Enhancing a cybersecurity curriculum development tool with a competence framework to meet industry needs for cybersecurity

Anne-Maarit Majanoja
amtmaj@utu.fi
University of Turku
Turku, Finland

Antti Hakkala
ajahak@utu.fi
University of Turku
Turku, Finland

ABSTRACT

Current and emerging cybersecurity and computing professionals must manage their competencies and skills according to current job market needs, including formal education, professional certifications, and experience. Recent studies show that cybersecurity skills will be in high demand in the industry in the coming years. There is currently a significant gap between available jobs and the skills of suitable candidates, and existing software engineering and cybersecurity training has an important role to play in addressing this. This puts pressure on cybersecurity education providers, such as universities, to align with industry needs and develop the content of cybersecurity courses and curricula more systematically based on business needs. We asked 88 Finnish IT professionals working in software development and cybersecurity how much time they spend developing their skills in a year, what types of training they use, and what topics they need more training on, in order to understand the industry's security assurance training needs and the level of competence required. The solution to systematically develop cybersecurity course and curriculum content is to create a planning framework that combines the European Cybersecurity Taxonomy and the European Cybersecurity Skills Framework, including the e-Competence level, and university course content, to identify role-based training needs and gaps in course content.

CCS CONCEPTS

• **Security and privacy** → Software security engineering; • **Social and professional topics** → **Software engineering education**; • **Applied computing** → **E-learning**;

KEYWORDS

Education, Cybersecurity, Industry survey, Training times and needs, Planning Framework, Curriculum and course development

ACM Reference Format:
Anne-Maarit Majanoja and Antti Hakkala. 2023. Enhancing a cybersecurity curriculum development tool with a competence framework to meet industry needs for cybersecurity. In *International Conference on Computer Systems and Technologies 2023 (CompSysTech '23), June 16–17, 2023, Ruse, Bulgaria.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3606305.3606325

CompSysTech '23, June 16–17, 2023, Ruse, Bulgaria
© 2023 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-0047-7/23/06.
https://doi.org/10.1145/3606305.3606325

1 INTRODUCTION

The rapid changes in technologies, practices, and requirements in the IT sector place different demands on the skills and competences that both organizations and individuals need to stay in business or in the labor market. Successful cybersecurity assurance requires up-to-date competences at both organizational and individual levels. Today, the most valuable and versatile asset of any organization is its skilled workforce [3].

Cybersecurity is becoming more diverse every day and is an integral part of software development. With cybersecurity, new professional responsibilities and roles are emerging with different competence levels and needs. Recent research shows a need for cybersecurity professionals in the private and public sectors [11]. However, finding skilled cybersecurity professionals is challenging, and educational institutions, such as universities, have a major role to play in producing cybersecurity skills to meet industry needs. The education sector is responding to this need by publishing cybersecurity-focused training programs and modifying or developing their existing training programs to meet industry expectations [19]. In many cases, the course content is the cybersecurity teacher's 'best guess', which is often sufficient, but the course content may be missing essential elements that are relevant to those working in the industry. The challenge is that there are currently no effective tools for designing and evaluating the content of university education that also takes into account the level of cybersecurity skills required by industry. Previous research [18] examines education based on the US National Cybersecurity Workforce Framework (NIST) [15] [16], but whether this reflects the European situation and needs is questionable.

In this paper, we examine how much time Finnish software developers spend on security assurance training in a year, what types of training they use, and what topics they need more training on, in order to understand the industry's security assurance training needs and the level of competence required, and how these needs can be better addressed in cybersecurity education and curricula at university level. As a solution, we propose a planning framework that combines the European Cybersecurity Skills Framework (ECSF) [4] with the e-Competence proficiency level [6] and the European Cybersecurity Taxonomy (ECT) [5] and university cybersecurity courses to identify possible gaps and priorities in course and curriculum content.

