Cyber Security in English Secondary Education Curricula: A Preliminary Study

Jordan Allison and Ollie Stepney

Abstract

Human error continues to be a contributing factor within the majority of cyber security incidents. Despite this, the education system is not providing the skills individuals need to protect themselves against cyber threats leading to poor cyber hygiene and a lack of cyber security professionals. Knowledge is primarily only available to those who partake in more advanced qualifications such as computer science. This paper utilises CyBOK, a cyber security content framework methodology alongside qualitative data collected from experienced computing educators in order to evaluate the current landscape of cyber security in English secondary education curricula. The content analysis of secondary education computing qualifications with regards to CyBOK, and the thematic analysis of interview data led to the discovery of how cyber security is an imperative educational topic that is largely absent in secondary education curricula. Interviews also revealed a discrepancy in pedagogical methods used to deliver computing education and assessed the issues associated with further inclusion of cyber security education.

CCS Concepts

• Social and professional topics → Computing education; K-12 education.

Keywords

Cyber Security, CyBOK, K-12, Computing Education, Curriculum

1 Introduction

Information security threats are an incessant hindrance globally. Despite systems being adequately prepared in most instances, the issue of human error persists, manifesting as a contributing factor in over 95% of security incidents [39]. Human error is often attributed to a lack of training and situational awareness [31], exacerbated by a blind confidence that is driven by incorrect assumptions of how computers operate [7].

Mitigations for human error are predominantly focused on system design and strict adherence to standards and policies [24]. The issues associated with this are users can still be ignorant of an interface and may violate policies to fulfil their tasks. Users may be aware of what is and is not allowed but without necessarily knowing the reasoning behind this. A deeper understanding of cyber security would provide this knowledge to users.

Some authors identify how there is a shortage of professionals with the right cyber security skills [11], while the Department for Digital Culture Media and Sport have documented that there is a "A cyber security capability gap" [15]. However, the development of cyber security attacks has meant that there is a need to address this talent shortage with individuals who possess the appropriate cyber security skills [20, 34]. This has led to an increased emphasis for including cyber security within education [14, 19, 23, 32]. While basic IT literacy has been ingrained throughout most English educational stages [9], cyber security content is only present in advanced computing courses resulting in the distribution of key skills to a minority, despite the current high demand for cyber security professionals [40]. This paper will utilise the framework methodology of CyBOK [25] to assess the presence of cyber security content within different computing qualifications in English secondary education curricula. The findings of this will be expanded and contrasted with qualitative data obtained from semi-

structured interviews with experienced secondary education computing educators in order to answer the following research question: *'What is the current landscape of cyber security in English secondary education curricula.'*

2 CyBOK Mapping 2.1 What is CyBOK

One concern when considering the implementation of cyber security within secondary education curricula is the lack of coherence and knowledge immaturity within its educational foundation. One paper emphasises that scientific disciplines such as mathematics and physics have clear learning pathways based on an established knowledge foundation, which the field of cyber security lacks [32]. Ivy, Lee, Franz and Crumpton [22] reinforce this, stating the need for a cyber security education pathway.

An emerging solution to the aforementioned lack of coherence is the Cyber Security Body Of Knowledge (CyBOK). CyBOK aims to codify the foundational and generally recognised knowledge on cyber security through distilling contemporary reports, articles and white papers to map established knowledge in to 21 knowledge areas (KAs) [25]. CyBOK compiles this knowledge with the premise of future educational programmes being based upon it.

There is evidence of CyBOK being used for analysis of secondary education curricula in existing literature. Riel and Romeike [35] utilised CyBOK to address how IT security is represented within computer science curricula in secondary education institutions internationally, and while expansive, the paper encompasses German curricula primarily and only briefly probes UK secondary education curricula. The U.S. National Institute of Standards and Technology (NIST) provides a similar initiative with their framework for improving critical infrastructure cybersecurity [26], but CyBOK was selected over NIST's framework because it is an English initiative and produced more recently, so it is therefore likely to be more relevant when assessing English secondary education curricula.

CyBOK will be utilised to assess the current presence of cyber security in secondary education curricula by contrasting qualification specifications provided by different examination boards against the CyBOK framework. The comparison will be executed by assessing whether each specification covers the KAs. A knowledge area will be deemed fulfilled if there is mention of it within the specification. Analysis will be conducted manually through scrutinisation of the specifications of eleven computing qualifications across both RQF Level 2 and RQF Level 3 (later discussed).

2.2 Qualification Choice

The analysis will scrutinise different qualifications including GCSEs (General Certificate of Secondary Education), BTECs (Business and Technology Education Council), A-Levels (Advanced Level) and TLevels (Technical Level). The analysis will take qualifications from the examination boards of: AQA, OCR, Pearson, WJEC and NCFE. GCSEs are how students attainment at age sixteen is measured in England, Wales and Northern Ireland [10].

