Overcoming the Challenges of Teaching Cybersecurity in UK Computer Science Degree Programmes

ABSTRACT

An article published in the Harvard Business Review in August 2019 argued that "*Every Computer Science Degree Should Require a Course in Cybersecurity*"[10]; in the UK, universities – alongside government, industry and professional bodies – have been championing this over recent years, focusing on computer science and cognate undergraduate degrees programmes. One professional body – BCS, The Chartered Institute for IT – has been mandating this in accredited undergraduate degree programmes since 2015[30]. Delivering cybersecurity effectively across general computer science programmes presents a number of challenges related to pedagogy, underpinning educational resources, available skills and technical resources. This paper explores the progress to date, as well as a starting call to arms to the UK higher education sector by highlighting a number of future challenges and opportunities.

CCS CONCEPTS

• **Security and privacy**; • **Social and professional topics** → **Accreditation**;

KEYWORDS

Accreditation, Cybersecurity, Computer Science Education

ACM Reference format:
. 2020. Overcoming the Challenges of Teaching Cybersecurity in UK Computer Science Degree Programmes. In *Proceedings of CEP '20: ACM Computing Education Practice, Durham, UK, January 9, 2020 (CEP '20),* 4 pages.
https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 WHAT IS IT?

This paper explores the diversity of challenges relating to the teaching of cybersecurity in UK higher education degree programmes, from policy, through to pedagogy and practice. It frames these challenges through concerns with the quality and availability of underpinning educational resources, the competencies and skills of faculty (especially focusing on pedagogy and assessment), and technical resources related to delivering sound cybersecurity content in general computer science and cognate degrees. There is a serious demand for cybersecurity specialists in the Uk and globally (estimates vary, but are always large); there is significant and growing higher education provision related to specialist undergraduate and postgraduate courses focusing on varying aspects of cybersecurity (for example cybersecurity, digital forensics, ethical hacking, computer security, networks and security, etc). To make our digital systems and products more secure, all in IT need to know *some* cybersecurity — thus, there is a case for depth as well as breadth [12, 17]. This is not a new concern [25], but it is a growing one. Computer science and cognate disciplines are evolving to meet these demands – both in school-level education, as well as tertiary – however, doing so is not without challenges. This paper explores the progress to date in the UK, highlights challenges for the future, as well as identifying a number of potential enhancement activities for the domain.

CEP '20, January 9, 2020, Durham, UK

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

2 WHY ARE YOU DOING IT?

Cybersecurity is becoming increasing pivotal to the operation of organisations of all sizes and organisations are increasingly expected to make reasonable adjustments to protect their activities. The UK Government is encouraging organisations of all sizes and types to take this seriously [15].

This focus on cybersecurity, includes calls for formal education – school-level as well as tertiary – to respond to this situation, at the individual level and via recommended curricula [3, 18] and professional accreditation requirements [8, 33]. This is further reinforced by a wider focus on digital skills and computer science education reform, especially across the nations of the UK [9, 20, 21, 32]. Embedding cybersecurity in computer science and related degrees is now the norm within the UK.

A number of Professional, Statutory and Regulatory Bodies (PSRBs) have responded to these expectations by adjusting their accreditation requirements. In the UK, BCS, The Chartered Institute for IT (BCS) has had a requirement to include information security in the curriculum since 2010, and has expected coverage of an agreed minimum cybersecurity syllabus since 2015, with the result that all accredited universities should be compliant by 2020 (due to the five-year accreditation cycle). More precisely, accredited degrees have been expected to demonstrate coverage of "*2.1.9 Knowledge and understanding of information security issues in relation to the design, development and the use of information systems*" [8, p. 30] since 2010 with an enhanced cybersecurity related definition of what this entails since 2015 [8, p. 17–18]. However, it is one thing to teach cybersecurity, but another to do it well.

3 WHERE DOES IT FIT

One way to evaluating how well cybersecurity is taught is to reflect upon the pedagogic approach used, the underpinning resources available, the disciplinary expertise of faculty and the required technical resources.

