Education and Information Technologies (2023) 28:1809–1831
https://doi.org/10.1007/s10639-022-11261-8

Analysis of cyber security knowledge gaps based on cyber security body of knowledge

Cagatay Catal[1] · Alper Ozcan[2] · Emrah Donmez[3] · Ahmet Kasif[4]

Received: 9 September 2021 / Accepted: 22 July 2022 / Published online: 5 August 2022

Abstract

Due to the increasing number of cyber incidents and overwhelming skills shortage, it is required to evaluate the knowledge gap between cyber security education and industrial needs. As such, the objective of this study is to identify the knowledge gaps in cyber security graduates who join the cyber security workforce. We designed and performed an opinion survey by using the Cyber Security Knowledge Areas (KAs) specified in the Cyber Security Body of Knowledge (CyBOK) that comprises 19 KAs. Our data was gathered from practitioners who work in cyber security organizations. The knowledge gap was measured and evaluated by acknowledging the assumption for employing sequent data as nominal data and improved it by deploying chi-squared test. Analyses demonstrate that there is a gap that can be utilized to enhance the quality of education. According to acquired final results, three key KAs with the highest knowledge gap are Web and Mobile Security, Security Operations and Incident Management. Also, Cyber-Physical Systems (CPS), Software Lifecycles, and Vulnerabilities are the knowledge areas with largest difference in perception of importance between less and more experienced personnel. We discuss several suggestions to improve the cyber security curriculum in order to minimize the knowledge gaps. There is an expanding demand for executive cyber security personnel in industry. High-quality university education is required to improve the qualification of upcoming workforce. The capability and capacity of the national cyber security workforce is crucial for nations and security organizations. A wide range of skills, namely technical skills, implementation skills, management skills, and soft skills are required in new cyber security graduates. The use of each CyBOK KA in the industry was measured in response to the extent of learning in university environments. This is the first study conducted in this field, it is considered that this research can inspire the way for further researches.

Keywords Cyber security · Cyber security body of knowledge · Data analysis · Data mining · education · Knowledge gaps · Skill gaps · Survey

✉ Alper Ozcan
alperozcan@akdeniz.edu.tr

Extended author information available on the last page of the article

1 Introduction

Cyber security employees are important for safety at the institutional and national level. The more experienced, productive, and educated the employees are, the better. Academic area needs to be aware what are the main gaps between what is taught at universities and what is expected later on in industry area. This is also a valid concern for software engineering educators who would like to know the knowledge gaps of their fresh graduates (Garousi et al., 2019).

Best cyber security experts can be much more productive than the low-skilled cyber security graduates. Skilled graduates in cybersecurity roles can help the nations address cyber security problems on time (National Research Council, 2013). Therefore, nations aim to address this skills gap in cyber security effectively and efficiently. One approach is to use the industry and government partnerships with education providers. Cyber security Challenge UK can be considered as the first example that aims to increase the number of cyber security professionals and improve the capacity in the UK. This not-for-profit British company organized several security competitions to solve the skills shortage problem in the UK and increase the number of skilled cyber security professionals (Vogel, 2016). Also, governments are working together with academic institutions to develop cyber security programs. In 2014, Government Communications Headquarters (GCHQ), which is a cyber security organization in UK, accredited cyber security MSc programs of six universities to fill the roles required for UK Vogel (2016).

The Center for Strategic and International Studies (CSIS) performed a survey on the cyber security skills in eight countries in 2016. The survey showed that 82 percent of employers refer to the shortage of cyber security skills and 71 percent of employers consider that this gap results in damage in their organizations (Crumpler and Lewis, 2019). This CSIS study also reported that the skills of cyber security operators, namely intrusion detection and secure software development, are the most difficult skills to find (Crumpler and Lewis, 2019). The workforce shortage is valid nearly for all positions in cyber security, however, the most important need is for highly skilled technical expertise (Crumpler and Lewis, 2019). This kind of missing skills have also been reported in software engineering field. Due to the missing skills in new hires, companies allocate resource investments for training of them Garousi et al. (2019). As in the case of software engineering, a similar concern exists on the mismatch between knowledge learned in universities and the cyber security industry needs.

In this paper, we follow a similar protocol and approach used by Garousi et al. who focused on software engineering knowledge gaps. However, our scope is cyber security graduates instead of software engineering graduates (Garousi et al., 2019). In addition, Garousi et al. had performed an in-depth analysis of the software engineering topic at the same time by performing a systematic review and meta-analysis of 35 studies in software engineering area (Garousi et al., 2019).

With the help of this study, we improve the body of knowledge on knowledge and skill gaps of new cyber security graduates who join the labor market. We determine the important topics that are required in practice and identify the missing skills. This objective is achieved with the help of a critical evaluation of programs and based on data collection from experts in cyber security industry. Our contributions to this study are listed as follows:

- To the best of our knowledge, this is the first study that uses Cyber Security Body of Knowledge (CyBOK) to identify knowledge gaps of cyber security professionals.
- We used the sub-KAs specified in CyBOK, which enabled us to provide very precise and specific recommendations for improvement of the cyber security curriculum.
- We applied the required statistical analysis approaches and focused on cyber security and CyBOK instead of software engineering and SWEBOK. This research can be performed in different countries with similar experiments and protocols to improve the cyber security education.
- CyBOK is an evolving knowledge base. This research demonstrated the benefits of this resource for improving the cyber security education.

This paper is structured as follows. Background and related work is presented in Section 2. Methodology is discussed in Section 3. The results are presented in Section 4. Section 5 provides the discussion. Finally, conclusions are discussed in Section 6.

2 Background and related work

With the rapid development of new technologies such as Blockchain, Deep Learning, Edge Computing, Digital Twins, the cyber world has a much greater impact on our lives. The Internet took place at the most critical points of our lives and became indispensable. The risks it brings threaten our life as well as our digital world, causing serious losses. Since cyber security is a process that needs to be kept alive, short-term solutions are not sufficient. As long as companies see the potential of cyber security as a part of their business processes, they can protect their employees and the company's valuable assets against potential risks. For most of the companies all around the world, the internal mechanisms of a computer are like a closed box (Denning, 2018). There is very little awareness and lack of knowledge about the cyber security. Users need cyber security experts for the security of data and applications, configuration of network security, and security-related maintenance and updates. The need in the field of cyber security has recently intensified because many operations are performed online, such as electronic banking, product purchase, and e-government operations.

So far, the need for cyber security experts has been met with computer scientists, computer engineers, software engineers, and programmers who have been trained on the relevant technologies. In recent years, some universities started to provide cyber security courses as part of the software engineering, computer science/engineering programs under different names, such as computer security and software security courses. Although these courses were initially offered as an elective course, it has transformed into a compulsory course in several programs. At a later stage, undergraduate programs related to cyber security have been opened and later, MSc programs have been designed at different universities all around the world.

There is a considerable number of studies in the literature on cyber security awareness. In these studies, parameters covering education, trained human resources, informatics policies, and regional differences are analyzed. However, most of these studies are based on the experts in the IT (information technologies) sector who are not directly involved in the relevant processes. Within the scope of our study, a comprehensive analysis was made with the data obtained based on the CyBOK, which defines the cyber security knowledge areas in a broad framework, and the cyber security experts who are constantly intertwined with the cyber incidents are involved.

According to the framework publication published by NIST, a reference infrastructure for education and other fields that defines the interdisciplinary relationship of the cyber security field is explained (Newhouse et al., 2017). Kaspersky and Furnell pointed out the importance of providing support to the industry by providing cyber security training to skilled professionals and ensuring adequate cyber security awareness among end users Kaspersky and Furnell (2014). Crumpler and Levis stated that organizations face serious difficulties in terms of the human resources they need to protect their existing systems from cyber security threats (Crumpler and Lewis, 2019).