The GCSE in ICT (Pearson) has been selected because computing education is compulsory in the English national curriculum [38] and is delivered through the GCSE ICT qualification. GCSEs in Computer Science (AQA and OCR) have also been selected as they provide a more advanced computing education option at this level. Also included is the BTEC Tech Award in Digital IT (Pearson). This qualification has been included as it provides a different learning experience, as the BTEC qualifications have more of a vocational focus as opposed to GCSEs which maintain an academic focus. The GCSE and BTEC Tech award materialize at Level 2 of the Regulated Qualifications Framework (RQF). The RQF assists in understanding regulated qualifications and how they relate to each other. The RQF can be collated with the European Qualifications Framework

(EQF), a framework that acts as a translation tool to make national qualifications easier to understand and more comparable across different countries [43]. RQF Level 2 is equivalent to EQF Level 3, and therefore the GCSEs and BTEC Tech award are classified as EQF Level 3 qualifications.

The CyBOK analysis will also cover a host of RQF Level 3 qualifications (EQF Level 4) including A-Levels, T-Levels and BTECs, that are predominantly studied by students aged 16-18. A-Levels will be scrutinized because they are the most common RQF Level 3 qualification within England, where nearly half (47%) of all 16-18 year olds study A-Levels [16]. Similarly to the RQF Level 2 qualifications, A-Level ICT (WJEC and Pearson) and A-Level Computer Science (AQA and OCR) will be analysed. T-Levels are a two-year level 3 qualification that are equivalent to three A-Levels, with approximately 1800 guided learning hours. T-Levels are an alternate route of education for students, and have been described as the 'gold standard' of English technical education [41], and contain approximately 45 days of work placement experience. They have been designed to support the UK industrial strategy and to enhance productivity as it has been identified that there are currently costly and growing skills gaps in key sectors [4]. The T-Levels scrutinized in the CyBOK analysis are the T-Level in Digital Support Services, and the T-Level in Digital Production, Design and Development, and they represent a more expansive course of study than individual A-Levels. The analysis also considers a RQF Level 3 BTEC qualification, the BTEC in IT (Pearson) which offers a more vocational option as opposed to the A-Level ICT qualification, and has been selected to provide some greater variation to the analysis.

3 CyBOK Analysis

The CyBOK mapping (see Table 1) is indicative that the mandatory GCSE ICT qualification offered by Pearson contains limited cyber security content, fulfilling only 29% of the CyBOK KAs. Contrastingly, optional qualifications at RQF Level 2 provide a greater scope of cyber security content. The GCSE Computer Science from OCR offers 43% coverage of CyBOK KAs while the BTEC in Digital IT qualification from Pearson covers 52% of KAs. This provides context to the aforementioned issue of cyber security content only being present in advanced computing courses [44].

The mapping also shows that computing qualifications offered at RQF Level 3 cover more KAs than their Level 2 counterparts, with the clear exception of the A-Level Computer Science qualifications offered by AQA and OCR which cover considerably less KAs at 19% and 14% respectively. This highlights the inconsistencies and immaturity of cyber security content within computing courses, disregarding the expectation that qualifications at this higher educational level would cover the more advanced KAs.

T-Level qualifications provide adequate cyber security content, especially the T-Level in Digital Support which covers 81% of KAs. However, it must be taken into consideration that the qualification has considerably more guided learning hours than individual A-Level qualifications due to it's weighting, allowing for more expansive content. This is also applicable to the T-Level in Digital Support (NCFE), and the BTEC in IT (Pearson). Furthermore, the BTEC and T-Level qualifications contain optional modules, therefore it is not guaranteed entrants will study content relating to certain KAs.

As indicated by the analysis in Table 1, most qualifications analysed cover the cyber security KAs of cryptography (100%), law and regulation (100%), network security (100%), and privacy and online rights (82%) but less common are KAs such as human factors (45%), authentication, authorisation and accountability (45%), and risk management and governance (36%). While certain KAs may be considered out of scope due to their technicality, which explains their absence within secondary education curricula, there are certain areas such as human factors that pertain to important cyber security constructs. It is argued that the world beyond organizations has become progressively more information-oriented and therefore security principles have become more applicable to the individual

