, FP_CDX,
Network Security	Nmap, ITML-TT
Cyber/ Physical Systems Security	AIT-IEA, Cuckoo, oletools, SmartViZ

the ECSF. The ECSF will also become the foundation of the EU Cybersecurity Skills Academy, a future EU initiative under the "Promoting our European way of life" strategic priority (European Cybersecurity Skills Framework).

The CyberSecPro project will embrace and contribute to the ECSF implementation by harmonising and making it as practical as possible the cybersecurity trainings. The training modules and mechanisms that will be developed will close the training supply and cybersecurity marketing demands, better preparing the new workforce. CyberSecPro will serve as best practice in upgrading the HEI to serve the needs of the digital transformation by establishing PPPs with the private sector involving entrepreneurship deeply into the educational system to offer as practical cybersecurity trainings as possible.

ACKNOWLEDGMENT

The research conducted in this paper was funded by the project 'A Dynamic and Self-Organized Artificial Swarm Intelligence Solution for Security and Privacy Threats in Healthcare ICT Infrastructures' (AI4HEALTHSEC) under grant agreement No 883273. The project was funded by the European Union's Horizon 2020 research and innovation programme. The authors are also grateful for the financial support provided for the 'Collaborative, Multimodal and Agile Professional Cybersecurity Training Program for a Skilled Workforce In the European Digital Single Market and Industries' (CyberSecPro) project. This project has received funding from the European Union's Digital Europe Programme (DEP) programme under grant agreement No 101083594. Special thanks to the partners of these projects and their contributions. The authors would also like to thank the European Union Agency

for Cybersecurity (ENISA), especially Dr Fabio di Franco and the members of the AHWG, for developing the ECSF, where the first author had the honour to serve as rapporteur. The authors would also like to express their gratitude to the University of Piraeus Research Center (UPRC) for its continuous support. Lastly, the views expressed in this paper represent only the views of the authors and not of the European Commission, or the partners in the above-mentioned projects, or University of Piraeus, or UPRC, or University of Essex, or trustilio B.V.

REFERENCES

(ISC) 2 Cybersecurity Workforce Study "A Resilient Cybersecurity Profession Charts the Path Forward" (2021). Available at: https://www.isc2.org/Research/Workforce-Study.

CYBERHEAD – ENISA Cybersecurity Higher Education Database. Available at: https://www.enisa.europa.eu/topics/education/cyberhead.

ENISA report "Addressing the EU cybersecurity skills shortage and gap through higher education." (2022). Available at: https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education/@@download/fullReport.

ENISA report – EU SMEs Cybersecurity awareness (no date). Available at: https://www.enisa.europa.eu/topics/cybersecurity-education/sme_cybersecurity.

EU institutions and bodies profiles (no date). Available at: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles_en.

European Cybersecurity Skills Framework (ECSF). Available at: https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework.

ISACA Research Study Report - State of Cybersecurity 2021. Available at: https://www.isaca.org/go/state-of-cybersecurity-2021.

Jones, K., Namin, A. and Armstrong, M. (2018) The Core Cyber-Defense Knowledge, Skills, and Abilities That Cybersecurity Students Should Learn in School: Results from Interviews with Cybersecurity Professionals, ACM, Volume 11, Issue 3.

Jones, K. S., Namin, A. S. and Armstrong, M. E. (2018). "The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school," ACM Transactions on Computing Education, 18(3), pp. 1–12. Available at: https://doi.org/10.1145/3152893.

Rashid, A. et al. (2018). Scoping the Cybersecurity Body of Knowledge, IEEE Security & Privacy, Volume: 16, Issue: 3.

SPART Skills Framework (2019). Available at: https://www.sparta.eu/assets/deliverables/SPARTA-D9.1-Cybersecurity-skills-framework-PU-M12.pdf.

Statista (2022) Number of SMEs in the European Union 2008-2022, by size. Available at: https://www.statista.com/statistics/878412/number-of-smes-in-europe-by-size/.

The Digital Skills and Jobs EU Platform (no date). Available at: https://digital-skills-jobs.europa.eu/en/about/digital-skills-and-jobs-coalition.

The Workforce Framework for Cybersecurity (NICE Framework) (2023). Available at: https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/workforce-framework-cybersecurity-nice.

Yamin, M. M. and Katt, B. (2019). "Cyber security skill set analysis for common curricula development," Proceedings of the 14th International Conference on Availability, Reliability and Security [Preprint]. Available at: https://doi.org/10.1145/3339252.3340527.