## Building a secure future: The role of secondary education in cyber security preparedness

*Jordan Allison, Senior Lecturer in Computer Science, School of Business, Computing and Social Sciences, University of Gloucestershire*

In today's digital world, cyber security, that is ‘how individuals and organisations reduce the risk of cyber attack’ (National Cyber Security Centre, 2024), has become a paramount concern. With the rise of cyber threats such as malware, denial-of-service attacks and phishing, there is a growing demand for cyber security professionals. However, studies have highlighted a shortage of individuals with adequate cyber security expertise, leading to what the then Department for Digital, Culture, Media and Sport (2019) referred to as a ‘cyber security capability gap’ within the UK.

In this blog post, I explore the growing concern of effective cyber security education for addressing this capability gap. As a lecturer teaching cyber security content within higher education, it is clear there is a skills discrepancy among learners entering our programmes, often dependent on prior educational background. Hence, we need to understand the context of these learners, which involves understanding how cyber security is embedded within secondary education.

While the British Computing Society Landscape Review of Computing Qualifications (2022) identified that basic IT literacy is ingrained throughout most English educational stages, little research explored the depth of cyber security within secondary education qualifications. To address this, Stepney and Allison (2023) employed CyBOK (Cyber Security Body of Knowledge) which categorises knowledge of cyber security into 21 knowledge areas (KAs) (Martin et al., 2021).

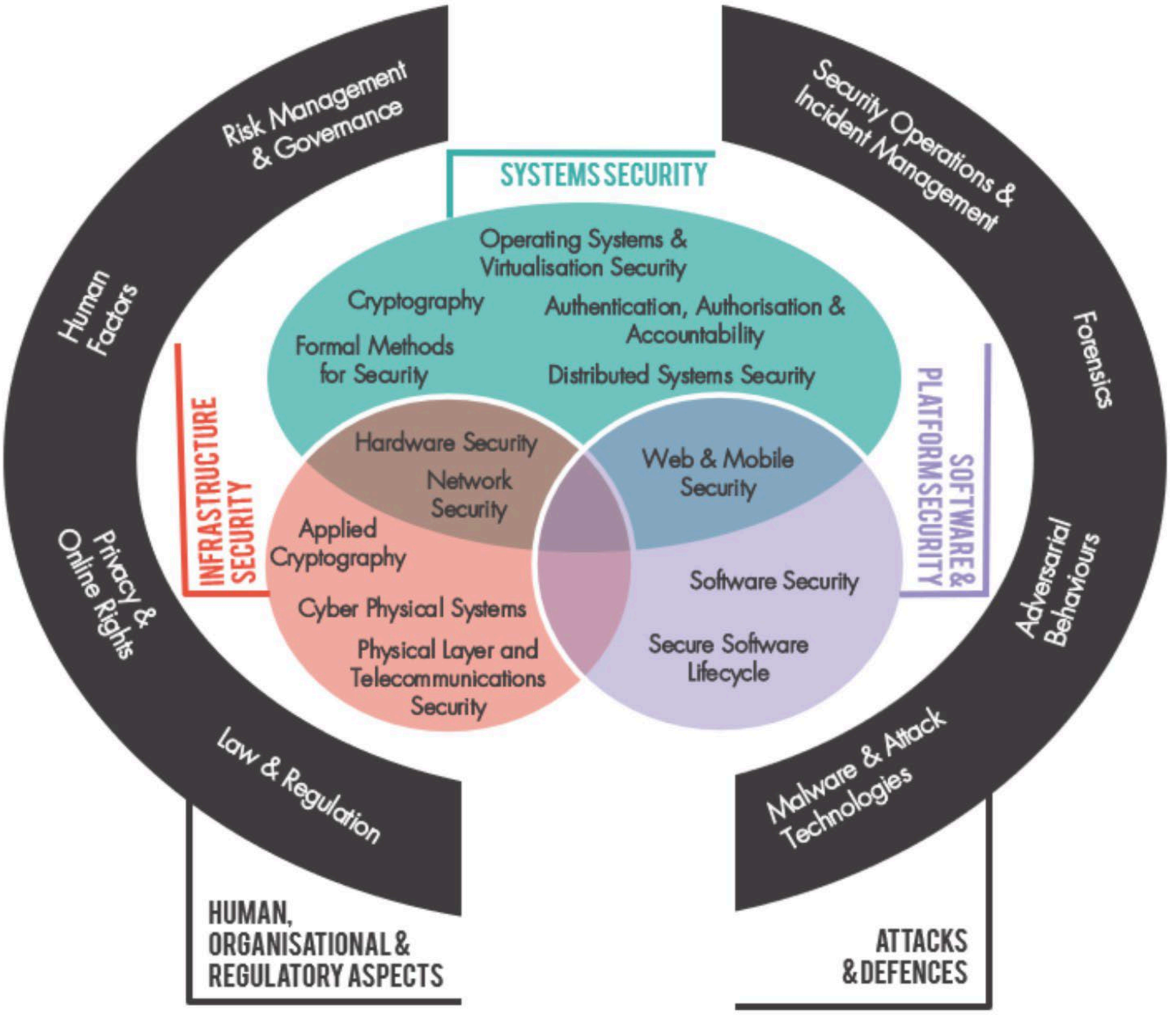
Risk Management & Governance
Human Factors
Privacy & Online Rights
Law & Regulation
HUMAN, ORGANISATIONAL & REGULATORY ASPECTS
SYSTEMS SECURITY
Operating Systems & Virtualisation Security
Cryptography
Authentication, Authorisation & Accountability
Formal Methods for Security
Distributed Systems Security
INFRASTRUCTURE SECURITY
Hardware Security
Network Security
Applied Cryptography
Cyber Physical Systems
Physical Layer and Telecommunications Security
Web & Mobile Security
Software Security
Secure Software Lifecycle
SOFTWARE & PLATFORM SECURITY
Security Operations & Incident Management
Forensics
Adversarial Behaviours
Malware & Attack Technologies
ATTACKS & DEFENCES