		RQF Level 2				RQF Level 3						
Categories	**CyBOK's Knowledge Areas**	GCSE ICT (Pearson 2017)	GCSE Comp. Science (AQA 2020)	GCSE Comp. Science (OCR 2021)	BTEC Digital IT (Pearson 2022)	A-Level ICT (WJEC 2017)	A-Level ICT (Pearson 2021)	A-Level Comp. Science (AQA 2019)	A-Level Comp. Science (OCR 2021)	T-Level Digital Support (NCFE 2022)	T-Level Digital Production (Pearson 2022)	BTEC IT (Pearson 2020)
Human, Organisational and Regulatory Aspects	Risk Management & Governance				x	x				x		x
	Law & Regulation	x	x	x	x	x	x	x	x	x	x	x
	Human Factors				x	x				x	x	x
	Privacy & Online Rights	x	x	x	x	x	x			x	x	x
Attacks and Defences	Malware & Attack Technologies	x	x	x	x	x				x	x	x
	Adversarial Behaviours	x	x	x	x	x				x	x	x
	Security Operations & Incident Management		x	x	x	x				x		x*
	Forensics											x*
Systems Security	Cryptography	x	x	x	x	x	x	x	x	x	x	x*
	Operating Systems & Virtualisation Security									x*	x	x*
	Distributed Systems Security									x*		
	Formal Methods for Security			x	x	x				x	x	x*
	Authentication, Authorisation & Accountability		x	x						x	x	x*
Software and Platform Security	Software Security				x					x	x	x*
	Web & Mobile Security											
	Secure Software Lifestyle					x					x	
Infrastructure Security	Applied Cryptography							x		x		x*
	Network Security	x	x	x	x	x	x	x	x	x	x	x
	Hardware Security											x*
	Cyber-Physical Systems Security						x			x*		x*
	Physical Layer & Telecommunications Security									x*		
	Curriculum KA Coverage (%)	29	38	43	52	52	24	19	14	81	57	81

* contained within optional specialist module within the qualification

Table 1: CyBOK Mapping to English RQF Level 2 and 3 Computing Related Qualifications

user [33]. Hence, topics such as social engineering are imperative due to the frequency of social engineering based attacks such as the increase in phishing attacks since the world transitioned to a higher dependence on remote working [27].

It must be considered that this analysis provides just an overview of cyber security in English secondary education curricula. KAs have been confirmed if the qualification specification mentions them. Therefore, this analysis does not assess the depth of knowledge the qualification provides of the relevant KAs and content may extend as far as only mentioning the knowledge area. Besides, just because something is part of a specification, this is not the only variable that indicates what is actually taught to students in the classroom [46]. For instance,

Falkner et al explain how there are differences in what may be an intended curriculum as described in a qualification specification, and the enacted curriculum of what is actually delivered in the classroom [17].

Furthermore, the CyBOK framework contains descriptors of each knowledge area, of which some KAs are far more technically advanced than their name may imply. For example, the Web and Mobile Security knowledge area relates to "Issues related to web applications and services distributed across devices and frameworks, including the diverse programming paradigms and protection models" [25]. Therefore due to programming knowledge being a prerequisite to this knowledge area, one would expect it to only be covered in advanced courses once a student has already established foundational knowledge of programming.

What can also be visualised from the analysis is that certain KAs (Secure Software Lifestyle, Applied Cryptography) are only present in RQF Level 3 qualifications. The rationale likely being that these KAs are comprised of more complex content and are therefore not suitable for qualifications at RQF Level 2. This highlights the advancement between RQF Level 2 and 3 computing qualifications, but there are still gaps. Hence, it is no surprise that Crick et al [14] highlight how it is important to teach cyber security issues somewhere than not at all, and give examples of how if teaching
SQL, then you should also teach SQL injection. Embedding security issues into the general education of computing topics will only enhance the teaching and coverage of cyber security.

Table 2: Participant Information

Participant	Institution	Job Role	Experience
1	A	IT and Computing Teacher	18 Years
2	B	Head of Computer Science and IT	19 Years
3	C	IT and Computing Teacher	12 Years

4 Further Analysis Methodology

To augment the findings of the CyBOK analysis, semi-structured interviews with experienced secondary level computing educators were conducted to obtain a different perspective of English computing curricula. Further analysis alleviates the shortcomings of the CyBOK analysis by providing a human perspective on the different curricula aspects such as content, pedagogy, and issues of further cyber security education implementation.

4.1 Data Collection

Interviews are frequently used for research based in educational environments as they can provide rich data [29], and are a useful mechanism to assess teacher knowledge [5]. Semi-structured interviews were utilised because they have the advantage of being reasonably objective while permitting a more thorough understanding of the respondent's opinions [13]. As just a preliminary study to augment the CyBOK analysis, a small sample of three participants were selected from different secondary institutions (see Table 2). Participants were screened through an initial analysis of their LinkedIn profile to gauge those with extensive experience in the sector for teaching computing and related areas.