2 LITERATURE REVIEW

The following search terms "skills" and "cybersecurity" or "cyber security" and "skills" and "education" and "curriculum" were chosen in the ACM Digital Library database to find recent research on cybersecurity skills development and education. The found articles were reviewed with the following inclusion criteria: the language used was English, the type of text was a scientific article (e.g., dissertations were excluded), the article was related to cybersecurity competence development or education development, and it was published between 2018-2023. Initially, the total number of articles found was 1813, then the articles were eliminated to 25 on the basis of the title and abstract, and then the elimination was done on the basis of the full article, leaving 11 articles for final evaluation of previous research (article id: 1, 2, 7, 10, 12, 14, 17, 18, 20, 21, 22).

Based on previous research, the role of professional certifications in computing occupations is highly valued, but the value is often based on the quality of the certification, with less well-known certifications being undervalued [20]. It also states that those with computer and mathematical degrees are the largest group, by formal education, holding certifications or licences. In particular, cybersecurity certifications are required to perform two main job roles: technical and managerial [22]. Research also brings a lengthy debate on industry requirements for Higher Education (HE) providers to provide graduates with required work skills and whether HE providers are able to prepare students to meet the new role requirements [10].

Several studies have highlighted the need for cybersecurity professionals, and the field has broadened beyond technical aspects to include also human factors, business processes and law [14]. The gap between available jobs and suitable candidates is significant. This creates demands, but also new opportunities for HE to increase diversity in cybersecurity. The need for security in computer science curricula has been steadily increasing and previous research shows that cybersecurity is now used as an umbrella term for a wide variety of similar disciplines, similar to 'engineering' and 'computer science' [17]. They [17] also suggest that cybersecurity should be formally characterized by a generic competency model to improve clarity and maturity, resulting in improved standards and objectives of cybersecurity programmes. In addition, IT educators are constantly reviewing and revising curricula to produce graduates who are ready for the ever-evolving workplace and industry roles [10]. However, these industry roles are not always clear to academia.

In order to ensure and build workplace relevance into HE, some researchers have developed their own set of requirements, for example based on cybersecurity certifications [22], for the assessment and development of cybersecurity curricula. And some researchers propose to use existing frameworks for the evaluation and development of cybersecurity education, such as the NICE framework [18], yet they found that when they evaluated the curricula based on NICE, not all categories/topics were implemented equally. In their research [18], they also found that the European Union Cybersecurity Taxonomy has been published, which can provide a way of classifying the cybersecurity industry sectors. To reduce the skills gap, the use of competency models has been proposed [2] However, the characteristics of competency models in relation to the cybersecurity domains are not well understood. In addition, the proposed models do not cover all the topics specified by the Cybersecurity Body of Knowledge [21]. Many models reduce the competency profile of a security expert to professional competencies. Alongside different models and frameworks, a typical approach in previous studies is to present an implementation solution for a particular course [12] or an existing cybersecurity programme by listing the courses and overall statistics of the programme [1], or approached by addressing digital tools or technologies to help teachers train specific cybersecurity competencies [7].