Ahmed and Roussev stated that the peer education model as a well-defined teaching protocol is a good tool that can be used to perform cyber security education effectively (Ahmed and Roussev, 2018). Wilk mentioned that cyber space creates great difficulties for computer experts (Wilk, 2016). As a result of the study, it is specified that the legal awareness of the students about privacy and IP (Intellectual Property) is crucial because these aspects affect all the computer professionals. Ricci et al. stated that people are generally the weakest link in the security chain in terms of cyber-attacks and identity theft Ricci et al. (2019). Cabaj et al. stated that the current cyber security workforce is not sufficient to meet the growing demand for qualified cyber security professionals and the shortage will increase (Cabaj et al., 2018).

Rashid et al. (2018) mentioned that cyber security has become an important element in the curriculum of all education levels. They stated that the basic information on which cyber security is developed is fragmented. Manson and Pike emphasized that the changes and innovations that occur in technology and security needs require ideal cyber security professionals to work with a certain amount of time (Manson and Pike, 2014). Conklin et al. analyzed the infrastructures created for efforts to train experts in cyber security and examined some of the critical but not addressed issues faced by different programs (Conklin et al., 2014).

A detailed quantitative survey about the cyber security labor market of the UK provides several recommendations (Research and analysis Cyber security skills in the UK labour market, 2020). The report discusses skills gaps, required training, qualifications, recruitment process, and skill shortages for the market. This study provides insights into the skill gaps that affect the industry and employers and discusses how much training the employees need to maintain the standard in the cyber security sector. It also mentions how the curriculum of the universities should be updated regularly to provide sufficient skill sets to new graduates. Furthermore, it discusses guidance paths for the qualification and training processes of the recruiters as well as the candidates. Finally, the report recommends specific roles for the government and industry to take responsibility and help to improve this sector.

Yonemura et al. (2021) analyzed the process of creating a sustainable and effective cybersecurity education methodology suitable for Japanese National Institute of Technology (KOSEN) staff and students. With the project activity carried out within the scope of the study, it is aimed to strengthen the technical infrastructure of the relevant unit in order to train talented students who have gained practical cyber security skills. Yoon et al. (2021) conducted a case study on designing and facilitating assignments for cyber security students enrolled in the fellowship program. As a result of the study, practical suggestions are given on how the assignment can be used for various classrooms or cyber security projects and how instructors can maximize their capacity. Popstojanova et al. (2021) aims to contribute to addressing government and industry need through program development for highly skilled cyber security professionals. The program objectives are: (1) to increase the annual enrollment of undergraduate students, (2) develop curricular and extra-curricular student support services and activities for students, (3) strengthen partnerships with computer and information technology employers, (4) to investigate the impact of curriculum activities on student achievement. Chou et al. (2021) developed a questionnaire within the scope of the study and it includes a series of categories, each of which includes questions to evaluate the workshop design and whether the system is suitable and useful for learning about cyber security. With the work carried out, the design of the workshop was explained and the focus was on the self-assessment of knowledge on topics in the cyber security category. Alrabaee and Manna (2021) examine the cyber threats that threaten users globally, as well as some attacks that took place especially during the COVID-19 pandemic. As a result of the study, they offered various suggestions on what can be done in the future to take precautions against these attacks and to improve cyber security awareness and prevent their reoccurrence. Troja et al. (2021) stated that the purpose of teaching Computer Science and Cyber Security courses efficiently during the COVID19 pandemic is more than pressure on education. In the study, they presented their approach to the appropriateness of using the WebEx HandsOn-Labs tool to bridge the educational gap between face-to-face and online education. Romanovs et al. (2021) developed a framework document within the scope of Cyber Security Curriculum Recommendations for Smart Grids. The study deals with a systematic reading and analysis of the literature and modern education in cyber security. Within the scope of the research, basic results were obtained and basic requirements and recommendations for cyber security research programs on smart grids were presented.

According to our literature search, we did not encounter any study that used CyBOK to identify the knowledge gaps in cyber security. However, we observed that knowledge gaps for software engineering discipline have been determined based on SWEBOK previously (Garousi et al., 2019). Since cyber security is a different specialized domain compared to software engineering, it is crucial to perform a research to determine the cyber security knowledge gaps. In this study, CyBOK has been used as a reference document to determine the cyber security knowledge gaps and an opinion survey was performed with cyber security experts.

3 Methodology

Research questions, survey design, the execution of survey, and the data analysis method are presented in this section.

3.1 Research questions (RQs)

The objective of this research is to analyze the knowledge gaps between the Cyber Security (CS) education and industry demands by using the Goal, Question, Measure (GQM) [4] approach. The following research questions were defined according to the overall objective:

- RQ 1: What are the most significant aspects of Cyber Security according to the experts in industry? This RQ has been divided into the following two sub questions:
  - RQ 1.1: What are the key points of Cyber Security according to the trained experts in industry?
  - RQ 1.2: How do experienced practitioners and recent graduates perceive the importance of knowledge areas (KAs) differently?
- RQ 2: How is the perceived importance of Cyber Security KAs in the workplace compared with the knowledge acquired at universities?
- RQ 3: What knowledge areas of Cyber Security are mostly adopted by experts and what areas have the largest gaps? The third RQ is designed to investigate the knowledge gaps where there is more need in training Cyber Security personnel.

3.2 Survey design

We developed an online survey to get the opinions of practitioners. CyBOK version 1.0 has been used in the study. The questionnaire starts with several number of demographic questions, comprising degrees, roles, and graduation year. Participants have been asked what they obtained during their university education on the 19 KAs and 118 sub KAs in CyBOK and how important each topic is in the workplace. An overview of the 19 KAs and 118 sub KAs of the CyBOK is provided in Fig. 1. The questionnaire includes the following three main parts: Demographics (i.e., seven questions), importance of topics in workplace & level of knowledge obtained in education (i.e., large number of questions), and comments (i.e., one question). A 5-point Likert scale was used to evaluate each topic, as shown in Table 1. A sample of the online survey is given in Fig. 2a, in which four of the Risk Management and Governance sub-KAs are shown.

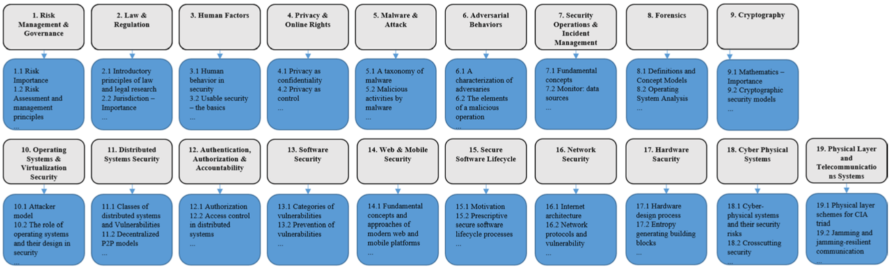
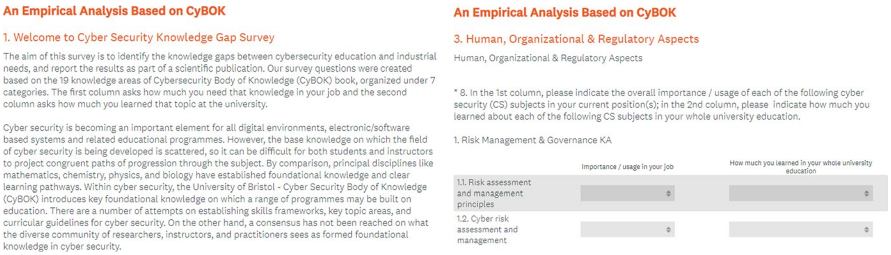

