Department: Head
Editor: Name, xxxx@email

Bringing Cyber To School: Integrating Cyber Security Into Secondary School Education

Denny Pencheva
University of Bristol

Joseph Hallett
University of Bristol

Awais Rashid
University of Bristol

***Abstract*—Based on 3 one-day workshops with teachers, we identify drivers and barriers for introducing cybersecurity into secondary school education. We find that students, though more knowledgeable in cybersecurity than their teachers, lacked understanding of career pathways and online safety. Teachers, however, though motivated lacked adequate knowledge and resources.**

THE ON-GOING shortage of cyber security workers continues to make it difficult to recruit cyber security specialists into open jobs [1]. An $(ISC)^2$ report [2] suggests that part of the reason for the continued shortage of cyber security professionals comes from a failure to recruit and train young people. The report points out that currently only 35% of cyber security workers are under the age of 40. By presenting assorted evidence, the report estimates a sustained shortfall of cyber security workers not only in the UK but also globally, of up to 2 million. Intergenerational gaps in terms of knowledge and lack of awareness of employability prospects are emphasised as the key factors for this shortage. Another report from the UK National Audit Office [3] suggested that it could take 20 years to address the cyber security skills gap at all levels of education.

We need to train more people to work in cyber security, and we need their training to come earlier in their careers in order to bridge the skills gap. Bringing cyber security education into schools, so that we can show the students that these career pathways exist and can start to train the new workforce, may go some way to addressing these issues.

But how do we bring cyber security into schools? We ran a series of evaluative and consultative workshops, where we asked teachers, educators and other practitioners what cyber secu-

 Published by the IEEE Computer Society

rity knowledge should be brought into secondary education (ages 12–16), and how to do it in a way that actively involves students in the learning process. We wanted to find out what were the current levels of cyber security knowledge and training and explore how the participants envisioned the integration of cyber security into secondary schools' education. This paper focuses on the UK context only, yet the findings can have relevance in other similar contexts worldwide; as the shortage of cyber security workers is an international and pressing issue.

Overall, based on the analysis of the workshop transcript materials, we found that there was strong agreement among the participants that the need for cyber security is an increasingly important part of life, as well as an overwhelming enthusiasm about integrating different aspects of cyber security into the curricula at their schools. However, we also found significant tensions, related to the existence of knowledge gaps and the lack of resources. It is around these tensions that we have identified the two core themes: *cyber teens or are they?* and *mind the gap!* The first theme explores the tension between teenagers' self-perception as invincible and their online vulnerabilities. The second theme looks at the tension between the overall willingness of teachers to teach cyber security and the lack of subject-specific training and off-the-shelf resources to do so. We need to help the students understand the threats they face online and how cyber security is an essential aspect to defending themselves. We also need to help the teachers to impart this key cyber security information—as at the moment cyber security content is primarily taught by enthusiastic teachers, yet with little support.

METHOD

We organized three interactive workshops across the UK where participants were actively encouraged to contribute to the discussions. The workshops were attended by twenty-one people—most were teachers and educators, but also some industry representatives attended the workshops and participated. We approached schools with existing outreach programmes. The workshops were delivered by an independent research facilitator who wrote up the findings from the workshop in a report. All workshop attendees were assured of anonymity and promised that their views would be conveyed faithfully to the commissioners of the research.

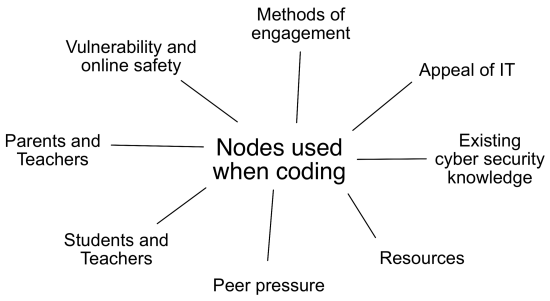

Figure 1. Thematic analysis themes

The format was designed to be as inclusive and interactive as possible. The participants collaboratively produced visual representations of their discussions (Figure) which the facilitator described when reporting the findings. The workshop discussions explored the current levels of cyber security knowledge of students and teaching staff, identified alarming and reassuring practices, provided examples of successful and less so pedagogical practices, and outlined practical visions for cyber security education.