Interviews were conducted online and recorded via Microsoft Teams, as participants had familiarity with this, and because online interviews can help increase efficiency, convenience and overcome geographical barriers [36]. Interviews were downloaded locally for transcription purposes. Interviews were approximately 30 minutes long where participants were asked questions regarding their background and role, their opinion on further

implementation and challenges of cyber security education in secondary education curricula, curriculum choice, and pedagogical methods used.

Participant information sheets were used to acquire informed consent and discuss confidentiality regarding the storing, use and access of collected data in line with EU GDPR (General Data Protection Regulation) which represents EU law on data protection and privacy. Participant information sheets were distributed to potential participants after initial positive contact post-invitation.

4.2 Data Analysis

Interviews were transcribed manually using oTranscribe. A manual approach was used because of interpretation inconsistencies in automated methods and to maintain good research practice [6]. Braun and Clarke's six-phase framework for conducting thematic analysis was used to code interview data [8]. This included data familiarisation, transcription, generating initial codes, searching for themes, reviewing themes, and defining and naming themes. Thematic analysis was conducted using computer-aided qualitative data analysis software NVivo, as it allows for systematically working through data and allows users to identify and uncover emerging themes while providing a surplus of visualisation tools for assessing data and sharing findings [45]. The themes (and sub-themes) found through the thematic analysis are shown in Figure 1.

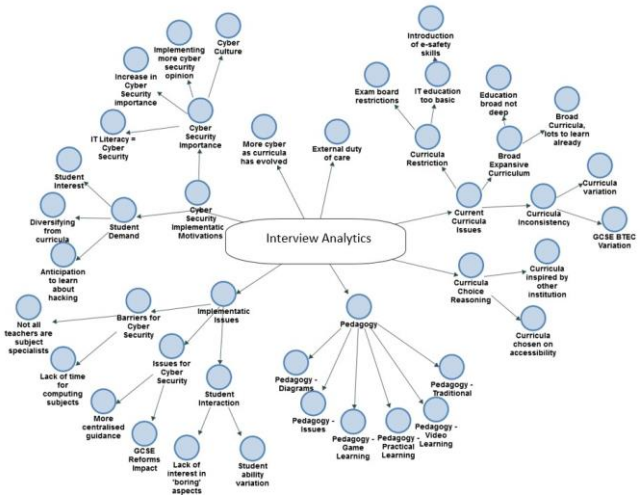

Figure 1: Thematic Analysis Map.

5 Findings and Discussion

This section will amalgamate the results of the CyBOK analysis with interview findings to drive a discussion on the current landscape of cyber security in English secondary education curricula. The discussion will be supported by the top-level view of curricula informed by qualification specifications and a ground-level view focused on the experience of educators delivering the curricula.

5.1 Importance of Cyber Security Education

An abundance of sources define cyber culture and propel its significance with regard to a personal, organisational or governmental context [21, 33, 42]. Literature also concludes that cyber security education is an essential pillar of a national cyber culture [3]. This is synonymous with the interview findings where participants agreed education would contribute towards a national cyber culture. Participants also magnified the importance of cyber security

education alluding it to a necessary personal skill and proclaiming its importance is on an upwards trajectory, highlighting its increasing value as an educational topic. For example, participant 1 explained:

> *'It should go hand in hand, understanding how to keep yourself safe and keep your work and devices secure should be a fundamental part of everyday life.'*

This interview finding supports existing literature which highlights the need for all IT users to possess a basic level of cyber security awareness and education [12]. Participant 3 also discussed the importance of cyber security education with regard to training future cyber experts claiming "we're just going to need more and more people with those skills" but extended the discussion to note the importance for those that "aren't going into the industry as it is going to affect other jobs", thus highlighting the importance of cyber security as a personal skill. Similarly, participant 2 exclaimed:

> *'If we could get more of that [cyber security] into GCSE... cybers good! It's people outside of computer science probably actually know a bit about it and are actually more curious about keeping themselves safe online and I think it should be more in the GCSE.'*

Contrary to the need of cyber security education, interviewees highlighted the responsibility of banks and service providers to provide protection to individuals and to better inform them of how they can protect themselves. Thus withdrawing the duty from educational institutions to implement more cyber security education and focusing more on service providers. Participant 1 stated:

> *'Service providers and banks have quite a big duty of care to look after their clients and to make sure that they provide them with regular updates and information. In that way they could increase the level of education of the nation.'*

Interviews highlighted that many students possess an abundance of technical knowledge. Literature contextualises this and claims that without a form of cyber security education they may not be able to adequately protect themselves [30]. A report from the UK Department for Digital, Culture, Media and Sport [15] acknowledged the cyber security capability gap within the UK. Within this, proposals were made for initiatives that encourage the uptake of Computer Science at GCSE, despite this there were no comprehensible plans to implement further cyber security education.