1. Risk Management & Governance
1.1 Risk Importance
1.2 Risk Assessment and management principles
...
2. Law & Regulation
2.1 Introductory principles of law and legal research
2.2 Jurisdiction – Importance
...
3. Human Factors
3.1 Human behavior in security
3.2 Usable security – the basics
...
4. Privacy & Online Rights
4.1 Privacy as confidentiality
4.2 Privacy as control
...
5. Malware & Attack
5.1 A taxonomy of malware
5.2 Malicious activities by malware
...
6. Adversarial Behaviors
6.1 A characterization of adversaries
6.2 The elements of a malicious operation
...
7. Security Operations & Incident Management
7.1 Fundamental concepts
7.2 Monitor: data sources
...
8. Forensics
8.1 Definitions and Concept Models
8.2 Operating System Analysis
...
9. Cryptography
9.1 Mathematics – Importance
9.2 Cryptographic security models
...
10. Operating Systems & Virtualization Security
10.1 Attacker model
10.2 The role of operating systems and their design in security
...
11. Distributed Systems Security
11.1 Classes of distributed systems and Vulnerabilities
11.2 Decentralized P2P models
...
12. Authentication, Authorization & Accountability
12.1 Authorization
12.2 Access control in distributed systems
...
13. Software Security
13.1 Categories of vulnerabilities
13.2 Prevention of vulnerabilities
...
14. Web & Mobile Security
14.1 Fundamental concepts and approaches of modern web and mobile platforms
...
15. Secure Software Lifecycle
15.1 Motivation
15.2 Prescriptive secure software lifecycle processes
...
16. Network Security
16.1 Internet architecture
16.2 Network protocols and vulnerability
...
17. Hardware Sacurity
17.1 Hardware design process
17.2 Entropy generating building blocks
...
18. Cyber Physical Systems
18.1 Cyber-physical systems and their security risks
18.2 Crosscutting security
...
19. Physical Layer and Telecommunicatio ns Systems
19.1 Physical layer schemes for CIA triad
19.2 Jamming and jamming-resilient communication
...

Fig. 1 12 KAs of CyBOK and their sub KAs (adopted from SWEBOK Garousi et al. 2019)

Table 1 5-point Likert scales utilized to evaluate learning and significance of topics at workplace

The Likert scale to evaluate university level learning	# of participants
(0) Learned nothing at all	(0) Completely useless
(1) Learned the basics	(1) Occasionally useful
(2) Moderate working knowledge	(2) Moderately useful
(3) Learned a lot	(3) Very useful
(4) Learned in depth (became expert)	(4) Critical to my work


An Empirical Analysis Based on CyBOK

1. Welcome to Cyber Security Knowledge Gap Survey

The aim of this survey is to identify the knowledge gaps between cybersecurity education and industrial needs, and report the results as part of a scientific publication. Our survey questions were created based on the 19 knowledge areas of Cybersecurity Body of Knowledge (CyBOK) book, organized under 7 categories. The first column asks how much you need that knowledge in your job and the second column asks how much you learned that topic at the university.

Cyber security is becoming an important element for all digital environments, electronic/software based systems and related educational programmes. However, the base knowledge on which the field of cyber security is being developed is scattered, so it can be difficult for both students and instructors to project congruent paths of progression through the subject. By comparison, principal disciplines like mathematics, chemistry, physics, and biology have established foundational knowledge and clear learning pathways. Within cyber security, the University of Bristol - Cyber Security Body of Knowledge (CyBOK) introduces key foundational knowledge on which a range of programmes may be built on education. There are a number of attempts on establishing skills frameworks, key topic areas, and curricular guidelines for cyber security. On the other hand, a consensus has not been reached on what the diverse community of researchers, instructors, and practitioners sees as formed foundational knowledge in cyber security.

An Empirical Analysis Based on CyBOK

3. Human, Organizational & Regulatory Aspects

Human, Organizational & Regulatory Aspects

* 8. In the 1st column, please indicate the overall importance / usage of each of the following cyber security (CS) subjects in your current position(s); in the 2nd column, please indicate how much you learned about each of the following CS subjects in your whole university education.

1. Risk Management & Governance KA

	Importance / usage in your job	How much you learned in your whole university education
1.1. Risk assessment and management principles		
1.2. Cyber risk assessment and management		

Fig. 2 **a**) A sample from the online survey, **b**) Screenshot from CyBOK summary presented to participants

A summary of CyBOK has been provided to the participants to inform them about CyBOK KAs and sub KAs, as shown in Fig. 2b. This information was accessible to all participants by clicking on a link. After preparing the initial version of the survey, we had five practitioners to complete the survey. The aim of this test work was to verify that the questions were clearly and easily understood by participants. According to the received feedback from the test work, we made slight changes to the initial survey. These changes were related to the wording we choose in the survey. For example, we avoided the use of some strong words not to bias our results and non-specific words were removed not to cause ambiguity in the survey. Also, questions which were vague were changed because direct questions would be better in these cases. The updated survey was shared with numerous experts at a later stage.

3.3 Survey execution

We shared the survey link through the social media platforms (i.e., LinkedIn and Twitter) to reach Cyber Security practitioners. The survey link was also forwarded to the personal emails of known Cyber Security experts to increase the response rate. This kind of sampling is known as compatibility sampling (a.k.a., convenience sampling) Valerio et al. (2014). An online survey hosted at www.surveymonkey.com was utilized to collect feedback from respondents. The survey was accessible between August 2020 and October 2020. We carefully selected responses only from Cyber Security experts who had a relevant education and therefore, we reached a total of 60 experts in this population. There were some additional experts, however, due to their irrelevant formal education, we were unable to include them in our analysis.

3.4 Demographics

Demographic state of the dataset is depicted in Table 2. The dataset has 60 data points, each of them corresponds to a responder. The academic degrees of the respondents are as follows: 11 respondents have PhD degrees, 23 of them have MSc degrees, and 26 of the respondents have BSc degrees. Therefore, 56,6% of the participants have post-graduate degrees. 85% of the respondents proclaimed their expertise in cyber security. All the participants hold Computer Science or Computer Engineering BSc degrees. This information indicates that our group of participants is very suitable for the planned survey study.

3.5 Data analysis method

The survey comprises sequential (i.e., ordinal) data for significance of knowledge and subjects instructed in the university. The sequential data can be utilized as nominal data (Van Belle, 2011; Norman, 2010). The graduation degree acquired by students (e.g., BSc, MSc, PhD) can be an instance of the nominal data. A number of nominal instances comprise a period of an engineer's experience or number of code lines generated in a certain time period. The mean and standard deviation parameters are convenient when sequential data is employed as nominal

Table 2 Academic degrees of respondents (n=60)

Degree	# of respondents	% of respondents
BSc	26	43.2
MSc	23	38.3
PhD	11	18.3
Cyber Security Expertise	# of respondents	% of respondents
Yes	51	85
No	9	15

data. This form of usage presumes that the distinction between (2) Moderately useful and (1) Occasionally useful is matched to the distinction between (3) Very useful and (2) Moderately useful. Moreover, when sequential data are utilized as nominal data (Jamieson, 2004), the distinction between (2) Moderately useful and Occasionally useful is not presumed to be equivalent to the distinction between (3) Very useful and (2) Moderately useful. It turned into feasible to put in order these parameters, but not utilize the standard deviation and the mean of them. This data representation approach corresponds to the Likert scale approach and is used in this study.

