Editors: Jelena Mirkovic, mirkovic@isi.edu | Bill Newhouse, newhouse@nist.gov

Bringing Cyber to School: Integrating Cybersecurity Into Secondary School Education

Denny Pencheva, Joseph Hallett, and Awais Rashid | University of Bristol, United Kingdom

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

There is an ongoing shortage of cybersecurity workers. This continues to make it difficult to recruit cybersecurity specialists into open jobs.[1] An International Information System Security Certification Consortium report[2] suggests that part of the reason for the continued shortage of cybersecurity professionals comes from a failure to recruit and train young people. The report points out that currently, only 35% of cybersecurity workers are under the age of 40. The report estimates a sustained shortfall of cybersecurity workers, not only in the United Kingdom but also globally, of up to 2 million. Intergenerational gaps in terms of knowledge and a lack of awareness of the potential employment prospects are emphasized as the key factors for this shortage. Another report from the U.K. National Audit Office[3] suggests that it could take 20 years to address the cybersecurity skills gap at all levels of education.

We need to train more people to work in cybersecurity. To bridge the skills gap, training needs to come earlier in people's careers. By bringing cybersecurity education into schools, we can show students that these career pathways exist and can start to train them. This may help address the skills gap.

But how do we bring cybersecurity into schools? We ran a series of evaluative and consultative workshops and asked teachers, educators, and other practitioners what cybersecurity knowledge should be brought into secondary education (ages 12–16). We also asked how to do it in a way that actively involves students in the learning process. In addition to exploring how teachers thought we could bring cybersecurity into schools, we also wanted to find out the current levels of cybersecurity knowledge and understanding. This article focuses on the U.K. context only, yet the findings can have relevance in other similar contexts worldwide as the shortage of cybersecurity workers is an international and pressing issue.

Our analysis of the workshop transcript materials revealed two key findings.

1. Participants agreed that there was a great need for cybersecurity teaching as it is an increasingly important part of life.
2. Participants were overwhelmingly enthusiastic about integrating different aspects of cybersecurity into the curricula at their schools.

Digital Object Identifier 10.1109/MSEC.2020.2969409
Date of current version: 19 March 2020

 Copublished by the IEEE Computer and Reliability Societies

We also found significant tensions, however, related to the existence of knowledge gaps and the lack of resources. It is around these discrepancies that we have identified the two core themes of this study: "Cyber Teens, or Are They?" and "Mind the Gap!"

"Cyber Teens, or Are They?" explores the divergence between teenagers' self-perceived invincibility and their online vulnerabilities. "Mind the Gap!" looks at the dichotomy between the overall willingness of teachers to teach cybersecurity and the lack of subject-specific training and off-the-shelf resources to do so. We need to help students understand the threats they face online and how cybersecurity is an essential aspect to defending themselves. We also need to enable the teachers to impart this key cybersecurity information; at the moment, cybersecurity content is primarily taught by enthusiastic teachers yet with little support.

Method

We organized three interactive workshops across the United Kingdom where participants were actively encouraged to contribute to the discussions. The workshops were attended by 21 people; most were teachers and educators, but some industry representatives also attended and participated. We approached schools with existing outreach programs. The workshops were delivered by an independent research facilitator who wrote up the findings in a report. All attendees were assured of anonymity and promised that their views would be conveyed faithfully to the commissioners of the research.

The format was designed to be as inclusive and interactive as possible. The participants collaboratively produced visual representations of their discussions (Figure 1), and the facilitator described these when reporting the findings. The workshop discussions explored the current levels of cybersecurity knowledge of students and teaching staff, identified alarming and reassuring practices, provided examples of successful and unsuccessful pedagogical methods, and outlined practical visions for cybersecurity education.

The workshop discussions were designed to be fairly structured, although 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 attendees varied across the different settings.