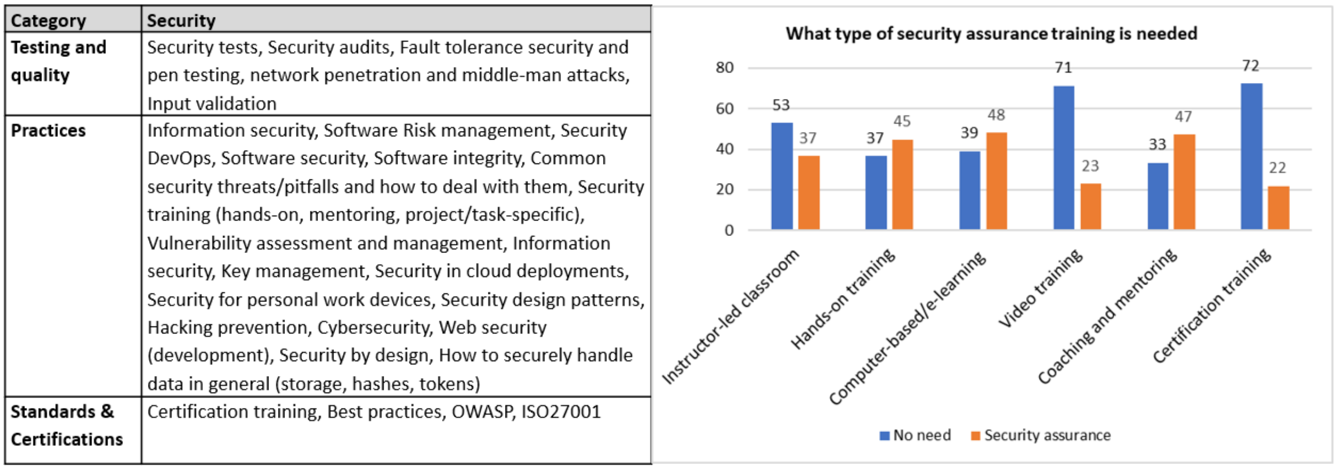
As can be seen from previous research, various methods and frameworks are used to develop cybersecurity education and curricula to ensure the accuracy and timeliness of the content. The aim is to incorporate industry requirements into course content delivery through methods and frameworks. Many of the frameworks are US based (e.g. NIST) and may not be sufficiently linked to work roles or requirements that would be applicable to European practice and cybersecurity education. The European Cybersecurity Skills Framework (ECSF) is developed by the European Union Agency for Cybersecurity (ENISA) [4]. The ECSF provides the first European framework and definitions for cybersecurity professionals. 12 role profiles are identified and the framework identifies the required key skills, knowledge, tasks and competencies. The ECSF framework is closely linked to the European e-Competence Framework (e-CF) [6], which is a common European framework for ICT professional competences, knowledge and skills, addressing the competences required and applied in the workplace [4]. The e-CF defines competence as a demonstrated ability to apply knowledge, skills and attitudes for achieving observable results [6]. There are five defined e-CF levels (e-1 to e-5), referencing 41 competencies as applied in ICT. For each cybersecurity role, a set of applicable e-CF was selected to be included in the ECSF role description. These e-CF levels define influence, complexity, autonomy, and behavior of the competence attainment [6]. Initial attempts to integrate the ECSF into curriculum design have already been published [8], but their approach lacks the ability to assess the content coverage of curricula for a specific cybersecurity role.

The European Cybersecurity Taxonomy (ECT) [5] was developed by the Joint Research Centre of the European Commission as a tool to categorize institutions and expertise across Europe. It is based on four dimensions: technologies, domains, sectors and use cases. This taxonomy provides clearer categorisations of topics required for cybersecurity skills and can be used for content design. In this paper, as a solution for the development of cybersecurity curricula and course content, we have used the domains of the ECSF, the e-CF and the ECT.

3 NEED OF SECURITY ASSURANCE TRAINING – INDUSTRY SURVEY

To get a starting point in addressing the raised issue, we conducted an industry survey that aims to provide insight to what software engineers in industry need in security training. Data from such surveys can be used to ensure that the needs of industry stakeholders are also considered when making future education investments and development in universities.

The survey targeted Finnish software engineers, software developers and others directly involved in software development processes. Software developers' role included also security related responsibilities. The survey focused on quality, security and privacy assurance practices. In this paper we focus only on the security aspects. The background information of the respondents was obtained by including some structured questions about work experience, role, company size, age, application area, and business sector.



Category	Security
Testing and quality	Security tests, Security audits, Fault tolerance security and pen testing, network penetration and middle-man attacks, Input validation
Practices	Information security, Software Risk management, Security DevOps, Software security, Software integrity, Common security threats/pitfalls and how to deal with them, Security training (hands-on, mentoring, project/task-specific), Vulnerability assessment and management, Information security, Key management, Security in cloud deployments, Security for personal work devices, Security design patterns, Hacking prevention, Cybersecurity, Web security (development), Security by design, How to securely handle data in general (storage, hashes, tokens)
Standards & Certifications	Certification training, Best practices, OWASP, ISO27001

Figure 1: Needed security assurance training topics and type of training

The questionnaire was tested with a pilot group of 18 international participants and some corrections were made to the wording and terminology of the questions based on the feedback. The research was conducted both as an invitation-based online survey and by sending personal email invitations. The survey was open from mid-October 2019 until the end of February 2020. A total of 88 valid responses were received. The open link approach was the most productive, as approximately 71 % of the responses were received using the public web link to the survey.