5.2 Current Lack of Cyber Security Education in Secondary Education Institutions

Allison investigated curriculum choice within UK colleges, who offer the whole spectrum of computing courses outlined in the CyBOK Analysis, and found that the choice surrounding curriculum depends upon four main factors [2]. These factors were labour market information, the relevance of a qualification to industry needs, the qualifications' attractiveness (factors such as familiarity and available funding), and current college resources (such as staff skill-set and IT resources) [2]. Many of these factors were also found within the sample of interviewees from school settings. For example, it was found that accessibility is a priority when selecting curricula - specifically regarding the objective of student achievement which Allison frames as "achieve good student outputs" [2]. It was noted that OCR was selected by Institution B because the AQA qualification was "a lot more difficult to get better results for kids", while participant 1 explained that former qualifications were more suitable because they could retake up to 3 times so they can "get an idea of what the test or exam is like", highlighting the importance of accessibility for students during curricula selection.

Participants claimed to have influence in their department's curricula choice for their respective subjects. Interviews investigated reasons a specific qualification is chosen over options from other exam boards. It was clear that curricula choice decisions are based upon credibility. If a qualification is used by the vast majority, then

an institution is more likely to select it. For example, participant 3 commented that their qualification was chosen as it was:

'being taught by the vast majority, so it sort of made sense to go with the people who had the biggest cohort.'

Another finding of the research was the interest from students to learn topics that relate to cyber security. Participant 1 claimed:

'they [students] want the technical, they want the details and the 'why' and the how does that work?'

Participants also highlighted enthusiasm from students towards learning hacking, participant 2 described:

'they [students] want to learn more about hacking, they want to learn about threats and how to break into something.'

This highlights the interest in cyber security content from students but creates a predicament in which students may be less inclined to enroll in qualifications that have a higher proportion of non-technical areas of cyber security, such as those outlined in the CyBOK category of human, organisational and regulatory aspects. However, recent analysis of job advertisements indicates how the technical aspects of cyber security needs to be complemented by the more human and managerial elements, as there are skills gaps in this area of cyber security in particular [18].

The CyBOK analysis indicates that secondary education curricula for computing topics is very basic and has more of an IT literacy focus. This point was synonymous with interview findings which revealed how IT education pertained to foundational aspects of digital literacy such as graphics, spreadsheets and PowerPoint. Interviewees also discussed how there is a large focus on e-safety, which is often mistaken for cyber security education yet relates more to simple security procedures such as the concept of not sharing passwords and their overall digital footprint.

A number of issues regarding current curricula were identified, primarily demonstrating how broad and expansive they can be, with some areas touched upon only very lightly. Participant 1 explained:

'The computer science curriculum for GCSE and ALevel is monstrously broad... There is far, far too much content in there which means it's really difficult to and it would be ill-advised to focus more on cyber security than is required for examination purposes.'

A content inconsistency was identified between the different qualifications at RQF level 2 and level 3, as evidenced in the CyBOK analysis (see Table 1). Participants also described how the current curricula is bound by examination boards, participant 1 exemplified this point by describing how they "tend to draw people in through that extracurricular route to build their interest in cyber security", highlighting the leeway restriction they have in regard to deviating from curricula specification. However, it is argued that teachers need to gain an understanding of how to embed cyber security content into curricula (of all subjects) [28] as by doing so, this may provoke interest in students to pursue cyber security (and more largely computing qualifications) when it is an optional choice.

5.3 Pedagogical Methods Discrepancy

Although not directly related to curriculum, some participants raised the important point of why cyber security may not be as prevalent in the CyBOK mapping of secondary education curricula as it could have been, and this is because of the challenges of teaching it. Illustrative of this point is participant 1 who exclaimed:

'it's incredibly difficult to teach" cyber security because "they're teenagers, so they're going to ignore it, they don't take it seriously.'

Interview findings suggest that linking topics with real-world current events can help improve student motivation. For example, participant 1 stated:

'Well, it's making it relevant to stuff that teenagers understand and that they have experience of.'

It was also acknowledged by [47] that there is a need for a unified pedagogy for computing subjects at GCSE level. This was apparent from the interviews in the disunity between responses towards pedagogical methods. While it was clear traditional methods were not suitable, combining them with diagrams or video based learning made them more effective. For example, participant 2 enthused the use of flipped learning for computing education stating that the premise of their teaching is:

'the kids watch the video first, it's called flipped learning, so you watch the video before the lesson, you come into the lesson already knowing bits.'