There are different concepts on employing sequential data as nominal data (Norman, 2010; Jamieson, 2004). Some analysts and researchers suggest that this can be enabled with some remarks (Van Belle, 2011), for instance, treating sequential data as distributed normally. Knapp (1990) and Anderson (1961) both specify that under equivalence, the power for both the nonparametric and parametric is proximate, and can be higher for the nonparametric in the events of violations of the normality hypothesis. Jamieson (2004) emphasizes that statistics performed with parametric can be utilized together with small sample sizes, Likert data, non-normal distributions, and uneven variances.

Lethbridge (1998, 2000) evaluated the significance and learning level by utilizing a Likert scale and investigated the findings (i.e., sequential data) employing methods and techniques suitable for the nominal data. Lethbridge (1998, 2000) computed the standard deviation and the mean of sequential data and formed knowledge gap as the distinction between the significance of a subject and the level of knowledge in this subject. Moreover, in another work for investigating knowledge gaps between software engineers, Kitchenham et al. (2005) opposes the approach proposed by Lethbridge for the sequential data. To evaluate significance and learning a degree of subjects in software engineering, they adopted to utilize only proportions, that are also introduced in Lethbridge's study. For example, the significance of a topic is computed with the following equation: Importance = number of elements which score three (3 or more / number of subjects and a six point scale, from 1 to 6) was utilized to determine significance and learning degree. The knowledge gap has been described as the distinction between learning degree and significance, both of them are explicated in percentages.

In this study, practices introduced by Lethbridge (1998, 2000) and Kitchenham et al. (2005) were utilized along with non-parametric chi-squared test. The knowledge gap was measured and evaluated by acknowledging Lethbridge's assumption for employing sequential data as nominal data and improved it by deploying chi-squared test. To measure the difference between the participants' perception of learning degree and importance of each KA, the chi-squared test is convenient. As such, the following hypotheses have been formed to evaluate the knowledge gap for each KA and answer RQs:

– H0: The mean of significance for the experiment set (or participants) is equivalent to the mean of participants' learning degree (i.e., the statistically important distinction between the significance and learning degree was not found, thus no knowledge gap was specified)

- H1: The mean of significance for the experiment set is not equivalent to the mean of the participants' learning degree (i.e., a statistically important distinction was found between the significance and learning degree, a knowledge gap is specified)

After the computation of the t parameter, it was compared to the critical value of t parameter with a degree of freedom (df) of 128 from the t table of distribution for a selected confidence value (i.e., 0.05 in our case). If the computed t parameter is greater than the critical t value, then the hypothesis H0 (which signifies the means are significantly different) is rejected. In this way, Lethbridge's analysis method was used and amplified by utilizing chi-squared to test the importance of differences. The formula of Kitchenham et al. (2005) was adapted to the Likert scales (see Table 2) as follows:

$$Importance/Learning\ Level = \frac{number\ of\ subjects\ scoring\ more\ than\ zero}{total\ number\ of\ subjects} \quad (1)$$

4 Experimental results

This section presents the demographics information of the participants, responses to research questions, and all the results of the survey.

4.1 RQ-1: Importance of cyber security topics in workplace

In this section, general importance perception of cyber security KA topics are evaluated. The analyzes are conducted based on the fact that the newly recruited staff members and experienced personnel would have different perceptions. In RQ 1.1, the general respondents' perception about Cyber Security Topics is depicted as a violin chart. In RQ 1.2, experienced personnels' perception is analyzed to see the impact.

4.1.1 RQ 1.1: General importance perception

Figure 3 illustrates the KA level importance assessments of the respondents. The figure is depicted as a violin plot Hintze and Nelson (1998). The Violin plot represents the distribution of data while reinforcing it with density information. Thickness of bars represents higher density, and the thinner bars imply less density. The dots in violin bars stand for the KAs median. The median value of Cyber Security KAs diverges between (2) Moderately useful and (3) Very useful, indicating an obvious incline in perception towards high importance.

Risk Management & Governance along with Authentication, Authorization & Accountability are two top KAs with the highest median and highest overall importance ratings. The distribution of data for top KAs is above (3) Very useful. The average median for these KAs is again three (3), showing that these KAs are vital

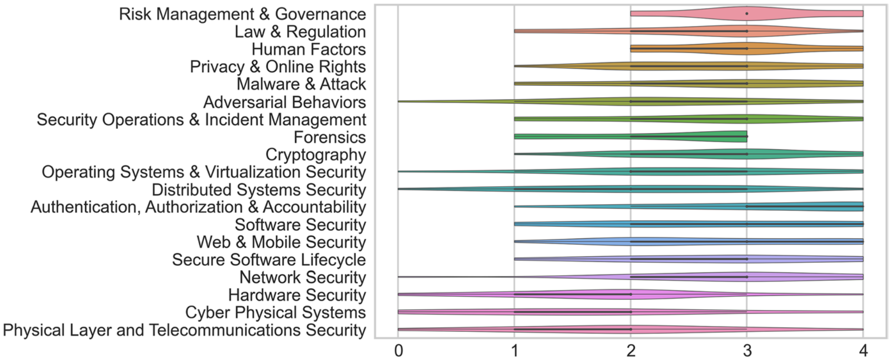


Fig. 3 Importance perception of CyBOK KAs (x-axis: Perception scores according to Likert scale, y-axis: CyBOK KAs)

factors for Cyber Security. Hardware Security and Cyber Physical Systems have been the least influential KAs, each possessing a median of two (2). Another point is that the distribution of data points for the least influential KAs is scattered and has only a minor concentration around the median. The remaining KAs pose less scattered distribution of data points. The distributions for Adversarial Behaviors, Operating Systems & Virtualization Security, Distributed Systems Security, Physical Layer and Telecommunications Security are more scattered while the other topics pose a more concentrated distribution.

4.1.2 RQ 1.2: Comparison of importance perceptions between less and more experienced respondents

RQ 1.2 investigates whether experienced personnel would have different perceptions of importance compared to new graduates. To evaluate this difference, the dataset is divided into two groups and an additional analysis is performed. First group comprises less experienced Cyber Security personnel (i.e., 1-10 years of experience). The second group is made of more experienced Cyber Security personnel, having

Table 3 KAs with largest difference in perception of importance between less and more experienced personnel

Rank	KA	Mean difference	Standard Deviation	Chi-squared
1	Cyber-physical systems	1.073	0.95	1.207
2	Software lifecycles	0.941	0.82	1.401
3	Vulnerabilities	0.823	0.95	1.302

over 10 years of working experience. The results show an obvious difference in the selection of importance of topics in Cyber Security.

Table 3 shows the most important topics where experienced and inexperienced engineers differ the most. The mean difference, standard deviation and t analysis are presented jointly to support this observation. Table is ordered with respect to mean difference and only top 3 KA's are shown. Mean difference shows the difference of perception between experienced and inexperienced personnel is supported with t analysis. Positive mean means that experienced personnel find the KA more important. T analysis is a statistical assessment to measure whether there is a meaningful variation between the means of two series. The topics discussed in Table 3 are experience-based topics and the statistical selection of these topics is meaningful. These topics require a lot of experience and are usually not well taught during university education. Among these topics, only the software lifecycles topic seems to find broader placement among course syllabuses.

4.2 RQ-2: Learned Topics vs. Importance at Work

CyBOK KAs and sub KAs comprise several answers of respondents. To get a stronger representation of all the responses, the 128 data points of answers are averaged. Thus, a single parameter is obtained to assess each KA and sub KA. The two scatterplots presented in Figs. 4 and 5 are designed using this single parameter. Both figures depict the importance of usage charts of the KAs. Figure 4 focuses on the KA level analysis, while Fig. 5 depicts the sub KA level analyses. The KA level analysis shown in Fig. 4 shows that Authentication, Authorization and Accountability, Risk Management and Governance and Cryptography are the topics with the most important/used at work, and also possess the most instructed course subjects at university.

