Report on CyBOK Usage in the Classroom

Nancy R. Mead Bastian Tenbergen

nrmcmu@gmail.com bastian.tenbergen@oswego.edu

August 2023

Table of Contents

Abstract

The Cyber Security Body of Knowledge (CyBOK) [1] has been developed to serve, among other uses, as an instructional reference for educators to prepare the next generation of security engineers in cybersecurity. We developed a survey which was distributed broadly, to elicit feedback from educators on the extent to which CyBOK is being used in the classroom. We were particularly interested in learning which of the CyBOK knowledge areas was being taught, desired learning outcomes, what other BOKs and curricula were in use, and additional topics that educators wished to have added to CyBOK.

The invitation to take the survey was distributed to the CSEE&T mailing list, the CyBOK subscribers, and it was posted various social media platforms, including the Software Assurance Education Group on LinkedIn, the Software Engineering Research and CSEE&T conference groups on Facebook, and Twitter. In all, the invitation went out to thousands of educators. We received 34 responses, 28 of which were complete. The others indicated that they did not teach cybersecurity in their courses, so those incomplete surveys were not included in the results. The invitation questions and responses appear here, as well as our personal assessment of the results, and suggestions for possible future work.

1 Introduction

As the increase and dependence on digitally enabled technology continues to impact almost every area of life, it has created a demand for innovative software-based solutions. However, developing secure software is a multi-faceted activity that can strain a project's budget, design, and overall functionality [2]. The demand for software often pits delivery value at high speed against high quality. In 2020, poor quality software cost organizations $2.08 trillion in the United States alone [3]. The U.S. government tracks software vulnerabilities in their National Vulnerability Database, which is fed by the Common Vulnerabilities and Exposures list. By 2020, more than 18,000 software code vulnerabilities had already been included [4].

In her 2000 paper, Mary Shaw [5] called, among other things, for software engineering education to start at the earliest feasible point during the students' university career and to seek out ways to improve role-specific software engineering education. Now, more than 20 years later, her call has been answered with many software engineering curricula offering broad experiences as well as avenues for specialization, for example, in requirements engineering [6], [7], testing [8], or supply chain risk management [9], [10]. Yet, in today's rapid development environment, security engineering has become a specialization that will only grow in demand [11]. As modern systems are increasingly interconnected and exchange mission-critical, confidential data with one another, they become attractive targets for attackers. Hence, systems must be sufficiently hardened against any type of vulnerability.

Designing such systems requires a substantial amount of security-relevant knowledge, attention to detail, and a considerable level of experience. To help educate the new generation of security engineers, a recent effort led by the University of Bristol compiled and produced a substantial resource called the "Cyber Security Body of Knowledge" (CyBOK) [1]. CyBOK 1.1 is structured in five parts and 21 chapters, each of which suggests knowledge areas (KAs) related to social, organizational, technical, and procedural issues in cybersecurity. CyBOK is intended to serve as a reference curriculum and resource material for instructors to structure cybersecurity education.

Over the course of our prior CyBOK work, we realized that we did not have any insight into whether those faculty teaching cybersecurity topics were aware of CyBOK and the associated resources on the CyBOK site, and whether they were using them in their courses. The purpose of the survey was to try to get a preliminary insight into what was happening in the classroom, and also to learn what might be useful to them in future editions of CyBOK, which can be investigated in further detail in future, more rigorous studies. This motivated us to survey a broad spectrum of educators who might be teaching cybersecurity topics and get a better understanding of what was being taught, the expected learning outcomes, and what they would like to see in future CyBOK editions.

This report is structured as follows. Section 2 gives some background on the CyBOK and includes the survey invitation. Section 3 describes the study design. Section 4, we discuss survey results based on the raw data presented in the Appendix. In Section 5, we make suggestions for actions to increase CyBOK classroom usage, and in Section 6 we discuss future related work.

2 Background & Related Work

The Cyber Security Body of Knowledge Version 1.1 (CyBOK) is a freely accessible community resource funded by the National Cyber Security Programme in the United Kingdom and published under the Open Government License [1]. CyBOK is an attempt to consolidate cybersecurity as a discipline, which in the past has been fragmented [12]. By contrast, in fields such as software engineering, computer science, or chemistry, there have been collaborations with leading professional societies that have codified key foundational knowledge on which educational programs have been designed and developed (e.g., the Software Engineering Body of Knowledge, SWEBOK, see [13]). Other efforts have established skills, tasks, competencies, risk, and cyber frameworks that exposed many facets to the discipline [14]. A more recent global undertaking with four leading professional societies and a host of academics and practitioners forming a Joint Task Force, resulted in a comprehensive curricular volume to structure the cybersecurity discipline and provide guidance for cybersecurity education [15]. However, among the diverse community of academics, practitioners, and researchers, there has not been progress in reaching a consensus of what is considered the foundational knowledge in cybersecurity [12], [15].

In CyBOK Version 1.1, 21 Knowledge Areas (KAs) form the scope of the CyBOK [1]. The 21 KA are grouped into the following five categories, as shown below. Note, that the numbering scheme herein adopts the chapter numbers from CyBOK, and therefore starts at “2”. A detailed description of the categories, knowledge areas is available in the CyBOK Version 1.1 companion text [16].

I. Human, Organisational & Regulatory Aspects
2. Risk Management and Governance
3. Law & Regulation
4. Human Factors
5. Privacy & Online Rights

II. Attacks & Defences
6. Malware & Attack Technologies
7. Adversarial Behaviour
8. Security Operations & Incident Management
9. Forensics

III. Systems Security
10. Cryptography
11. Operating Systems & Virtualisation
12. Formal Methods for Security
13. Distributed Systems Security
14. Authentication, Authorisation & Accountability

IV. Software Platform Security
15. Software Security
16. Web & Mobile Security
17. Secure Software Lifecycle

V. Infrastructure Security

18. Applied Cryptography
19. Network Security
20. Hardware Security
21. Cyber-Physical Systems Security
22. Physical Layer & Telecommunications

In our earlier work, we focused our efforts on artifacts that could be used in the classroom to teach CyBOK topics. A number of other authors of CyBOK resources had the same goal, with the result that a large body of resources appears on the CyBOK website. However, this did not provide us with an indicator of how much CyBOK or those resources was actually being used to teach cybersecurity topics. The survey was developed to give us a preliminary indication of classroom use of CyBOK, to better guide future, more detailed investigations, the development of CyBOK content, as well as marketing and outreach efforts.