All discussions were transcribed, coded, and subsequently analyzed using a thematic analysis (see Figure 2). The process of coding was strictly inductive and based on a close reading of the workshop

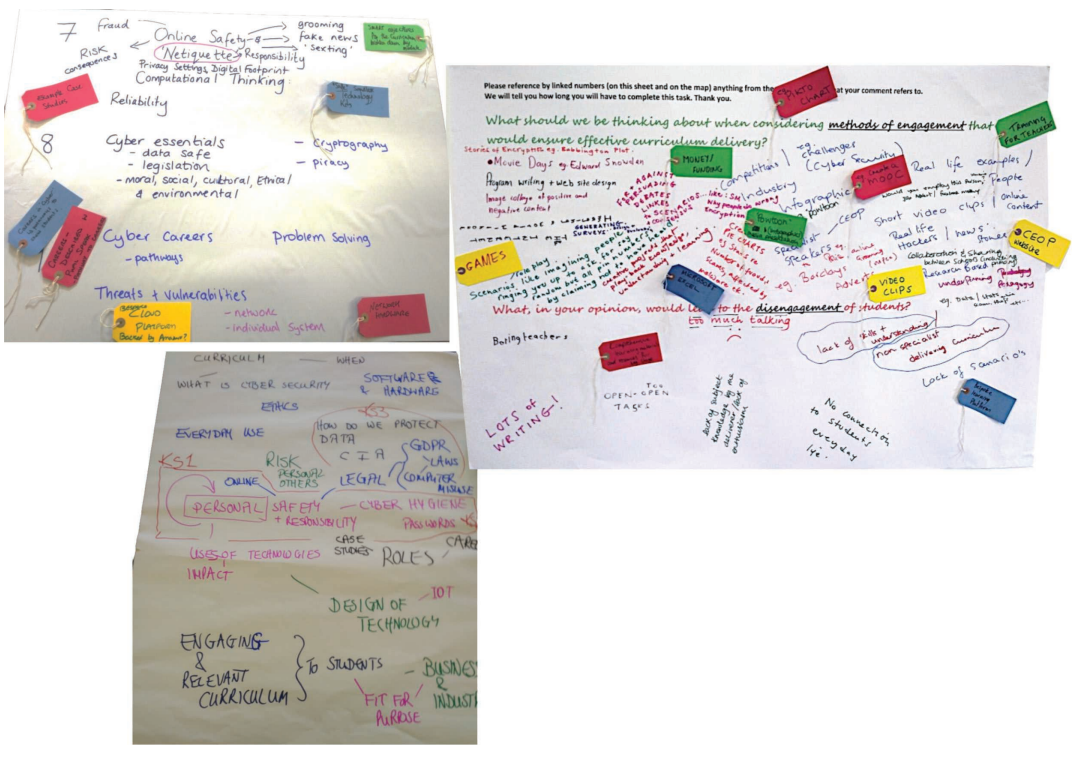

Figure 1. Some samples of diagrams produced during the workshops.

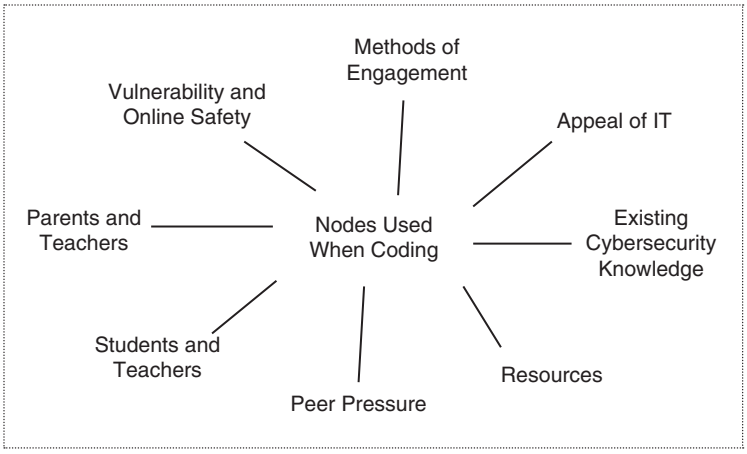

Figure 2. A thematic analysis of workshop discussions.

transcripts. To ensure rigor and minimize the possibility of selection bias, we used peer coding—a process where a second coder corroborates the initial coding.