3.1 What pedagogical approach to adopt?

What is the most appropriate way to teach cybersecurity? [37] highlights there are benefits from teaching this in a practical manner.

Real world case studies can be employed [7]. Use can be made of guest lectures by industrialists to share practical insights and hence providing students with micro-exposure to the world of work is another positive contribution. One further approach is the inclusion of appropriate cybersecurity standards within the curricula.

The PCI DSS [26] is one such standard that has been used in precisely this manner. PCI DSS underpins all processing of credit/debit cards. Nevertheless, it is very rarely mentioned in generalist computer scientist courses. This would not matter so much if everyone handling payments data were sent by their employers on an effective PCI DSS course. However, the payments business is now so spread across websites, often run by small and medium enterprises (SME), or non-specialists. Even larger enterprises are not immune: [7] reports that the recent British Airways breach was caused by a failure to adhere to PCI DSS in website maintenance.

Another way of adopting a more practical pedagogy is by teaching cybersecurity through the lens of hacking or the hacker curriculum [6]. Such an approach facilitates students to be more experimental and creative in their exploration of the discipline and can have corresponding benefits for their engagement.

3.2 Quality of resources to support cybersecurity education?

Effective teaching requires appropriate supporting resources. The extent to which appropriate resources are available and suitable will be evaluated next. This evaluation highlights a number of occasions when underpinning resources could be improved.

3.2.1 SQL Injection. It is 15 years since [14] wrote "*All the topics listed above should be presented in the first Database Course*", and the first such topic was SQL injection [4, 29]. SQL injection as an attack has been around for twenty years [16], has its own cartoon and website. Nevertheless SQL injection is still a major weakness: number one in the Open Web Application Security Project (OWASP) Top 10 [23], and has been in the Top 10 since at least 2003.

Clearly such a major weakness should be well-taught; in general it is hard to determine what is actually delivered as part of a specific degree programme, but a reasonable proxy for this is the content of recommended textbooks. This was the rationale for a 2019 analysis of database textbooks used by 44 of the top 50 computer science departments in the USA [31]. There were seven such books, but three books accounted for the 36 of the 44 universities. Five of the seven (30 of the 44) had no mention of SQL injection. Of the other two, the more popular one has a seriously flawed discussion, and the other, while generally excellent, had a presentational problem [31].

3.2.2 The Case of Java. Many textbooks go nowhere near security applications, despite their ubiquity. But this means that the programmer who has to implement security is left to the documentation of the package/API being used, and to informal resources. [19] analysed 503 cybersecurity-related postings on the popular Stack Overflow online resource. 53% were about the Spring Security framework, dominated by authentication (45%). The discussion [19, §4.3.1] of cross-site request forgery (CSRF) is especially worrying. By default, Spring implicitly enables protection against this. But all the accepted answers to CSRF-related failures simply suggested disabling the check. There were no negative comments about this, and indeed a typical response is

> *"Adding csrf().disable() solved the issue!!! I have no idea why it was enabled by default."*

As of writing, there were no negative comments about this disabling of a vital security feature. This research was further developed by [11] (and popularised in a security community in [38]). Their first finding was:

> "*644 out of the 1,429 inspected answer posts (45%) are insecure, meaning that insecure suggestions popularly exist on SO. Insecure answers dominate, in particular, the SSL/TLS category*"
> [355 insecure versus 150 secure, i.e. > 70%].

3.2.3 Android. Many Android textbooks do not rigorously consider cybersecurity. [13] looked specifically at the use of resources from Stack Overflow in Android applications. The key finding was:

> "*We found that 15.4% of all 1.3 million Android applications contained security-related code snippets from Stack Overflow. Out of these 97.9% contain at least one insecure code snippet.*"

Two caveats (in opposite directions) should be noted. The labelling was conservative, in that snippets were only labelled as insecure if that was demonstrable, and, for example, mere use of outdated SSL/TLS was not automatically deemed insecure. On the other hand, the insecure snippet might have been used in a way that did not expose the insecurity. The uncritical reading of Stack Overflow was also noted in [36, Slide 29]. Their key recommendation [36, Slide 32] was "*Improve documentation: Clarify what you can(not) copy/paste*".