3 Study Design

In this section, we describe the study design. The study was intended as a market analysis to generate useful results quickly and with sufficient rigor, by probing the likely "customer base" of CyBOK, i.e., educators teaching cybersecurity in software engineering courses. For this reason, study design and sampling focused on an established community of educators in this area.

3.1 Research Questions

There were two primary research questions that we wanted to answer, which had not been addressed adequately in our prior CyBOK work. We had anecdotal feedback on some of these research question, but that was all, and it seemed that this was the case for other CyBOK resource contributors as well. These questions were:

R1: To what extent are CyBOK 1.1 topics being taught in the classroom?

R2: What additional resources would help to transition CyBOK 1.1 into broad classroom usage?

We wanted to survey a large pool of instructors. We knew that surveys tend to result in a relatively small response rate, but a survey would balance results from questionnaires and individual inquiries to faculty who were known to already be teaching CyBOK 1.1. In addition to these broadly stated research questions, we wanted to obtain results for each CyBOK 1.1 topic, rather than a simple yes/no as to whether CyBOK 1.1 was being taught, and this was reflected in the survey questions.

We also wanted to understand whether additional transition resources would result in broader usage of CyBOK 1.1 in the classroom. To answer this question, we included a number of questions about the resources already being used by instructors who were teaching CyBOK 1.1 topics, and prompted the instructors responding to the survey by itemizing all of the resources we thought were likely to be used. These included not only the materials on the CyBOK site but other cybersecurity and software engineering resources.

3.2 Methodology

3.2.1 Survey Instrument

The survey instrument was created based on the Technology Acceptance Model v3 (TAM3, see [17]) items pertaining to an individual's familiarity with a given technology (RQ1) and their ability to apply it, given their professional context (RQ2). In other words, we took the TAM3 topics pertaining to the "Perception of External Control" and "Objective Usability". According to TAM3, these items are defined as follows [CyBOK-specific definition adaptations shown in brackets]:

- ***Objective Familiarity:*** *A "comparison [of Cybersecurity Frameworks] based on the actual level (rather than perceptions) to effort required to use [CyBOK in instruction]."*
- ***Perception of External Control:*** *The degree to which an individual believes that organizational and technical resources exist to support the use of [CyBOK in instruction].*

Our rationale for selecting these TAM3 topics for inquiry was that "Objective Familiarity" investigates whether or not CyBOK has generated sufficient awareness among educators in the field of cybersecurity to enable adoption in the classroom. This addresses RQ1. Correspondingly, the TAM3 topic "Perception of External Control" investigates whether, given the awareness and awareness of competing cybersecurity educational frameworks, educators are likely to select CyBOK, why they would, or rather: which obstacles do they face. Together with free-form reflection questions inviting the participants to introspect about CyBOK adoption, this addresses RQ2.

Since it was our aim to generate as many responses as possible, we opted for a brief survey that could be filled out quickly by participants. We hence defined questions pertaining to the above-referenced TAM3 topics and defined a logical structure to guide the participants through the survey. For questions pertaining to familiarity, we defined a 4-point Likert-style semantic differential with ordinates roughly corresponding to Bloom's Taxonomy [18] to assess which proficiency levels with CyBOK topics educators strive to teach their students.

The survey instrument was conceived and validated for completeness and conciseness between both authors by taking turns, before it was implemented in Google Forms (to foster participant privacy). After its implementation, it was piloted and validated by external reviewers for correctness and logical adequacy.

For legal reasons pertaining to ethics approval and user privacy in the United States, the survey was kept 100% anonymous and no identifying data were collected from participants.

3.2.2 Sampling Method

Once implementation and validation of the survey instrument concluded, the survey was distributed through the Mailing List maintained by the Steering Committee of the International Conference of Software Engineering Education & Training (CSEE&T). At the time of sending the invitation for participation, this mailing list included roughly 1,000 subscribers. Using the mailing list provider's social media integration plugin, the invitation was simultaneously forwarded to roughly 250 followers on Twitter (now X) and roughly 500 followers on Facebook, including those in the Software Engineering Research group. Corresponding posts and invitations were sent out by both authors through their LinkedIn accounts, groups therein, such as the Software Assurance Education group (until LinkedIn discontinued the group feature), and personally to colleagues. In total, we estimate roughly 2,000 unique individuals to have been invited.

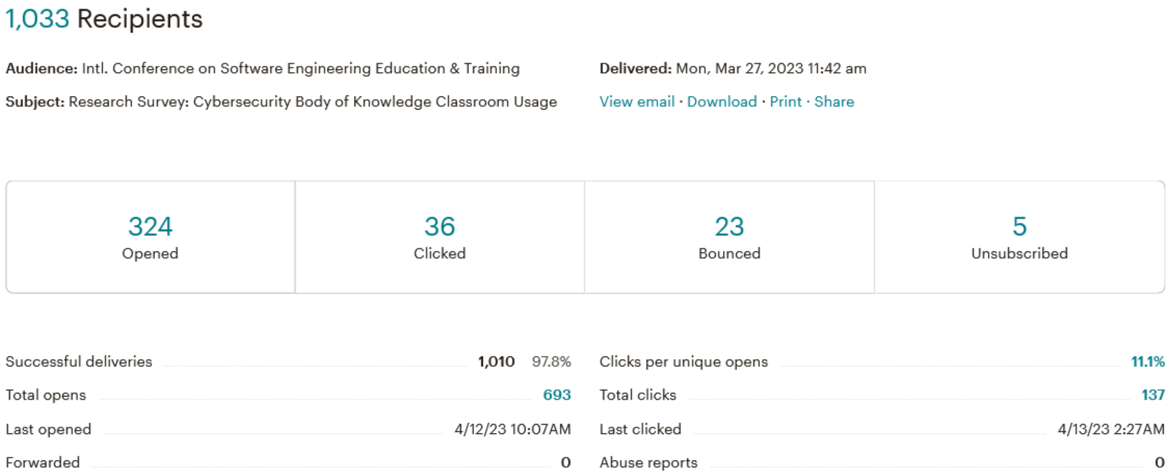
In our invitation, we were careful to assure participants that their input would be collected anonymously and only appear in summary form. This had the advantage of encouraging participation and alleviated any concerns we might have had about whether this was human subject research. However, a disadvantage was that we did not know who filled out the survey, what they actually were teaching and where they were located, nor were we able to go back and ask follow-up questions. The text of the invitation to participate appears below, and the invitation also included our names and Email addresses:

> *Colleagues,*
> *Over the last few years we have contributed to the freely available resources associated with the Cyber Body of Knowledge https://www.cybok.org/, through*

> *their small projects. We are currently working on a small project that includes a survey of the extent to which CyBOK is being used in the classroom. It would really help us if you could complete this short survey by April 7. The results will only be reported in summary form and your participation will be anonymous. Of course, in addition to participating in the survey, you can always feel free to contact us via Email. We really appreciate your support!*

3.2.3 Demographics

Since data collection was anonymous, response patterns via social media and personal contacts cannot be tracked. However, the CSEE&T mailing list provider indicated that about 1/3 of mailing list recipients opened the email, with about then 11% of them clicking on the link included therein, as seen below. These results are roughly equivalent to regular CSEE&T mailing list performance. Although these numbers at first glance seem low, given past experiences with solicitations via this mailing list, we consider this to be highly successful. Moreover, these results are in line with decreased participant interactivity via online questionnaires since the COVID-19 pandemic and seems to indicate that participants grow increasingly tired of articulating responses digitally. Nevertheless, we felt that the survey responses provided valuable input to the CyBOK program.


1,033 Recipients

Audience: Intl. Conference on Software Engineering Education & Training

Subject: Research Survey: Cybersecurity Body of Knowledge Classroom Usage

Delivered: Mon, Mar 27, 2023 11:42 am

324	36	23	5
Opened	Clicked	Bounced	Unsubscribed

Successful deliveries	1,010	97.8%	Clicks per unique opens	11.1%
Total opens	693		Total clicks	137
Last opened	4/12/23 10:07AM		Last clicked	4/13/23 2:27AM
Forwarded	0		Abuse reports	0

In total, the survey generated more than 100 partial responses on Google Forms (unfortunately, most of them only answered one question, therefore yielding no reliable results). Pruning incomplete datasets yielded a total of 28 high-quality responses, which we subjected to analysis.

3.3 Analysis Procedure

As noted in the discussion by Wohlin et al [19] our goal for the survey was to reach a representative sample of the target audience, namely those instructors who were likely to be teaching topics included in CyBOK 1.1. We elected to cast a wide net, so that we would not be surveying only those instructors who were known to be teaching CyBOK 1.1 topics, but also those who were teaching software engineering, software assurance, or cybersecurity more broadly. In this way the sample could be considered broader rather than targeted. A different survey might have assessed whether instructors who were already known to be teaching CyBOK 1.1 topics found the CyBOK website materials useful, or whether different materials would be more useful to them in the classroom.

One of our objectives in the survey design was to gather information in such a way that basic results could be summarized automatically, thus easing the analysis burden. To that end, we minimized the number of open-ended questions that might result in lengthy responses requiring manual analysis. It’s worth noting that the requirement for anonymity for the responders meant that we could not go back to them for clarification on their answers in any case. We were thus able to obtain a considerable amount or basic statistics automatically, as will be seen in Section 4 of this report. Once we had the basic results, it was fairly easy to see the common threads in the results. These appear in Section 5.

3.4 Threats to Validity

Despite careful deliberation on method, analysis, and procedure, some threats to validity remain in any study. These are described based on Wohlin et al.'s [19] suggested structure:

Internal Validity. Internal validity pertains to threats to the validity of results due to the fundamental purpose and design of the study. The most significant threat to this study is the aim and scope. This study was not intended as a classical research study, but rather as preliminary market analysis, independent of CyBOK's own efforts. As market analyses do not require ethics board approval (exception status according to 45 US CFR 46.104(d) (2), "consumer acceptance survey"), provided that identifiable information are not collected (subpart (6)). This limitation was necessary due to the brief CyBOK project interval and the fact that ethics board approval requires upward of 9 months of lead-up time between survey instrument creation and data collection. Hence, this study was designed as a preliminary market analysis to guide a future, more in-depth and empirically sound investigation. As a consequence, the insights gained from this study are limited to that of participant familiarity and external control of applying CyBOK in their curriculum.

Construct Validity. Construct validity pertains to threats to result validity due to improperly designed instruments that do not fit the operational purpose of the study. As outlined in Section 3.2.1, we took great care to design a logically coherent and pedagogically adequate instrument despite the market research classification of the study. We used accepted standard software engineering instruments, i.e., the Technology Acceptance Model version 3, as the guide to create the instrument and subjected it to several weeks of refinement and iteration. Albeit sampling was convenient, mailing list and social media outreach is comparable to other CSEE&T publicity and therefore considered highly successful, given the brief data collection period (2 weeks given the short project period). Longer data collection time and repeated solicitation may have increased response count, but also the likelihood of unsubscribes to the mailing list, which would have been very bad for the CSEE&T conference and would probably not have resulted in much different results, hence minimizing this threat.

Conclusion Validity. Conclusion validity pertains to the degree to which conclusions are biased by the experimenters or data collection method, and hence not supported by the data. We the authors were quite aware of the limitation of the study and therefore refrained from hypothesis testing or analytical conjecture. While we are strongly and positively biased in favor of CyBOK and its use and receive partial compensation for conducting the study, we nevertheless took great care as to not let our personal opinions dictate a particular outcome of the study. We therefore restricted ourselves to objective and descriptive analysis of survey results, rendering conclusions in the form of recommendations for CyBOK to further improve market penetration.

External Validity. External validity pertains to the degree to which conclusions are representative of the sampled population and hence generalizable. Despite the objectively low response rate of only 28 complete participant responses, the response rate is roughly in line with typical online survey return rates (ca. 11.6% of people who read the invitation mail and ca. 77% of people who followed the invitation link, based on mailing list statistics alone, see Section 3.2.3). Given the diversity and general population of the solicited population, we believe that the results are therefore representative and generalizable to a general population.