Flipped learning was not raised by other participants, but has been assessed positively within literature as it makes students responsible for their own learning process and pace, thus encouraging them to engage more with the content [1]. However, participant 3 claimed that they "don't think video teaching is brilliant for most students" which highlights the discrepancy in views. Games based learning was also discussed by participants and dismissed because students can be more engaged with the game then the content. For instance, participant 1 stated:

'The danger of having games based engagement is they are engaged with the game rather than the content.'

Participants generally condemned the use of traditional classroom learning as an effective delivery method, but participant 1 raised the viability of a combination of video-based learning and traditional learning that "allows you to teach classically how these things work" contending that some topics are difficult to visualise. This point was also raised for the importance of the use of diagrams in traditional learning by participant 2.

5.4 Acknowledging Issues of Further Cyber Security Education Implementation

Interview findings identified that the lack of cyber security education is partially a result of curricula restrictions. Not only does the CyBOK mapping indicate how areas of cyber security are lacking, but institutions are confined from deviating from the curricula to teach other topics to the point where institutions are conducting cyber security education in the form of extracurricular activities due to a lack of time. Participant 2 described how "there is only an hour a fortnight for key stage 3 [RQF Level 2]" and further explained:

'you just have to weigh up 'have you got the curriculum time to do that?'

Research has discussed how a lack of funding, resources and teacher training are issues that stop further cyber security education implementation [30]. Interview findings echoed the issue of teacher training explaining how many computing teachers are not subject specialists, meaning they may find it difficult to deliver technical cyber security topics. For instance, participant 2 stated "they might not have the underlying knowledge [of cyber security] and it would be a bit more for them to do", highlighting the skill gap of educators. Issues were also raised about the variation in student ability. For example, participant 3 stated that:

'do you teach everyone the same thing to the same level? I think it would have to be structured carefully for ability groups.'

Interview findings also highlighted the impact of previous GCSE reforms within UK education. Participant 2 discussed how many IT qualifications have been reformed already while participant 3 discussed how a previous course "had a decent cyber security element", but this qualification has been discontinued. Hence, it is important to recognise that while qualification reform could be a suggested method to ensure adequate cyber security coverage within education, this has already taken place, while the transition to new curriculum can take many years [37].

Participant 2 also exclaimed that “if there was some sort of centralised guidance on what to cover that would be great” in terms of IT. Participant 1 amplified this point by stating:

> *‘I think there does need to be more resources or secure environments where they can actually play with this stuff and see what happens.’*

6 Conclusions and Recommendations

The motivation behind this research was to depict the current landscape of cyber security in English secondary education curricula. The CyBOK analysis identified that cyber security content is largely absent within secondary education curricula. This was contextualised by the interview findings which also highlighted the importance of cyber security education, issues of implementation and a current discrepancy in pedagogical methods.

While it is clear cyber security content is currently dictated by exam boards, where does the onus lie? Is it with policy makers or is it the responsibility of senior leadership teams within institutions, computing teachers, or industry employers? Regardless of this, there are gaps in English secondary education computing curricula and other studies could replicate a similar approach to this to assess the wider cyber security education landscape.

Considering cyber threats are a global issue, other countries could employ such a framework to conduct a similar analysis. However, it must be noted that this is only a preliminary study, while each country will have their own political and educational context so further studies are required to see how English secondary education compares. Still, this paper demonstrates how the CyBOK methodology framework can be used to analyse an educational landscape, and is the first example of it’s use in the context of English secondary education curricula. Further studies could also develop upon the method employed to conduct the analysis. For example, adjusting KA definitions to fine-tune the analysis for different educational stages.

Referenes

[1] Gokce Akcayir and Murat Akcayır. 2018. The flipped classroom: A review of its advantages and challenges. *Computers & Education* 126 (2018), 334–345.

[2] Jordan Allison. 2022. The who , how and why of choosing post-16 computing curricula : a case study of English further education colleges. *Journal of Further and Higher Education* (2022), 1–18. https://doi.org/10.1080/0309877X.2022.2088269 [3] Mohammed A. Alnatheer. 2015. Information Security Culture Critical Success Factors. In *2015 12th International Conference on Information Technology - New Generations*. 731–735. https://doi.org/10.1109/ITNG.2015.124

[4] Association of Colleges. 2019. *Skills shortages and funding gaps: An analysis of the costs of under-investment in skills*. Technical Report. Association of Colleges, London.

[5] M Bassey. 1999. *Case study research in educational settings*. Open University Press, Maidenhead.

[6] Galina Bolden. 2015. Transcribing as research: "Manual transcription" and Conversation Analysis. Research on Language and Social Interaction. *Research on Language and Social Interaction* 48 (07 2015), 276–280. https://doi.org/10.1080/
08351813.2015.1058603

[7] Sergey Bratus, Chris Masone, and Sean W. Smith. 2008. Why Do Street-Smart
People Do Stupid Things Online? *IEEE Security & Privacy* 6, 3 (2008), 71–74. https://doi.org/10.1109/MSP.2008.79

[8] Virginia Braun and Victoria Clarke. 2013. *Successful qualitative research: a practical guide for beginners*. SAGE Publications, London.