Topics such as Cyber Physical Systems, Hardware Security and Physical Layer and Telecommunications Security show least learning level in Fig. 4. This shows that insufficient information is provided during the university education. The importance

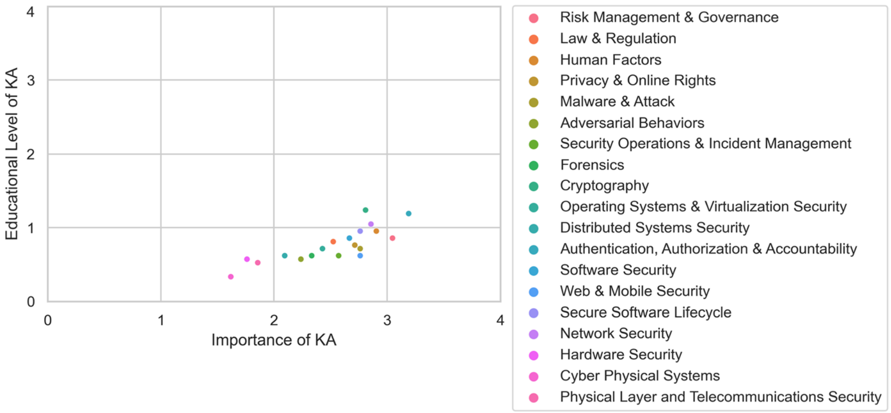


Fig. 4 Perception of respondents about importance vs. learned topics in the university per KA

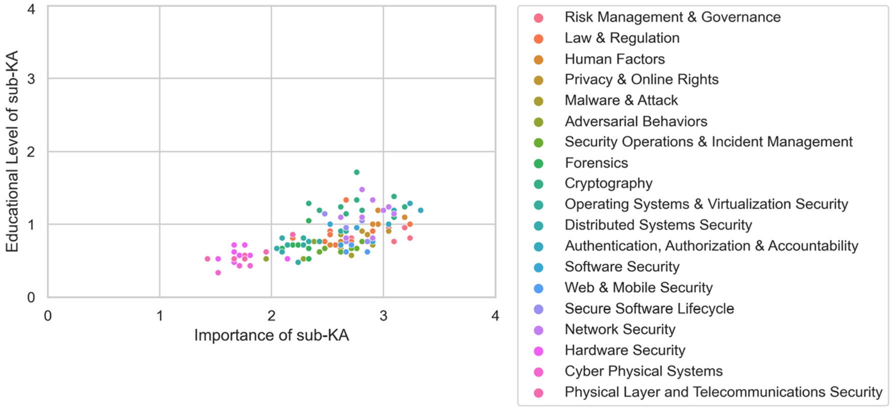


Fig. 5 Perception of respondents about importance vs. learned topics in the university per sub KA

ratings of these topics are slightly below moderate, as such, the gap seems to be minimal. The topics with the highest gap are Web and Mobile Security, along with Security Operations and Incident Management. These two KAs have been regarded as moderately or very useful at work by many respondents. Besides, the educational perception of these topics is rated only slightly below moderate. These observations denote that the university educators should invest more into these KAs in the related courses.

Figure 5 demonstrates that the clusters of sub KAs are largely consolidated. This denotes that respondents consider both importance and respective educative level of sub KAs of a particular KA similarly. From another perspective, among the CyBOK KAs, we do not have a topic that has a small impact in practice but gets acute attention in university syllabuses. Likewise, the average perceptions of learning in most instances are around 1 out of 4, which stands for the lack of education in university in almost all instances. However, this is not a negative observation. Granted the vast range of topics and concepts in Cyber Security, coverage of all topics in university syllabuses is a quite challenging task. As a result, most universities aim to equip their graduates with essential skills to start in industry. Thus, students are expected to fill the gaps as they gain experience throughout their career.

4.3 RQ 3: Knowledge Gaps: Fields to Reconsider

RQ 3 presents an investigation of the knowledge gaps in both KA and sub KA level. The investigation considers both experienced and newly recruited respondents. The knowledge gap analysis involves two approaches. Both approaches use quantitative measurements to see which fields demand further attention in the university education. The first of these approaches is Lethbridge's approach Lethbridge (1998, 2000), enriched with chi-squared test and used in Table 4. Table 4 demonstrates the mean knowledge gap of CyBOK KAs according to Lethbridge's approach. The chi-squared test used in analyses shows that there is an important gap between the workplace importance and learning level of each KA. Kitchenham's approach

Table 4 CyBOK KAs sorted by mean of knowledge gap

Rank	KA	Mean Gap	Standard Deviation	Chi-squared
1	Risk Management Governance	2.190	1.250	1.210
2	Web Mobile Security	2.095	1.480	3.010
3	Malware Attack Technologies	2.048	1.244	3.062
4	Security Operations Incident Management	2.000	1.264	2.724
5	Authentication, Authorization Accountability	2.000	1.483	3.465
6	Privacy Online Rights	1.905	1.261	4.203
7	Software Security	1.905	1.375	2.110
8	Human Factors	1.810	1.123	1.216
9	Network Security	1.810	1.327	2.120
10	Secure Software Lifecycle	1.762	1.411	4.236
11	Adversarial Behaviors	1.619	1.284	2.572
12	Forensics	1.619	0.973	4.026
13	Operating Systems Virtualization Security	1.619	1.396	2.003
14	Law Regulation	1.571	1.076	4.275
15	Cryptography	1.476	1.123	1.275
16	Distributed Systems Security	1.476	1.250	2.420
17	Cyber Physical Systems	1.286	1.231	1.043
18	Hardware Security	1.143	1.062	1.902
19	Physical Layer and Telecommunications Security	1.095	1.179	2.008

Kitchenham et al. (2005) is the second method where the knowledge gaps are sought to be identified. The results of Kithchenham analysis are illustrated in Table 5.

The largest knowledge gaps appear in KAs Web and Mobile Security and Security Operations and Incident Management. These KAs find themselves in the top four positions in both analyses. On the other hand, the most notable conflicting result is that while Cyber Physical Systems is rated as one of the KAs with the largest knowledge gap in Table 5, it is ranked as seventeenth in Table 4. To further investigate the reason of conflict such as this one, the data points used in these tables is plotted in Figs. 6 and 7. Figure 6 depicts the gaps according to Lethbridge's approach and uses means, while in Fig. 7, the gaps are calculated as percentages. In obtaining of both figures, the calculation of the knowledge gap is evaluated as the difference between importance and learning level. The figures are sorted in descending order according to the knowledge gap.

Figure 6 presents the data points according to Lethbridge's Lethbridge (1998, 2000) analysis. The analysis consists of mean of KA scores, standard deviation scores, and t scores. Data points are sorted with respect to descending order of mean values.