3.2.4 Agile. Many Agile textbooks have little consideration of cybersecurity. Many authors have found disconnects between Agile practices and secure software development: notably [5] for small projects and [35] for large projects. Agile's preference for functionality over non-functional requirements is clearly displayed in practice. [22] asked 20 student developers to imagine they were part of a team working on creating a social networking site for our university and to implement a password storage mechanism for this. 10 ("primed") were explicitly told that the storage had to be secure and 10 ("unprimed") were not. None of the unprimed ones implemented any security.

3.2.5 Informal Tutorials. The web abounds with informal resources, such as tutorials and code snippets. How good are these, and how good are people at using these? This has been looked at by [34], taking the top five search results from Google for six queries. Of these 30 tutorials, six had SQL injection weaknesses, and three had Cross-Site Scripting weaknesses. Searching for these fragments in PHP projects on GitHub found 820 instances of these fragments, of which 117 were verified manually to be vulnerable — 80% of which were vulnerable to SQL injection. Some students clearly make use of these resources; thus a recommendation of future work is to explore and evaluate students' (and indeed others') use of such informal resources.

3.3 Are the right skills and infrastructure available?

It is well known that cybersecurity skills are in short supply, in both industry [1] and academia [28]. The demand for cybersecurity skills in industry makes it difficult for academia to attract academics with knowledge, practical experience, research background and academic aspirations. As universities expand their cybersecurity provision it is not uncommon to find multiple jobs advertised at the same time. Recent example have included a professor of cybersecurity, two senior academic positions and two junior academic positions in one advert. There are other examples in the UK of cybersecurity lecturing jobs remaining unfilled for longer than a year; there are also examples of cybersecurity research groups moving en masse from one university to another.

Delivering a practical take upon cybersecurity often requires specialist computing resources. Commonly such a laboratory will be not directly connected to the Janet network in order not to breach the operating conditions of the network. This creates further challenges in the form of acquisition and maintenance of specialist laboratory provision.

4 DOES IT WORK?

The UK situation appears relatively advanced compared to other jurisdictions. 61% of UK courses offer mandatory cybersecurity content, and this research was based on web scraping [27, Table 1]. As such it represents a lower bound since not all coverage will necessarily be clearly articulated in publicly available documentation online.

BCS have reported good progress in the mandating of the inclusion of cyber security within the programmes the body accredits. [30] reported progress up to autumn 2018. To provide an update from the start of the Autumn 2015 term, up to and including the Summer 2019 term, the BCS has carried out 82 accreditation visits including five international visits (2 in South Africa and 1 in Brunei, Cyprus, and Ireland) . The BCS identified action was required to address concerns related to cybersecurity at 23 institutions; thus, 59 institutions were already delivering cybersecurity in line with the BCS expectations.

Long-term actions ('*At Threshold* ' judgements) were expected from 14 institutions (six in 2015/16, three in 2016/17 and five in 2018/19). 13 of these judgments were across all programmes; one was specifically against a generalist masters programme only. This indicates that the BCS will expect adjustments to have taken place before the next accreditation visit. It was commonly the case that adjustments had been made to design of the programmes of study, however, the adjusted programme had not yet been delivered so the evidence base was incomplete in terms of how cybersecurity was assessed.