Respondents are generally highly experienced IT professionals and work in different organisations. The range presumably reflects the current structure of Finnish software companies, as presented in Table 1. About 69 % of companies delivered to the private sector and 43 % to the public sector.

The results show that IT professionals have not spent much time on security assurance training during the year. Looking specifically at the security responses, 38 % of respondents did not study security topics at all, 41 % spent only 1-3 days on security and only 20-30 % spent more than 1-3 days on security training in a year. Interestingly, there was little correlation between company size, age or employee experience in terms of time spent on training.

The most commonly used type of training was internal training. Computer and e-learning solutions were the most frequently used forms of learning. Based on the open field responses, internal training included approaches such as company internal training materials/learning platforms, team training and self-learning. A positive correlation was found between security and internal training (0.212). This may indicate that security topics are often studied and addressed through internal training that is tailored to the company’s practices and needs. 26 % of respondents had not taken any internal training in the last year and 52 % of them worked in a company with less than 50 employees. This suggests that internal training is more likely to be used in larger organisations. External instructor-led training was not widely used and 60 % of respondents had not attended any such training in the past year. Only 20 % had attended external instructor-led training and 80 % of these worked in a company with more than 100 employees.

Table 1: Survey respondent statistics

Developer’s experience (years)	Company size (persons)	Company age (years)
<1: 3 %	<10: 10 %	<4: 11 %
1-5: 22 %	10-50: 22 %	5-9: 13 %
6-10: 16 %	51-100: 13 %	10-14: 16 %
11-15: 13 %	101-250: 9 %	15-20: 13 %
>16: 46 %	>250: 44 %	>20: 47 %

Only 2 % had security certification (e.g. SSCP, Systems Security Certified Practitioner) and 89 % of respondents had not used any type of certification training and 72 % did not see the need for certification training in the future. Only 33 % of the IT professionals had any kind of professional certificate (e.g., project management/Scrum, quality and testing, technology related). This discovery of certificates and the lack of need for them is surprising, as professional certificates are highly valued in the security sector as a means of demonstrating not only educational but also professional competence.

As seen in Figure 1, the most preferred forms of training were e-learning, coaching and mentoring, and hands-on training. The topics that the respondents identified as necessary or highly beneficial to their own work are also shown. The training form preferences correspond with the required competence level of the topics, as more advanced concepts and themes require more experienced instructors/mentors that can be interacted with, preferably in person.

It was found that training needs varied somewhat by company size. Smaller organisations (under 50 employees) had very direct practical needs, such as software and system testing, security testing, privacy and data protection, DevOps, development best practices, test-driven development, requirements and risk management. Medium-sized companies (less than 250 employees) had more practical needs, such as test automation, project management practices,

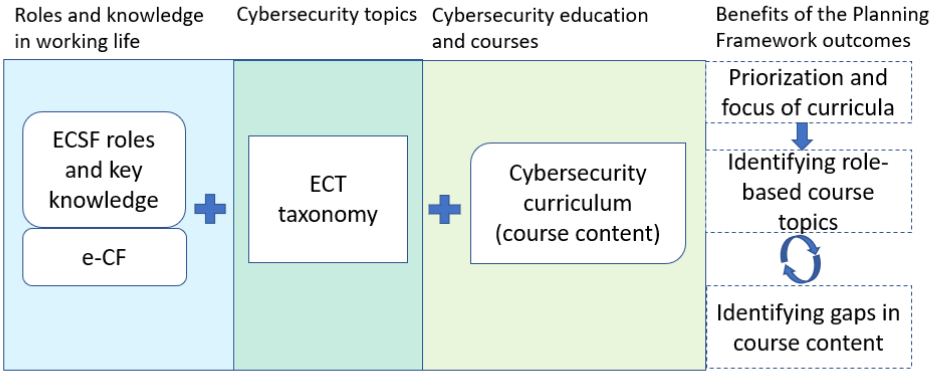

Roles and knowledge in working life
Cybersecurity topics
Cybersecurity education and courses
Benefits of the Planning Framework outcomes
ECSF roles and key knowledge
e-CF
ECT taxonomy
Cybersecurity curriculum (course content)
Priorization and focus of curricula
Identifying role-based course topics
Identifying gaps in course content