As presented in Fig. 7, Kitchenham's approach Kitchenham et al. (2005) suggests the translation of binary coding of importance scores. The operation divides the likert scale scores given in Table 1, using a delimiter. This delimiter is selected as zero in this study and can be described as % of participants scored greater than zero and

Table 5 CyBOK KAs sorted by percentage (%) of knowledge gap based on Kitchenham et al.'s approach Kitchenham et al. (2005)

Rank	KA	Knowledge Gap (%)
1	Adversarial Behaviors	57%
2	Web Mobile Security	57%
3	Cyber Physical Systems	57%
4	Security Operations Incident Management	52%
5	Forensics	52%
6	Physical Layer and Telecommunications Security	52%
7	Law Regulation	48%
8	Privacy Online Rights	48%
9	Malware Attack Technologies	48%
10	Hardware Security	48%
11	Risk Management Governance	43%
12	Distributed Systems Security	43%
13	Software Security	43%
14	Secure Software Lifecycle	43%
15	Operating Systems Virtualization Security	38%
16	Human Factors	33%
17	Authentication, Authorization Accountability	33%
18	Cryptography	24%
19	Network Security	24%

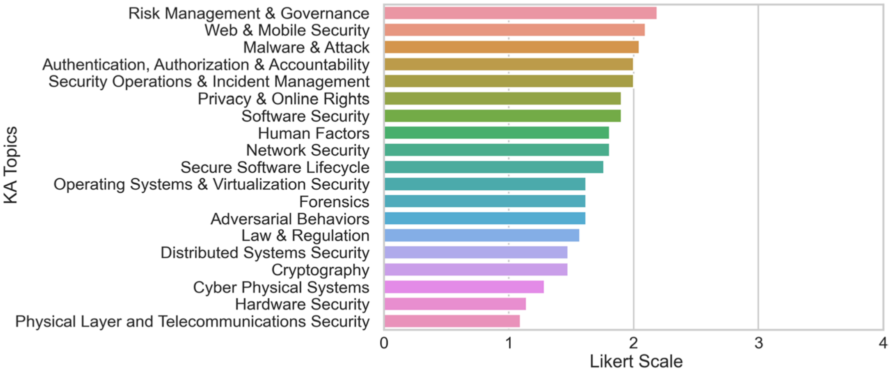


Fig. 6 KA level knowledge gap distribution based on Lethbridge's approach Lethbridge (1998, 2000)

% of participants scored zero. Educative scores are also merged into two groups with the same delimiter. One caveat of this approach is that the discrimination of respondents' answer is not possible. Considering Tables 6 and 7 together, Cyber Physical Systems KA draws the attention. The KA are rated as 1.286 out of 4 in Fig. 6, while in Table 7 presents a rate of 57%. This shows that while Kitchenham et al. (2005)

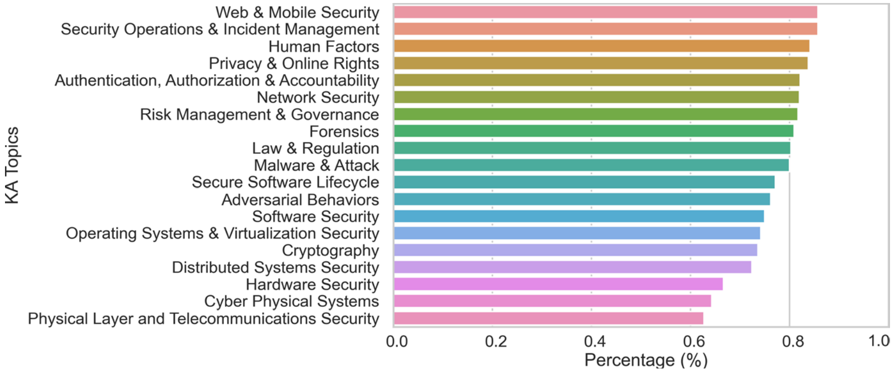


Fig. 7 KA level knowledge gap distribution based on Kitchenham's approach Kitchenham et al. (2005)

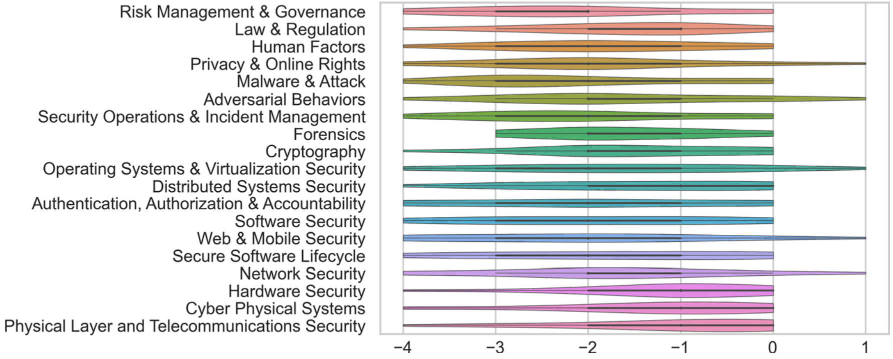


Fig. 8 Knowledge gaps of different KAs as a violin plot (x-axis: knowledge gap, y-axis: CyBOK KAs)

rates the KA slightly below moderately importance, Lethbridge's method Kitchenham et al. (2005) reports a higher importance. Hence, it can be derived from the analysis that the approaches stand out from each other.

Figure 8 depicts another violin plot to present the knowledge gap distribution of each KA. The figure depicts all KAs with negative gap rates, showing that the overall perception about the Cyber Security KAs is that they all have knowledge gaps. The university education lacks the overall quality to catch up with industry. Moreover, this also points out the general view of participants on the topic, as most of the participants agree on similar knowledge gaps. The figure also shows leaning to the left-hand side of Fig. 8. While most KAs have the same median as minus two, Risk Management & Governance, Malware & Attack, Authentication, Authorization & Accountability & Software Security KAs have the overall lowest values, hence having highest gaps.

Table 6 displays the results of chi-squared test for the top 20 sub KAs with the largest knowledge gaps. The table shows that more than half of sub KAs belong to Risk Management & Governance (five sub KAs), Malware & Attack (three sub

Table 6 Top 20 CyBOK sub-KAs with the largest knowledge gap sorted by mean of knowledge gap based on chi-squared test

Rank	Sub-KA	Mean Gap	Std. Dev.	Chi-squared	Table 7 Rank
1	1.6. Business continuity	2.429	1.469	1.278	17
2	1.3. Cyber risk assessment and management	2.333	1.461	1.106	15
3	1.1. Risk	2.238	1.338	2.492	–
4	2.4. Data protection	2.238	1.480	2.438	–
5	14.3. Server side vulnerabilities and mitigations	2.238	1.375	1.072	14
6	5.5. Malware response	2.190	1.327	1.002	–
7	1.4. Risk governance	2.143	1.276	1.463	16
8	4.1. Privacy as confidentiality	2.143	1.195	2.446	–
9	5.3. Malware analysis	2.143	1.195	1.665	–
10	5.4. Malware detection	2.143	1.352	1.131	–
11	12.3. Authentication	2.143	1.424	2.253	–
12	13.3. Detection of vulnerabilities	2.143	1.389	1.268	–
13	1.2. Risk assessment and management principles	2.095	1.700	2.646	–
14	3.3. Human error	2.095	1.338	1.251	–
15	7.2. Monitor: data sources	2.095	1.179	2.143	–
16	15.4. Adopting a secure software lifecycle	2.095	1.375	2.496	–
17	16.7. Network defense tools	2.095	1.480	1.402	–
18	4.5. Privacy engineering	2.048	1.322	1.320	–
19	7.1. Fundamental concepts	2.048	1.071	2.408	–
20	7.3. Analyze: analysis methods	2.048	1.244	2.730	–

KAs) & Security Operations & Incident Management (three sub KAs). The other 9 sub KAs are from eight KAs where only Privacy & Online Rights is represented with two sub KAs. Table 7 shows the analysis done for sub KAs using Kitchenham's approach Kitchenham et al. (2005). We can see that 16 sub KAs out of 20 are under Risk Management & Governance (four sub KAs), Law & Regulation (four sub KAs), Security Operations & Incident Management (three sub KAs), Web & Mobile Security (three sub KAs) & Forensics (three sub KAs). Two sub KAs belong to Security Operations & Incident Management (two sub KAs) and one sub KA belongs to Cyber Physical Systems.

The rankings of all top KAs by respective approaches are provided in Tables 6 and 7 as the last columns. There are 4 sub KAs common in these tables, while remaining 16 sub KAs differ between both approaches. These 4 sub KAs were classified under two KAs, i.e. Risk Management & Governance and Web & Mobile Security.