4 Survey Results

In this section, we present the raw responses from the participants and provide a discussion of their implications. The summary for the 28 detailed responses to our survey follows here. In the survey itself, in order to keep it simple, most of the questions have yes/no or multiple-choice answers, with the opportunity for a few text inputs. The questions were grouped into topic areas based on TAM3 topics. We will discuss results pertaining to the topic areas as follows, raw survey results can be found in the Appendix.

4.1 CyBOK Familiarity

Most of the respondents, probably due to the way it was distributed, were familiar with CyBOK and taught courses that included cybersecurity topics. About half of them used CyBOK in their courses. Some used other BOKs or curricula instead of or in conjunction with CyBOK, but others apparently did not rely on a specific reference when teaching cybersecurity.

4.2 CyBOK Usage

We were pleased to note that nearly half of the respondents teaching cybersecurity used CyBOK in their courses. Considering the number of other curricula and BOKs available, we thought that this was a high usage percentage. Among the other half not using CyBOK, no particular curriculum or body of knowledge stood out as being a dominant competitor. SWEBOK, which is not specific to cybersecurity, was cited more, but the numbers were too small to draw any conclusions. It's worth noting that among the participants not using CyBOK exclusively, a majority still used CyBOK in conjunction with other sources.

4.3 CyBOK Topic Coverage (and expected student learning outcomes)

When it came to specific CyBOK topics, some respondents in every topic area indicated that student learning outcomes included the ability to contribute to the topic, and not just apply it. In addition, in many cases students were expected to be able to apply their knowledge of CyBOK topics, and not just be familiar with it, hence suggesting that educators strive for higher levels in Bloom's taxonomy. On the other hand, some topic areas were not taught as extensively, probably for a variety of reasons. For example, it's understandable that *Law & Regulation* would not be a topic that was treated in depth in a standard course focusing on technical aspects of software engineering. Similarly, students might lack the background or not have the need to apply *Forensics*, *Formal Methods*, or *Hardware Security* due to the large amount of prerequisite knowledge (e.g., most universities teach formal methods in graduate programs). In many cases, the goal was for students to have a level of awareness. This would be typical for students taking an intro course in cybersecurity, for example. Also, if cybersecurity was sandwiched into a course on another topic, such as a more traditional software engineering or computer science course, there would not be much time to devote to it.

4.4 CyBOK Reflection

In the Reflection section of the survey, insufficient time was also a response to the question of why some CyBOK topics were not taught. For the cybersecurity topics that were taught, around 2/3 of the respondents were either unaware of the resources on the CyBOK site or did not use them. This was disappointing and triggered some of the recommendations in Section 5 of this report.

There were fewer suggestions on topics to add to future editions of CyBOK. However, we suggest that the CyBOK sponsors specifically consider the answers to that question when new versions of CyBOK are developed. Overall, the survey provided valuable information. Considering the size of our distribution lists, the number of respondents to the survey was relatively small. This could indicate that the people on our lists either don't teach cybersecurity topics as a primary focus, they are too busy, or that they are asked to respond to so many surveys, that they just deleted the request. This last assertion is supported by the fact that statistics for the CSEE&T mailing list outlined in Section 3.2.3.

5 Recommendations

The complexities of software engineering and the competencies expected of software application developers are continually increasing. Central to building competencies is knowledge that must be organized, systematically communicated, and applied to real-world situations. Learning the requisite knowledge is critical for the security of an organization, however, educators have often struggled in understanding how learning occurs. To aid in this understanding, a variety of learning models have been developed along with measuring specific outcomes, setting threshold standards, and the development of learning frameworks [20]. The many learning models that have been developed provide the basis to help understand learning behaviors and ultimately to inform the design of instruction in the classroom. Real-world case studies have been instrumental and are often utilized to assist software engineers in obtaining requisite knowledge as well as to develop problem solving skills for projects they will encounter after graduation.

Our objective for the survey and this report was to gain an initial understanding of CyBOK classroom usage. Based on the results of the survey, we would recommend the following:

- The CyBOK website [1] contains excellent resources that are of interest to a broad audience, not just those who are teaching cybersecurity. Since the topic is of international interest, ***we recommend a much broader publicity campaign***. When we work only with our immediate colleagues, we may not realize that our work is going unnoticed elsewhere. Such a publicity campaign could include:
    - Providing flyers about CyBOK to all major cybersecurity, software engineering, and education conferences worldwide
    - Branching out to additional publicity venues, such as the media, particularly at an international level
    - Giving virtual (and in-person) talks on CyBOK and the associated resources
    - Placing associated resources of funded CyBOK projects at a central place in outreach activities.
- Those who are teaching cybersecurity are often using their own materials in lieu of CyBOK. This could be because their own materials were developed in advance of CyBOK, or because they are experts in their own right and don't feel the need to use resources from elsewhere. ***We suggest activities to make it easier to adopt CyBOK for classroom use***. These could include:
    - Conducting seminars and workshops on CyBOK and its resources at international conferences. During a workshop, attendees could be encouraged to develop materials for their own use, with CyBOK as a baseline. Generally, this would involve a preliminary course design with CyBOK as a resource, with one or two example lectures or classroom activities.
    - Conducting in-depth professional development workshops for both industry and academe, as well as government training organizations, in train-the-trainer mode, so that the attendees finish the workshops with actual course materials.
- If organizations are not aware of CyBOK, they won't be contributing to its evolution. ***We encourage continuing to press industry, government, and academe to be involved in future CyBOK development.*** Once again, if organizations are not aware of CyBOK's existence, they can't contribute to its usage or future development.

6 Conclusion and Future Work

In this report, we presented the results of a survey on CyBOK usage in the classroom. The work was supported by The UK National Cyber Security Centre [1], [16]. The purpose of the survey was to gain a preliminary understanding regarding the extent to which faculty were aware of and using CyBOK and its resources in courses that included cybersecurity topics in order to drive marketing and funding campaigns as well as future investigations into CyBOK's market status. A secondary goal was to gather feedback on which other bodies of knowledge and curricula were in use, as well as the participants recommendations for future iterations of CyBOK. Future work could include a similar survey to gain follow-up information on whether there has been increased adoption of CyBOK for classroom use. Also, if we were to reach beyond the classroom, it would be good to conduct a survey to learn the extent to which CyBOK and its resources are being used in practice.