Figure 2: Incorporating the ECSF roles and key knowledge, ECT taxonomy and cybersecurity curriculum.

software lifecycle models, certification types of training, vulnerability assessment, security design patterns and OWASP (The Open Worldwide Application Security Project). Large companies (250+ employees) also had SAFe (Scaled Agile Framework), clear code practices, exploratory testing, CMMI (Capability Maturity Model Integration), ISO security standards, continuous delivery and monitoring, input validation, common pitfalls, PMBOK (Project Management Body of Knowledge), accessibility testing and audits. A clear difference in required competence levels can be found between training needs of different sized companies, where larger organizations favor strategy and executive leadership levels, whereas smaller organizations are more implementation oriented.

The results of the survey show that students moving into security roles need to be persuaded to maintain their skills once they enter the workforce. The software and security industry is changing so rapidly that those who do not actively update their skills can be left behind. Universities should ensure that this message is delivered as part of their courses and education. These survey results also provide direct feedback and insight into the training needs and methods used by those working in organisations. The training needs highlighted in the survey often relate to the most basic skills, but should be addressed in some way as part of the studies. There might be a question as to whether there have been shortcomings in the definition of the content of the courses. It is possible that the content of cybersecurity education offered at universities should be more systematic, and that the content of courses should provide different skills and competencies for different roles in the cybersecurity industry.

4 PLANNING FRAMEWORK - SYSTEMATIC APPROACH TO COURSE CONTENT DEVELOPMENT

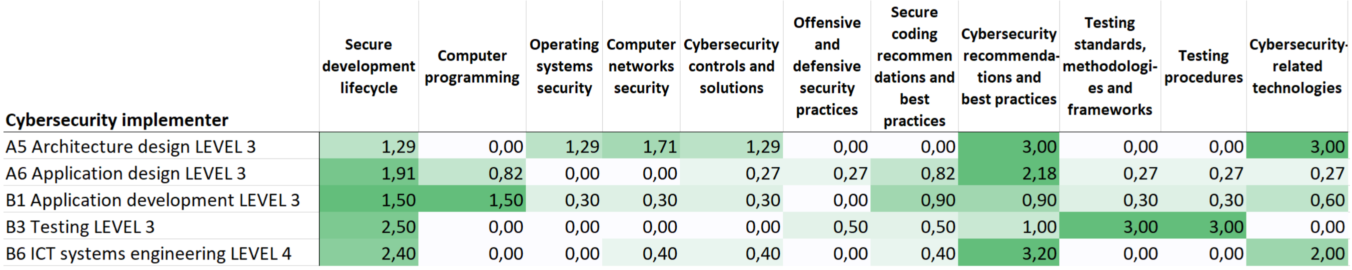
In order to determine the content of cybersecurity education and courses in a more systematic way, a tool is needed that helps to examine and identify possible shortcomings, but also to highlight which competence area(s) the learning outcomes of the course are aimed at in working life. Our solution is to implement a Planning Framework that links ECSF roles and key knowledge, including the e-CF for prioritisation, and the ECT taxonomy to a university cybersecurity curriculum. This systematic approach highlights potential gaps in course content. It also allows for the prioritization and focus of cybersecurity education.

Our Planning Framework [9] (Figure 2) is designed to help universities develop cybersecurity curriculum that provides key knowledge and skills for each role profile, based on a European standard ECSF on common terminology, key skills, knowledge and competences. The ECT taxonomy provides a clear categorisation of the topics that are necessary for cybersecurity skills and can be used in the design of the course content. External resources, such as the Cybersecurity Body of Knowledge [21], can be used to enrich the ECSF framework and the ECT taxonomy.

The idea is to map existing course content to the ECT categories. This will show which topics are already covered and how well the courses cover the whole field of cybersecurity. Weights based on course level (e.g. basic, intermediate or advanced) and type (e.g. practical vs. theoretical) and learning objectives can be added by the responsible teacher.