This article presents the qualitative analysis of the information learned from the workshops. To avoid overgeneralization, we discuss the data with reference to the discussion in the workshops. The insights that come from this analysis of the data are presented in "Takeaway Points: Cyber Teens" and "Takeaway Points: Mind the Gap!"

Cyber Teens, or Are They?

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

The workshop discussions suggested that young people generally have high levels of self-taught technical skills. Teachers believed this was because they have been exposed to technology from a young age. Many students, even at the primary level, had their own websites and YouTube channels and were confident users of social media.

Teenagers Are Tech Savvy

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

Hacking Is Glamorous

Students tend to view hacking as glamorous. The teachers noted that their students were able to overcome blocks and restrictions and access school systems. These systems included: individual teachers' devices, school printers, information they were not privy to, and, in one case, the school server itself.

Online Invincibility

The discussions also revealed important caveats regarding students' knowledge: in particular, where these related to online safety. Students appeared not to understand when it was appropriate to use their technical skills. The students also regularly chose to disregard online safety rules. In short, the sense of online invincibility appeared to override notions of safe and respectful usage of online space.

While the students did have an idea of online safety, the term *cybersecurity* was relatively unknown to them—when they did know the term, they believed online safety was the same as cybersecurity, rather than being a subset of it.[4] Students are often unaware of their cyber footprint (the profile that they leave online) and are happy to give away information. This lack of knowledge of cyber hygiene led to students posting illegal content online, such as sexualized images of either themselves or fellow classmates. Workshop participants disclosed that they had seen cases of such images being circulated by children as young as nine years old; they believed the images' distribution was driven by peer pressure. Teachers noted a number of students had social media accounts despite being underage for many sites. Younger students took part in activities for older children and adults, such as online games like *Fortnite* where conversations can quickly become inappropriate. One workshop participant highlighted that students "take mean pictures at sleepovers," make inappropriate comments on social media, and post inappropriate images of friends without their permission.

Online Vulnerability

The teachers believed that the extensive, and not always safe, use of social media by young people led to students seeking approval. They also linked social media use to other social woes, such as the fear of missing out, peer pressure, low self-esteem, and mental health issues caused by other students not liking or sharing their posts.

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, and 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 faced by students was the lack of adequate adult support networks. Although teachers suggested that some students know how to access support if needed, it became clear from the discussions that teachers and parents are somewhat alienated from their students and children. The children's advanced technical knowledge often surpassed that of their parents and teachers. If a student is the technical expert at home and school, they might struggle to find appropriate help when they need it. This suggests that fixing the skills gap cannot be entirely achieved through educating the next generation of workers. In addition to improving education, we also need to build support networks and resources, not just for the students but for those supervising them as well.

Teachers agreed that they have a limited understanding about the specific situations in which students find themselves. There is a lack of parental understanding of the appropriate age to use social media platforms such as Facebook and Instagram. Schools do not necessarily know the difference between personal safety and cybersecurity, and they might not be sufficiently equipped to support students in the challenges they are facing. This lack of understanding was not just in secondary education but also in primary education. Teachers often lacked relevant knowledge and did not know how to teach basic cybersecurity.

Takeaway Points: Cyber Teens

- We need to make young peoples' cybersecurity 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 between the enthusiasm to embed cybersecurity within schools' curricula and the lack of resources (technological and human as well as the teaching materials) to do so.

The support for including cybersecurity training in secondary school education could be explained by the knowledge gap between students and their parents, teachers, and school administrators. It was indicated that students seemed to appreciate the labor market significance of cybersecurity skills. However, teachers felt that students lacked in-depth and systematic knowledge of possible cyber career paths. The workshop discussions suggested that a key outcome of an embedded cybersecurity education should be a smoother transition between secondary school and higher education and higher education and industry.

Participants were asked to suggest resources that they felt would be needed to deliver cybersecurity-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
- teacher training.