Acknowledgements

The authors appreciate the kind funding from The UK National Cyber Security Centre to facilitate CyBOK usage, and to collect feedback on the extent to which this is occurring. We thank the survey participants for their input and recommendations for this valuable effort.

References

[1] The National Cyber Security Centre, The Cyber Security Body of Knowledge (CyBOK), Version 1.1. © Crown Copyright, 2021, UK Open Government License. Accessed 12/31/2021, available at: https://www.cybok.org/

[2] Chowdhury, N., Adam, M., Skinner, G., The Impact of Time and Pressure on Cybersecurity Behavior: A Systematic Literature Review. Behavior & Information Technology 38(12), 2019, pp. 1290-1308.

[3] Krasner, H. The Cost of Poor Software Quality in the US: A 2020 Report. Consortium for Information & Software Quality. 2021. https://www.it-cisq.org/pdf/CPSQ-2020-report.pdf

[4] O'Driscoll, A. 25+ cyber security vulnerabilities statistics and facts of 2021. Comparitech, 2021, https://www.comparitech.com/blog/information-security/cybersecurity-vulnerability-statistics/

[5] Shaw, M., Software Engineering Education: A Roadmap. In Proc. Future of Software Engineering, 2000, pp. 371-380.

[6] Sedelmaier, Y., Landes, D., Systematic evolution of a learning setting for requirements engineering education based on competence-oriented didactics. In Proceedings of the IEEE Global Engineering Education Conference, 2018, pp. 1062–1070.

[7] Gabrysiak, G., M. Guentert, R. Hebig, and H. Giese, Teaching requirements engineering with authentic stakeholders: Towards a scalable course setting. In Proceedings of the First International Workshop on Software Engineering Education Based on Real-World Experiences 2012, pp. 1–4.

[8] Mishra, D., Ostrovska, S., Tuna, H., Exploring and expanding students' success in software testing, Information Technology and People 30(4), pp. 927-945, 2017. DOI:10.1108/ITP-06-2016-0129.

[9] Sonatype, 2020 State of the Software Supply Chain: The 6th annual report on global open-source software development, Fulton, MD. https://www.sonatype.com/hubfs/Corporate/Software%20Supply%20Chain/2020/SON_SSSC-Report-2020_final_aug11.pdf

[10] Shoemaker, D., Mead, N., Kohnke, A., Teaching Secure Acquisition in Higher Education. IEEE Security & Privacy 18(4), pp. 60-66, 2020.

[11] Bosch, J., Speed, Data, and Ecosystems: The Future of Software Engineering. IEEE Software 33(1), 2015, pp. 82-88.

[12] Ramirez, R., Choucri, N., Improving Interdisciplinary Communication with Standardized Cyber Security Terminology: A Literature Review. IEEE Access 4, 2016, pp. 2216-2243.

[13] Bourque, P., Fairley, R., Guide to the Software Engineering Body of Knowledge (SWEBOK ®), Version 3.0. IEEE Computer Society Press, 2014.

[14] Švábenský, V., Vykopal, J., Čeleda, P., What are Cybersecurity Education Papers About? A Systematic Literature Review of SIGSCE and ITiCSE Conferences. In Proceedings of the 51st ACM Technical Symposium on Computer Science Education, pp. 2-8, 2020.

[15] Joint Task Force on Cybersecurity Education: Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity Education. accessed 5/27/21, available at: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

[16] Rashid, A., Chivers, H., Danezis, G., Lupu, E., Martin, A. (Eds.), The Cyber Security Body of Knowledge. © Crown Copyright, The National Cyber Security Centre, 2021. Accessed 12/31/21, available at: https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf

[17] Venkatesh, V., Bala, H.: Technology Acceptance Model 3 and a Research Agenda on Interventions. Decision Sciences 39(2), May 2008, pp. 273-315.

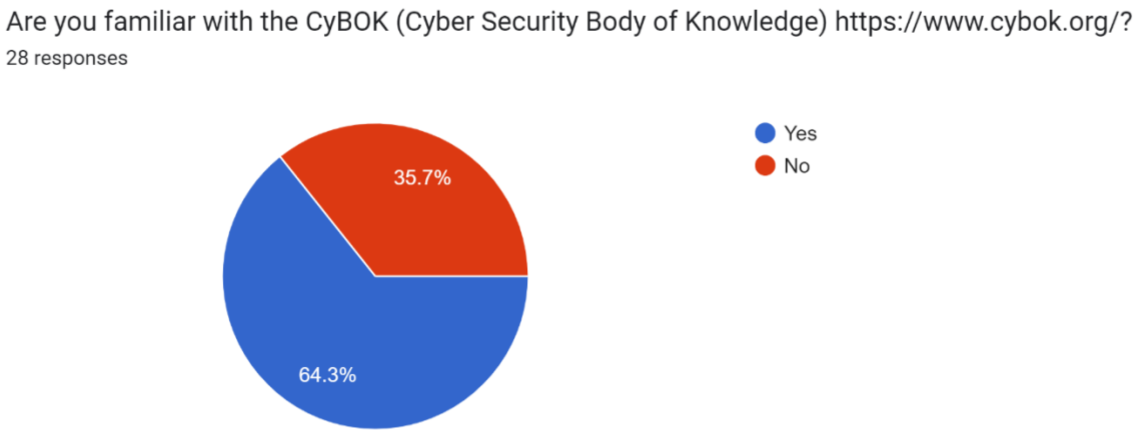
[18] Bloom, B.S., Engelhart, M.D., Furst, E.J., Hill, W.H., Krathwohl, D.R.: Taxonomy of Educational Objectives: The Classification of Educational Goals. Handbook I: Cognitive Domain. David McKay Company, 1958.

[19] Wohlin, C., Runeson, P., Höst, M., Ohlsson, M.C., Regnell, B., Wesslén, A.: Experimentation in Software Engineering. Springer, 2012.

[20] Voorhees, R.A., Competency Based Learning Models: A Necessary Future, New Directions for Institutional Research, 2001, No. 110, Summer, John Wiley & Sons, Inc.