Whilst the workshop discussions were designed as fairly structured, some flexibility was required with regard to the format due to the variation of the number of attendees. The workshops were advertised but because participation was strictly voluntary, the number of participants who attended varied across the different settings.

All workshop discussions were transcribed, coded and subsequently analysed using a thematic analysis (see Figure 1). The gprocess of coding was strictly inductive and was based on a close reading of the workshop transcripts. In order to ensure rigour and to minimise the possibility of selection bias, we undertook peer coding: a process, where a second coder corroborates the initial coding.

CYBER TEENS OR ARE THEY?

The first theme explicitly focuses on the students and their relationship with technology. We noted a tension between teenagers' self-perception of invincibility and their online vulnerability. The latter was due to knowledge gaps

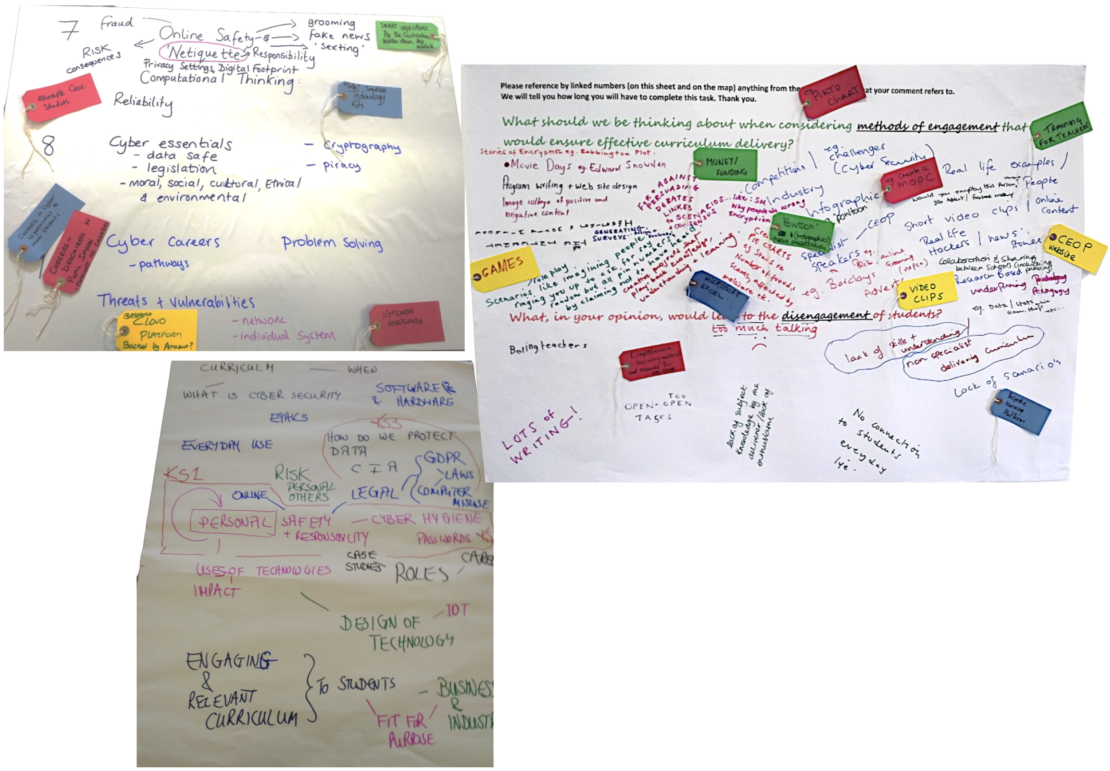

Figure 2. Diagrams produced during the workshops

and lack of adult support networks.

The workshop discussions suggested that young people generally have high levels of self-taught technical skills because they have been exposed to technology from a young age. During the group discussions it was noted that many students, even at primary level, have their own web sites and YouTube channels and were said to be confident users of social media.