Table 7 Top 20 CyBOK sub-KAs with the largest knowledge gap based on based on Kitchenham et al.'s approach Kitchenham et al. (2005)

Rank	Sub-KA	Percentage	Table 6 Rank
1	6.2. The elements of a malicious operation	62%	–
2	8.5. Cloud forensics	62%	–
3	18.4. Policy and political aspects of cps security	62%	–
4	2.12. Public international law	57%	–
5	6.3. Models to understand malicious operations	57%	–
6	7.4. Plan: security information and event management	57%	–
7	1.5. Risk assessment and management principles	57%	–
8	7.6. Knowledge: intelligence and analytics	57%	–
9	7.7. Human factors: incident management	57%	–
10	8.3. Main memory forensics	57%	–
11	8.6. Artifact analysis	57%	–
12	14.1. Fundamental concepts of modern platforms affecting security	57%	–
13	14.2. Client side vulnerabilities and mitigations	57%	–
14	14.3. Server side vulnerabilities and mitigations	57%	5
15	1.3. Cyber risk assessment and management	52%	2
16	1.4. Risk governance	52%	7
17	1.6. Business continuity: incident response and recovery planning	52%	1
18	2.3. Privacy laws in general and electronic interception	52%	–
19	2.7. Tort	52%	–
20	2.11. Regularity matters - Importance / usage in your job	52%	–

5 Discussion

In Section 3.1, we presented the RQs of this study, and here we discuss our research findings. Our responses for each of these RQs are presented as follows:

- Response to RQ 1.1: According to our survey, Risk Management & Governance, Authentication, Authorization, & Accountability have been considered being the vital for cyber security whereas hardware security and cyber physical systems have been considered the least influential KAs. As known in computer security literature, Confidentiality, Integrity, and Availability (CIA Triad) are the core goals of Computer Security. For Confidentiality, there are four tools, namely Encryption, Authentication, Access Control, and Authorization. When we consider the confidentiality goal and the corresponding tools, we can easily understand why participants considered these KAs as vital for cyber security. Since hardware development is limited compared to the software development in the country of the participants, they might have selected hardware security as the least influential KA. Similar case might be valid for cyber physical systems because the development of sensors and single board computers is relatively limited. Another reason might be related to the application domain of respondents.

If their company does not develop their own hardware components, their importance might be neglected while responding. In a different country, the result might be different.

- Response to RQ 1.2: Experienced and inexperienced participants differ the most in the following KAs: Cyber Physical Systems, Software Life Cycles, and Vulnerabilities. Experienced experts found these KAs more important compared to the inexperienced cyber security specialists. New graduates might not have seen the importance of software life cycle yet, they might need more time to understand the importance of processes. Also, the huge vulnerability space can be understood after several years' of experience in the field. Cyber Physical Systems might have been neglected by new graduates because they might not have worked with these systems yet.
- Response to RQ 2: Authentication, Authorization, & Accountability, Risk Management & Governance, and Cryptography KAs are considered the most important at work and most instructed subjects at the university. Since cryptography is an old discipline, it is taught in computer security courses in detail. The other KAs are also well known and well described topics in computer security textbooks. Our analysis showed that Web and Mobile Security, Security Operations and Incident Management are the topics that have the highest gap. Since web application development and mobile app development are evolving and new techniques and platforms are being developed day by day, the security aspects related to these technologies might not have been taught in the universities sufficiently. Since incident management and security operations include less technical aspects, they might have been neglected during the courses.
- Response to RQ 3: The largest knowledge gaps appear in the following KAs: Web and Mobile Security, Security Operations and Incident Management. These KAs find themselves in the top four positions in two analyses. This suggests that educators must design new courses on the security aspects of web application development and mobile app development. Also, less non-technical aspects such as incident management must also be covered in the cyber security courses (e.g., computer security).

A similar analysis can be carried out by other cyber security researchers in different countries and different results can be reached. Since this is the first study in this field, we consider that this research can pave the way for further research in this field. Cyber security programs must be enhanced based on the needs in cyber security industry and this kind of research is one of feasible approaches to determine the potential problems in the education system. Finding the right participants for the survey is not an easy task because some of these cyber security experts do not have a formal computer science or computer engineering education and most of them are very busy to respond the detailed questions in this research. Fortunately, we were able to find appropriate participants in this research, however, it would be better if we could increase the number of participants in further research. CyBOK is also evolving and, therefore, the survey might need to be adapted to the new versions in further research. There might be additional KAs and sub KAs in the new versions of CyBOK. However, the general structure of the survey, the followed protocol, and the statistical analysis will be similar. We believe that this study will trigger other cyber security educators to perform similar analysis in near future to improve the quality of their education.

6 Conclusions and future work

There is a growing need for competent Cyber Security personnel in industry. High-quality university education is needed to improve the competency of upcoming workforce. In this study, a questionnaire was designed using the KAs specified in the CyBOK consisting of 19 KA. We analyzed the responses of participants using statistical approaches. The respondents have relevant university degrees and work experience. Two of the most used approaches (i.e., Lethbridge and Kitchenham) are applied to get a broad view on the current state of the university education. Both KA and sub-KA level analysis show that there is a gap that can be exploited to enhance the quality of education. However, we plan to carry out a survey of existing programs/curriculum to make a deeper analysis of the gaps because statistical analysis provides a limited perspective for this statement. For this purpose, we decided to investigate two cyber security programs of leading research intensive universities in the UK, which have a global reputation for excellence. We will also change the format of our interviews because semi-structured interviews are more interesting to analyze relevant university degrees, work experience, and triangulate information about the participants' curriculum.

The following recommendations are provided for educators:

1. Recommendation 1: According to the results, there is a necessity to make some adjustments to the university education. We suggest educators to design new courses on web and mobile security, security operations and incident management, and cyber physical systems. It was determined that adversarial behaviors, web and mobile security, and cyber physical systems are the three key KAs with the highest information gap. The use of each CyBOK KA in the industry was measured in response to the extent of learning in university environments. We recommend educators to address security aspects in these courses (i.e., web programming, mobile programming, cyber physical systems, computer security) or update the curriculum with the addition of these courses.
2. Recommendation 2: To introduce web and mobile application security courses in depth, it is recommended to collaborate with industrial partners because developers in private sector use secure coding principles in daily basis, use automated security testing, and perform penetration testing for mobile applications. Workshops are suggested to be organized and guest lecturers from industry are suggested to be invited in these courses that require state-of-the-practice besides the state-of-the-art. Practical sessions led by industry experts are also suggested to train the students.
3. Recommendation 3: While inexperienced participants did not consider the importance of software development life cycles, experienced ones appreciated their contribution to their daily tasks. Based on this evidence, we suggest educators to cover at least one secure software development life cycle in one of their lectures.

For example, CLASP, the Microsoft Secure Development Lifecycle, and the Software Security Touchpoints are some of the example secure life cycles/processes.

4. Recommendation 4: Vulnerabilities were evaluated differently by the experienced and inexperienced participants. However, vulnerabilities are one of the most important elements of the security. Because of the incomplete patches, hackers can exploit the same zero-day vulnerability over and over in different organizations. Many companies do not shut down the flaws and therefore, hackers keep exploiting the same zero-days. During the formal education of students, it should be emphasized that vulnerabilities must be closely watched and their root causes must be determined to avoid a similar type of problems.
5. Recommendation 5: Hardware security has been considered the least influential knowledge area. This is also the general impression in industry and that is why the hardware security has received limited attention so far. However, recently two security vulnerabilities that allow access to memory locations without the user permission, which are called Meltdown and Spectre, were discovered in modern microprocessors. These flaws were found in several processors from AMD, ARM, Intel and other vendors. Therefore, we suggest educators to emphasize the importance of not only software security but also hardware security because hardware vulnerabilities are growing exponentially over the last few years.
6. Recommendation 6: CyBOK is a very valuable resource for educators. Therefore, different sections of this book can be explained in some courses. These knowledge areas can be discussed in computer security courses to increase the awareness of the students.
7. Recommendation 7: Cyber physical systems have been neglected by new graduates according to survey results. New courses are needed to engineer cyber physical systems because the required knowledge and skills are not gained during the formal education.
8. Recommendation 8: There is a necessity to create long-term job and internship opportunities for the students/graduates and hence, improve their skill sets by encouraging and guiding them through their career paths.
9. Recommendation 9: Non-technical aspects such as incident management and security operations must be also addressed in computer security courses besides the technical topics. Some educators prefer only the technical issues, but this type of non-technical subjects are also crucial for organizational security.