*Figure 1. CyBOK knowledge areas (Martin et al., 2021). CyBOK © Crown Copyright, The National Cyber Security Centre 2021, licensed under the Open Government Licence: http://www.nationalarchives.gov.uk/doc/opengovernment-licence/*

[Block quote]

‘Greater links should be created between schools, higher education providers and industry to foster a greater understanding of each other’s challenges in building the future talent pipeline for cyber security professionals.’

[End block quote]

The CyBOK mapping revealed disparities in cyber security content across 11 computing qualifications within England. For students aged 14 to 16, mandatory General Certificate of Secondary Education (GCSE) ICT qualifications by Pearson cover only 29 per cent of CyBOK KAs, while optional qualifications at Level 2 of the Regulated Qualifications Framework (RQF) offer broader coverage. However, at RQF Level 3, predominantly studied by students aged 16 to 18, Advanced-Level (A-Level) Computer Science qualifications from the exam boards of Assessment and Qualifications Alliance, and Oxford, Cambridge and RSA Examinations, cover only 19 per cent and 14 per cent of KAs, respectively. These inconsistencies between age groups highlight the lack of focus of cyber security content within some computing courses. Nevertheless, the analysis revealed T-Level qualifications offer substantial cyber security content, covering up to 81 per cent of the defined KAs. However, T-Level qualifications involve more guided learning hours compared to individual A-Level qualifications. Additionally, while most qualifications cover areas such as cryptography, law and regulation, and network security, the research revealed notable gaps in areas like human factors, authentication and risk management, the last of which should be easier to incorporate given the less technical nature of the subject matter.

Unfortunately, curricular constraints such as lack of time or insufficient IT equipment often limit the inclusion of cyber security topics, leaving educators to supplement learning through extracurricular activities. This discrepancy between intended curriculum specifications and what has been described as the enacted curriculum delivery (Falkner et al., 2019) has further complications. For instance, one participant interviewed in the Stepney and Allison (2023) study stated, 'The computer science curriculum for GCSE and A-Level is monstrously broad... it would be ill-advised to focus more on cyber security than is required for examination purposes'. Furthermore, limited funding, resources and teacher training exacerbate these challenges of effective inclusion of cyber security within secondary education, with many computing teachers lacking the expertise to effectively deliver technical cyber security content (Pencheva et al., 2020).

Addressing these challenges requires a concerted effort from policymakers, educators and industry stakeholders. Greater links should be created between schools, higher education providers and industry to foster a greater understanding of each other's challenges in building the future talent pipeline for cyber security professionals. Regardless, by prioritising cyber security education, we can empower students with the knowledge and skills needed to navigate the digital landscape securely. Furthermore, initiatives aimed at enhancing teacher training and curriculum flexibility are essential to bridge the cyber security capability gap effectively.

**References**

British Computer Society. (2022). *BCS landscape review: Computing qualifications in the UK. Technical report*.

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.*

Falkner, K., Sentance, S., Vivian, R., Barksdale, S., Busuttil, L., Cole, E., Liebe, C., Maiorana, F., McGill, M. M., & Quille, K. (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* (pp. 1–10).

Martin, A., Rashid, A., Chivers, H., Schneider, S., Lupu, E., & Danezis, G. (2021). *Introduction to CyBOK knowledge area version 1.1.0.*

National Cyber Security Centre (2024). *What is cyber security?* https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security

Pencheva, D., Hallett, J., & Rashid, A. (2020). Bringing cyber to school: Integrating cybersecurity into secondary school education. *IEEE Security & Privacy, 18*(2), 68–74.

Stepney, O., & Allison, J. (2023). Cyber security in English secondary education curricula: A preliminary study. In *Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 1* (pp. 193–199).

Jordan Allison is a Senior Lecturer in Computer Science within the School of Business, Computing and Social Sciences at the University of Gloucestershire, where he teaches on a range of cyber security modules at both undergraduate and postgraduate level. Jordan is a Fellow of the Higher Education Academy (FHEA), a Professional Member of the Association of Computing Machinery (MACM) and a Professional Member of the British Computer Society (MBCS), the Chartered Institute for IT. His research primarily focuses on computing education pedagogy, curriculum design and teacher development, with an emphasis on qualitative research.