There was a general agreement among participants that any new learning content needs to be communicated appropriately to students. This means not just tailoring content to their age and skill levels but also establishing clear pathways that inform students of cyber career opportunities, whether they be forensics and penetration testing, secure data handling, risk management, or any of the other cyber careers.

Off-the-Shelf Resources

The desired materials expressed by the teachers indicate a general problem with underfunding of schools, understaffing, and isolation from the resources available to universities and industry. They wanted off-the-shelf resources that would build on what they already have; any new training must not overburden staff by being lengthy and complicated or require the design of brand new teaching content. Otherwise, any changes to a school's curricula could be rendered unsustainable if they required extensive and expensive staffing and support. Teachers stressed that it is also incredibly important that any off-the-shelf resource works the first time. When students see a demo that doesn't work right away, they become disengaged. Online resources, such as the Cybersecurity Labs and Resource Knowledge-base,[5] are not well known to teachers. When they did know about online resources, they struggled to get these labs running on restrictive school networks.

Participants raised numerous questions about the challenges of making room for cybersecurity in the existing curriculum. They questioned who was going to teach it,

what the training would look like, and what the subject content would look like given how quickly the subject updates. There was a worry that cybersecurity needs "constant updating." This might put staff under considerable strain without continued investment in the required resources.

What Exactly Is Cybersecurity?

As one participant put it: "What would a course like this offer a student that a combination of math, physics, and computer studies couldn't?" This prompted other participants to debate how cybersecurity was distinct from existing information and communications technology modules and basic online safety currently taught in personal, social, health, and economic studies units. There was a consensus that any new curriculum should be explicit, follow official government guidelines, and be embedded in existing subjects. That is, it should be based on a more cross-curricula approach using a full suite of subjects (math, English, and science, for example). It was also noted that continuity of cybersecurity 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!*

In addition, we noted the positive impact of the involvement of universities in offering specialized courses and outreach activities in schools. The proximity to universities meant that, while they felt frustratingly under-resourced, educators nonetheless remained committed to delivering a high standard of cybersecurity awareness and practice to their students. As one participant explained: "This affects people's lives daily and their habits have to adapt daily; otherwise they will fall victim to it."

Some schools were more fortunate than others in that they had already done work with students about ethical hacking and digital forensics. All participants, however, emphasized 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 cybersecurity-enhanced curriculum was to be a successful endeavor. In the words of one participant: "We need proper staff training. And proper teacher training before then. We need [the training]!"

Another added: "We need access to the right resources and the right infrastructure to support [the program]."

All attendees held passionate views about the need for better teacher training and support. Some teachers reported that they had taught themselves cybersecurity—they 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 the purpose. We need off-the-shelf practical materials that will really work.*

Another 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 emphasized that: "Cybersecurity 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 cybersecurity education. Discussions evolved around four subthemes (Figure 3):

1. cyber skills
2. cyber hygiene
3. device protection
4. career prospects.

All three workshops' participants focused on data protection and the relationship of their students to hardware, applications, and social media. They also examined how to maximize every opportunity for hands-on student experience using scenarios and

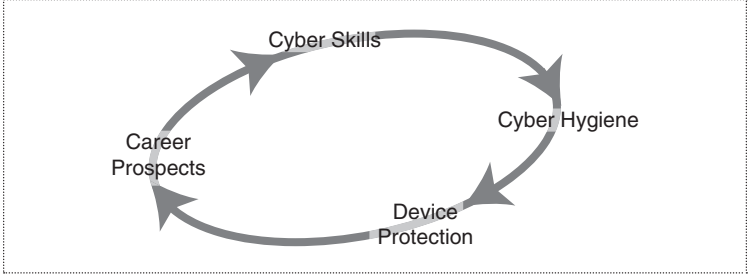

Figure 3. The recommendations for cybersecurity education.

simulations. Participants suggested that breadth and depth of knowledge are 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 cybersecurity career prospects alongside the more established noncyber career pathways already provided.