Short term actions were required from nine institutions; the outcomes of these actions were as follows: (*i*) of the eleven UG programmes involved all were approved '*At Threshold*'; (*ii*) of the nine UG programmes involved, eight were approved and one refused; (*iii*) of the five UG programmes involved, all were approved '*At Threshold*'; and (*iv*) of the three UG programmes involved, all were refused; and (*v*) a further five which at the time of writing the outcome is not known

Good practice was identified at three universities by the commendation:

> "*The second-year project provides an opportunity for exploring security aspects in depth with an industrial use case.*"
>
> "*Hacktivity and related learning and teaching approaches*"
>
> "*Cyber Security Centre which permeates both the course and supports external links and opportunities for students.*"

In summary, this shows that many accredited institutions have now embedded cybersecurity in their provision, a number are in the process of doing so and a minority have chosen not to. This suggests that in the UK inclusion of cybersecurity within computer science and related degrees is becoming the norm.

5 WHO ELSE HAS DONE THIS?

In jurisdictions other than the UK, PSRB's have also adjusted their expectations to enhance the cybersecurity provision. For example in the United States of America (USA), the Association of Computing Machinery (ACM) has equally had cybersecurity (IAS: "Information Assurance and Security") in the curriculum since 2013 [2], but it is not the accrediting body. The Accreditation Board for Engineering and Technology (ABET) is, and is requiring IAS with effect from the 2019-20 cycle (self-study reports due 1 July 2019): more precisely [24, Table 3] "*The computing topics must include: … Principles and practices for secure computing…*". This should mean that all accredited universities should be compliant by 2025 (due to their six-year cycle).However the challenges related to pedagogy, underpinning educational resources, skills shortages and resource requirements are a global challenge.

6 WHAT WILL YOU DO NEXT?

As indicated in the previous section there are a number of challenges that have not been fully addressed:

1. There is a need for research related to the effectiveness of alternative pedagogies for the delivery of cybersecurity
2. Many of the common underpinning resources (textbooks or informal resources) do not address cybersecurity satisfactorily. This is a development opportunity for the computer science education community to address this;
3. There is a skills gap. The computer science education community could help address this by growing the number of appropriate qualified potential lecturers;
4. The effectiveness of alternative resources to support the provision of cyber security is another area that could benefit from further research.

7 WHY ARE YOU TELLING US THIS?

Most institutions in the UK now include aspects of cybersecurity in their general undergraduate computer science provision in the same manner that they include legal, social, ethical and professional issues; it is now time to consider how to further enhance the quality of provision, with a focus on pedagogy, assessment and progression. How can cybersecurity receive the same level of attention in terms of pedagogic research and practice as say, programming

or CS1? We feel that there is a significant opportunity for the UK computer science academic community, in collaboration with a range of key stakeholders, to drive forward this new educational research priority.

8 ACKNOWLEDGMENTS

The authors wish to thank Sally Pearce, Academic Accreditation Manager at BCS, The Chartered Institute for IT for supplying the summary information related to accreditation of UK degree programmes. Many people, accreditors and accredited, have contributed to accreditation practice in the UK (and elsewhere), and spreading good practice. All authors' institutions are members of the Institute of Coding, an initiative funded by the Office for Students (England) and the Higher Education Funding Council for Wales.

REFERENCES

[1] R. Ackerman. 2019. Too few cybersecurity professionals is a gigantic problem for 2019. https://techcrunch.com/2019/01/27/too-few-cybersecurity-professionals-is-a-gigantic-problem-for-2019/. (2019).

[2] ACM/IEEE-CS Joint Task Force on Computing Curricula. 2013. *Computer Science Curricula 2013.* Technical Report. ACM Press and IEEE Computer Society Press. https://dx.doi.org/10.1145/2534860.

[3] ACM/IEEE-CS/AIS SIGSEC/IFIP WG 11.8 Joint Task Force on Computing Curricula. 2017. Cybersecurity Curricula 2017. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf. (December 2017).

[4] Anonymous. 2018. CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'). https://cwe.mitre.org/data/definitions/89.html. (2018).

[5] S. Bartsch. 2011. Practitioners' Perspectives on Security in Agile Development. In *Proc. of Int. Conf. on Availability Reliability and Security.* ACM, Washinton DC, USA, 479–484.