The Planning Framework then combines the ECT with key knowledge items defined for each ECSF role, thus also mapping course content to roles via the taxonomy. In addition, the ECSF integrates the e-CF levels for each key knowledge, giving us a tool for designing a cybersecurity curriculum that ensures key knowledge items are present in proper depth in the curriculum. In previous research where ECSF has been used, e-CF has not been mapped into the construction of the course content [8], because e-CF is perceived as difficult to map into the course content. Mapping e-CF directly into existing curricula can be challenging, but in our Planning Framework, mapping through ECT allows us to look at content at competency levels in addition. The e-CF gives a certain weighting to the contents of the ECT. Higher levels of competence can only be achieved through work experience, but the focus allows teachers to emphasise certain aspects of the cybersecurity course content.

In Figure 3 we show how the e-CF competences can be integrated to our Planning Framework. The mapping is done through matching ECSF role key knowledge items to e-CF knowledge with weight corresponding to the competence level (1-5). In the mapping we take the key knowledge items for the ECSF cybersecurity implementer role and compare them against the e-CF knowledge



Cybersecurity implementer	Secure development lifecycle	Computer programming	Operating systems security	Computer networks security	Cybersecurity controls and solutions	Offensive and defensive security practices	Secure coding recommendations and best practices	Cybersecurity recommenda- tions and best practices	Testing standards, methodologi- es and frameworks	Testing procedures	Cybersecurity-related technologies
A5 Architecture design LEVEL 3	1,29	0,00	1,29	1,71	1,29	0,00	0,00	3,00	0,00	0,00	3,00
A6 Application design LEVEL 3	1,91	0,82	0,00	0,00	0,27	0,27	0,82	2,18	0,27	0,27	0,27
B1 Application development LEVEL 3	1,50	1,50	0,30	0,30	0,30	0,00	0,90	0,90	0,30	0,30	0,60
B3 Testing LEVEL 3	2,50	0,00	0,00	0,00	0,00	0,50	0,50	1,00	3,00	3,00	0,00
B6 ICT systems engineering LEVEL 4	2,40	0,00	0,00	0,40	0,40	0,00	0,40	3,20	0,00	0,00	2,00

Figure 3: Illustration of e-Competence mapping to key knowledge areas for cybersecurity implementer ECSF role.

examples for each competence assigned for the role. Each e-CF knowledge example can match to any number of key knowledge areas, and the normalized, weighted count of matches is shown in the Figure 3.

Subsequently, we can map competences to curriculum content though the mapping between competences, role key knowledge, taxonomy and course content. This would not be possible without the ECT, which we use to connect these different models. Now it is possible to both evaluate how suitable an existing cybersecurity curriculum is for educating students to specific ECSF roles, and to evaluate what are the essential building blocks for a solid cybersecurity curriculum that targets key ECSF roles.

Future work. Now that we have established a connection between educational content and role-based competence levels, the next step is to assess an existing curriculum to see how the addition of e-competence levels reflect on the educational content. The results can be then further used to build more targeted courses and curricula for specific needs, including continuous learning courses for software engineering and cybersecurity professionals.

5 DISCUSSION

Although cybersecurity education emphasized security concepts and secure coding practices, general software engineering education conveys the necessary building blocks for developers. The lack of generic programming knowledge items in the ECSF framework is explained by the fact that a basic knowledge and understanding of software development and coding practices is needed for most security roles. The further the developer ventures into the realm of secure development, both software development and security become increasingly important. Thus, for example, the descriptions of the e-CF standard are not directly applicable to cybersecurity roles, but are very valid for building the basic knowledge through software engineering competences and thus also for cybersecurity education. It would be prudent to have a major subject of secure software development within universities that offer software and cybersecurity engineering education.

The answers to needed security topics and training modes in Figure 2 are in line with our assessment that universities currently provide the fundamental knowledge and competences, but when experience accumulates and responsibilities and organizations grow, so do the required competences. While a student with no work experience may prefer to work alone and avoid reflection with their peers, the further we go into more demanding competence levels, the more hands-on training, mentoring and reflection gain traction.