Consensus was achieved by following a series of small group discussions. These discussions considered other elements in introducing pupils to cybersecurity, including the role of primary schools. To ensure that basic cyber hygiene is taught as early as possible, change needs to be implemented in primary schools. A headteacher from a community secondary school described how his or her school encourages primary schools to interact with the school. Their initiative, called *Swim/Cook/Code*, introduces cybersecurity by stealth by allowing primary students packaged access to the secondary school's facilities.

When discussing methods to engage students as well as approaches that would disengage them, all participants suggested a need for a coproduced curriculum to actively engage students in the learning process by offering structured opportunities for learning through active connections to real world situations (see Figure 4). The high levels of cyber knowledge and skills in secondary students were also reiterated along with the need to ensure they are adequately equipped for the future.

Working with program designers, government, and the teachers themselves to produce a cybersecurity curriculum could successfully bridge the knowledge gap by actively utilizing students' existing cyber knowledge and interest in cybersecurity. Developing 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 smooth the transition from school to higher education and industry. Highlighting the relevance of cybersecurity knowledge to multiple areas, such as politics, would be beneficial in terms of career development. Participants unequivocally suggested that there is an important relationship between learning and engagement.

The use of scenarios with which pupils can actively engage was also emphasized. One example included a scenario where a phishing crime has been committed and evidence has to be recovered. Another example was one where a telephone caller tries to find out PINs by deception. A further example was a scenario where pupils play the part of an employer and investigate different Facebook accounts to select candidates for jobs.

Another method of engagement was the use of simulations that actively involve pupils. Examples included:

- hacking systems, accounts, networks, and phones

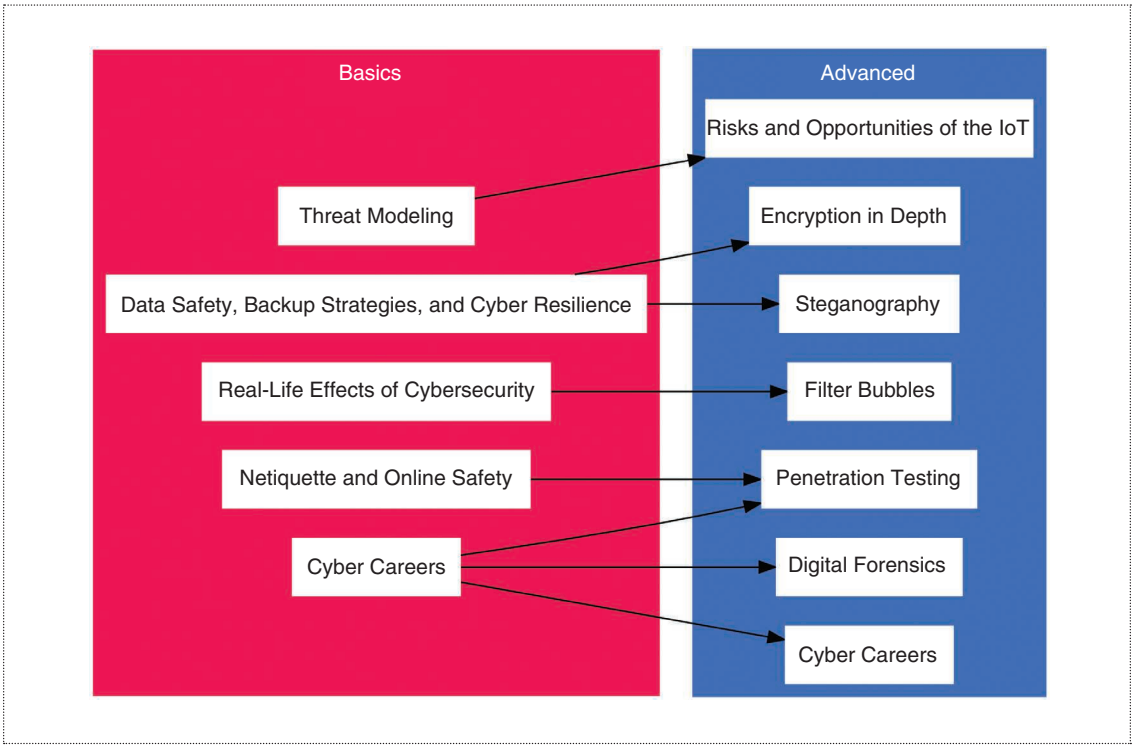

Figure 4. The proposals for cybersecurity education on the basic and advanced levels. IoT: Internet of Things.