Teenagers are tech-savvy

Students were said to spend significant amounts of time online and to be confident on the Internet. All participants agreed that many of their students find computer science and IT fields appealing and that most are keen to improve their knowledge and technical skills. Participants noted a growing willingness on the part of students to explore cyber security, to improve their technical and problem-solving skills. Teachers noted that pupil knowledge had increased from the same year groups three years ago, and that many students had a basic understanding of web security. Participants also noted that some pupils' understanding of cyber security, programming and cyber safety surpasses that of teachers.

Hacking is glamorous

During the discussions, teachers suggested that some students tend to view hacking as glamorous, that they were able to overcome blocks and restrictions and to breach security systems. It was noted that some students have been able to access school systems, individual teachers' devices, information and school printers, and were able to attack the school server.

Online invincibility

However, the discussions also revealed important caveats regarding students' knowledge, in particular where these related to online safety. Teachers suggested that students have little understanding of the context in which they are using these technical skills and often choose to disregard online safety rules. Indeed, the sense of online invincibility appeared to override notions

of safe and respectful usage of online space.

Whilst the teachers' students did have an idea of online safety, the term cyber security was relatively unknown to them—when they did know the term they tended to believe it was synonymous with cyber security rather than being a subset of it [4]. During the discussions, it was suggested that students are often unaware of their cyber footprint (the profile that they leave online) and demonstrate a certain willingness to give away information. Such lack of knowledge of cyber etiquette has led some students to post illegal content online—such as sexualized images either of themselves or of fellow classmates. Workshop participants disclosed that they had seen cases of such images being circulated by children as young as 9 and that they believed that the images' distribution was more than likely driven by peer pressure. Many students were said to have social media accounts—despite being bellow the required age threshold for many sites—and would find themselves operating within areas for older children and adults, such as in gaming circles—in particular Fortnite—where conversations can quickly become inappropriate. One workshop participant highlighted that some students *"take mean pictures at sleepovers"*, make inappropriate comments during social media interactions and post inappropriate images of friends without their permission.

Online vulnerability

Young people's extensive and not always safe engagement with social media was said to exacerbate students' need for approval and was linked to other social phenomena, such as the fear of missing out, peer pressure, low self-esteem and mental health issues. The number of likes, shares or followers that students acquire is symptomatic of such competitive digital engagement.

Further, workshop participants spoke of some technical gaps of knowledge that facilitate students' online vulnerability. These included leaving electronic devices logged on, duplicating passwords, not deleting online data, passwords and login details that are too short, copied, written down, used unchanged for several sites or shared with peers, inappropriate responses to scams or phishing attacks (such as opening such links or forwarding them to friends).

No adequate adult support networks

Another barrier that sustained this tension concerned the lack of adequate adult support networks. Although it was suggested that some students are aware of how to access support if needed, it became clear from the discussions that there is a sense of alienation between teachers and parents on the one hand, and students on the other. This is compounded by the fact that the childrens' technical knowledge often surpassed that of their parents and teachers. If the students are effectively the technical experts at home and at school then they can struggle to find appropriate help when they're in need. This suggests that fixing the skills gap cannot be entirely achieved through educating the next generation of workers, but that as well as improving education we also need to build the support networks and have resources for the students as well as those supervising them.

Overall, there was a consensus that there is limited understanding from parents and teachers about specific situations students find themselves in. It was suggested that there is a lack of parental understanding of age permissions with regard to using social media platforms, such as Facebook and Instagram. Participants also highlighted that schools do not necessarily know the difference between personal safety and cyber security and might not be sufficiently equipped to support students in the challenges they are facing. Furthermore, respondents noted, that it wasn't just in secondary education but in primary schools that teachers often lacked relevant knowledge and did not know how to engage or teach even basic cyber security.

TAKE AWAY POINTS

- We need to make young peoples' cyber security knowledge more diverse and substantial.
- Parents and teachers need to raise their game to the computing level of their children.

MIND THE GAP!

The second core theme was based around the tensions that arose between the overwhelming willingness and enthusiasm to embed cyber security within schools' curricula, and the lack of resources (technological, human, as well as

teaching materials) to do so.