[6] Sergey Bratus, Anna Shubina, and Michael E Locasto. 2010. Teaching the principles of the hacker curriculum to undergraduates. In *Proceedings of the 41st ACM technical symposium on Computer science education.* ACM, ACM, USA, 122–126.

[7] British Airways. 2018. Customer data theft. https://www.britishairways.com/en-gb/information/incident/data-theft/latest-information. (2018).

[8] British Computer Society. 2018. Guidelines on course accreditation (May 2018). http://www.bcs.org/content/ConMediaFile/30202. (2018).

[9] Neil C. C. Brown, Sue Sentance, Tom Crick, and Simon Humphreys. 2014. Restart: The Resurgence of Computer Science in UK Schools. *ACM Trans. on Computer Science Education* 14, 2 (2014), 1–22.

[10] J Cable. 2019. Every Computer Science Degree Should Require a Course in Cybersecurity. (Aug 2019). https://hbr.org/2019/08/every-computer-science-degree-should-require-a-course-in-cybersecurity

[11] M. Chen, F. Fischer, N. Meng, X. Wang, and J. Grossklags. 2019. How Reliable is the Crowdsourced Knowledge of Security Implementation? https://arxiv.org/abs/1901.01327. (2019).

[12] James H. Davenport, Alan Hayes, Rachid Hourizi, and Tom Crick. 2016. Innovative Pedagogical Practices in the Craft of Computing. In *Proc. of 4th Int. Conf. on Learning and Teaching in Computing and Engineering (LaTiCE 2016).* IEEE Press, Mumbai, India, 115–119.

[13] F. Fischer, K. Böttinger, H. Xiao, C. Stransky, Y. Acar, M. Backes, and S. Fahl. 2017. Stack Overflow Considered Harmful? The Impact of Copy&Paste on Android Application Security. In *38th IEEE Symposium on Security and Privacy.* IEEE, San Jose, CA, USA, 121–136.

[14] Mario Guimaraes, Herb Mattord, and Richard Austin. 2004. Incorporating security components into database courses. In *Proc. of 1st Annual Conf. on Information Security Curriculum Development.* ACM, ACM, Kennesaw, Georgia, USA, 49–52.

[15] R. Hannigan. 2019. Engineering-based industries are often not very good at cyber security. https://events.theiet.org/cyber-ics/interview.cfm. (2019).

[16] Matthew Horner and Thomas Hyslip. 2017. SQL Injection: The Longest Running Sequel in Programming History. *Journal of Digital Forensics, Security and Law* 12, 2 (2017), 97–107. https://doi.org/10.15394/jdfsl.2017.1475

[17] Daniel Manson and Ronald Pike. 2013. The case for depth in cybersecurity education. *ACM Inroads* 5, 1 (2013), 47–52.

[18] Andrew McGettrick, Lillian N. Cassel, Melissa Dark, Elizabeth K. Hawthorne, and John Impagliazzo. 2014. Toward curricular guidelines for cybersecurity. In *Proc. of SIGCSE 2014.* ACM, USA, 81–82.

[19] N. Meng, S. Nagy, D. Yao, W. Zhuang, and G. Arango Argoty. 2018. Secure coding practices in Java: Challenges and vulnerabilities. In *IEEE/ACM 40th Int. Conf. on Software Engineering.* IEEE, Gothenburg, Sweden, 372–383.

[20] Faron Moller and Tom Crick. 2018. A University-Based Model for Supporting Computer Science Curriculum Reform. *Journal of Computers in Education* 5, 4 (2018), 415–434.

[21] Ellen Murphy, Tom Crick, and James H. Davenport. 2017. An Analysis of Introductory Programming Courses at UK Universities. *The Art, Science, and Engineering of Programming* 1(2), 18 (2017), 1–23.