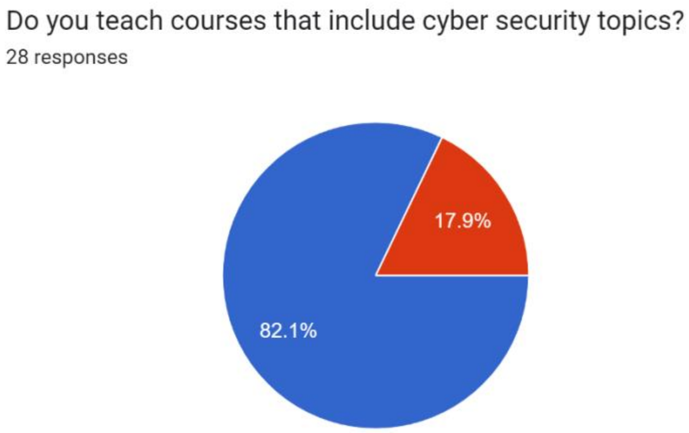
Appendix: Raw Survey Responses

1. CyBOK Familiarity



Are you familiar with the CyBOK (Cyber Security Body of Knowledge) https://www.cybok.org/?

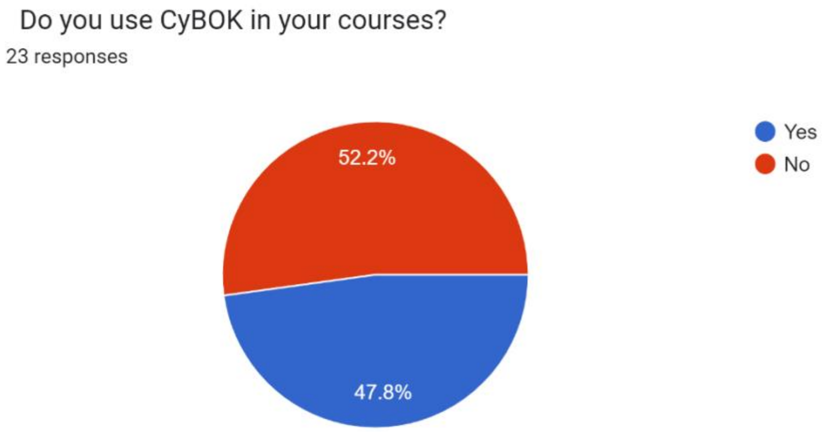
28 responses



Do you teach courses that include cyber security topics?

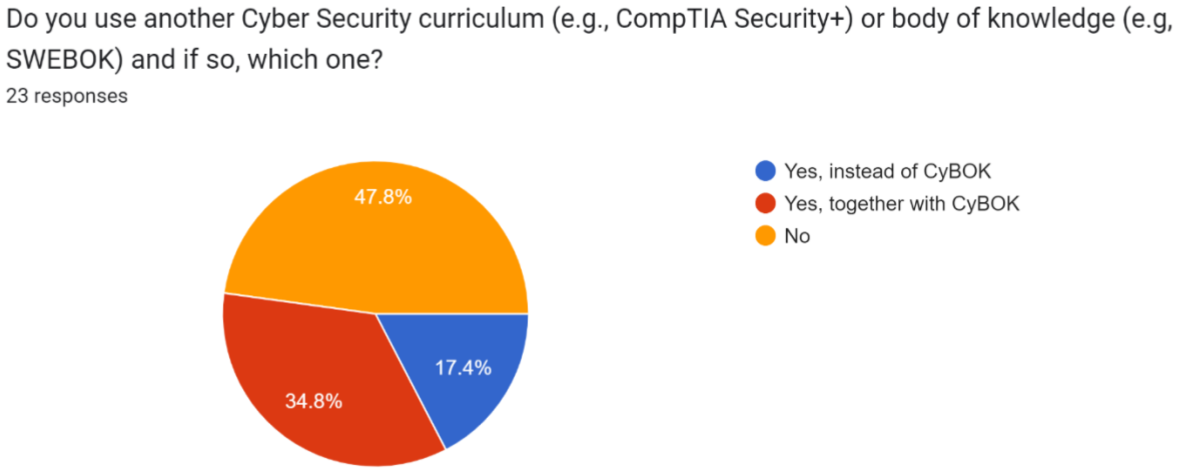
28 responses

2. CyBOK Usage



Do you use CyBOK in your courses?

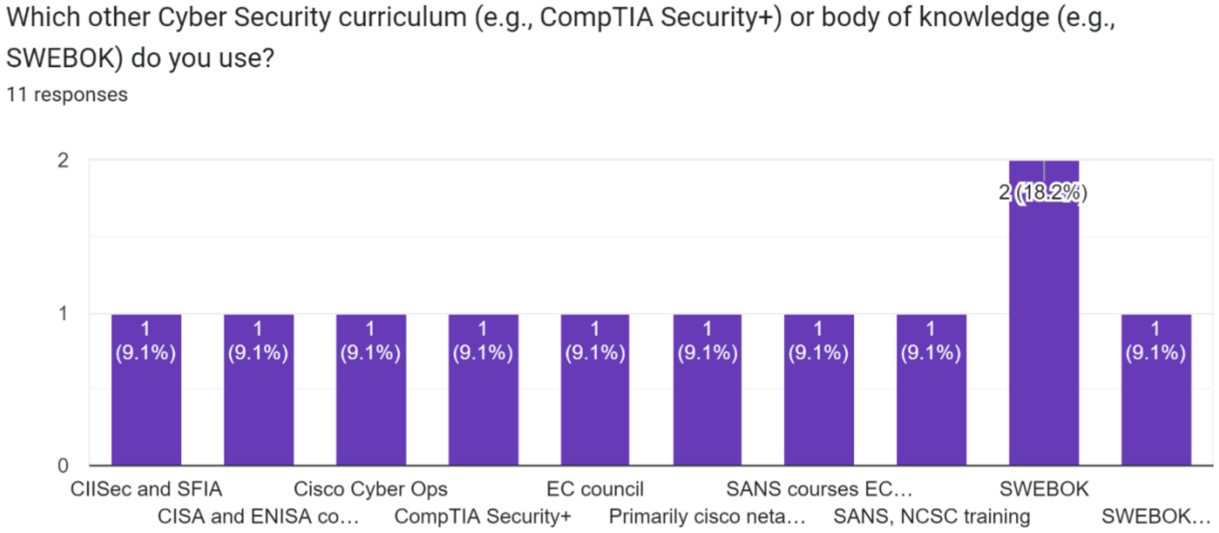
23 responses



Do you use another Cyber Security curriculum (e.g., CompTIA Security+) or body of knowledge (e.g, SWEBOK) and if so, which one?