[9] British Computer Society. 2022. *BCS Landscape Review: Computing Qualifications in the UK*. Technical Report. British Computer Society, Swindon.

[10] Kerry Brown and Kevin Woods. 2022. Thirty years of GCSE: A review of student views and experiences. *Assessment in Education: Principles, Policy & Practice* 29, 1 (2022), 1–26. https://doi.org/10.1080/0969594X.2022.2053946

[11] T Caldwell. 2013. Plugging the cyber-security skills gap. *Computer Fraud & Security* 7 (2013), 5–10.

[12] Charlie Chen, B. Medlin, and Ruey-Shiang Shaw. 2008. A cross-cultural investigation of situational information security awareness programs. *Information Management Computer Security* 16 (10 2008), 360–376. https://doi.org/10.1108/09685220810908787

[13] L Cohen, L Manion, and K Morrison. 2018. *Research methods in education* (8 ed.). Routledge, Abingdon.

[14] Tom Crick, James H. Davenport, Alastair Irons, and Tom Prickett. 2019. A UK Case Study on Cybersecurity Education and Accreditation. In *2019 IEEE Frontiers in Education Conference (FIE)*. IEEE, Covington, 1–9. https://doi.org/10.1109/ FIE43999.2019.9028407 arXiv:1906.09584

[15] Department for Digital Culture Media and Sport. 2019. *Initial National Cyber Security Skills Strategy: increasing the UK's cyber security capability - a call for views, Executive Summary*. Technical Report. Department for Digital, Culture, Media and Sport, London.

[16] Department for Education. 2019. *Students and qualifications at level 3 and below in England*. Technical Report. Department for Education, London.

[17] Katrina Falkner, Sue Sentance, Rebecca Vivian, Sarah Barksdale, Leonard Busuttil, Elizabeth Cole, Christine Liebe, Francesco Maiorana, Monica M. McGill, and Keith Quille. 2019. An International Comparison of K-12 Computer Science Education Intended and Enacted Curricula. In *Proceedings of the 19th Koli Calling International Conference on Computing Education Research*. ACM, Koli, Finland, 1–10. https://doi.org/10.1145/3364510.3364517

[18] Francois Goupil, Pavel Laskov, Irdin Pekaric, Michael Felderer, Alexander Dürr, and Frederic Thiesse. 2022. Towards Understanding the Skill Gap in Cybersecurity. In *Proceedings of the 27th ACM Conference on on Innovation and Technology in Computer Science Education Vol. 1*. ACM, New York, NY, USA, 477–483. https://doi.org/10.1145/3502718.3524807

[19] Jan Hajny, Sara Ricci, Edmundas Piesarskas, and Marek Sikora. 2021. Cybersecurity Curricula Designer. In *The 16th International Conference on Availability, Reliability and Security*. ACM, New York, 1–7. https://doi.org/10.1145/3465481.3469183

[20] Jim Hoag. 2013. Evolution of a Cybersecurity curriculum. In *Proceedings of the 2013 Information Security Curriculum Development Conference - InfoSecCD '13*. ACM, New York, 94–99. https://doi.org/10.1145/2528908.2528925

[21] Keman Huang and Keri Pearlson. 2019. For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture. In *52nd Hawaii International Conference on System Sciences*. ScholarSpace / AIS Electronic Library (AISeL), Grand Wailea, Maui, Hawaii, USA, 1–10. http://hdl.handle.net/10125/60074

[22] Jessica Ivy, Sarah B. Lee, Dana Franz, and Joseph Crumpton. 2019. Seeding Cybersecurity Workforce Pathways With Secondary Education. *Computer* 52, 3 (2019), 67–75. https://doi.org/10.1109/MC.2018.2884671

[23] Joint Task Force on Cybersecurity Education. 2017. *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity*. Vol. Version 1. Association for Computing Machinery, New York. 1–111 pages. https://doi.org/10.1145/3184594

[24] M.G. Lee. 2012. Securing the human to protect the system: Human factors in cyber security. In *7th IET International Conference on System Safety, incorporating*

the Cyber Security Conference 2012. Edinburgh, UK. https://doi.org/10.1049/cp. 2012.1519

[25] Andrew Martin, Awais Rashid, Howard Chivers, Steve Schneider, Emil Lupu, and George Danezis. 2021. *Introduction to CyBOK Knowledge Areas*. Technical Report. Bristol Cyber Security Group, Bristol. 22 pages.