[22] A. Naiakshina, A. Danilova, C. Tiefenau, M. Herzog, S. Dechand, and M. Smith. 2017. Why Do Developers Get Password Storage Wrong?: A Qualitative Usability Study. *Proc. 2017 ACM SIGSAC Conf. on Computer and Communications Security* (2017), 311–328.

[23] Open Web Application Security Project (OWASP). 2017. The Ten Most Critical Web Application Security Risks. https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=Main. (2017).

[24] M.J. Oudshoorn, S. Thomas, R.K. Raj, and A. Parrish. 2018. Understanding the New ABET Computer Science Criteria. In *Proc. of SIGCSE 2018.* ACM, USA, 429–434.

[25] C. Parr. 2014. Cybersecurity skills need boost in computer science degrees. https://www.timeshighereducation.com/news/cybersecurity-skills-need-boost-in-computer-science-degrees/2016933.article. (2014).

[26] Payment Card Industry Security Standards Council (PCI SSC). 2018. Requirements and Security Assessment Procedures Version 3.2.1. https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss. (2018).

[27] Rodrigo Ruiz. 2019. A Study of the UK Undergraduate Computer Science Curriculum: A Vision of Cybersecurity. In *Proc. of 12th IEEE Int. Conf. on Global Security, Safety and Sustainability.* IEEE, London, UK, 1–8.

[28] Fred B. Schneider. 2013. Cybersecurity Education in Universities. *IEEE Security and Privacy* 11, 4 (2013), 3–4.

[29] SPI Dynamics. 2002. White paper SQL Injection 07-31-02.doc. https://web.archive.org/web/20030605171750/http://www.spidynamics.com:80/papers/SQLInjectionWhitePaper.pdf. (2002).

[30] A. Irons T. Crick, J. Davenport and T. Prickett. 2019. A UK Case Study on Cybersecurity Education and Accreditation. In *Proc. IEEE Frontiers in Education Conference.* IEEE.

[31] Cynthia Taylor and Saheeel Sakharkar. 2019. ';DROP TABLE textbooks;– An Argument for SQL Injection Coverage in Database Textbooks. In *Proc. of SIGCSE 2019.* ACM, USA, 191–197.

[32] Theo Tryfonas and Tom Crick. 2018. Public Policy and Skills for Smart Cities: The UK Outlook. In *Proc. of 11th Int. Conf. on PErvasive Technologies Related to Assistive Environments (PETRA).* ACM, Corfu, Greece, 116–117.

[33] UK National Cyber Security Centre. 2017. NCSC-certified degrees. https://www.ncsc.gov.uk/information/ncsc-certified-degrees. (August 2017).

[34] T. Unruh, B. Shastry, M. Skoruppa, F. Maggi, K. Rieck, J.-P. Seifert, and F. Yamaguchi. 2017. Leveraging Flawed Tutorials for Seeding Large-Scale Web Vulnerability Discovery. In *Proc. of 11th USENIX Workshop on Offensive Technologies (WOOT 2017).* USENIX, the Advanced Computing Systems Association, Vancouver, BC, Canada.

[35] Amber van der Heijden, Cosmin Broasca, and Alexander Serebrenik. 2018. An Empirical Perspective on Security Challenges in Large-scale Agile Software Development. In *Proc. ESEM'18.* ACM, Oulu, Finland, 45:1–45:4.

[36] D. Votipka, K. Fulton, J. Parker, M. Hou, M. Mazurek, and M. Hicks. 2019. Understanding Security Mistakes Developers Make. https://rwc.iacr.org/2019/slides/RWC-BIBIFI-qual.pdf. (2019).

[37] Richard Weiss, Jens Mache, and Erik Nilsen. 2013. Top 10 Hands-on Cybersecurity Exercises. *Journal of Computing Sciences in Colleges* 29, 1 (Oct. 2013), 140–147.

[38] Z. Zorz. 2019. Popular coding advice doesn't necessarily equal secure coding advice. https://www.helpnetsecurity.com/2019/01/09/insecure-coding-advice/. (2019).