Declarations

Conflicts of interest The authors have no conflicts of interest to declare that are relevant to the content of this article.

References

Ahmed, I., & Roussev, V. (2018). Peer instruction teaching methodology for cybersecurity education. *IEEE Security & Privacy, 16*(4), 88–91.

Anderson, N. H. (1961). Scales and statistics: parametric and nonparametric. *Psychological Bulletin., 58*(4), 305.

Cabaj, K., Domingos D., Kotulski, Z. & Respício, A., (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. Computers & Security, 24

Conklin, W.A., Cline, R.E. & Roosa, T. (2014). Re-engineering cybersecurity education in the US: an analysis of the critical factors. In: IEEE 2014 47th Hawaii International Conference on System Sciences.

Crumpler, W., Lewis, J.A. (2019). Cybersecurity Workforce Gap. JSTOR.

Denning, P. J. (2018). The computing profession. *Communications of the ACM, 61*(3), 33–35.

Garousi, V., Giray, G., & Tuzun, E. (2019). Understanding the knowledge gaps of software engineers: an empirical analysis based on SWEBOK. *ACM Transactions on Computing Education (TOCE) ACM New York, 20*(1), 1–33.

Garousi, V., Giray, G., Tuzun, E., Catal, C., & Felderer, M. (2019). Aligning software engineering education with industrial needs: a meta-analysis. *Journal of Systems and Software. Elsevier., 156*(1), 65–83.

Hintze, J. L., & Nelson, R. D. (1998). Violin plots: a box plot-density trace synergism. *The American Statistician., 52*(2), 181–184.

Jamieson, S. (2004). Likert scales: How to (ab) use them ? *Medical Education., 38*(12), 1217–1218.

Kaspersky, E., & Furnell, S. (2014). A security education Q&A. Emerald Group Publishing Limited.

Kitchenham, B., Budgen, D., Brereton, P., & Woodall, P. (2005). An investigation of software engineering curricula.

Knapp, T. R. (1990). Treating ordinal scales as interval scales: an attempt to resolve the controversy. *Nursing Research., 39*(2), 121–123.

Lethbridge, T. C. (1998). The relevance of software education: A survey and some recommendations. *Annals of Software Engineering., 6*(1), 91–110.

Lethbridge, T.C. (2000). What knowledge is important to a software professional?. Computer. 33(5).

Manson, D., & Pike, R. (2014). The case for depth in cybersecurity education. *Acm Inroads, 5*(1), 47–52.

National Research Council. (2013). Professionalizing the nation's cybersecurity workforce?: Criteria for decision-making. National Academies Press.

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework. *NIST Special Publication, 800*(2017), 181.

Norman, G. (2010). Likert scales, levels of measurement and the laws of statistics. *Advances in Health Sciences Education., 15*(5), 625–632.

Rashid, A., Danezis, G., Chivers, H., Lupu, E., Martin, A., Lewis, M., & Peersman, C. (2018). Scoping the cyber security body of knowledge. IEEE Security & Privacy 16(3).

Research and analysis Cyber security skills in the UK labour market. (2020). Department for Digital, Culture, Media and Sport of UK Government, https://www.gov.uk/government/publications/cyber-security-skills-in-the-uk-labour-market-2020/cyber-security-skills-in-the-uk-labour-market-2020. Accessed 20 Dec 2021.

Yonemura, K., Kobayashi, H., Sato, J., Taketani, H., Oyama, S., Yamada, S., Izumi, S., Okamoto, H., Fujimoto, Y., Sakamoto, Y., Noguchi, K. & Kishimoto, S. (2021). Cybersecurity Teaching Expert Development Project by KOSEN Security Educational Community. In: 2021 IEEE Global Engineering Education Conference (EDUCON). pp. 468-477.

Yoon, K. & Chang, S. (2021). Teaching Team Collaboration in Cybersecurity: A Case Study from the Transactive Memory Systems Perspective. In: 2021 IEEE Global Engineering Education Conference (EDUCON). pp. 841-845.

Goseva-Popstojanova, K., & Hensel, R. A. (2021). Educating the Next Generation of Cybersecurity Experts. In: 2021 ASEE Virtual Annual Conference Content Access, Virtual Conference.

Chou, T., & Mohammed, T. (2021). Self-assessment of Knowledge Levels in the Subjects of Cyber Attacks and Defense in a Cybersecurity Awareness Education Workshop. In: 2021 ASEE Virtual Annual Conference Content Access, Virtual Conference.

Alrabaee, S. & Manna, R. (2021). Boosting Students and Teachers Cybersecurity Awareness During COVID-19 Pandemic. In: 2021 IEEE Global Engineering Education Conference (EDUCON). pp. 726-731.

Troja, E., DeBello, J. & Roman, N. (2021). Teaching Efficient Computer Science and Cybersecurity Courses Amidst the COVID-19 Pandemic. In: 2021 IEEE Global Engineering Education Conference (EDUCON). pp. 510-520.

Romanovs, A., Bikovska, J., Peksa, J., Vartiainen, T., Kotsampopoulos, P., Eltahawy, B., Lehnhoff, S., Brand, M. & Strebko, J. (2021). State of the Art in Cybersecurity and Smart Grid Education. In: IEEE EUROCON 2021 - 19th International Conference On Smart Technologies. pp. 571-576.

Ricci, J., Breitinger, F., & Baggili, I. (2019). Survey results on adults and cybersecurity education. *Education and Information Technologies., 24*(1), 231–249.

Valerio, M. A., Rodriguez, N., Winkler, P., Lopez, J., Dennison, M., Liang, Y., & Turner, B. J. (2014). Comparing two sampling methods to engage hard-to-reach communities in research priority setting. A survey of controlled experiments in software engineering. *BMC Medical Research Methodology, 16*(1), 1–11.

Van Belle, G. (2011). Statistical rules of thumb. *BMC medical Research Methodology, 16*(1), 1–11 (John Wiley & Sons).

Vogel, R. (2016). Closing the cybersecurity skills gap. *Salus Journal, 4*(2), 32–46.

Wilk, A. (2016). Cyber security education and law. In: IEEE International Conference on Software Science, Technology and Engineering (SWSTE). pp. 94–103.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Authors and Affiliations

Cagatay Catal[1] · Alper Ozcan[2] · Emrah Donmez[3] · Ahmet Kasif[4]

✉ Alper Ozcan
alperozcan@akdeniz.edu.tr

Cagatay Catal
ccatal@qu.edu.qa

Emrah Donmez
emrahdonmez@bandirma.edu.tr

Ahmet Kasif
ahmet.kasif@btu.edu.tr

[1] Department of Computer Science and Engineering, Qatar University, Doha, Qatar

[2] Department of Computer Engineering, Akdeniz University, Antalya, Turkey

[3] Department of Software Engineering, Bandirma Onyedi Eylul University, Balikesir, Turkey

[4] Department of Computer Engineering, Bursa Technical University, Bursa, Turkey