23 responses

Other BOKs

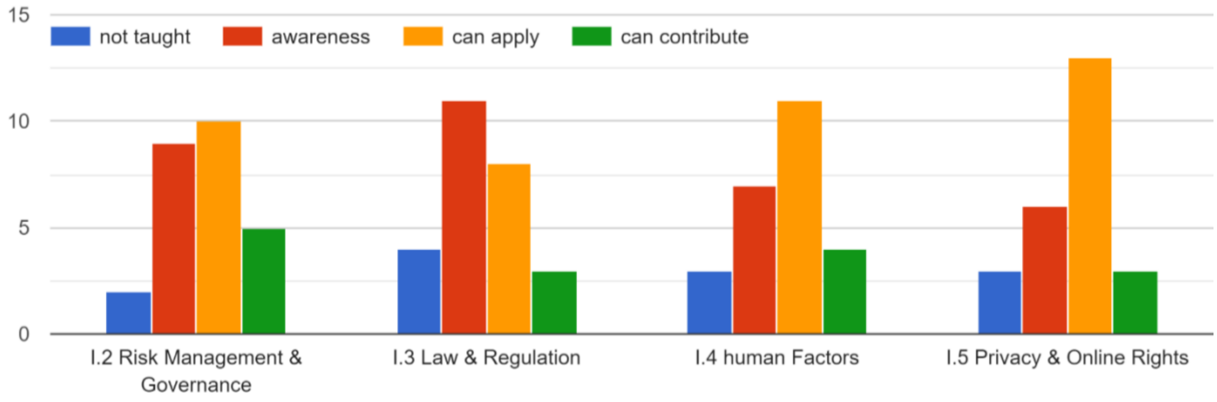


Which other Cyber Security curriculum (e.g., CompTIA Security+) or body of knowledge (e.g., SWEBOK) do you use?

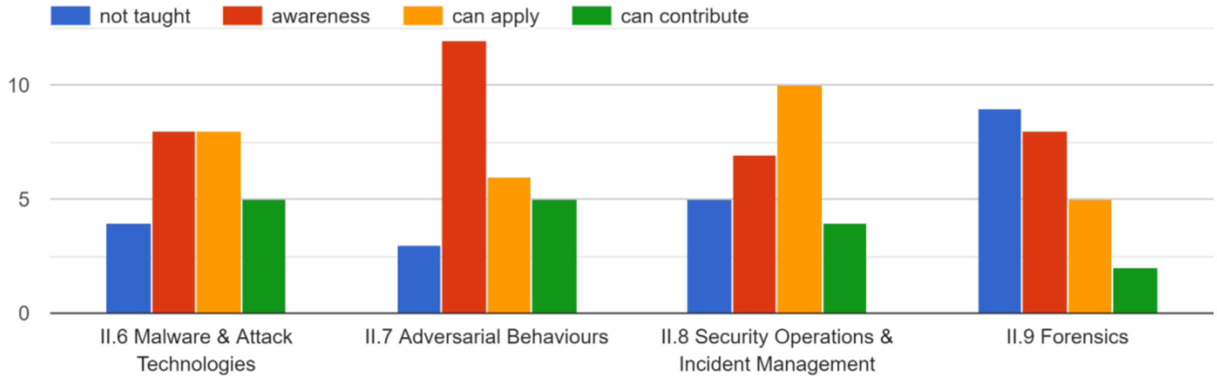
11 responses

3. CyBOK Topic Coverage

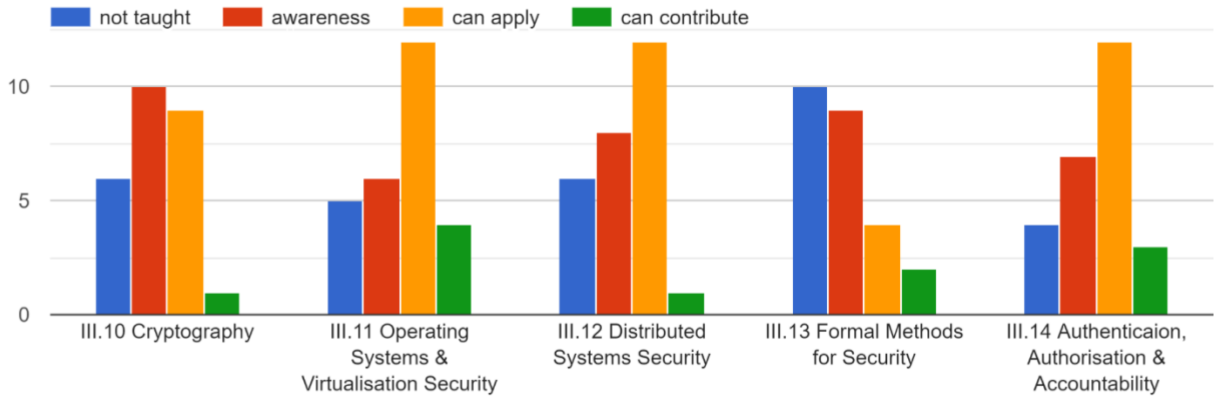
Human, Organizational and Regulatory Aspects