[26] National Institute of Standards and Technology. 2018. Framework for Improving Critical Infrastructure Cybersecurity. https://nvlpubs.nist.gov/nistpubs/CSWP/ NIST.CSWP.04162018.pdf

[27] Paloalto Networks. 2022. *2022 UNIT 42 Network Threat Trends Research Report*. Technical Report. Palo Alto Networks, Santa Clara.

[28] Don Passey. 2017. Computer science (CS) in the compulsory education curriculum: Implications for future research. *Education and Information Technologies* 22, 2 (2017), 421–443. https://doi.org/10.1007/s10639-016-9475-z

[29] Anil Pathak and Charatdao Intratat. 2012. Use of Semi-Structured Interviews to Investigate Teacher Perceptions of Student Collaboration. *Malaysian Journal of ELT Research* 8 (2012), 1–10.

[30] Denny Pencheva, Joseph Hallett, and Awais Rashid. 2020. Bringing Cyber to School: Integrating Cybersecurity Into Secondary School Education. *IEEE Security & Privacy* 18 (2020), 68–74. https://doi.org/10.1109/MSEC.2020.2969409

[31] Tommy Pollock. 2017. Reducing human error in cyber security using the Human Factors Analysis Classification System (HFACS). In *KSU Proceedings on Cybersecurity Education, Research and Practice*. Kennesaw, GA, USA.

[32] Awais Rashid, George Danezis, Howard Chivers, Emil Lupu, Andrew Martin, Makayla Lewis, and Claudia Peersman. 2018. Scoping the Cyber Security Body of Knowledge. *IEEE Security & Privacy* 16, 3 (2018), 96–102. https://doi.org/10. 1109/MSP.2018.2701150

[33] Rayne Reid and Johan van Niekerk. 2014. From Information Security to Cyber Security Cultures Organizations to Societies. In *Information Security South Africa (ISSA)*. Johannesburg, South Africa.

[34] Sara Ricci, Vladimir Janout, Simon Parker, Jan Jerabek, Jan Hajny, Argyro Chatzopoulou, and Remi Badonnel. 2021. PESTLE Analysis of Cybersecurity Education. In *The 16th International Conference on Availability, Reliability and Security*. ACM, New York, 1–8. https://doi.org/10.1145/3465481.3469184 [35] Manuel Riel and Ralf Romeike. 2020. IT Security in Secondary CS Education: Is it missing in Today's Curricula? A Qualitative Comparison. In *Proceedings of the 15th Workshop in Primary and Secondary Computing Education (WiPSCE '20)*. ACM, Virtual Event, 1–2. https://doi.org/10.1145/3421590.3421623

[36] Janet Salmons. 2012. *Cases in Online Interview Research*. SAGE Publications, Inc., Glasgow, UK.

[37] Sue Sentance and Jane Waite. 2018. Computing in the classroom: Tales from the chalkface. *IT - Information Technology* 60, 2 (2018), 103–112. https://doi.org/10. 1515/itit-2017-0014

[38] Government Digital Service. 2014. The national curriculum. https://www.gov. uk/national-curriculum/key-stage-3-and-4

[39] IBM Global Technology Services. 2014. IBM Security Services 2014 Cyber Security Intelligence. https://i.crn.com/sites/default/files/ckfinderimages/userfiles/ images/crn/custom/IBMSecurityServices2014.PDF

[40] Nigel Shadbolt. 2016. *Shadbolt Review of Computer Sciences Degree Accreditation and Graduate Employability*. Department for Business, Innovation and Skills, London.

[41] Suzanne Straw and David Sims. 2019. *T Levels Research: How Are Providers Preparing For Delivery? Follow-Up Report*. NFER, Slough.

[42] Peter Trim and D. Upton. 2013. *Cyber security culture: counteracting cyber threats through organizational learning and training*. Routledge, Abingdon, UK.

[43] European Union. 2022. The European Qualifications Framework. https://europa. eu/europass/en/european-qualifications-framework-eqf

[44] Isabella Venter, Renette Blignaut, Karen Renaud, and M. Venter. 2019. Cyber security education is as essential as “the three R’s”. *Heliyon Computer Science* 5, 12 (12 2019). https://doi.org/10.1016/j.heliyon.2019.e02855

[45] Fiona Wiltshier. 2011. Researching With NVivo. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research* 12 (01 2011).

[46] Alison Wolf. 2011. *Review of Vocational Education-The Wolf Report*. Department for Education, London.

[47] Peter Yiatrou, Irene Polycarpou, Janet C Read, and Maria Zeniou. 2016. The synthesis of a unified pedagogy for the design and evaluation of e-learning software for high-school computing. In *2016 Federated Conference on Computer Science and Information Systems (FedCSIS)*. 927–931.