- programming
- website design
- digital cleaning sessions, including dusting and cleaning digital profiles
- closing old accounts and getting rid of data.

Also, teachers proposed the use of various practical activities, such as finding data hidden in files (steganography), and encryption techniques. Employing case studies based on real life situations could enhance the learning process, focusing students' attention to areas such as the Internet of Things (IoT), filter bubbles, and echo chambers.

Other suggestions included practical demonstrations, visiting real cybersecurity 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 wanted to compile a glossary with essential terminology to be distributed to parents and grandparents and shared between schools not only to help them better understand the students but also to facilitate the creation of improved adult support networks.

Participants recognized 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 the theoretical and legal aspects of cybersecurity and online safety, could easily discourage and disincentivize students. Therefore, such an innovative devised curriculum should strike the right balance of teacher–student involvement to avoid overwhelming or underwhelming students and staff alike.

Takeaway Points: Mind the Gap!

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

Integrating cybersecurity into secondary school education will have multiple benefits. First, it will help young people pursue a professional cybersecurity career by equipping them with the right technical and social skills. This is important because we still lack an effective means to bring new people into the workforce and address the cyber skills shortage. Second, integrating cybersecurity into secondary school education could help bridge the gap between students and their teachers and parents. It could also promote adequate adult support networks for young people who might find themselves in dangerous situations.

Bringing cybersecurity into secondary education does not just benefit tech-savvy students; it also raises awareness of cybersecurity for all students. Cyber-aware students will be safer online and better positioned to enter into cybersecurity jobs. Such students will be more open to gaining the skills needed to take on cybersecurity careers. If we want our children to be safe online, we also need to make children more cyber aware. Bringing cybersecurity into secondary education is a necessary step to both of these goals. ■

Acknowledgments

This work is supported by the United Kingdom's National Cyber Security Program. © Crown Copyright 2019.

References

1. S. Furnell, P. Fischer, and A. Finch, "Can't get the staff? The growing need for cyber security skills," *Comput. Fraud Secur. Bull.*, vol. 2017, no. 2, pp. 5–10, 2017. doi: 10.1016/S1361-3723(17)30013-1.
2. "Cybersecurity professionals focus on developing new skills as workforce gap widens," (ISC)^2, Clearwater, FL, 2018. [Online]. Available: https://www.isc2.org/-/media/7CC1598DE430469195F81017658B15D0.ashx
3. V. Marshall, L. Mills, J. Weingard, J. Young, and S. Howes, *The UK Cyber Security Strategy: Landscape Review*. London: National Audit Office, 2013.
4. A. Rashid et al., "Scoping the cyber security body of knowledge," *IEEE Security Privacy*, vol. 16, no. 3, pp. 96–102, 2018. doi: 10.1109/MSP.2018.2701150.
5. M. Dark, S. Kaza and B. Taylor, "CLARK: The cybersecurity labs and resource knowledge-base: A living digital library," in *Proc. USENIX Advances Security Education Workshop*, Baltimore, MA, 2018.

Denny Pencheva is a research associate at the University of Bristol, United Kingdom. Contact him at denny.pencheva@bristol.ac.uk

Joseph Hallett is a research associate at the University of Bristol, United Kingdom. Contact him at joseph.hallett@bristol.ac.uk.

Awais Rashid is a professor of cybersecurity at the University of Bristol, United Kingdom. He is a Member of the IEEE. Contact him at awais.rashid@bristol.ac.uk.