The results of the industry survey on the lack of competence development and certifications also raise the question of whether students are too confident that a Master's degree is sufficient without the need for further formal study or certifications while working. Cybersecurity is a specialized field that requires a theoretical background and practical experience. Therefore, the levels of competence and degrees defined in the standards or frameworks do not correspond to practice. For example, an undergraduate or graduate degree does not directly guarantee the ability to perform cybersecurity activities at the e-CF 3-5 levels.

It is important for students to understand that cybersecurity and software engineering as fields are changing so rapidly that formal maintenance of competencies and development of practical skills throughout work life is a prerequisite for operating and obtaining e-CF 3-5 level positions. One way to communicate the importance of continuing education and practical experience to students is to explain to them the university's cybersecurity curriculum and course content and how it is structured. For example, our Planning Framework provides a way to teachers to describe and open up the course topics and their emphases. In this way, cybersecurity students can be made aware that if they want to work in a particular role they should acquire additional training in these areas in addition to their Master's level education.

In addition to basic education, universities should plan and invest more in real continuous learning training for students moving into the industry. Universities are familiar places for them to maintain their competence. However, this requires universities to improve their operation, for example enabling universities to grant professional certificates [13]. In the business world, official certificates are valued more than university credits because certificates are much more useful in procurement and tendering situations.

For future work in this field, we see that the actual value of various cybersecurity (and other fields as well) certifications should be more extensively and systematically researched.

6 CONCLUSION

In this paper we examined via an industry survey what are the industry security assurance training needs and the needed level of competence for Finnish software engineers. The results provide industry expectations and needs towards cybersecurity education at university level, and these can be used to develop existing cybersecurity curricula in a systematic manner. For this purpose we have developed a framework for curriculum development and analysis. This paper extends the framework by adding industry needs and requirements for cybersecurity professionals, represented by weights corresponding to appropriate e-Competence levels.

REFERENCES

[1] Muhammad Rizwan Asghar and Andrew Luxton-Reilly. 2021. A Case Study of a Cybersecurity Programme: Curriculum Design, Resource Management, and Reflections. *InThe 51st ACM Technical Symposium on Computer ScienceEducation (SIGCSE '20), March 11–14, 2020, Portland, OR, USA.ACM, NewYork, NY, USA,* (2021), 7. https://doi.org/10.1145/3328778.3366918

[2] Daniel Bendler and Michael Felderer. 2022. Competency Models for Information Security and Cybersecurity Professionals: Analysis of Existing Work and a New Model. *ACM Transactions on Computing Education* (2022). https://doi.org/10.1145/3573205

[3] S Bosworth, ME Kabay, and E Whyne. 2014. Professional certification and training. In *Computer Security Handbook*. Vol. 1.

[4] ENISA. 2022. European Cybersecurity Skills Framework. Available online at https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework, Accessed 25.3.2023.

[5] European Commission Joint Research Centre (JRC). 2021. European Cybersecurity Taxonomy. Available online at https://cybersecurity-atlas.ec.europa.eu/cybersecurity-taxonomy, Accessed 25.03.2023.

[6] European Committee for Standardization. 2019. SFS-EN 16234-1 : 2019 : en (e-CF). A common European Framework for ICT Professionals e-Competence Framework (e-CF). A common European Framework.

[7] Małgorzata Gawlik-Kobylińska and Paweł Maciejewski. 2019. New Technologies in Education for Security and Safety. *ICEIT 2019, March 2–4, 2019, Cambridge, United Kingdom ©2019 Association for Computing Machinery* (2019). https://doi.org/10.1145/3318396.3318432

[8] Jan Hajny, Marek Sikora, Athanasios Vasileios Grammatopoulos, and Fabio Di Franco. 2022. Adding European Cybersecurity Skills Framework into Curricula Designer. *ACM International Conference Proceeding Series* (aug 2022). https://doi.org/10.1145/3538969.3543799

[9] Antti Hakkala, Anne-Maarit Majanoja, Ville Leppänen, and Seppo Virtanen. 2023. Framework for the Evaluation of Cybersecurity Curriculum Educational Content. In *Proceedings of the 19th International CDIO Conference, hosted by NTNU, Trondheim, Norway, June 26—29, 2023.*