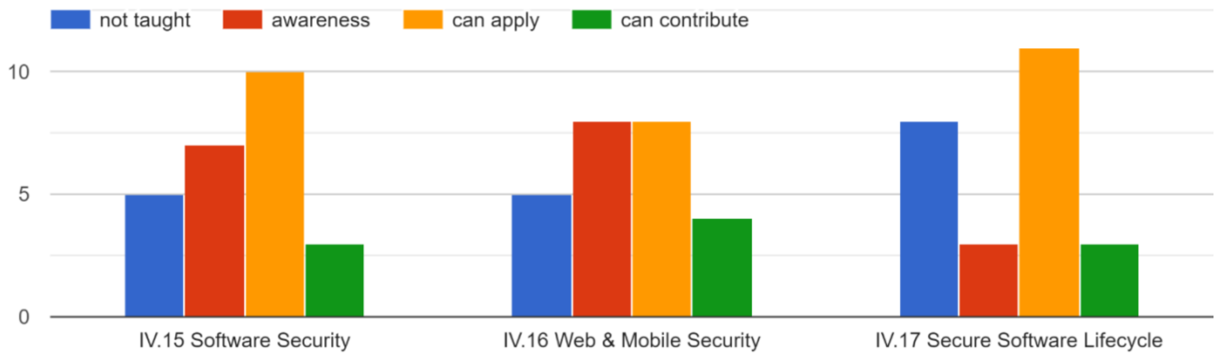
Attacks and Defences



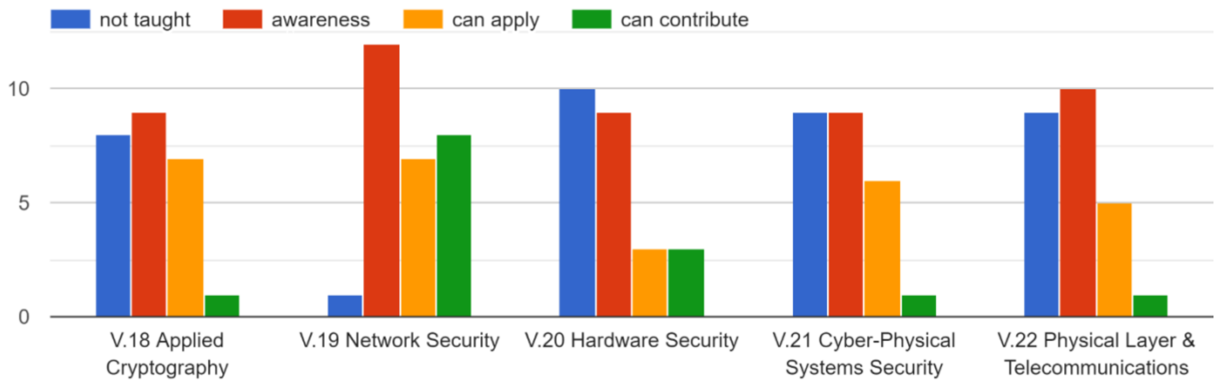
Systems Security



Software Platform Security



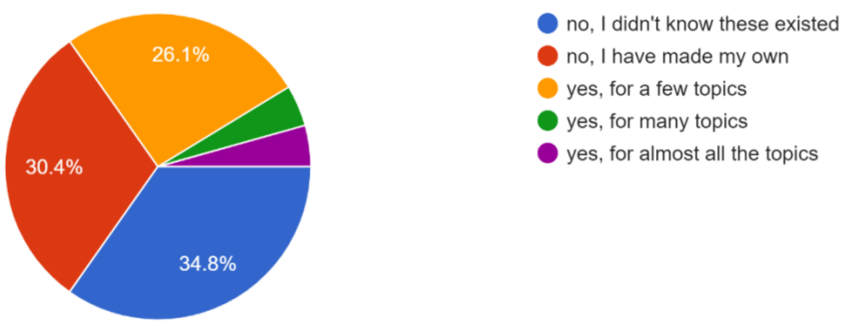
Infrastructure Security

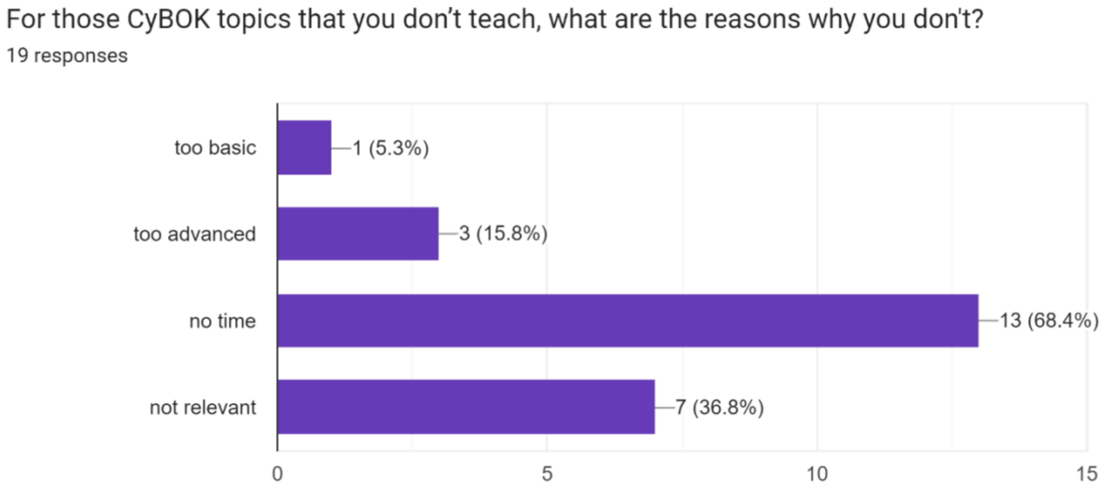


4. CyBOK Reflection

For those Cyber Security topics that you teach, do you use the CyBOK resources provided on the site (https://www.cybok.org/resources_developed_through_funded_projects)?

23 responses




For those CyBOK topics that you don’t teach, what are the reasons why you don't?

19 responses

Are there cybersecurity topics that are not included in CyBOK that you think should be added in a future release? *9 responses (note that these are verbatim responses, with no attempt to correct grammatical errors)*

- Artificial Intelligence
- Not really
- Will aware then will be able to answer
- I think there really needs to be more examples / usage of security tools as they apply to cyber security and the software development lifecycle. It is also very hard to navigate, as there currently is not a search functionality across all areas. For example, I am trying to find what may be present related to DevSecOps. But, I cannot search all the documents to find it.
- Web 3.0, crisis management as well as the BCM element (which is way too light in CyBOK).
- None of the CyBOK resources are actually useful teaching resources. Do these honestly map on to actual learning and teaching activities? It isn’t topics that are missing, it requires educational expertise to produce useful material.
- Cloud IIot IoT security, security Governance
- Psychology of cybercrime
- Critical infrastructure