The overwhelming support for including cyber security training in secondary schools' education could be explained by the aforementioned knowledge gap between students on the one hand, and their parents, teachers and school administrators on the other. It was indicated that students seem to appreciate the labour market significance of their cyber security skills, however, they lack in-depth and systematic knowledge of possible career paths. In this respect, workshop discussions suggested that a key outcome of an embedded cyber security education should be a smoother transition between secondary school–higher education–industry.

Participants were asked to suggest resources that they felt would be needed to deliver cyber security-enhanced education. Generally speaking, everyone wanted comprehensive learning materials and resources. More specifically, attendees discussed issues related to funding, online resources for teaching but also for booking industry speakers, access to data sets, multimedia platforms, and teacher training. There was a general agreement amongst participants that any new learning content needs to be communicated appropriately to students, based on their age and skill levels, but also to establish clear pathways that inform students of career opportunities in the cyber security sector, whether that be forensics and penetration testing, secure data handling, risk management or any of the other cyber security careers.

Off-the-shelf resources

Broadly speaking, the listed ideas of learning materials and resources indicate what participants considered to be a general problem with underfunding of schools, understaffing and isolation from the resources available to universities and industry. In terms of resources, there appeared to be a consensus that teachers and educators wanted off-the-shelf resources that would build on what they already have available without overburdening staff with lengthy and possibly complicated training followed by the need to design brand new teaching content. Otherwise any changes to schools' curricula could be rendered unsustainable if these required extensive and expensive staffing and support. Teachers stressed that it is also incredibly important that any off-the-shelf resource works first time. When students see a demo that doesn't work straight away, the teachers found that their students became disengaged. Online resources, such as CLARK [5], are not well known to teachers and they can struggle to get these labs running on restrictive school networks.

To this effect, participants raised numerous questions about the challenges of making room for cyber security in the existing curriculum. Further, there were queries about teacher training: who is going to teach it? What would the training look like? What would the content of the subject look like bearing in mind the dynamic and ever-changing nature of the subject? There was a detectable worry that cyber security needs "constant updating", which might put staff under considerable strain without continued investment in the required resources.

What exactly is cyber security?

Another concern related to the distinctive character of cyber security. As one participant put it: *"what would a course like this offer a student that a combination of Maths, Physics and Computer Studies couldn't?"*. This prompted other participants to debate to what extent cyber security was distinct, from existing ICT modules or basic online safety, which is currently taught in PSHE (personal, social, health and economic studies) units. There was a consensus that any new curriculum should be explicit, follow official government guidelines and embedded, that is it should be based on a more cross-curricula approach using a full suite of subjects (Maths, English, Science, for example). It was also noted that continuity of cyber security education between primary and secondary levels is essential. In the words of one participant:

> "We mustn't lose sight of primary schools because year-on-year children are having access to the Internet and are therefore making themselves vulnerable. Secondary schools and primary schools need to work more collaboratively to share and to learn together. Digital footprints are being generated much earlier, so action is needed now!"

Further to this point, we noted that the pres-

ence and active involvement of universities in offering specialised courses and outreach activities had a positive impact on the levels of cyber security knowledge in schools. The proximity to universities meant that, whilst they felt frustratingly under-resourced, educators nonetheless remained committed to delivering a high standard of cyber security awareness and practice to their students. As one participant eloquently explained:

> "This affects people's lives daily and their habits have to adapt daily otherwise they will fall victim to it."

In this respect some schools were more fortunate than others in that they had already done work with students around ethical hacking and digital forensics. However, all participants emphasised that good will and ambition are often trumped by problems with understaffing and lack of teacher training. Everyone agreed that staff and teacher training was of paramount importance if a cyber security-enhanced curriculum was to be a successful endeavour. In the words of one participant:

> "We need proper staff training. And proper teacher training before then. We need *[the training]*!"

Another attendee added:

> "We need access to the right resources and the right infrastructure to support *[the programme]*."