[10] Ana Hol and James Mcgovern. 2023. A New Sustainable Model for Aligning Industry Requirements and University Programs. *ACM Inroads* 14, 1 (2023), 30–39. https://doi.org/10.1145/3583086

[11] Martti Lehto (Ed.). 2022. Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimus – hankkeen loppuraportti. *Informaatioteknologian tiedekunnan julkaisuja* 93 (2022). https://jyx.jyu.fi/handle/123456789/82709

[12] Qiang Liu, Wentao Zhao, Ruijin Wang, and Jiangyong Shi. 2021. A Competence-Based Three-Layer Cybersecurity Education Framework and Its Application. *ACM Turing Award Celebration Conference - China (ACM TURC), July 30-August 1, 2021, Hefei, China. ACM, 7 pages* (2021). https://doi.org/10.1145/3472634.3472649

[13] Anne-Maarit Majanoja, Antti Hakkala, Seppo Virtanen, and Ville Leppänen. 2023. Motivation for Continuous Software Engineering Expertise Development Through Lifelong Learning. In *Proceedings of the 19th International CDIO Conference, hosted by NTNU, Trondheim, Norway, June 26—29, 2023.*

[14] Xenia Mountrouidou, David Vosen, Chadi Kari, Mohammad Q Azhar, Sajal Bhatia, Greg Gagne, Joseph Maguire, Liviana Tudor, and Timothy T Yuen. 2019. Securing the Human: A Review of Literature on Broadening Diversity in Cybersecurity Education. *ITiCSE-WGR '19, July 15–17, 2019, Aberdeen, Scotland Uk© 2019 Association for Computing Machinery* 19 (2019). https://doi.org/10.1145/3344429.3372507

[15] NIST. 2020. NICE Framework Supplemental Material. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/nice-framework-supplemental-material.

[16] NIST. 2020. NIST Special Publication 800-181 Revision 1: Workforce Frame-work for Cybersecurity (NICE Framework). https://cybersecurity.att.com/resource-center/solution-briefs/nist-compliance-usm-anywhere

[17] Allen Parrish, John Impagliazzo, Rajendra K Raj, Henrique Santos, Muhammad Rizwan Asghar, Audun Jøsang, Teresa Pereira, Eliana Stavrou, and Muhammad Rizwan Asghar. 2018. Global Perspectives on Cybersecurity Education for 2030: A Case for a Meta-discipline. *ITiCSE '18 Companion, July 2–4, 2018, Larnaca, Cyprus©2018 Association for Computing Machinery* (2018), 19. https://doi.org/10.1145/3293881.3295778

[18] Karo Saharinen, Jaakko Backlund, and Nevala Jarmo. 2020. Assessing Cyber Security Education through NICE Cybersecurity Workforce Framework. *ICETC'20, October 23–26, 2020, London, United Kingdom©2020 Association for Computing Machinery* (2020). https://doi.org/10.1145/3436756.3437041

[19] Karo Saharinen, Mika Karjalainen, and Tero Kokkonen. 2019. A Design Model for a Degree Programme in Cyber Security. *ICETC 2019, October 28-31, 2019, Amsterdam, Netherlands. ©2019 Association for Computing Machinery.* (2019). https://doi.org/10.1145/3369255.3369266

[20] Tannian Mark and Coston Willie. 2021. The Role of Professional Certifications in Computer Occupations. *COMMUNICATIONS OF THE ACM* 64, 10 (2021). https://doi.org/10.1145/3474359

[21] University of Bristol Cyber Security Group. 2021. CyBOK – The Cyber Security Body of Knowledge. https://www.cybok.org/

[22] Muhammad Mudassar Yamin and Basel Katt. 2019. Cyber Security Skill Set Analysis for Common Curricula Development. *ARES '19, August 26–29, 2019, Canterbury, United Kingdom© 2019 Association for Computing Machinery* (2019). https://doi.org/10.1145/3339252.3340527

Received xx Month 2023; revised xx Month 2023; accepted xx Month 2023