All attendees held passionate views about the need for better teacher training and support. Some talked about how they were self-taught and welcomed the opportunity presented by the workshop to share their experiences and learn from each other. One participant noted that:

> "The lack of materials is a real issue—we've been developing our own. Existing materials are just not fit for purpose. We need off-the-shelf practical materials that will really work."

Another participant stated that:

> "A new curriculum needs to be set up so we can teach it properly and cascade it down. That way we will create ambassadors in each year group and then that will increase uptake year on year."

Their colleague further emphasised that:

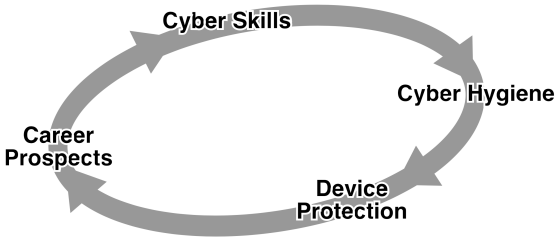

Figure 3. What should we be teaching?

> "Cyber security should be made more interdisciplinary by linking what is done to everything across the curriculum."

WHAT SHOULD WE BE TEACHING AND HOW SHOULD WE BE TEACHING IT?

Given the inclusive and interactive nature of the three workshops, participants were asked to come up with recommendations for cyber security education. Discussions evolved around four subthemes: cyber skills, cyber: hygiene, device protection and career prospects (Figure 3)

All three workshops' participants focused on data protection and the relationship of their students to hardware, applications and social media but also on the need to maximise every opportunity for hands-on student experience using scenarios and simulations. Participants suggested that breadth and depth of knowledge are equally important because there are huge gaps in what is currently being delivered. Another key component of discussions was the need to provide more information to students about cyber security career prospects.

Consensus was achieved by following a series of small group discussions which considered other elements including the role of primary schools in introducing pupils to cyber security. There was a real sense that change needed to be implemented in primary schools to ensure basic hygiene is taught as early as possible. A headteacher from a community secondary school described his approach to encouraging primary schools into his school for an initiative which introduces cyber security by stealth through offering a packaged access to his school's facilities in a programme he called *Swim/Cook/Code*.

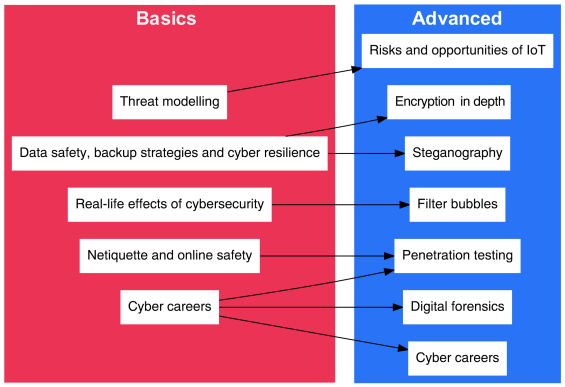

Figure 4. Proposals for cyber security education on the basic and advanced levels

When discussing methods to engage students, and approaches that would disengage as well, all participants from all three workshops advanced the idea that there is a need for a devised curriculum. In other words, a co-produced curriculum that actively engages students in the learning process, thus offering structured opportunities for learning through active connections to real world situations. The high levels of cyber knowledge and skills in secondary students was also reiterated, as well as the need to ensure they're adequately equipped for the future.

Working with programme designers, government and the teachers themselves to produce a cyber security curriculum could successfully bridge the aforementioned knowledge gap by actively utilising the existing cyber knowledge and interest in cyber security of students. Further to this point, developing fruitful relationships with industry—be that in the form of guest speakers, career talks or the provision of technological equipment, would facilitate the process of active learning and will smoothen the transition from school to higher education and industry. Highlighting the relevance of cyber security knowledge to areas, such as politics, was also said to be beneficial in terms of career development. Put simply, participants unequivocally suggested that there is an important relationship between learning and engagement.

More specifically, participants suggested the use of scenarios with which pupils can actively engage. Examples included a scenario where a phishing crime has been committed and evidence has to be recovered, another one where a telephone caller tries to find out PINs by deception, or a scenario where pupils play the part of employer, investigate different Facebook accounts and selecting candidates for jobs.

Another method of engagement was the use of simulations that actively involve pupils. Examples included hacking systems, accounts, networks, phones, programming, website design, as well as digital cleaning sessions including dusting and cleaning digital profiles, closing down old accounts and getting rid of data. Further to that, teachers proposed the use of various practical activities, such as finding data hidden in files (steganography) and the use of encryption techniques. It was also suggested that the use of case studies based on real life situations could enhance the learning process via focusing students' attention to areas such as the Internet of Things (IoT), filter bubbles and echo chambers.

Other suggestions included practical demonstrations, visiting real cyber security workplaces such as banks or law enforcement, creative and visual exercises, designing surveys and infographics. Topics and stories that have real life value and drama, such as the Babington Plot or the stories of Edward Snowden and Julian Assange were also a popular choice of pedagogical engagement. The attendees expressed the ambition to compile a glossary with all essential terminology that is to be distributed to parents, family members and grandparents and shared between schools in order to bridge the knowledge gap, but also to facilitate the creation of better adult support networks.

All that being said, participants recognised that any lack of teachers' enthusiasm and training, coupled with poor execution could easily cripple such a devised curriculum. It was suggested that the classic speaker-receiver classroom paradigm, as well as too much emphasis on theoretical, legal aspects of cyber security and online safety, could easily discourage and disincentivise students. It was noted that such an innovative devised curriculum should strike the right balance between teacher-student involvement in order to avoid overwhelming or underwhelming students and staff alike.

TAKE AWAY POINTS

- We need to better promote cyber security career prospects.
- We need to help teachers to teach cyber security.
- We need to make sure that we provide usable cyber security teaching materials—it must work first time!

CONCLUSION

Integrating cyber security into secondary school education will have multiple benefits: first, it will set young people on the track of pursuing a professional cyber security career by equipping them with the right technical and social set of skills. This is important because the shortage of cyber security professionals is likely to as we still lack an effective means to bring new people into the workforce. Secondly integrating cyber security modules into secondary school education could effectively bridge the intergenerational gap between students on the one hand, and their teachers and parents on the other. Whilst this is a benefit in and of itself, it could also help promote adequate adult support networks for young people who might find themselves in dangerous situations. Our workshops with teachers have further emphasised the need to bring cyber security into secondary education. Not just for the benefit of the tech-savvy students, but to raise awareness of cyber security, and cyber hygiene for all students. If we want close the cyber skills gap we need more cyber aware students. If we want our children to be safe online we also need to make children more cyber aware. Bringing cyber security into secondary education is a necessary step to both these goals.

ACKNOWLEDGMENT

This work is supported by the UK's National Cyber Security Programme.

REFERENCES

1. S. Furnell, P. Fischer and A. Finch, "Can't get the staff? the growing need for cyber-security skills," Computer Fraud & Security, vol. 2017, no. 2, p. 5–10, 2017.
2. (ISC)^2, "Cybersecurity professionals focus on developing new skills as workforce gap widens," (ISC)^2, 2018.
3. V. Marshall, L. Mills, J. Weingard, J. Young and S. Howes, "The UK cyber security strategy: Landscape review," National Audit Office, 2013.
4. A. Rashid, G. Danezis, H. Chivers, E. Lupu, A. Martin, M. Lewis and C. Peersman, "Scoping the Cyber Security Body of Knowledge," IEEE Security & Privacy, vol. 16, no. 3, p. 96–102, 2018.
5. M. Dark, S. Kaza and B. Taylor, "CLARK – The Cybersecurity Labs and Resource Knowledge-base – A Living Digital Library," in USENIX Advances on Security Education Workshop, Baltimore, MA, 2018.

Denny Pencheva is a Research Associate at the University of Bristol, UK. Contact them at denny.pencheva@bristol.ac.uk

Joseph Hallett is a Research Associate at the University of Bristol, UK. Contact them at joseph.hallett@bristol.ac.uk.

Awais Rashid is Professor of Cyber Security at University of Bristol, UK. Contact them at awais.rashid@bristol.ac.uk.